Amtsblatt
der Europäischen Union

DE
Reihe L

2025/2540

12.12.2025

DURCHFÜHRUNGSVERORDNUNG (EU) 2025/2540 DER KOMMISSION

vom 9. Dezember 2025

mit Durchführungsbestimmungen zur Verordnung (EU) 2019/881 des Europäischen Parlaments und des Rates hinsichtlich der Einrichtung des Plans für die gegenseitige Begutachtung

(Text von Bedeutung für den EWR)

DIE EUROPÄISCHE KOMMISSION —

gestützt auf den Vertrag über die Arbeitsweise der Europäischen Union,

gestützt auf die Verordnung (EU) 2019/881 des Europäischen Parlaments und des Rates vom 17. April 2019 über die ENISA (Agentur der Europäischen Union für Cybersicherheit) und über die Zertifizierung der Cybersicherheit von Informations- und Kommunikationstechnik und zur Aufhebung der Verordnung (EU) Nr. 526/2013 (Rechtsakt zur Cybersicherheit) ([1]), insbesondere auf Artikel 59 Absatz 5,

in Erwägung nachstehender Gründe:

(1) Gemäß Artikel 59 Absatz 4 der Verordnung (EU) 2019/881 erfolgen durch nationale Behörden für die Cybersicherheitszertifizierung durchgeführte gegenseitige Begutachtungen durch zwei nationale Behörden für die Cybersicherheitszertifizierung anderer Mitgliedstaaten und die Kommission. Um gleichwertige Standards für europäische Cybersicherheitszertifikate und EU-Konformitätserklärungen zu erreichen, sollte die Kommission Aspekte im Zusammenhang mit der Einhaltung dieser Verordnung überwachen und sicherstellen, dass gegenseitige Begutachtungen in der gesamten Union einheitlich durchgeführt werden. Zur Ermittlung von bewährten Verfahren, Herausforderungen und Lehren aus der Umsetzung der europäischen Systeme für die Cybersicherheitszertifizierung sollte die Agentur der Europäischen Union für Cybersicherheit (ENISA) die Möglichkeit haben, als Beobachterin an den gegenseitigen Begutachtungen teilzunehmen. Um die harmonisierte Umsetzung der Bestimmungen dieser Verordnung zu unterstützen, sollte die ENISA in Zusammenarbeit mit der Kommission und der Europäischen Gruppe für die Cybersicherheitszertifizierung auch die Möglichkeit haben, Vorlagen auszuarbeiten.

(2) Zur Gewährleistung von Planungssicherheit und einer effizienten Ressourcenallokation sollten die gegenseitigen Begutachtungen jeder nationalen Behörde für die Cybersicherheitszertifizierung nach einem festgelegten Zeitplan durchgeführt werden. Eine nationale Behörde für die Cybersicherheitszertifizierung sollte die Möglichkeit haben, unter außergewöhnlichen Umständen wie unerwartetem Personalmangel oder Fällen höherer Gewalt eine Verzögerung ihrer gegenseitigen Begutachtung zu beantragen. Zu diesem Zweck müssen die Modalitäten für die Prüfung dieses Antrags festgelegt werden, wobei sicherzustellen ist, dass der übergeordnete Zeitplan eingehalten wird und die Ziele des Mechanismus der gegenseitigen Begutachtung nicht beeinträchtigt werden.

(3) Damit alle Mitgliedstaaten zur Umsetzung des Mechanismus der gegenseitigen Begutachtung beitragen und dabei voneinander lernen können, sollten die nationalen Behörden für die Cybersicherheitszertifizierung der einzelnen Mitgliedstaaten in einem Fünfjahreszeitraum jeweils zwei gegenseitige Begutachtungen durchführen. Daher sollte ein Rotationssystem eingerichtet werden, das es den nationalen Behörden für die Cybersicherheitszertifizierung aller Mitgliedstaaten ermöglicht, ihre Teilnahme zu organisieren. Außerdem müssen Kriterien festgelegt werden, die die nationalen Behörden für die Cybersicherheitszertifizierung bei der Auswahl von Vertretern für die Durchführung gegenseitiger Begutachtungen berücksichtigen sollten, damit diese über angemessene Fachkenntnisse und Kompetenzen verfügen. Die nationalen Behörden für die Cybersicherheitszertifizierung sollten ferner die Möglichkeit haben, als Beobachter an gegenseitigen Begutachtungen teilzunehmen, um das Verfahren zu verfolgen und daraus zu lernen. In solchen Fällen sollte nicht verlangt werden, dass deren Vertreter über die gleichen Fachkenntnisse und Kompetenzen verfügen, die von den Vertretern der die gegenseitigen Begutachtungen durchführenden nationalen Behörden für die Cybersicherheitszertifizierung erwartet werden.

(4) Damit eine nationale Behörde für die Cybersicherheitszertifizierung von mindestens einer nationalen Behörde für die Cybersicherheitszertifizierung einer gegenseitigen Begutachtung unterzogen wird, die denselben Ansatz für die Ausstellung von Zertifikaten für die Vertrauenswürdigkeitsstufe „hoch“ anwendet, sollte die ENISA bei der Aufforderung der nationalen Behörden für die Cybersicherheitszertifizierung, ihr Interesse an der Durchführung gegenseitiger Begutachtungen zu bekunden, angeben, ob die begutachtete nationale Behörde für die Cybersicherheitszertifizierung selbst Zertifikate für die Vertrauenswürdigkeitsstufe „hoch“ ausstellt, das in Artikel 56 Absatz 6 Buchstabe a der Verordnung (EU) 2019/881 genannte Modell der vorherigen Zustimmung verwendet, die Aufgabe gemäß Buchstabe b des genannten Absatzes allgemein übertragen hat oder eine Kombination dieser Ansätze verfolgt.

([1]) ABl. L 151 vom 7.6.2019, S. 15, ELI: http://data.europa.eu/eli/reg/2019/881/oj.

(5) Um für unionsweit einheitliche Bewertungskriterien und -verfahren für die Durchführung von gegenseitigen Begutachtungen zu sorgen, sollte jede gegenseitige Begutachtung stets einen Fragenkatalog zur Selbstbewertung, eine Dokumentationsprüfung und einen Ortstermin sowie Befragungen umfassen. Nach dem Ortstermin sollte das Begutachtungsteam die Ergebnisse mit der begutachteten nationalen Behörde für die Cybersicherheitszertifizierung erörtern, einen Berichtsentwurf erstellen und ihn der begutachteten nationalen Behörde für die Cybersicherheitszertifizierung zur Stellungnahme vorlegen, um nach Möglichkeit für Konsens zu sorgen. Das Begutachtungsteam sollte der europäischen Gruppe für die Cybersicherheitszertifizierung den Abschlussbericht vorlegen, der Leitlinien oder Empfehlungen für die Verbesserung der begutachteten nationalen Behörde für die Cybersicherheitszertifizierung enthalten kann. Die europäische Gruppe für die Cybersicherheitszertifizierung sollte ferner einen vom Begutachtungsteam vorgeschlagenen zusammenfassenden Bericht billigen, der der Öffentlichkeit zugänglich gemacht wird.

(6) Damit die im Rahmen des Verfahrens der gegenseitigen Begutachtung gewonnenen Informationen auf sichere Weise verarbeitet werden, sollte das Begutachtungsteam die Nutzung sicherer Kommunikationskanäle wie einer sicheren Plattform für die Speicherung und Weitergabe von Dokumenten und die Anwendung geeigneter Schutzvorkehrungen für vertrauliche Daten, die zwischen den Mitgliedern des Begutachtungsteams ausgetauscht werden, gewährleisten. Die ENISA sollte unter Berücksichtigung der bestehenden bewährten Verfahren der nationalen Behörden für die Cybersicherheitszertifizierung außerdem Leitlinien dazu entwickeln können, wie eine sichere Kommunikation gewährleistet werden kann, insbesondere um sicherzustellen, dass das von dem Begutachtungsteam bei der Sammlung, Weitergabe und Verarbeitung von Informationen angewandte Sicherheitsniveau auf die Sicherheitsanforderungen der begutachteten nationalen Behörde für die Cybersicherheitszertifizierung abgestimmt ist.

(7) Um die Zusammenarbeit und den wirksamen Informationsaustausch zwischen den nationalen Behörden für die Cybersicherheitszertifizierung zu erleichtern, sollte die europäische Gruppe für die Cybersicherheitszertifizierung, insbesondere deren Untergruppe für die gegenseitige Begutachtung, zur Ausarbeitung von Vorlagen beitragen und die Kommission bei der Durchführung dieser Verordnung unterstützen.

(8) Der Mechanismus für die gegenseitige Begutachtung stellt einen transeuropäischen digitalen öffentlichen Dienst im Sinne der Verordnung (EU) 2024/903 des Europäischen Parlaments und des Rates [2] dar. Mit der vorliegenden Verordnung werden neue verbindliche Anforderungen eingeführt; somit ist diese einer Interoperabilitätsbewertung gemäß Artikel 3 der Verordnung (EU) 2024/903 zu unterziehen. Dementsprechend wurde eine Interoperabilitätsbewertung durchgeführt, und der daraus resultierende Bericht soll auf dem Portal für ein interoperables Europa veröffentlicht werden.

(9) Bei der Ausarbeitung der vorliegenden Verordnung hat die Kommission die Standpunkte der europäischen Gruppe für die Cybersicherheitszertifizierung, einschließlich deren Untergruppe für die gegenseitige Begutachtung, berücksichtigt.

(10) Die in dieser Verordnung vorgesehenen Maßnahmen entsprechen der Stellungnahme des nach Artikel 66 der Verordnung (EU) 2019/881 eingesetzten Ausschusses —

HAT FOLGENDE VERORDNUNG ERLASSEN:

Artikel 1

Zeitplan, Häufigkeit und Kosten der gegenseitigen Begutachtung

(1) Die gegenseitigen Begutachtungen der nationalen Behörden für die Cybersicherheitszertifizierung werden nach dem in Anhang I festgelegten Zeitplan durchgeführt. Jede gegenseitige Begutachtung wird bis zu dem in diesem Zeitplan angegebenen Zeitpunkt abgeschlossen und danach alle fünf Jahre durchgeführt.

(2) Unter außergewöhnlichen Umständen kann eine begutachtete nationale Behörde für die Cybersicherheitszertifizierung bei der Kommission einen hinreichend begründeten Antrag auf Verschiebung ihrer gegenseitigen Begutachtung über das in der Liste in Anhang I angegebene Datum hinaus stellen. Die Kommission prüft in Zusammenarbeit mit der durch Artikel 62 der Verordnung (EU) 2019/881 eingesetzten europäischen Gruppe für die Cybersicherheitszertifizierung den Antrag und unterrichtet alle Beteiligten rechtzeitig über das Ergebnis.

[2] Verordnung (EU) 2024/903 des Europäischen Parlaments und des Rates vom 13. März 2024 über Maßnahmen für ein hohes Maß an Interoperabilität des öffentlichen Sektors in der Union (Verordnung für ein interoperables Europa) (ABl. L, 2024/903, 22.3.2024, ELI: http://data.europa.eu/eli/reg/2024/903/oj).

(3) Hat ein Mitgliedstaat im Einklang mit Artikel 58 Absatz 1 der Verordnung (EU) 2019/881

a) mehr als eine nationale Behörde für die Cybersicherheitszertifizierung in seinem Hoheitsgebiet benannt, werden alle nationalen Behörden für die Cybersicherheitszertifizierung dieses Mitgliedstaats parallel einer gegenseitigen Begutachtung unterzogen;

b) die nationale(n) Behörde(n) für die Cybersicherheitszertifizierung eines anderen Mitgliedstaats benannt, kann bzw. können diese nationale(n) Behörde(n) für die Cybersicherheitszertifizierung nach dem Zeitplan, der entweder für den benennenden Mitgliedstaat oder für den Mitgliedstaat der benannten nationale(n) Behörde(n) für die Cybersicherheitszertifizierung festgelegt wurde, in Bezug auf die in dem benennenden Mitgliedstaat wahrgenommenen Aufsichtsaufgaben einer gegenseitigen Begutachtung unterzogen werden.

(4) Die Agentur der Europäischen Union für Cybersicherheit (ENISA) macht die folgenden Informationen auf der gemäß Artikel 50 der Verordnung (EU) 2019/881 eingerichteten Website zu europäischen Schemata für die Cybersicherheitszertifizierung öffentlich zugänglich:

a) Informationen zum Zeitplan gemäß Anhang I;

b) die nach Artikel 2 Absatz 5 geführte Liste der die gegenseitige Begutachtung durchführenden nationalen Behörden für die Cybersicherheitszertifizierung.

(5) Jede nationale Behörde für die Cybersicherheitszertifizierung trägt selbst die Kosten ihrer Beteiligung.

Artikel 2

Rotationssystem für die gegenseitige Begutachtung durchführende nationale Behörden für die Cybersicherheitszertifizierung

(1) Gemäß Artikel 59 Absatz 4 der Verordnung (EU) 2019/881 erfolgt jede gegenseitige Begutachtung durch zwei die gegenseitige Begutachtung durchführende nationale Behörden für die Cybersicherheitszertifizierung anderer Mitgliedstaaten und die Kommission. Die nationalen Behörden für die Cybersicherheitszertifizierung der einzelnen Mitgliedstaaten nehmen während jedes in Anhang I festgelegten Zeitraums an der gegenseitigen Begutachtung von mindestens zwei nationalen Behörden für die Cybersicherheitszertifizierung teil.

(2) Die nationalen Behörden für die Cybersicherheitszertifizierung anderer Mitgliedstaaten können mit Zustimmung der begutachteten nationalen Behörde für die Cybersicherheitszertifizierung, der die gegenseitige Begutachtung durchführenden nationalen Behörden für die Cybersicherheitszertifizierung und der Kommission als Beobachter mit einem oder mehreren Vertretern an der gegenseitigen Begutachtung teilnehmen.

(3) Ein Vertreter der ENISA kann als Beobachter an der gegenseitigen Beurteilung teilnehmen. Weitere Vertreter können mit Zustimmung der begutachteten nationalen Behörde für die Cybersicherheitszertifizierung, der die gegenseitige Begutachtung durchführenden nationalen Behörden für die Cybersicherheitszertifizierung und der Kommission ebenfalls teilnehmen.

(4) Beobachter haben Zugang zu denselben Informationen wie die anderen Mitglieder des Begutachtungsteams, nehmen jedoch keine Aufgaben im Zusammenhang mit der Durchführung der gegenseitigen Begutachtung wahr.

(5) Die ENISA schlägt in Zusammenarbeit mit der Kommission und der europäischen Gruppe für die Cybersicherheitszertifizierung die Liste der die gegenseitige Begutachtung durchführenden nationalen Behörden für die Cybersicherheitszertifizierung vor, die den in Anhang I festgelegten Zeitplan umsetzen sollen, und führt diese Liste. Jedes Jahr fordert die ENISA in Zusammenarbeit mit der Kommission die nationalen Behörden für die Cybersicherheitszertifizierung auf, ihr Interesse an der Durchführung von oder der Teilnahme als Beobachter an den in Anhang I für das folgende Jahr vorgesehenen gegenseitigen Begutachtungen der nationalen Behörden für die Cybersicherheitszertifizierung zu bekunden.

(6) Bekunden mehr als zwei nationale Behörden für die Cybersicherheitszertifizierung ihr Interesse an der Durchführung der gegenseitigen Begutachtung derselben nationalen Behörde für die Cybersicherheitszertifizierung, konsultieren die Kommission und die ENISA die interessierten nationalen Behörden für die Cybersicherheitszertifizierung und entscheiden über die Teilnehmer der gegenseitigen Begutachtung.

(7) Gibt es in einem bestimmten Jahr nicht genügend die gegenseitige Begutachtung durchführende Behörden, die ihr Interesse an der Durchführung der gegenseitigen Begutachtungen bekunden, so wählt die Kommission nach Konsultation der europäischen Gruppe für die Cybersicherheitszertifizierung die nationalen Behörden für die Cybersicherheitszertifizierung aus, die die gegenseitigen Begutachtungen durchführen. Bei ihrer Auswahl berücksichtigt die Kommission die Verpflichtung der nationalen Behörden für die Cybersicherheitszertifizierung der einzelnen Mitgliedstaaten zur Teilnahme an der gegenseitigen Begutachtung von mindestens zwei nationalen Behörden für die Cybersicherheitszertifizierung gemäß Absatz 1.

Artikel 3

Kriterien für die Zusammensetzung des die gegenseitige Begutachtung durchführenden Teams

(1) Rechtzeitig vor Beginn der gegenseitigen Begutachtung benennt jede die gegenseitige Begutachtung durchführende Behörde einen Vertreter für die Durchführung der gegenseitigen Begutachtung. Die die gegenseitige Begutachtung durchführenden nationalen Behörden für die Cybersicherheitszertifizierung können mehr als einen Vertreter benennen, wenn dies erforderlich ist, um sicherzustellen, dass das Begutachtungsteam über die erforderlichen Kompetenzen für die Durchführung der gegenseitigen Begutachtung verfügt.

(2) Der Vertreter der die gegenseitige Begutachtung durchführenden nationalen Behörden für die Cybersicherheitszertifizierung, mit Ausnahme der Vertreter von nationalen Behörden für die Cybersicherheitszertifizierung, die als Beobachter teilnehmen, muss folgende Kriterien erfüllen:

a) verfügt über mindestens zwei Jahre Arbeitserfahrung bei der die gegenseitige Begutachtung durchführenden nationalen Behörde für die Cybersicherheitszertifizierung oder hat an mindestens zwei gegenseitigen Begutachtungen als Beobachter teilgenommen;

b) verfügt über ausreichende Kenntnisse des in der Verordnung (EU) 2019/881 festgelegten Rahmens für die Cybersicherheitszertifizierung;

c) hat gute praktische Kenntnisse des Englischen und, soweit möglich, einer oder mehrerer der in dem Mitgliedstaat der begutachteten nationalen Behörden für die Cybersicherheitszertifizierung gesprochenen Sprachen;

d) handelt unabhängig von der begutachteten nationalen Behörde für die Cybersicherheitszertifizierung.

(3) Die die gegenseitige Begutachtung durchführenden Behörden für die Cybersicherheitszertifizierung stellen sicher, dass jegliches Risiko eines Interessenkonflikts im Zusammenhang mit den benannten Vertretern den anderen Behörden für die Cybersicherheitszertifizierung, der Kommission und der ENISA vor Beginn der gegenseitigen Begutachtung offengelegt wird. Die begutachtete nationale Behörde für die Cybersicherheitszertifizierung kann Einwand gegen die Benennung bestimmter Vertreter gemäß Absatz 5 erheben.

(4) Die die gegenseitige Begutachtung durchführenden Behörden für die Cybersicherheitszertifizierung wählen aus ihrer Mitte einen Vertreter (im Folgenden „Teamleiter“) aus, der die gegenseitige Begutachtung koordiniert.

(5) Die Kommission übermittelt der begutachteten nationalen Behörde für die Cybersicherheitszertifizierung vor Beginn des Verfahrens der gegenseitigen Begutachtung die Namen und Kontaktdaten der Vertreter der die gegenseitige Begutachtung durchführenden nationalen Behörden für die Cybersicherheitszertifizierung. Möchte die begutachtete nationale Behörde für die Cybersicherheitszertifizierung Einwand gegen die Benennung eines oder mehrerer Vertreter erheben, so legt sie der Kommission innerhalb von zwei Wochen eine klare Begründung vor, unterrichtet die ENISA und die europäische Gruppe für die Cybersicherheitszertifizierung und fordert die die gegenseitige Begutachtung durchführende nationale Behörde für die Cybersicherheitszertifizierung auf, einen anderen Vertreter zu benennen.

(6) Führt das Verfahren nach Absatz 5 aufgrund außergewöhnlicher Umstände zu unangemessenen Verzögerungen bei der Einleitung der gegenseitigen Begutachtung, so entscheidet die Kommission in Absprache mit der ENISA und der europäischen Gruppe für die Cybersicherheitszertifizierung über die Zusammensetzung des Begutachtungsteams.

Artikel 4

Methode für die gegenseitige Begutachtung

(1) Im Rahmen der gegenseitigen Begutachtung werden die in Anhang II aufgeführten Aspekte gemäß Artikel 59 Absatz 3 der Verordnung (EU) 2019/881 bewertet.

(2) Die ENISA kann in Zusammenarbeit mit der europäischen Gruppe für die Cybersicherheitszertifizierung und der Kommission Vorlagen für die Bewertung der von der begutachteten nationalen Behörde für die Cybersicherheitszertifizierung festgelegten Verfahren ausarbeiten.

(3) Die gegenseitige Begutachtung umfasst Folgendes:

a) einen Fragenkatalog zur Selbstbewertung,

b) eine Bewertung der einschlägigen Dokumentation,

c) Online- und/oder persönliche Befragungen,

d) einen Ortstermin.

(4) Die Dauer der gegenseitigen Begutachtung kann je nach Umfang und Komplexität der Tätigkeiten der begutachteten nationalen Behörde für die Cybersicherheitszertifizierung vorab zwischen dem Begutachtungsteam und der begutachteten nationalen Behörde für die Cybersicherheitszertifizierung vereinbart werden. Der Ortstermin darf nicht länger als drei Arbeitstage dauern.

(5) Sofern von dem Begutachtungsteam, der begutachteten nationalen Behörde für die Cybersicherheitszertifizierung und der Kommission nicht anders vereinbart, erfolgt die Zusammenarbeit in englischer Sprache. Der in Absatz 5 genannte Bericht über die gegenseitige Begutachtung ist zumindest in englischer Sprache zu erstellen.

(6) Die begutachtete nationale Behörde für die Cybersicherheitszertifizierung arbeitet mit dem Begutachtungsteam zusammen und gewährt ihm Zugang zu den Informationen und Unterlagen, die für die Durchführung der gegenseitigen Begutachtung erforderlich sind. Die begutachtete nationale Behörde für die Cybersicherheitszertifizierung übermittelt den Fragekatalog zur Selbstbewertung und den letzten gemäß Artikel 58 Absatz 7 Buchstabe g der Verordnung (EU) 2019/881 angenommenen zusammenfassenden Jahresbericht mindestens 21 Tage vor dem Datum des Ortstermins. Zusätzliche Unterlagen werden auf Ersuchen des Begutachtungsteams innerhalb von sieben Tagen nach Eingang des entsprechenden Ersuchens übermittelt.

(7) Die Unterlagen sind in englischer Sprache vorzulegen, sofern gemäß Absatz 5 nicht anders vereinbart. Werden die Unterlagen nicht in englischer Sprache vorgelegt, kann das Begutachtungsteam verlangen, dass die für die Durchführung der gegenseitigen Begutachtung erforderlichen Unterlagen ins Englische übersetzt werden.

(8) Vor der Erstellung des Berichts über die gegenseitige Begutachtung gemäß Artikel 5 erörtert das Begutachtungsteam vorläufige Ergebnisse mit der begutachteten nationalen Behörde für die Cybersicherheitszertifizierung.

Artikel 5

Bericht über die gegenseitige Begutachtung

(1) Innerhalb von 21 Tagen nach Durchführung der gegenseitigen Begutachtung erstellt das Begutachtungsteam den Entwurf eines Berichts über die gegenseitige Begutachtung, in dem der Mitgliedstaat der begutachteten nationalen Behörde für die Cybersicherheitszertifizierung, die die gegenseitige Begutachtung durchführenden nationalen Behörden für die Cybersicherheitszertifizierung, die Kommission und etwaige Beobachter angegeben sind und der die Ergebnisse und Schlussfolgerungen der gegenseitigen Begutachtung enthält. Der Bericht enthält erforderlichenfalls Empfehlungen zur Verbesserung der im Rahmen der gegenseitigen Begutachtung behandelten Aspekte.

(2) Die ENISA kann in Zusammenarbeit mit der Kommission und der europäischen Gruppe für die Cybersicherheitszertifizierung eine Vorlage für den Bericht über die gegenseitige Begutachtung ausarbeiten.

(3) Nach Erstellung des Entwurfs des Berichts über die gegenseitige Begutachtung gemäß Absatz 1 legt das Begutachtungsteam diesen der begutachteten nationalen Behörde für die Cybersicherheitszertifizierung zur Stellungnahme innerhalb von 14 Tagen vor. Das Begutachtungsteam bewertet die Anmerkungen und nimmt sie, soweit möglich, in den Abschlussbericht auf, um für Konsens zu sorgen. Im Falle von Meinungsverschiedenheiten wird die Antwort der begutachteten nationalen Behörde für die Cybersicherheitszertifizierung dem Abschlussbericht beigefügt.

(4) Der Abschlussbericht wird der europäischen Gruppe für die Cybersicherheitszertifizierung innerhalb von zwei Monaten nach Durchführung der gegenseitigen Begutachtung übermittelt, einschließlich einer Zusammenfassung zur Veröffentlichung. Gemäß Artikel 59 Absatz 6 der Verordnung (EU) 2019/881 prüft die europäische Gruppe für die Cybersicherheitszertifizierung den Bericht und billigt seine Zusammenfassung, die auf der gemäß Artikel 50 der Verordnung (EU) 2019/881 eingerichteten Website zu europäischen Schemata für die Cybersicherheitszertifizierung veröffentlicht wird. Die Zusammenfassung enthält auch die Antwort der begutachteten nationalen Behörde für die Cybersicherheitszertifizierung oder Teile davon im Einvernehmen mit der begutachteten nationalen Behörde für die Cybersicherheitszertifizierung.

(5) Das Begutachtungsteam anonymisiert personenbezogene Daten, die es möglicherweise während der gegenseitigen Begutachtung gesammelt hat, bevor es den Bericht über die gegenseitige Begutachtung über das Begutachtungsteam hinaus verbreitet.

Artikel 6

Vertraulichkeit

(1) Alle an den gegenseitigen Begutachtungen Beteiligten wahren die Vertraulichkeit der Informationen und Daten, von denen sie in Ausübung ihrer Aufgaben und Tätigkeiten Kenntnis erlangen, und schützen dabei insbesondere Folgendes:

a) Rechte des geistigen Eigentums, vertrauliche Geschäftsinformationen oder Geschäftsgeheimnisse natürlicher oder juristischer Personen, auch Quellcode, mit Ausnahme der in Artikel 5 der Richtlinie (EU) 2016/943 des Europäischen Parlaments und des Rates ([3]) genannten Fälle,

b) die wirksame Durchführung dieser Verordnung,

c) öffentliche und nationale Sicherheitsinteressen,

d) die Integrität von Straf- oder Verwaltungsverfahren.

(2) Das Begutachtungsteam stellt sicher, dass alle im Rahmen des Verfahrens der gegenseitigen Begutachtung erlangten Informationen sicher verarbeitet werden. Nach Erstellung des Abschlussberichts und der Zusammenfassung gemäß Artikel 5 Absatz 4 löscht oder vernichtet das Begutachtungsteam, einschließlich etwaiger Beobachter, alle im Rahmen des Verfahrens der gegenseitigen Begutachtung gesammelten oder erstellten Dokumente mit Ausnahme des Abschlussberichts und der Zusammenfassung.

(3) Die ENISA kann unter Berücksichtigung bestehender bewährter Verfahren der nationalen Behörden für die Cybersicherheitszertifizierung in Zusammenarbeit mit der europäischen Gruppe für die Cybersicherheitszertifizierung Leitlinien für sichere und vertrauliche Kommunikation ausarbeiten.

([3]) Richtlinie (EU) 2016/943 des Europäischen Parlaments und des Rates vom 8. Juni 2016 über den Schutz vertraulichen Know-hows und vertraulicher Geschäftsinformationen (Geschäftsgeheimnisse) vor rechtswidrigem Erwerb sowie rechtswidriger Nutzung und Offenlegung (ABl. L 157 vom 15.6.2016, S. 1, ELI: http://data.europa.eu/eli/dir/2016/943/oj).

Artikel 7

Kapazitätsaufbau

Die ENISA analysiert die aggregierten Ergebnisse der gegenseitigen Begutachtung und hebt die gewonnenen Erkenntnisse und bewährten Verfahren hervor, um zum Kapazitätsaufbau bei den nationalen Behörden für die Cybersicherheitszertifizierung und zur Aufrechterhaltung der europäischen Systeme für die Cybersicherheitszertifizierung beizutragen. Diese Analyse kann, soweit erforderlich, Schulungen und zusätzliche Leitlinien für die nationalen Behörden für die Cybersicherheitszertifizierung umfassen, die gemeinsam mit der europäischen Gruppe für die Cybersicherheitszertifizierung ausgearbeitet werden.

Artikel 8

Inkrafttreten

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.

Brüssel, den 9. Dezember 2025

Für die Kommission
Die Präsidentin
Ursula VON DER LEYEN

ANHANG I

Zeitplan für die nationalen Behörden für die Cybersicherheitszertifizierung, die einer gegenseitigen Begutachtung unterliegen

Die gegenseitigen Begutachtungen der nationalen Behörden für die Cybersicherheitszertifizierung der folgenden Mitgliedstaaten werden bis zum 31. Dezember 2026 und danach alle fünf Jahre durchgeführt:

Belgien, Tschechien, Deutschland, Malta, Slowakei, Schweden

Die gegenseitigen Begutachtungen der nationalen Behörden für die Cybersicherheitszertifizierung der folgenden Mitgliedstaaten werden bis zum 31. Dezember 2027 und danach alle fünf Jahre durchgeführt:

Estland, Griechenland, Italien, Ungarn, Niederlande, Slowenien

Die gegenseitigen Begutachtungen der nationalen Behörden für die Cybersicherheitszertifizierung der folgenden Mitgliedstaaten werden bis zum 31. Dezember 2028 und danach alle fünf Jahre durchgeführt:

Bulgarien, Dänemark, Irland, Spanien, Kroatien, Litauen

Die gegenseitigen Begutachtungen der nationalen Behörden für die Cybersicherheitszertifizierung der folgenden Mitgliedstaaten werden bis zum 31. Dezember 2029 und danach alle fünf Jahre durchgeführt:

Lettland, Luxemburg, Österreich, Polen, Rumänien, Finnland

Die gegenseitigen Begutachtungen der nationalen Behörden für die Cybersicherheitszertifizierung der folgenden Mitgliedstaaten und der folgenden dem EWR angehörenden EFTA-Staaten werden bis zum 31. Dezember 2030 und danach alle fünf Jahre durchgeführt:

Frankreich, Zypern, Portugal, Island, Liechtenstein, Norwegen

ANHANG II

Methode für die gegenseitige Begutachtung

II.1 **Trennung zwischen Zertifizierungs- und Aufsichtstätigkeiten**

Bei der Bewertung hinsichtlich der Trennung zwischen den Zertifizierungstätigkeiten und den Aufsichtstätigkeiten der begutachteten nationalen Behörde für die Cybersicherheitszertifizierung gemäß Artikel 59 Absatz 3 Buchstabe a der Verordnung (EU) 2019/881 werden im Rahmen der gegenseitigen Begutachtung mindestens die folgenden Aspekte bewertet:

a) eine detaillierte Beschreibung der Arbeitsweise der begutachteten nationalen Behörde für die Cybersicherheitszertifizierung, in der die verschiedenen Stellen und/oder Abteilungen, die an der Durchführung der Verordnung (EU) 2019/881 beteiligt sind, eindeutig angegeben sind;

b) eine Bestandsaufnahme der Tätigkeiten der begutachteten nationalen Behörde für die Cybersicherheitszertifizierung im Vergleich zu den in Artikel 58 Absatz 7 der Verordnung (EU) 2019/881 aufgeführten Aufgaben;

c) sofern die begutachtete nationale Behörde für die Cybersicherheitszertifizierung Zertifikate ausstellt, eine Erläuterung, aus der hervorgeht, dass keine Überschneidungen zwischen ihren Zertifizierungstätigkeiten und den unter Buchstabe b genannten Aufsichtstätigkeiten vorliegen.

II.2 **Beaufsichtigung und Durchsetzung der Vorschriften für die Überwachung der Übereinstimmung mit den Zertifikaten**

Bei der Bewertung der Verfahren der begutachteten nationalen Behörde für die Cybersicherheitszertifizierung für die Beaufsichtigung und Durchsetzung der Vorschriften für die Überwachung der Übereinstimmung der IKT-Produkte, -Dienste und -Prozesse und verwalteten Sicherheitsdienste mit den in Artikel 59 Absatz 3 Buchstabe b der Verordnung (EU) 2019/881 genannten europäischen Cybersicherheitszertifikaten werden im Rahmen der gegenseitigen Begutachtung mindestens die folgenden Aspekte bewertet:

a) die Qualität und das Niveau der detaillierten Beschreibung dieser Prozesse und Verfahren sowie der Umfang ihrer Dokumentation;

b) ob und in welchem Umfang diese Prozesse und Verfahren die jeweiligen europäischen Systeme für die Cybersicherheitszertifizierung abdecken;

c) ob die begutachtete nationale Behörde für die Cybersicherheitszertifizierung tatsächlich befugt ist, Konformitätsbewertungsstellen, die Zertifikate ausstellen, zu überprüfen und erforderlichenfalls Zertifikate zu widerrufen;

d) inwiefern die begutachtete nationale Behörde für die Cybersicherheitszertifizierung mit den zuständigen Marktüberwachungsbehörden zusammenarbeitet;

e) ob die begutachtete nationale Behörde für die Cybersicherheitszertifizierung über einen nach Artikel 58 Absatz 7 Buchstabe f der Verordnung (EU) 2019/881 erforderlichen Mechanismus zur Bearbeitung von Beschwerden von natürlichen oder juristischen Personen verfügt, einschließlich Nachweisen in Bezug darauf, ob natürliche und juristische Personen das Recht haben, eine Beschwerde und einen wirksamen gerichtlichen Rechtsbehelf gemäß Artikel 63 bzw. 64 der genannten Verordnung einzulegen.

II.3 **Überwachung und Durchsetzung der Verpflichtungen der Hersteller oder Anbieter**

Bei der Bewertung der Verfahren der begutachteten nationalen Behörde für die Cybersicherheitszertifizierung für die Überwachung und Durchsetzung der Verpflichtungen der Hersteller oder Anbieter gemäß Artikel 59 Absatz 3 Buchstabe c der Verordnung (EU) 2019/881, die eine Selbstbewertung der Konformität durchführen, werden im Rahmen der gegenseitigen Begutachtung mindestens die folgenden Aspekte bewertet:

a) ob die begutachtete nationale Behörde für die Cybersicherheitszertifizierung solche Verfahren eingeführt hat und in welchem Umfang diese dokumentiert sind, insbesondere ob sie einen Mechanismus für den Erhalt und die Verarbeitung von Informationen aus externen Quellen eingerichtet hat;

b) ob und in welchem Umfang diese Verfahren die jeweiligen europäischen Systeme für die Cybersicherheitszertifizierung abdecken;

c) ob und in welchem Umfang die begutachtete nationale Behörde für die Cybersicherheitszertifizierung eigene Untersuchungen durchführt und ob die Verpflichtungen der Hersteller gemäß Artikel 53 Absätze 2 und 3 der Verordnung (EU) 2019/881 und den entsprechenden europäischen Systemen für die Cybersicherheitszertifizierung im Rahmen der Untersuchung berücksichtigt werden;

d) ob es ein Verfahren für den Austausch von Informationen im Rahmen der Zertifizierungstätigkeiten und der Aufsichtstätigkeiten der begutachteten nationalen Behörde für die Cybersicherheitszertifizierung gibt, die für die Überwachung und Durchsetzung der Verpflichtungen der Hersteller oder Anbieter relevant sind.

II.4 **Überwachung, Genehmigung und Beaufsichtigung der Konformitätsbewertungsstellen**

Bei der Bewertung der Verfahren der begutachteten nationalen Behörde für die Cybersicherheitszertifizierung für die Überwachung, Genehmigung und Beaufsichtigung der Tätigkeiten der Konformitätsbewertungsstellen gemäß Artikel 59 Absatz 3 Buchstabe d der Verordnung (EU) 2019/881 werden im Rahmen der gegenseitigen Begutachtung mindestens die folgenden Aspekte bewertet:

a) die Qualität und das Niveau der detaillierten Beschreibung solcher Verfahren sowie der Umfang ihrer Dokumentation, auch im Hinblick auf die Zusammenarbeit mit der nationalen Akkreditierungsstelle;

b) die wichtigsten Statistiken zur Zahl der erteilten, ausgesetzten oder widerrufenen Ermächtigungen, die Gesamtzahl der aktiv tätigen Konformitätsbewertungsstellen, die Zahl der ausgestellten Zertifikate und die Zahl der von der begutachteten nationalen Behörde für die Cybersicherheitszertifizierung ergriffenen Korrekturmaßnahmen;

c) sofern die begutachtete nationale Behörde für die Cybersicherheitszertifizierung die Ausstellung europäischer Cybersicherheitszertifikate auf der Vertrauenswürdigkeitsstufe „hoch“ nach vorheriger Zustimmung oder auf der Grundlage einer allgemeinen Übertragung der Aufgabe gemäß Artikel 56 Absatz 6 der Verordnung (EU) 2019/881 gestattet, die Fachkenntnisse des Personals und die Verfahren, mit denen die begutachtete nationale Behörde für die Cybersicherheitszertifizierung die Tätigkeiten der Konformitätsbewertungsstellen überwacht und beaufsichtigt.