

# Kommunikation & Recht

K&R

4 | April 2026  
29. Jahrgang  
Seiten 217 - 292

**Chefredaktion**

RA Torsten Kutschke

**Stellvertretende  
Chefredaktion**

RAin Dr. Anja Keller

**Redaktion**

Dr. Maximilian Leicht  
Sarah Selke

**Redaktionsassistentz**

Stefanie Lichtenberg

[www.kommunikationundrecht.de](http://www.kommunikationundrecht.de)

**dfv** Mediengruppe  
Frankfurt am Main

- Plattformregulierung als geopolitische Machtfrage  
**Dr. Torsten Kraul**
- 217 Die geplanten Neuerungen des Digital Network Act  
**Dr. Michael Biendl**
- 221 Schluss mit Greenwashing? – Die Umsetzung der EmpCo-Richtlinie in deutsches Recht  
**Dr. Sophie-Isabelle Horst**
- 226 K&R Kompakt: Der Entwurf zum Cybersecurity Act 2  
**Stephan Schmidt**
- 231 Update: Besteuerung der digitalen Wirtschaft 2025/2026 – Teil 1  
**Prof. Dr. Jens M. Schmittmann**
- 236 Länderreport Österreich  
**Prof. Dr. Clemens Thiele**
- 239 **EuGH:** Wunner: Gerichtsstand bei deliktischen Ansprüchen aus illegalem Online-Glücksspiel
- 242 **BGH:** Keine Klagebefugnis ausländischer Staaten bei Verdachtsäußerung der Presse  
mit Kommentar von **Dr. Christoph Matras**
- 260 **OLG Karlsruhe:** Kennzeichnungspflicht von Influencer-Beiträgen bei Gegenleistung
- 275 **AG München:** Kein Urheberrechtsschutz für mit KI erstellte Logos
- 277 **VG Schleswig-Holstein:** Keine äußerungsrechtliche Zurechnung parteipolitischer Aussagen zum Land  
mit Kommentar von **Prof. Dr. Dr. Karl-Heinz Ladeur**
- 282 **VG Köln:** Zulässige Veröffentlichung eines BSI-Berichts über sicherheitskritische Software  
mit Kommentar von **Jens Ferner**
- 286 **VG Köln:** Voraussetzungen für versteckte Überwachungsanlagen i. S. d. TDDDG  
mit Kommentar von **Martina Emrich und Christian Weber**
- 292 **K&R Standpunkt**  
Buchhandlungspreis: Rechtsschutz? Nicht vorgesehen.  
**Dr. Jasper Prigge**

turanleitungen und Reparatureinschränkungen.<sup>68</sup> Schließlich müssen Unternehmer über verfügbare umweltfreundliche Lieferoptionen<sup>69</sup> wie gebündelte Versandoptionen oder die Lieferung mit elektrischen Fahrzeugen informieren.<sup>70</sup>

#### IV. Praktische Herausforderungen und drohende Sanktionen

Die Umsetzungsvorschriften treten bereits am 27.9.2026 in Kraft, also nur rund sieben Monate nach ihrer Verkündung. Unternehmen bleibt damit eine extrem kurze Zeitspanne, um Websites, Marketingmaterialien und Produktverpackungen anzupassen. Der Bundesrat wies bereits im Oktober 2025 darauf hin, dass womöglich ohne hinreichende Abverkaufsfrist Verpackungen und verpackte Produkte in großem Umfang vernichtet werden müssten.<sup>71</sup> Die Bundesregierung sah für eine Abverkaufsfrist jedoch keinen Raum.<sup>72</sup> Der Bundestag forderte die Bundesregierung daher auf, sich bei der Kommission für eine einjährige Abverkaufsfrist für alle bis zum 27.3.2026 produzierten Produkte einzusetzen.<sup>73</sup> Bislang zeichnet sich eine solche Frist nicht ab. Die Kommission hat ihrerseits vorgeschlagen, Umweltaussagen oder Nachhaltigkeitssiegel auf bestehenden Produktverpackungen, die den neuen Anforderungen nicht genügen, etwa durch Sticker zu überdecken<sup>74</sup> – eine Lösung, deren Praktikabilität zweifelhaft ist.

Gelingt es den Unternehmen nicht, die neuen Anforderungen umzusetzen, sind sie einem erheblichen Haftungsrisiko ausgesetzt, das von Abmahnungen über Unterlassungsklagen bis zu Schadensersatzansprüchen reichen kann.<sup>75</sup> Besonders groß ist das Risiko für Unternehmen, die in mehreren EU-Mitgliedstaaten mit unzulässigen Nachhaltigkeitssiegeln oder Umweltaussagen werben. Denn dann können koordinierte Maßnahmen des Consumer Protection Cooperation Network („CPC“) drohen. Das CPC ist in den vergangenen Jahren bereits mehrfach in Bezug auf die Nachhaltigkeitskommunikation von Unternehmen tätig geworden.<sup>76</sup> Es ist zu erwarten, dass die Anzahl solcher Maßnahmen nach Inkrafttreten der Umsetzungsvorschriften zur EmpCo-Richtlinie in Europa steigen wird. Gerade im grenzüberschreitenden E-Commerce, in dem Umweltaussagen Verbraucher in mehreren Mitgliedstaaten gleichzeitig erreichen, ist das Risiko von CPC-Maßnahmen hoch.

RA Stephan Schmidt\*

## K&R Kompakt: Der Entwurf zum Cybersecurity Act 2

Vom Koordinationsinstrument zur europäischen Cybersicherheitssteuerung

### Kurz und Knapp

Im Januar 2026 wurde der Entwurf des Cybersecurity Act 2 vorgestellt, mit dem die EU eine grundlegende Reformierung ihrer Cybersicherheitsarchitektur anstrebt. Die Europäische Agentur für Netz- und Informationssicherheit soll

### V. Fazit und Ausblick

Die Umsetzung der EmpCo-Richtlinie in deutsches Recht stellt Unternehmer vor die Herausforderung, wirkungsvolles Marketing mit verschärften Anforderungen für Umweltaussagen in Einklang zu bringen. Unternehmer, die ihre Produkte und Dienstleistungen mit Umweltaussagen oder Nachhaltigkeitssiegeln bewerben, müssen ihre Kommunikationsstrategien grundlegend überprüfen und anpassen. Zertifizierungssysteme werden durchleuchtet, Werbeaussagen konkretisiert und Umsetzungspläne zur Untermauerung zukunftsgerichteter Umweltaussagen mit erheblichem Aufwand entwickelt werden müssen. Ob spezifischere und oftmals spitzfindig formulierte Umweltaussagen oder komplexe Umsetzungspläne aber wirklich mehr Klarheit für die Verbraucher bedeuten, ist zweifelhaft.

E-Commerce-Unternehmen werden zudem insbesondere Bestellprozesse anpassen müssen, um ihren erweiterten Informationspflichten nachzukommen. Da viele dieser Pflichten nur gelten, soweit dem Unternehmer die betreffenden Informationen vom Hersteller übermittelt wurden, bleibt fraglich, wie groß ihr praktischer Mehrwert sein wird.



© RSM Ebner Stolz

#### Dr. Sophie-Isabelle Horst

Studium und Promotion an der Universität Hamburg; Rechtsanwältin seit 2018; seit 2025 Counsel bei der RSM Ebner Stolz Wirtschaftsprüfer Steuerberater Rechtsanwälte Partnerschaft mbB; Schwerpunktbereiche: Prozessführung und Schiedsverfahren, insbesondere wettbewerbsrechtliche Streitigkeiten in den Bereichen E-Commerce und ESG.

68 Art. 246 Abs. 1 Nr. 10, Art. 246a § 1 Abs. 1 S. 1 Nr. 21 EGBGB n.F.

69 Art. 246a § 1 Abs. 1 S. 1 Nr. 10 EGBGB n.F.

70 BT-Drs. 21/1856, S. 51.

71 Stellungnahme des Bundesrates und Gegenäußerung der Bundesregierung, BT-Drs. 21/2464, S. 1.

72 BT-Drs. 21/2464, S. 3.

73 Beschlussempfehlung und Bericht des Ausschusses für Recht und Verbraucherschutz zu dem Gesetzentwurf der Bundesregierung (Drucksachen 21/1855, 21/2464, 21/2669 Nr. 21), BT-Drs. 21/3327, S. 3.

74 FAQ der Kommission zur EmpCo-Richtlinie, S. 17.

75 Für letztere dürfte der Kausalitätsnachweis oftmals schwierig werden.

76 Eine Übersicht der bisherigen Koordinierten Maßnahmen ist abrufbar unter <https://ruw.link/2026/66> (commission.europa.eu).

gestärkt, die Zertifizierung als Compliance-Instrument neu ausgerichtet und die Sicherheit der Lieferkette im Bereich der Informations- und Kommunikationstechnologie neu

\* Mehr über den Autor erfahren Sie am Ende des Beitrags. Alle zitierten Internetquellen wurden zuletzt abgerufen am 9.3.2026.

gestaltet werden. Der Beitrag ordnet den Entwurf systematisch und hinsichtlich seiner Bedeutung für die Fortentwicklung des europäischen IT- und Sicherheitsrechts ein und nimmt eine erste Bewertung der praktischen Auswirkungen vor.

## I. Einleitung

Cybersicherheit hat sich in den vergangenen Jahren von einer primär technischen Querschnittsmaterie zu einem zentralen Regelungsfeld des europäischen Wirtschafts-, Sicherheits- und Digitalrechts entwickelt. Cyberangriffe betreffen längst nicht mehr nur einzelne IT-Systeme oder Datenbestände, sondern entfalten erhebliche Auswirkungen auf kritische Infrastrukturen, wirtschaftliche Stabilität, staatliche Handlungsfähigkeit und gesellschaftliches Vertrauen. Spätestens seit der Zunahme staatlich oder staatsnah gesteuerter Cyberoperationen ist Cybersicherheit zudem als Bestandteil hybrider Bedrohungslagen anerkannt.

Der Cybersecurity Act von 2019 (VO (EU) 2019/881)<sup>1</sup> (nachfolgend „CSA 2019“) markiert einen wesentlichen Meilenstein in der Entwicklung des europäischen Cybersicherheitsrechts. Die Verordnung verfolgte einen doppelten Regelungsansatz: Einerseits etablierte sie die Europäische Agentur für Cybersicherheit (ENISA) mit einem permanenten Mandat und erweiterten Kompetenzen, andererseits schaffte sie einen unionsweiten Rahmen für die Cybersicherheits-Zertifizierung von Informations- und Kommunikationstechnik.<sup>2</sup> Kernstück des Zertifizierungsrahmens war die Einführung europäischer Schemata für die Zertifizierung von Informations- und Kommunikationstechnologie-Produkten (IKT-Produkten), IKT-Diensten und IKT-Prozessen. Diese basieren auf drei unterschiedlichen Vertrauenswürdigkeitsstufen (niedrig, mittel, hoch) und verfolgen einen risikobasierten Ansatz (Art. 52 CSA 2019).<sup>3</sup> Mit der Verordnung fanden zudem die Prinzipien „Security by Design“ und „Security by Default“ explizit Eingang in die europäische Gesetzgebung und ergänzten damit die bereits in der DSGVO für den Datenschutz etablierten Maßstäbe.<sup>4</sup>

Die ENISA wurde durch den CSA 2019 als europäisches Pendant zum nationalen BSI positioniert und erhielt Aufgaben hinsichtlich der Förderung der Cybersicherheit, der Unterstützung der Mitgliedstaaten sowie der Entwicklung von Zertifizierungsschemata.<sup>5</sup> Trotz dieser weitreichenden Regelungen blieb der Cybersecurity Act 2019 in der Praxis hinter den Erwartungen zurück. Die Zertifizierungsschemata entwickelten sich nur langsam, die Governance-Strukturen erwiesen sich als unzureichend und die Marktdurchdringung blieb gering.<sup>6</sup>

In den vergangenen Jahren hat die Europäische Union ihr Cyberrechtsregime schrittweise verdichtet. Das daraus resultierende Normgefüge ist durch eine zunehmende Fragmentierung gekennzeichnet und wird durch diverse Richtlinien, Verordnungen sowie sektoralen Sonderregelungen bestimmt. Der bislang geltende Cybersecurity Act vermochte diese Entwicklung nur noch unzureichend abzubilden.

Am 20.1.2026 wurde der Entwurf eines „EU Cybersecurity Act 2“ (COM(2026) 11 final)<sup>7</sup> vorgelegt, der 270 Seiten umfasst. Der vorliegende Regulierungsentwurf, der von der Kommission als wichtiger Schritt zur Sicherung der europäischen technologischen Souveränität und zur Gewährleistung einer größeren Sicherheit für alle bezeichnet wird,<sup>8</sup> zielt darauf ab, die bestehenden Defizite strukturell zu beheben. Der Verord-

nungsentwurf beschränkt sich dabei nicht auf punktuelle Anpassungen, sondern zielt auf eine grundlegende Neuausrichtung der europäischen Cybersicherheitsarchitektur ab. Zentrale Elemente des Entwurfs sind die signifikante Stärkung und funktionale Neuausrichtung der ENISA, die Reform des Europäischen Cybersicherheits-Zertifizierungsrahmens sowie die erstmalige Schaffung eines unionsweit verbindlichen Rahmens zur Absicherung kritischer IKT-Lieferketten gegen nicht-technische Risiken.

## II. Regulatorischer Kontext und systematische Einordnung

Der Entwurf des Cybersecurity Act 2 fügt sich in ein inzwischen dichtes Geflecht unionsrechtlicher Cybersicherheitsregulierungen ein. Mit der NIS-2-Richtlinie wurde ein umfassender Rahmen für das Risikomanagement und die Incident-Response-Pflichten kritischer und wichtiger Einrichtungen geschaffen. Maßnahmen zur physischen Sicherheit sind in der „Schwesterrichtlinie“, der Richtlinie über die Widerstandsfähigkeit kritischer Einrichtungen (CER-Richtlinie), definiert, während der Cyber Resilience Act produktbezogene Sicherheitsanforderungen für digitale Produkte normiert. Hinzu treten sektorspezifische Regelwerke wie der Digital Operational Resilience Act (DORA)<sup>9</sup> für den Finanzsektor, der Network Code on Cybersecurity (NCCS)<sup>10</sup> im Elektrizitätssektor sowie flankierende Instrumente wie der Cyber Solidarity Act<sup>11</sup> zur Stärkung unionsweiter Reaktionskapazitäten.

Diese Rechtsakte verfolgen jeweils eigenständige Regelungsziele, sind jedoch funktional eng miteinander verflochten. Der Entwurf des Cybersecurity Act 2 soll in diesem Normgefüge eine horizontale Ordnungsfunktion übernehmen. Der Verordnungsentwurf ist nicht primär auf die Begründung neuer materieller Sicherheitsanforderungen gerichtet, sondern auf die Strukturierung von Governance, Durchsetzung und Kohärenz des europäischen Cybersicherheitsrechts.

- 1 VO (EU) 2019/881 des Europäischen Parlaments und des Rates vom 17. 4. 2019 über die ENISA (Agentur der Europäischen Union für Cybersicherheit) und über die Zertifizierung der Cybersicherheit von Informations- und Kommunikationstechnik und zur Aufhebung der VO (EU) Nr. 526/2013 (Rechtsakt zur Cybersicherheit).
- 2 *Martini*, in: Paal/Pauly (Hrsg.), DSGVO/BDSG, 4. Aufl. 2026, VO (EU) 2016/679 Art. 32 Rn. 17 - 17 d.
- 3 *Skierka-Canton*, in: Hornung/Schallbruch (Hrsg.), IT-Sicherheitsrecht, 2. Aufl. 2024, § 8 Rn. 108 - 112; *Kipker/Scholz*, DuD 2018, 701.
- 4 *Martini*, in: Paal/Pauly (Fn. 2), Art. 32 Rn. 17 a.
- 5 *Eckhardt/Rüpke/v. Lewinski*, in: v. Lewinski/Rüpke/Eckhardt, Datenschutzrecht, 3. Aufl. 2025, § 19 Rn. 57, 58.
- 6 *Skierka-Canton*, in: Hornung/Schallbruch (Fn. 3), § 8 Messung, Prüfung und Nachweis von IT-Sicherheit Rn. 111 - 112.
- 7 Proposal for a Regulation of the European Parliament and of the Council on the European Union Agency for Cybersecurity (ENISA), the European cybersecurity certification framework, and ICT supply chain security and repealing Regulation (EU) 2019/881 (The Cybersecurity Act 2) (2026/0011 (COD)) abrufbar unter <https://ruw.link/2026/44> (digital-strategy.ec.europa.eu).
- 8 <https://ruw.link/2026/45> (ec.europa.eu).
- 9 VO (EU) 2022/2554 des Europäischen Parlaments und des Rates vom 14. 12. 2022 über die digitale operationale Resilienz im Finanzsektor und zur Änderung der Verordnungen (EG) Nr. 1060/2009, (EU) Nr. 648/2012, (EU) Nr. 600/2014, (EU) Nr. 909/2014 und (EU) 2016/1011.
- 10 Delegierte VO (EU) 2024/1366 der Kommission vom 11. 3. 2024 zur Ergänzung der VO (EU) 2019/943 des Europäischen Parlaments und des Rates durch Festlegung eines Netzkodex mit sektorspezifischen Vorschriften für Cybersicherheitsaspekte grenzüberschreitender Stromflüsse.
- 11 VO (EU) 2025/38 des Europäischen Parlaments und des Rates vom 19. 12. 2024 über Maßnahmen zur Stärkung der Solidarität und der Kapazitäten in der Union für die Erkennung von, Vorsorge für und Bewältigung von Cyberbedrohungen und Sicherheitsvorfällen und zur Änderung der VO (EU) 2021/694 (Cybersolidaritätsverordnung).

Gemäß dieser Konzeption wird Cybersicherheit somit als eine Querschnittsmaterie identifiziert, die sich über das Binnenmarktrecht, das Organisationsrecht und das Sicherheitsrecht erstreckt. Der Entwurf des Cybersecurity Act 2 zielt darauf ab, bestehende Fragmentierungen zu überwinden und gemeinsame Instrumente bereitzustellen, die sektorübergreifend wirksam sind.

Der nun vorliegende Entwurf folgt auf zwischen 2023 und 2025 mit Interessengruppen und den Mitgliedstaaten durchgeführte Konsultationen, sowohl im Rahmen der Bewertung als auch Überarbeitung des CSA 2019.<sup>12</sup>

Zeitgleich mit dem Entwurf des Cybersecurity Act 2 hat die Kommission auch den Entwurf einer Richtlinie zur Einführung gezielter Änderungen der NIS-2-Richtlinie vorgestellt.<sup>13</sup> Diese zielen darauf ab, die Rechtsklarheit zu erhöhen.

### III. Die Neuausrichtung der EU-Cybersicherheitsbehörde ENISA

#### 1. Vom Kompetenzzentrum zur operativen Schlüsselinstitution

Kernstück des Cybersecurity Act 2 soll nach dem Entwurf die grundlegende Neujustierung der Rolle der ENISA sein. Während die ENISA nach Art. 5 bis 12 CSA 2019 bislang primär beratend, koordinierend und analytisch tätig war,<sup>14</sup> soll ihr Mandat nun deutlich erweitert werden. Die Agentur soll nicht mehr nur Wissen bündeln, sondern nach Art. 3 CSA 2-E aktiv zur operativen Resilienz der Union beitragen.

Diese Entwicklung ist Ausdruck eines Funktionswandels europäischer Agenturen insgesamt. Die ENISA wird nicht zur Sicherheitsbehörde im klassischen Sinne, erhält jedoch eine zentrale Rolle im operativen Vorfeld staatlichen Handelns, insbesondere durch Lagebilder, Frühwarnmechanismen und technische Unterstützung. Für Unternehmen ergibt sich daraus, dass nicht mehr nur nachgelagerte Dokumentations- oder Auditprozesse berücksichtigt werden müssen, um regulatorische Vorgaben zu erfüllen, sondern es wird, im Sinne eines verbindlichen „Security by Design“-Ansatzes, eine frühzeitige Integration der von der ENISA entwickelten technischen und organisatorischen Sicherheitsanforderungen in die Produkt- und Dienstentwicklung erforderlich, da dies eines der erklärten Ziele des Cybersicherheits-Zertifizierungsrahmens ist (Art. 80 Abs. 1 lit. a CSA 2-E).

#### 2. Operative Unterstützungsfunktionen

Besonders deutlich wird dies an der vorgesehenen Rolle bei der Bewältigung schwerer Cybervorfälle und insbesondere von Ransomware-Angriffen. Mit dem nach Art. 13 CSA 2-E vorgesehenen Betrieb der mit der Cybersolidaritätsverordnung<sup>15</sup> eingeführten EU-Cybersicherheitsreserve erhält die ENISA die Aufgabe, Mitgliedstaaten auf deren Ersuchen hin und in Abstimmung mit Europol und CSIRTS<sup>16</sup> oder anderen zuständigen Behörden bei Vorbereitung, Reaktion und Wiederherstellung zu unterstützen. Zu diesem Zweck soll die ENISA nach Art. 13 Abs. 3 CSA 2-E einen Helpdesk einrichten und insbesondere die verbesserte gemeinsame Lageerfassung hinsichtlich der Cyberbedrohungs- und -vorfallssituation (Art. 11 Abs. 1 lit. a und g CSA 2-E) nutzen. Diese Unterstützungsleistungen bleiben zwar formal subsidiär, entfalten jedoch faktisch erhebliche Steuerungswirkung.

Hinzu treten Aufgaben im Bereich der unionsweiten Lagebildherstellung, der Sammlung und Analyse von Bedrohungsinfo-

mationen (Art. 11 CSA 2-E) sowie der Ausgabe von Frühwarnungen (Art. 12 CSA 2-E). Zudem sieht der Entwurf die Einrichtung einer zentralen Meldestelle („single entry-point“) unter Aufsicht der ENISA vor. Die Behörde wird damit zum zentralen Knotenpunkt situativer Cybersicherheitsinformation auf Unionsebene.

#### 3. Kompetenzabgrenzung zu nationalen Behörden

Dogmatisch bemerkenswert ist, dass der Cybersecurity Act 2 die Zuständigkeiten nationaler CSIRTS ausdrücklich unangestastet lässt, zugleich aber ein Geflecht von Unterstützungs-, Koordinierungs- und Informationsfunktionen etabliert, das faktisch zu einer Europäisierung operativer Entscheidungsgrundlagen führt. Die Grenze zwischen Unterstützung und Steuerung wird dadurch zunehmend fluide.

#### 4. Governance, Ressourcen und Legitimation

Die erhebliche Ausweitung der Aufgaben wird durch eine deutliche Erhöhung der personellen und finanziellen Ausstattung flankiert. Das jährliche Budget der ENISA soll nach den Angaben im Entwurfstext im Vergleich zum Jahr 2025 um 81,5 % auf 49 Millionen Euro steigen. Hinzu kommen neue Gebührenmodelle, die ENISA eine teilweise Eigenfinanzierung ermöglichen sollen. Der Entwurf sieht drei Arten von Gebühren vor, die zum Haushalt der ENISA beitragen werden: Gebühren für die Erteilung von Genehmigungen für Qualifikationsnachweise, Gebühren für die Prüfung von Tools und Gebühren für die Unterstützung der Aufrechterhaltung der europäischen Cybersicherheits-Zertifizierungssysteme.<sup>17</sup> Damit wird die Agentur institutionell aufgewertet, zugleich aber auch stärker in Legitimations- und Kontrollmechanismen eingebunden, etwa durch erweiterte Governance-Strukturen und Rechtsbehelfsverfahren.

### IV. Reform des Europäischen Cybersicherheits-Zertifizierungsrahmens (ECCF)

Der bisherige ECCF blieb trotz hoher Erwartungen weitgehend wirkungslos. Verzögerte Verfahren, unklare Governance-Strukturen und eine geringe Marktdurchdringung führten dazu, dass die Zertifizierung ihre intendierte Steuerungswirkung nicht entfalten konnte.<sup>18</sup> Bisher konnte nur ein Zertifizierungsschema für die Cybersicherheit von allgemeinen IKT-Produkten (EUCC) umgesetzt werden.<sup>19</sup> Die Abstimmung über ein Schema für Cloud-Dienste ist nach jahrelangem Streit über mögliche Teilausschlüsse außereuropäischer Anbieter gescheitert.

12 Vgl. Proposal 2026/0011 (COD), S. 9.

13 Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL amending Directive (EU) 2022/2555 as regards simplification measures and alignment with the [Proposal for the Cybersecurity Act 2], COM(2026) 13 final abrufbar unter <https://ruw.link/2026/67> (eur-lex.europa.eu).

14 Vgl. die in Kapitel II CSA 2019 geregelten Aufgaben.

15 VO (EU) 2025/38 des Europäischen Parlaments und des Rates vom 19. 12. 2024 über Maßnahmen zur Stärkung der Solidarität und der Kapazitäten in der Union für die Erkennung von, Vorsorge für und Bewältigung von Cyberbedrohungen und Sicherheitsvorfällen und zur Änderung der VO (EU) 2021/694 (Cybersolidaritätsverordnung).

16 Computer-Notfallteams (Computer Security Incident Response Teams) oder CSIRT bezeichnet ein CSIRT im Sinne von Art. 10 NIS2-RL.

17 Vgl. Art. 22 Abs. 1, 47 Abs. 2 und 47 Abs. 3 CSA 2-E.

18 Ausführlich dazu Weiß, in: Kipker/Reusch/Ritter, Recht der Informationssicherheit, 2023, CSA Art. 46 Rn. 1-6.

19 Deusch/Eggendorfer, Update IT-Sicherheitsrecht, DSRITB 2021, 321, 323; <https://ruw.link/2026/46> (certification.enisa.europa.eu).

In Deutschland wurde erst Anfang Januar 2026 das erste EUCC-Zertifikat an ein Unternehmen vergeben.<sup>20</sup>

Der Entwurf des Cybersecurity Act 2 begegnet diesen Defiziten mit einer umfassenden Verfahrensreform und einer Harmonisierung der Zertifizierungen. Klare Fristen für die Entwicklung von Zertifizierungsschemata (z. B. Art. 74 Abs. 1, 5 und 7 CSA 2-E) und transparente Konsultationsmechanismen sowie verbindliche Wartungs- und Evaluationsprozesse (z. B. Art. 76 CSA 2-E) sollen die Agilität des Systems erhöhen. Mindestens einmal im Jahr soll es eine europäische Versammlung zum Thema Cybersicherheits-Zertifizierung geben (Art. 72 Abs. 1 CSA 2-E). Die ENISA wird dabei zur zentralen Trägerin der inhaltlichen Ausgestaltung.

Besonders weitreichend ist die Ausdehnung des Zertifizierungsgegenstands. Neben Produkten und Diensten sollen nach Art. 73 Abs. 1 CSA 2-E künftig auch Prozesse, Managed Security Services und erstmals der Cybersicherheitsstatus von Einrichtungen (cyber posture of entities) zertifiziert werden. Damit verschiebt sich der Fokus von punktueller Produktsicherheit hin zu organisationsbezogener Sicherheitsfähigkeit.

Zugleich wird Zertifizierung ausdrücklich als Instrument zur Erfüllung unionsrechtlicher Pflichten positioniert (Art. 78 CSA 2-E), was für Unternehmen zur Rechtssicherheit beitragen und Doppelprüfungen reduzieren kann. Für die Erstellung von Schemata im Zertifizierungsrahmen sieht die Kommission in ihrem Entwurf pauschal eine Frist von zwölf Monaten vor. Das Verfahren soll also deutlich beschleunigt werden.

Obwohl die Zertifizierung formal freiwillig bleiben soll, besteht die Gefahr einer faktischen Pflichtzertifizierung. Aufsichtspraktiken, Haftungsrisiken und vergaberechtliche Anforderungen könnten dazu führen, dass Unternehmen ohne Zertifikat erhebliche Nachteile erleiden.

## V. Der neue EU-Rahmen zur Sicherheit von IKT-Lieferketten

Der Entwurf des Cybersecurity Act 2 definiert in Art. 2 Nr. 40 CSA 2-E IKT-Lieferketten als Gesamtheit der IKT-Dienstleistungen, IKT-Produkte und IKT-Prozesse, die alle Aktivitäten und Akteure umfassen, die in allen Phasen vor der Bereitstellung eines Produkts oder einer Dienstleistung auf dem Markt beteiligt sind. Die vorgeschlagenen Regelungen schaffen erstmals einen verbindlichen unionsweiten Rahmen zur Bewältigung nicht-technischer Risiken in IKT-Lieferketten innerhalb der aus der NIS-2-RL bekannten Sektoren und zählt so auf die digitale Souveränität der Mitgliedstaaten ein. Ausgangspunkt ist die Erkenntnis, dass Abhängigkeiten von bestimmten Drittstaaten oder Anbietern erhebliche Sicherheitsrisiken begründen können, auch unabhängig von der technischen Qualität einzelner Produkte. Nach Art. 98 Abs. 1 CSA 2-E sollen betroffene IKT-Komponenten in kritischen IKT-Lieferketten identifiziert und angemessene Maßnahmen für betroffene Unternehmen verankert werden. Ausdrücklich sollen Mitgliedstaaten durch den neuen Rahmen jedoch nicht daran gehindert werden, Vorschriften zu erlassen oder beizubehalten, die ein höheres Maß an Cybersicherheit in den IKT-Lieferketten gewährleisten, sofern diese Vorschriften mit ihren Verpflichtungen aus dem Unionsrecht im Einklang stehen (Art. 98 Abs. 3 CSA 2-E).

Ausgelöst wird das Verfahren nach Art. 99 CSA 2-E durch eine von der NIS Kooperationsgruppe durchgeführte EU-weit koordinierte Sicherheitsrisikobewertung, in der anhand verschiedener Kriterien „Hochrisiko-Drittstaaten“ identifiziert werden

(Art. 100 CSA 2-E). Der Prozess zur Überprüfung, ob ein Drittland solche Bedenken aufwirft, ist jedoch ausgesprochen vage. Kriterien können von dem Land ausgegangene böswillige Cyberaktivitäten sein, aber auch Gesetze, die Unternehmen dazu verpflichten, Schwachstellen zu melden, oder fehlende unabhängige Kontrollmechanismen. In einem zweiten Schritt werden dann „Hochrisiko-Lieferanten“ aus den Hochrisiko-Staaten benannt. Betroffen sind die 18 in der NIS-2-Richtlinie benannten kritischen Sektoren, wobei für die Betroffenheit von Unternehmen – anders als bei der NIS-2-Richtlinie – keine Schwellenwerte, wie Mitarbeiter-, Umsatz- oder Bilanzsummengrenzen gelten. Ausschlaggebend soll vielmehr sein, welche Rolle das Unternehmen in der IKT-Lieferkette einnimmt und welches Risiko durch Produkte oder Dienstleistungen des betroffenen Unternehmens für die Resilienz der IKT-Infrastruktur der EU entsteht.

Basierend auf dieser Bewertung soll die Kommission dann über Durchführungsrechtsakte wichtige IKT-Anlagen identifizieren (Art. 100, 102 CSA 2-E) und Maßnahmen zur Risikominderung auferlegen, darunter Beschränkungen und/oder Verbote für die Nutzung, Installation oder Integration von IKT-Komponenten von Hochrisikolieferanten in diesen wichtigen IKT-Anlagen. Ebenfalls über Durchführungsrechtsakte können Übergangs- und Auslaufphasen geregelt werden (Art. 103 CSA 2-E).

Abweichend von dem vorstehend geschilderten Vorgehen kann die Kommission, wenn sie ausreichende Gründe zu der Annahme hat, dass die Verwendung bestimmter, von einem Unternehmen aus einem Drittland bereitgestellter, IKT-Komponenten, für mindestens drei Mitgliedstaaten „ein erhebliches nichttechnisches Cybersicherheitsrisiko“ darstellt, Beschränkungen für deren Verwendung auferlegen, ohne das betroffene Drittland als Cybersicherheitsrisiko einzustufen (Art. 103 Abs. 6 CSA 2-E). Ein solches Risiko wird als gegeben angesehen, wenn bei der Verwendung der IKT-Komponente davon ausgegangen werden kann, dass sie mit hoher Wahrscheinlichkeit einen Vorfall verursacht, der schwerwiegende negative Auswirkungen haben könnte, einschließlich erheblicher materieller oder immaterieller Verluste oder Störungen.

Die Risikobewertung erfolgt unionsweit koordiniert. Die Kommission erhält eine zentrale Rolle bei der Bewertung und Einstufung von Drittstaaten, welche Anlass zu Bedenken hinsichtlich der Cybersicherheit geben („posing cybersecurity concerns“). Diese Bewertung entfaltet unmittelbare Rechtsfolgen für Marktteilnehmer. Anbieter aus entsprechend eingestuften Drittstaaten können von der Lieferung kritischer IKT-Komponenten ausgeschlossen werden, haben aber die Möglichkeit, eine Ausnahmegenehmigung zu beantragen (Art. 105 CSA 2-E). Dann müssten sie darlegen, wie sie die identifizierten Risiken mindern. Betroffene Unternehmen können zudem bei wesentlichen Änderungen in ihren Strukturen eine Neubewertung beantragen (Art. 104 CSA 2-E).

Für einen Sektor wird im Entwurf dann auch schon ganz konkret geregelt, was der Rahmen zur Bewältigung nicht-technischer Risiken in IKT-Lieferketten für diesen Sektor bedeutet. Für mobile, feste und satellitengestützte elektronische Kommunikationsnetze wendet der Entwurf, in Anknüpfung an das EU-Instrumentarium für 5G-Sicherheit, den Rahmen auf wichtige Netzkomponenten an, welche in Anhang II

20 Pressemeldung des Bundesamts für Sicherheit in der Informationstechnik vom 13. 1. 2026, abrufbar unter <https://ruw.link/2026/47> (bsi.bund.de).

aufgelistet werden, und führt eine Auslaufverpflichtung für IKT-Komponenten von Hochrisikolieferanten innerhalb von 36 Monaten nach Veröffentlichung der entsprechenden Liste der Hochrisikolieferanten ein (Art. 110 CSA 2-E). Art. 111 CSA 2-E regelt schließlich ein Verbot der Verwendung, Installation oder Integration von IKT-Komponenten und Komponenten, die IKT-Komponenten von Hochrisikolieferanten enthalten.

## VI. Kompetenz- und verfassungsrechtliche Einordnung

Die Kommission stützt sich auf Art. 114 AEUV. Diese Wahl unterstreicht wie schon beim CSA 2019 die Binnenmarktorientierung des Cybersecurity Act 2.

Zugleich zeigt der Entwurf, wie weit die funktionale Reichweite dieser Kompetenznorm inzwischen reicht. Sicherheits- und geopolitische Erwägungen werden konsequent in das Binnenmarktrecht integriert, da unterschiedliche nationale Ansätze zu einer höheren Anfälligkeit einiger Mitgliedstaaten führen könnten und dies Ausstrahlungseffekte auf die gesamte Union haben kann.

Subsidiarität und Verhältnismäßigkeit werden dabei im Wesentlichen mit der grenzüberschreitenden Natur von Cyber Risiken begründet.<sup>21</sup> Der Entwurf des Cybersecurity Act 2 ist damit Ausdruck einer fortschreitenden Europäisierung digitaler Sicherheitsverwaltung, ohne dass formell eine sicherheitspolitische Kompetenz begründet würde.

## VII. Vorschläge zu Änderungen der NIS-2-Richtlinie

Zeitgleich mit dem Vorschlag für den Cybersecurity Act 2 hat die Kommission auch Vorschläge zu Änderungen der NIS-2-Richtlinie vorgelegt, welche punktuell Erleichterungen schaffen und die Rechtssicherheit erhöhen sollen.

So sollen Unternehmen zur Nachweiserleichterung im Einklang mit dem Verordnungsvorschlag Zertifikate im Rahmen von organisatorischen Cybersicherheits-Zertifizierungssystemen erhalten können, die innerhalb des ECCF entwickelt wurden.

Die ENISA soll zukünftig Mitgliedstaaten bei der Beaufsichtigung von Unternehmen unterstützen, welche in mehreren Ländern tätig sind und der Aufsicht durch die zuständigen Behörden mehrerer Mitgliedstaaten unterliegen. So soll die gegenseitige Amtshilfe erleichtert und ein besserer Überblick über die Unternehmen geschaffen werden.

Zudem soll die Kommission zukünftig Leitlinien für die Anwendung der Anforderungen an die Sicherheit der Lieferkette verabschieden. So soll auch verhindert werden, dass Unternehmen, die in den Anwendungsbereich der NIS-2-Richtlinie fallen, an ihre Lieferanten, die selbst nicht direkt in den Anwendungsbereich fallen, unangemessene Verpflichtungen weitergeben.

Weitere vorgeschlagene Änderungen der NIS-2-Richtlinie umfassen: (a) verschiedene Klarstellungen zum Anwendungsbereich und zu den Begriffsbestimmungen (z. B. durch die Einführung einer Mindestleistung von 1 Megawatt für Energieerzeuger); (b) Streichung von Kleinst- und Kleinunternehmen, die DNS-Dienste anbieten, aus dem Anwendungsbereich; (c) Einführung einer neuen Kategorie kleiner mittelständischer Unternehmen im Einklang mit der Empfehlung der Kommission von 2025 zur Definition kleiner mittelständischer Unter-

nehmen; Unternehmen, die als kleine mittelständische Unternehmen gelten, sollen als wichtige Unternehmen herab- bzw. eingestuft werden, wodurch sich ihr Compliance-Aufwand und der Aufsichtsaufwand für die zuständigen Behörden verringern;<sup>22</sup> (d) Verpflichtung der Mitgliedstaaten, Maßnahmen für die Umstellung auf Post-Quantum-Kryptografie (PQC) zu ergreifen und (e) die Einführung einer harmonisierten Erhebung von Daten über Ransomware-Angriffe.

Beachtenswert ist in diesem Zusammenhang, dass es keine Änderung bei der Einbeziehung von Managed (Security) Service Providern geben soll und diese weiter bei Erreichen der relevanten Schwellenwerte in den Anwendungsbereich fallen sollen. Dies gilt auch dann, wenn es sich um Anbieter innerhalb einer Unternehmensgruppe handelt. Auch eine andere Einschränkung von Nebentätigkeiten gibt es nicht, so dass der deutsche Sonderweg für vernachlässigbare Tätigkeiten weiterhin sehr kritisch zu sehen ist.<sup>23</sup>

## VIII. Fazit und Ausblick

Der vorliegende Entwurf des Cybersecurity Act 2 sowie die Modifikationen der NIS-2-Richtlinie offerieren substanzielle Möglichkeiten zur Gewährleistung von Kohärenz, Resilienz und strategischer Autonomie der Union innerhalb des europäischen Regulierungsrahmens für Cybersicherheit. Der Entwurf birgt jedoch auch Risiken in Form einer zunehmenden Kompetenzverdichtung auf Unionsebene, einer faktischen Regulierung jenseits formaler Verpflichtungen sowie einer hohen Abhängigkeit von effektiver Governance.

Für Unternehmen impliziert der Entwurf des Cybersecurity Act 2 demnach sowohl eine Simplifizierung durch Harmonisierung als auch neue Herausforderungen und strategische Anforderungen an Transparenz, Dokumentation und Zertifizierungsstrategien. Verstöße gegen Maßnahmen sowie gegen Meldepflichten sind mit Bußgeldern von bis zu 7 % des weltweiten Jahresumsatzes bewehrt.

Der Entwurf des Cybersecurity Act 2 markiert einen fundamentalen Wandel im europäischen Cybersicherheitsrecht. Er transformiert Cybersicherheit von einer reaktiven Technikregulierung zu einem präventiven, strukturellen Steuerungsinstrument und dauerhaften Governance-Thema.

Da sowohl der Cybersecurity Act 2 als auch die geplanten NIS-2-Änderungen noch durch das Trilogverfahren zu führen sind, ist mit einem Inkrafttreten nicht vor dem zweiten Quartal 2027 zu rechnen. Der Cybersecurity Act 2 würde als Verordnung unmittelbar gelten, die NIS-2-Änderung sollen die Mitgliedstaaten innerhalb eines Jahres in nationale Regelungen umsetzen müssen.



**Stephan Schmidt**

ist Fachanwalt für IT-Recht und Gründungspartner bei TCI Rechtsanwälte in Mainz. Er ist Mitglied im Geschäftsführenden Ausschuss der Arbeitsgemeinschaft IT-Recht im deutschen Anwaltverein (davit).

21 Section 2 of the Explanatory Memorandum of Proposal 2026/0011 (COD), S. 5 f.

22 Hessel/Schneider, MMR-Aktuell 2026, 01147.

23 Vgl. Schmidt, RD 2024, 550, 552; Hessel/Schneider, MMR-Aktuell 2026, 01147.