Nomos **PRAXIS**

Wiebe [Hrsg.]

# Das neue Recht der Cyberresilienz

Cyber Resilience Act (CRA)

Nomos

Nomos**PRAXIS**

**Dr. Gerhard Wiebe**

# Das neue Recht der Cyberresilienz

## Cyber Resilience Act (CRA)

**Dr. Jonas Jossen,** Mag. rer. publ., Bundesamt für Sicherheit in der Informationstechnik, Bonn | Prof. **Dr. Johannes Schäffer,** HWR Berlin | RAin **Dr. Zeynep Schreitmüller,** Augsburg | RA **Thorsten Sörup,** FAIT-Recht u. FAArbR, Frankfurt a.M. | RA **Dr. Gerhard Wiebe,** Berlin | RA **Philipp Wolf,** LL.M. (University of Queensland), Berlin

Nomos

**Zitiervorschlag:** Wiebe Der neue CRA § ... Rn.

**Die Deutsche Nationalbibliothek** verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.d-nb.de abrufbar.

ISBN 978-3-7560-0473-7 (Print)
ISBN 978-3-7489-3969-6 (ePDF)

1. Auflage 2025

## Vorwort

Digitalisierung und Cybersicherheit sind schon seit geraumer Zeit einer der bestimmenden Themen in der Produktregulierung. Mit der am 10.12.2024 in Kraft getretenen Verordnung (EU) 2024/2847 (sog. Cyber Resilience Act – CRA) hat die EU den Versuch unternommen, produktbezogene Cybergefahren rechtlich zu domestizieren und die entsprechende Lücke in der Rechtslandschaft zu schließen. Damit hat die EU auf wachsende Bedrohungen reagiert, die von IT-Sicherheitslücken bei Produkten und Cyberattacken ausgehen. Wie gut es ihr gelungen ist das hehre Ziel – Schaffung eines hohen Cybersicherheitsniveaus bei Produkten mit digitalen Elementen – zu erreichen, wird sich ab dem Geltungsbeginn des CRA am 11.12.2027 zeigen.

Als klassischer CE-Rechtsakt, der dem sog. New Legislative Framework (NLF) folgt, statuiert der CRA erstmals cybersicherheitsbezogene Produktanforderungen und erlegt den Wirtschaftsakteuren korrespondierende Pflichten auf. Mitunter beschreitet er dabei neue, in der Literatur und Industrie nicht unkritisch beäugte Pfade (zB Pflicht zu Sicherheitsaktualisierungen). Die Erforderlichkeit dafür begründen besondere Herausforderungen, die vor allem mit der Regelungsmaterie und den Schutzgütern zusammenhängen: Produktbezogene Cybersicherheit beschreibt den Schutz von Produkten vor Menschen (zum Schutz anderer Menschen), weil böswilliges Verhalten Dritter cyberbezogene Gefahr auslösen, für die die Hersteller in die Pflicht genommen werden. Zweitens sind die Parameter, um Cybersicherheit zu erreichen und zu messen, nur schwer zu greifen und ständig im Fluss; eine Prüf- und Messstandardisierung erweist sich als schwierig. Drittens erfasst der CRA sowohl physische als auch digitale Produkte.

Dieser Einführungsband versucht, gleichsam die althergebrachten Rechtsinstitute des NLF im Gewand und Kontext des CRA und die neu eingeführten Instrumente „leicht verdaulich" genauso wie praxisnah anhand der Gesetzesstruktur zu erläutern. Zudem werden für identifizierte Probleme und relevante Rechtsfragen praxistaugliche Lösungen angeboten; in diesem Sinne ist das Werk mit vielzähligen impliziten und ausdrücklichen Praxishinweisen gespickt. Dementsprechend richtet sich das von ausgewiesenen Fachleuten verfasste Buch als Handreichung für einen vertiefenden Einstieg in die neue Materie gleichermaßen an juristische und technische Praktikerinnen und Praktiker, die sich mit der produktbezogenen Cybersicherheit beschäftigen. Dabei sind die verschiedenen Perspektiven und Querbezüge zu anderen Rechtsbereich bei der Erschließung des CRA besonders gewinnbringend.

Ich möchte mich bei Dr. Jonas Jossen, Prof. Dr. Johannes Schäffer, Dr. Zeynep Schreitmüller, Thorsten Sörup und Philipp Wolf für ihr Mitwirken und die zur Verfügung gestellte Expertise ganz herzlich bedanken. Ebenso danke ich Dr. Marco Ganzhorn für seine abermalige verlagsseitige Unterstützung bei der Realisierung des Buchs. Mein besonderer Dank gilt Louisa – meiner Gefährtin und Komplizin, schärfsten Kritikerin und größten Unterstützerin. Ohne ihre kritischen Gedanken, ihren Zuspruch und ihre Geduld (wie jetzt im Urlaub) wären mir solche Publikationsprojekte nicht möglich. Ihr widme ich mein Zutun zu diesem Werk als Herausgeber und Mitautor.

Ich hoffe, dass der Einführungsband einen Mehrwert bei der Auseinandersetzung mit dem CRA bietet, und bin dankbar für neue Impulse, Kritik und Vorschläge (E-Mail: wiebe@produktkanzlei.com).

Tejakula (Bali), im Juni 2025 *Gerhard Wiebe*

# Inhaltsverzeichnis

## Bearbeiterverzeichnis

*Dr. Jonas Jossen, Mag. rer. publ.*
Referent, Bundesamt für Sicherheit in der Informationstechnik, Bonn

*Prof. Dr. Johannes Schäffer*
HWR Berlin

*Dr. Zeynep Schreitmüller*
Rechtsanwältin, Augsburg

*Thorsten Sörup*
Rechtsanwalt, Fachanwalt für IT-Recht, Fachanwalt für Arbeitsrecht, Frankfurt a.M.

*Dr. Gerhard Wiebe*
Rechtsanwalt, Berlin

*Philipp Wolf, LL.M. (University of Queensland)*
Rechtsanwalt, Berlin

# § 1 Einleitung



## A. Anlass und rechtspolitischer Hintergrund

Das grundsätzliche Potenzial von Cyberangriffen bzw. Cyberattacken und die damit einhergehende Bedrohungslage innerhalb der EU sieht sich einer stetigen Steigerung und Verschärfung ausgesetzt, die sowohl in Bezug auf die Anzahl und Vielfalt als auch auf die resultierenden Folgen dieser Vorfälle neue Maßstäbe setzen. Zu dieser Feststellung kommt die ENISA – European Union Agency For Cybersecurity – in ihrem Report zur Cybersicherheit für das Jahr 2024.[1] Schon mehrere Jahre zuvor (2019) vertrat die ENISA die Ansicht, dass in Bezug auf sog. „connected devices" oftmals nicht einmal die einfachsten Cybersicherheitsmechanismen vorhanden sind, wodurch diese Art von Geräten bereits leichte Angriffsziele primitiver Cyberattacken seien.[2] Die Brisanz fehlender bzw. nicht ausreichender Sicherheitsanforderungen zur Vermeidung und Risikominimierung vor Cyberangriffen lässt sich auch in finanzielle Zahlen fassen. In ihrem Entwurf zum CRA bezifferte die Kommission die **jährlichen Kosten** der Cyberkriminalität bis zum Jahr 2021 auf **5,5 Billionen EUR**.[3] 1

Kurze Zeit später entschied sich die EU mit ihrer **Cyberstrategie für die digitale Dekade** (2020) dazu, den Schutz und Standard in Bezug auf das Niveau der Cybersicherheit zu erhöhen. Die Widerstandsfähigkeit innerhalb der EU sollte erhöht und gestärkt werden und kreierte das Schlagwort: *„thinking global, acting european"*.[4] Der CRA fügt sich in die von der EU erstellte Strategie ein, mit der die digitale Zukunft Europas sichergestellt werden soll. Insoweit tritt der CRA neben die bereits bestehenden EU-Rechtsakte, wie ua NIS-2-Richtlinie (Richtline (EU) 2022/2555), DORA (VO (EU) 2022/2554) oder den Cybersecurity Act (VO (EU) 2019/881). 2

Zudem bleibt festzuhalten, dass auf europäischer Ebene bereits verschiedene – aber eben nur speziell auf **einzelne Sektoren zugeschnittene** – Rechtsakte in Kraft sind, wie zB RL (EU) 2014/53 (sog. Funkanlagenrichtlinie), VO (EU) 2017/745 (sog. EU-Medizinprodukteverordnung), VO (EU) 2017/745 (sog. EU-In-vitro-Diagnostikaverordnung), VO (EU) 2019/1139 (sog. EU-Verordnung über gemeinsame Regeln für die Regulierung der Zivilluftfahrt) oder VO (EU) 2023/1230 (sog. EU-Maschinenverordnung). 3

Mit dem CRA wird nicht nur ein weiterer Schritt aus dem Konzept für Europas digitale Dekade unternommen. Es wird mit dem CRA auch ein **EU-weiter, allgemeingültiger Rechtsrahmen** etabliert, der eben nicht nur auf konkrete Sektoren zugeschnitten ist. Diese Handlungsweise erscheint auch logisch, da es sich bei Cybersicherheit grundsätzlich um eine internationale/EU-weite Thematik handelt, die wegen ihres Schadenspotenzials und ihrer Risiken eben auch als eine EU-weite Problematik begriffen werden 4

1 European Union Agency For Cybersecurity, 2024 Report on the State of Cybersecurity in the Union, S. 14.
2 European Union Agency For Cybersecurity, Opinion Consumers and IoT security, September 2019, S. 3.
3 COM(2021) 454 final, 1.
4 Cybersicherheitsrichtlinien (The EU's Cybersecurity Strategy for the Digital Decade), S. 4.

kann. Sicherheitsrisiken infolge von Cyberangriffen wirken sich grenzüberschreitend, über mehrere Sektoren und Produkte hinweg aus.

## B. Gesetzgebungsverlauf

5 Am 15.9.2022 legte die Kommission ihren Vorschlag für den CRA vor.[5] Dieser Vorschlag betonte folgende **Ziele**, die mit einem CRA verfolgt und erreicht werden sollten:

- die Schaffung der Bedingungen für die Entwicklung sicherer Produkte mit digitalen Elementen, damit Hardware- und Softwareprodukte mit weniger Schwachstellen in Verkehr gebracht werden und damit die Hersteller sich während des **gesamten Lebenszyklus** eines Produkts ernsthaft um die Sicherheit kümmern;
- die Schaffung von Bedingungen, die es den Nutzern ermöglichen, bei der **Auswahl** und **Verwendung** von Produkten mit digitalen Elementen die Cybersicherheit zu berücksichtigen;
- Gewährleistung, dass die Hersteller die Sicherheit von Produkten mit digitalen Elementen schon ab der **Konzeptions- und Entwicklungsphase und über den gesamten Lebenszyklus verbessern**;
- Gewährleistung eines **kohärenten Cybersicherheitsrahmens**, der den Hardware- und Software-Herstellern die Einhaltung der Vorschriften erleichtert;
- Erhöhung der **Transparenz** der Sicherheitseigenschaften von Produkten mit digitalen Elementen;
- **Befähigung der Unternehmen und Verbraucher**, damit sie Produkte mit digitalen Elementen sicher verwenden können.[6]

6 Der Europäische Datenschutzbeauftragte hat seine Stellungnahme am 9.11.2022 abgegeben.[7] Daneben hat auch der Europäische Wirtschafts- und Sozialausschuss (EWSA) seine Stellungnahme am 14.12.2022 veröffentlicht.[8] Hingegen hat der Ausschuss der Regionen trotz dessen Konsultation davon abgesehen, eine Stellungnahme abzugeben.[9]

7 Der Europäische Datenschutzbeauftragte sprach sich in dessen Stellungnahme ausdrücklich dafür aus, dass vor allem die Medizinprodukteverordnung (VO (EU) 2017/745) gerade nicht aus dem Anwendungsbereich des CRA herausdefiniert werden sollte, also auch der CRA vollends auf die Sachverhalte der Medizinprodukteverordnung Anwendung finden solle.[10] Augenscheinlich blieb diese Empfehlung für den weiteren Gesetzgebungsverlauf **unberücksichtigt**, da die Medizinprodukteverordnung gerade vom Anwendungsbereich des CRA ausgenommen ist (vgl. Art. 2 Abs. 2 lit. A CRA). Hingegen scheint die Empfehlung des Europäischen Datenschutzbeauftragten zur **Implementierung** des **Datenschutzgrundsatzes durch Technikgestaltung** und durch **datenschutzfreundliche Voreinstellungen** als grundlegende Cybersicherheitsanforderung für Produkte mit digitalen Elementen Berücksichtigung gefunden zu haben (vgl. Erwgr. 32).

5 COM(2021) 454 final.
6 COM(2021) 454 final, 2 f.
7 ABl. 2022/C 452/7.
8 ABl. 2023/C 100/15.
9 Vgl. COM(2022/0272(COD)), 13757/24.
10 ABl. 2022/C 452/7.

Der EWSA hat bereits in seiner Stellungnahme auf das Thema der **Ressourcenerhöhung** zugunsten der ENISA hingewiesen, damit diese mit der Hilfe von **personell und fachlich angemessener Ausstattung** die ihr übertragenen sensiblen Aufgaben wirksam erfüllen könne.[11] 8

Der Rat teilte seine Position zum Entwurf des CRA mit, wonach verschiedene Teile des Kommissionsvorschlags als änderungsbedürftig angesehen wurden.[12] Der Rat nahm das **Verhandlungsmandat** mit dem EU-Parlament im Ausschuss der ständigen Vertreter am 19.7.2023 an.[13] 9

Das EU-Parlament hat unter Beteiligung der beiden **Ausschüsse** Industrie, Forschung und Energie (**ITRE**) und Binnenmarkt und Verbraucherschutz (**IMCO**) am 27.7.2023 seine Position mitgeteilt, wonach Änderungen am Entwurf zum CRA vorgesehen waren bzw. für notwendig erachtet wurden.[14] 10

Im Anschluss hieran traten die Institutionen in das **Trilogverfahren** ein und konnten sich schließlich am 30.11.2023 auf einen **Kompromisstext** einigen.[15] Ergebnis des Trilogverfahrens ist auch, dass der Einigung eine **gemeinsame Erklärung** des Europäischen Parlaments, des Rates und der Kommission zu den **Ressourcen der ENISA** zugrunde liegen soll.[16] Zukünftig sollen insbesondere die **personellen Ressourcen aufgestockt** werden, damit auf Seiten der ENISA Fachwissen vorhanden ist, das den technischen Vorgaben nach dem CRA entspricht. Nach dieser gemeinsamen Erklärung könne der Personalbedarf im jährlichen Verfahren im Zusammenhang mit dem Stellenplan der ENISA vorgesehen werden. 11

Das EU-Parlament hat den Kompromisstext am 12.3.2024 in erster Lesung angenommen.[17] Der Rat hat den Standpunkt des EU-Parlaments in erster Lesung am 10.10.2024 gebilligt.[18] 12

## C. Instrument

Der europäische Gesetzgeber stellt in seinen Erwägungsgründen zum CRA fest, dass in Bezug auf die Materie Cybersicherheit ein „[…] **legislativer Flickenteppich** innerhalb des Binnenmarkts entstanden ist, der zu einer großen **Rechtsunsicherheit** sowohl für die Hersteller als auch für die Nutzer von solchen Produkten und zu einer größeren unnötigen Belastung der Unternehmen und Organisationen führt."[19] 13

Der CRA ist als **Verordnung** erlassen und besitzt damit allgemeine Geltung und ist in allen Teilen verbindlich sowie innerhalb der Mitgliedstaaten unmittelbar anwendbar. Daher ist die Verordnung (Art. 288 Abs. 2 AEUV) als Rechtsakt grundsätzlich dazu geeignet, legislative Unterschiede und Lücken innerhalb des Binnenmarkts zu nivellieren. 14

11 ABl. 2023/C 100/15.
12 Vgl. https://data.consilium.europa.eu/doc/document/ST-11726-2023-INIT/en/pdf.
13 Vgl. COM(2022/0272(COD)), 12536/23.
14 Ausführlich hierzu: vgl. COM(2022) 0454 – C9–0308/2022 – 2022/0272(COD), A9–0253/2023.
15 Rat der Europäischen Union, Pressemitteilung, 30.11.2023; 17000/23.
16 Vgl. COM(2022) 0454 – C9–0308/2022 – 2022/0272(COD), Annex III.
17 ABl. C/2025/1022.
18 Siehe ABl. L v. 20.11.2024, Fn. 2; vgl. auch Pressemitteilung Rat der Europäischen Union, 10.10.2024, abrufbar unter https://www.consilium.europa.eu/de/press/press-releases/2024/10/10/cyber-resilience-act-council-adopts-new-law-on-security-requirements-for-digital-products/ mit Verweis auf Dokument PE-CONS 100/1/23.
19 Erwgr. 4.

15 Für den EU-Gesetzgeber liegt es auf der Hand, dass Produkte mit digitalen Elementen unter Umständen böswilligen Akteuren als Angriffsvektor dienen können (vgl. Erwgr. 10). Daher wird auf der europäischen Ebene versucht, per Verordnung als Legislativakt (Verordnung, Art. 288 Abs. 2 AEUV) das **Gesamtniveau** der **Cybersicherheit** aller im Binnenmarkt in Verkehr gebrachten Produkte mit digitalen Elementen zu erhöhen, indem **grundlegende Cybersicherheitsanforderungen** aufgestellt werden, die sodann **horizontal** gegenüber den Adressaten/Verpflichteten gelten sollen.[20] Daher ist auch die Richtlinie kein geeignetes Instrument, weil sie nur hinsichtlich ihres Ziels verbindlich ist, aber nicht bzgl. der durch die Mitgliedstaaten eingesetzten Umsetzungsakte und deren konkreter Ausgestaltung (vgl. Art. 288 Abs. 3 AEUV). Damit besteht bei der Richtlinie die potenzielle Gefahr, dass bei der Ausgestaltung des Umsetzungsermessens der einzelnen Mitgliedstaaten unterschiedliche Maßstäbe angesetzt werden könnten, wodurch gerade das Ziel von **Rechtssicherheit** durch einen **einheitlichen Rechtsrahmen** volatil wäre und einer **Fragmentierung unterschiedlicher Rechtsrahmen** nicht wirksam entgegengetreten werden kann.

## D. Rechtsgrundlage

16 Der CRA stützt sich auf die Rechtsgrundlage nach Art. 114 AEUV. Diese Vorschrift stellt grundsätzlich eine Ermächtigung für sog. **Harmonisierungsmaßnahmen** betreffend den Binnenmarkt dar. Im Einklang mit dem in der EU geltenden Prinzip der begrenzten Einzelermächtigung (Art. 5 Abs. 1 EUV) basiert das gesetzgeberische Handeln der EU auf der Rechtsgrundlage von Art. 114 AEUV, um das (bessere) Funktionieren des europäischen Binnenmarkts sicherzustellen, indem Rechts- und Verwaltungsvorschriften innerhalb der EU angeglichen werden (vgl. Art. 26 AEUV).

## E. Inkrafttreten und Anwendung

17 Auch der CRA unterscheidet zwischen dem Zeitpunkt seines Inkrafttretens und dem Zeitpunkt des Geltungsbeginns/Anwendungsbeginns (vgl. Art. 71 CRA).

18 Nach Art. 71 Abs. 1 CRA tritt die Verordnung 20 Tage nach der Veröffentlichung im Amtsblatt der Europäischen Union in Kraft. Dementsprechend ist der CRA seit dem 10.12.2024 in Kraft.

19 Nach Art. 71 Abs. 2 CRA **gelten die Regelungen des CRA** ab dem **11.12.2027** (→ § 4 Rn. 41 ff.). Demnach beträgt der **Übergangszeitraum** zwischen Inkrafttreten und Anwendungsbeginn **36 Monate**. Damit ist dieser Zeitraum grundsätzlich länger ausgestaltet, als es noch zunächst im Entwurf des CRA angedacht war. Nach Art. 57 UAbs. 2 CRA-E waren lediglich 24 Monate vorgesehen, damit sich Hersteller, notifizierte Stelle und Mitgliedstaaten auf die neuen Anforderungen einstellen. Gleichwohl erfolgt für den CRA – ähnlich wie bei anderen Rechtsakten aus dem digitalen Umfeld – ein **zeitlich abgestufter Geltungsbeginn**.

20 Damit entfalten die Vorgaben und Pflichten aus dem CRA nicht an einem Tag ihre Geltung. Die Verpflichtung zur Meldung von Vorfällen und Schwachstellen (→ § 6 Rn. 44)

20 Erwgr. 8.

gilt bereits ab dem **11.9.2026** (vgl. Art. 14 CRA). Ebenfalls gilt für die Regelungen aus Kapitel IV (Art. 35–51 CRA) ein kürzerer bzw. vorgezogener Geltungsbeginn; diese Vorgaben gegenüber den Mitgliedstaaten zur Notifizierung von Konformitätsbewertungsstellen gelten bereits ab dem **11.6.2026**. Der in diesem Zusammenhang bestehende vorgezogene Geltungsbeginn resultiert aus der Verpflichtung, dass die Mitgliedstaaten dafür Sorge tragen müssen, dass es bis zum **11.12.2026** „in der Union eine ausreichende Zahl notifizierter Stellen gibt, die Konformitätsbewertungen durchführen können, um Engpässe und Hindernisse mit Blick auf den Marktzugang zu verhindern" (vgl. Art. 35 Abs. 2 CRA). Zumindest in diesem Zusammenhang bleibt festzuhalten, dass es faktisch zu einem kürzeren Zeitraum zwischen Inkrafttreten und Geltungsbeginn gekommen ist, als es im Entwurf angedacht wurde.

Während der CRA-Entwurf lediglich den vorgezogenen Geltungsbeginn gegenüber den Herstellern vorsah (Verpflichtung zur Meldung von Vorfällen und Schwachstellen), wurden nunmehr mit der finalen Fassung des CRA auch die Mitgliedstaaten bzgl. der Regelungen aus Kapitel IV (Art. 35–51 CRA) mit einem vorgezogenen Geltungsbeginn bedacht. 21

## F. Aufhebungen und Änderungen anderer EU-Rechtsakte

Mit dem CRA werden jedenfalls keine anderen EU-Rechtsakte aufgehoben. Vielmehr ist darauf hinzuweisen, dass es zu Änderungen anderer Verordnungen und Richtlinien kommen kann. 22

Die Verordnung (EU) Nr. 168/2013 wird ergänzt; konkret wird Anhang II Teil C1 der Verordnung (EU) Nr. 168/2013 erweitert. Mit dieser Ergänzung wird nunmehr der „Schutz des Fahrzeugs gegen Cyberangriffe" betreffend Fahrzeuge der Klasse L gemäß VO (EU) Nr. 168/2013 materielle Anforderung werden. Damit legt der CRA jedoch keine neuen Standards und Voraussetzungen fest. Die Ergänzung hat wohl nur **klarstellende bzw. komplettierende Funktion**. Denn bereits mit der Verordnung (EU) 2019/2144 wurden Anforderungen an die Typgenehmigung von Kraftfahrzeugen sowie von Systemen und Bauteilen für diese Fahrzeuge festgelegt und bestimmte Cybersicherheitsanforderungen eingeführt. 23

Die Verordnung (EU) 2019/1020 wird ergänzt; konkret wird diese zukünftig auch für die Produkte mit digitalen Elementen gelten, soweit diese Produkte in den Anwendungsbereich des CRA fallen. Die Erweiterung des Anwendungsbereichs der Verordnung (EU) 2019/1020 im vorgenannten Sinne ist auch nur logisch und konsequent. Die Marktüberwachung ist für die Gewährleistung der korrekten und einheitlichen Anwendung des Unionsrechts ein wesentliches Instrument. Soweit durch den CRA ein **einheitlicher Rechtsrahmen** – also eine einheitliche Voraussetzungsebene – geschaffen wird, soll „reflexartig" auch eine **einheitliche Kontrollebene** geschaffen werden. 24

Die Richtlinie (EU) 2020/1828 wird zukünftig auch auf Sachverhalte im Zusammenhang mit den Verpflichtungen nach dem CRA Anwendung finden. Demnach können grundsätzlich Verbandsklagen gegen Verstöße durch Unternehmer möglich werden, wenn diese gegen den CRA verstoßen und dadurch die Kollektivinteressen der Verbraucher beeinträchtigt werden oder sie diese zu beeinträchtigen drohen (vgl. Art. 2 Abs. 1 Richtlinie (EU) 2020/1828). 25

26 Im CRA ist das Verhältnis zur Funkanlagenrichtlinie nicht ausdrücklich geregelt. Aufgrund der Regelungen aus Art. 1 Abs. 1 VO (EU) 2022/30 kommt es zwischen dem CRA und der Funkanlagenrichtlinie zur **Anwendungsüberschneidung**. Während der Entwurf zum CRA dies noch erkannt hatte und in diesem Zusammenhang die Absicht der Kommission erkennen ließ, die Durchführungsverordnung (VO (EU) 2022/30) insoweit aufzuheben oder zu ändern.[21] Interessanterweise ist der CRA in diesem Punkt weniger klar und lässt sogar erkennen, dass es zu einem (wohl längeren) Übergangszeitraum kommen könne, wenn sogar davon ausgegangen wird, dass die Kommission den Herstellern Leitlinien an die Hand geben werde, damit diese den Nachweis zur Einhaltung beider Verordnungen leichter erbringen können.[22]

21 COM(2022) 454 final, 4.
22 Erwgr. 30.

## § 2 New Legislative Framework als Regelungskonzept

**Literatur:** Heckmann/Ziegler, Der Cyber Resilience Act: Ein Gesetz „mit digitalen Elementen", ITRB 2024, 159; Klindt, Der „new approach" im Produktrecht des europäischen Binnenmarkts: Vermutungswirkung technischer Normung, EuZW 2002, 133; Schucht, 30 Jahre New Approach im europäischen Produktsicherheitsrecht – prägendes Steuerungsmodell oder leere Hülle?, EuZW 2017, 46; Wiebe/Daelen/Kerger, Der neue Cyber Resilience Act – Regulierung der produktbezogenen Cybersicherheit, K&R 2025, 79.

Der CRA basiert auf dem Regelungskonzept des sog. **New Legislative Framework** (**NLF**) und folgt einem **risikobasierten Security-by-Design-Ansatz**.[1] Bei dem NLF handelt es sich um einen neuen Rechtsrahmen für die Gestaltung von europäischen Produktrechtsvorschriften, der den sog. **New Approach** als Rechtssetzungsmodell und als (nach wie vor geltendes) industriepolitisches Konzept modifiziert hat.[2] Die Grundelemente des New Approach bzw. des NLF sind:[3] 1

- Verankerung bloß **grundlegender rechtlicher Anforderungen**
- **Detailkonkretisierung mittels technischer Normen**
- **widerlegbare Konformitätsvermutung bei der Anwendung harmonisierter, im EU-Amtsblatt veröffentlichter Normen**
- **Rechtsunverbindlichkeit technischer Normen**

Das rechtliche Korsett des NLF formt der **Beschluss Nr. 768/2008/EG** bzw. die in seinem Anhang I enthaltenen „Musterbestimmungen für die Ausarbeitung von Rechtsvorschriften der Gemeinschaft zur Harmonisierung der Bedingungen für die Vermarktung von Produkten". Die rechtskonzeptionelle Basis des NLF und die Orientierung des CRA an den Musterbestimmungen des Beschlusses Nr. 768/2008/EG zeigen sich bereits in dessen **strukturellem Aufbau** und Systematik sowie in einer Vielzahl der **Legaldefinitionen** gem. Art. 3 CRA (vgl. Art. R1 des Anhangs I des Beschlusses Nr. 768/2008/EG). Die **Pflichtenkonzepte der Wirtschaftsakteure** in Kap. II (→ § 6 Rn. 1 ff.) nehmen Anleihen an Kap. R2 des Anhangs I des Beschlusses Nr. 768/2008/EG. Die Regelungen zur **Konformität des Produkts** in Kap. III folgen den Vorgaben in Kap. R3 des Anhangs I des Beschlusses Nr. 768/2008/EG. Dies gilt insbesondere für die **Konformitätsbewertungsverfahren** gem. Art. 32 CRA iVm Anhang VIII (→ § 5 Rn. 11 ff.) sowie die **Konformitätsvermutung** gem. Art. 27 CRA (→ § 5 Rn. 149). Die für den New Approach charakteristischen Bestimmungen zur **EU-Konformitätserklärung** und **CE-Kennzeichnung** gem. Art. 28 ff. CRA (→ § 5 Rn. 89 ff.) entsprechen den Art. R10 ff. des Anhangs I des Beschlusses Nr. 768/2008/EG, was dem CRA den Anstrich eines CE-Rechtsakts verleiht. Ferner enthält Kap. V in Anlehnung an Kap. R4 des Anhangs I des Beschlusses Nr. 768/2008/EG Vorschriften zur **Notifizierung von Konformitätsbewertungsstellen**. Schließlich wurzelt das **Schutzklauselverfahren** iSd Kap. VI in Kap. R5 des Anhangs I des Beschlusses Nr. 768/2008/EG. 2

Der NLF hat sich mittlerweile als klassisches Regelungsmodell bei der Produktregulierung etabliert. Bieten doch die Grundmerkmale des NLF einen verlässlichen Rechtsrah- 3

1 Wiebe/Daelen/Kerger K&R 2025, 79; Heckmann/Ziegler ITRB 2024, 159 (160).
2 Zum „New Approach" Schucht EuZW 2017, 46; Klindt EuZW 2002, 133.

men bei gleichzeitiger **Innovationsoffenheit** und **Technologieneutralität**, was sich auch der CRA zunutze macht.[4] Allerdings ist der NLF a priori auf die Regulierung physischer Produkte ausgelegt. Bei der Eins-zu-eins-Übertragung der Regelungsstrukturen und -techniken des NLF auf **unverkörperte Softwareprodukte** tun sich daher Friktionen und Unstimmigkeiten auf. An einigen Stellen wurden die entsprechenden Besonderheiten von rein digitalen Produkten berücksichtigt; etwa beim **Anbringungsort der CE-Kennzeichnung** gem. Art. 30 Abs. 1 S. 2 CRA (→ § 5 Rn. 92). Hingegen passt der Begriff des **Inverkehrbringens** iSv Art. 3 Nr. 21 CRA bzw. der **Bereitstellung auf dem Markt** iSv Art. 3 Nr. 22 CRA, wonach eine Abgabe des Produkts verlangt wird, nicht bei nicht körperlicher Software (→ § 4 Rn. 18). Als kritische Würdigung lässt sich festhalten, dass es insgesamt mehr Anpassungen des NLF auf Stand-alone-Software als Regulierungsgegenstand bedurft hätte.

3 Blue Guide 2022, Abschnitt 1.1.3.
4 Erwgr. 8.

# § 3 Regelungsgegenstand und Ziele des CRA

**Literatur:** Wiebe, Cybersicherheit 2.0 – Vorschlag eines Cyber Resilience Act, ZRP 2023, 73; Wiebe/Daelen, Der Cyber Resilience Act aus produktsicherheitsrechtlicher Perspektive, EuZW 2023, 257; Wiebe/Daelen/Kerger, Der neue Cyber Resilience Act, K&R 2025, 79.



## A. Regelungsgegenstand

Der CRA zielt darauf ab, ein einheitliches europäisches Regelwerk betreffend Produkte mit digitalen Elementen zu schaffen, um schließlich deren Cybersicherheit zu verbessern. Der CRA enthält Vorschriften, die Hersteller, Importeure und Händler verpflichten, bestimmte Cybersicherheitsanforderungen einzuhalten. Dazu zählen unter anderem Anforderungen an sichere Entwicklung und Herstellung, das Management von Schwachstellen sowie die Pflicht zur Bereitstellung von Sicherheitsupdates. Darüber hinaus schafft der Rechtsakt Transparenzpflichten hinsichtlich der Cybersicherheitsmerkmale von Produkten und legt Marktüberwachungsmechanismen fest. 1

Im Kern regelt der CRA die Gestaltung, Entwicklung und Inverkehrbringung von Produkten mit digitalen Elementen in Bezug auf deren Cybersicherheit über den gesamten Lebenszyklus hinweg. Den **Regelungsgegenstand** umreißt Art. 1 CRA, wobei dieser die zentralen Inhalte der Verordnung definiert. Es werden vier zentrale Bereiche vom Rechtsakt erfasst: 2

- Vorschriften für die Bereitstellung von Produkten mit digitalen Elementen auf dem Markt: Ziel ist es, ein **hohes Maß an Cybersicherheit** bei der **Inverkehrbringung** und **Bereitstellung** solcher Produkte innerhalb des Binnenmarkts sicherzustellen (→ Rn. 10).
- Grundlegende Cybersicherheitsanforderungen an Konzeption, Entwicklung und Herstellung: Die Verordnung legt **technische** und **organisatorische Anforderungen** fest, die Hersteller bei der **Produktgestaltung** berücksichtigen müssen, um ein angemessenes Schutzniveau gegen Sicherheitsrisiken zu gewährleisten. Ergänzend werden Pflichten der Wirtschaftsakteure (Hersteller (→ § 6 Rn. 5 ff.)., Importeure (→ § 6 Rn. 74 ff.), Händler (→ § 6 Rn. 108 ff.)) zur Unterstützung der Produktsicherheit geregelt.
- Cybersicherheitsanforderungen an das Schwachstellenmanagement: Hersteller müssen Verfahren zur **Identifizierung**, **Behebung** und **Meldung** von **Schwachstellen** über die erwartete Nutzungsdauer eines Produkts hinweg etablieren. Auch hier trifft die Verordnung begleitende Pflichten für andere Wirtschaftsakteure.
- Vorschriften zur Marktüberwachung und Durchsetzung: Die Verordnung regelt die **Rolle** und **Befugnisse** der **nationalen Behörden** in Bezug auf Kontrolle, Überwachung und Sanktionierung bei Verstößen gegen die vorgenannten Anforderungen.

3 Diese zentralen Bereiche finden sich in den Regelungen des CRA wieder und tragen dazu bei, sowohl den Binnenmarkt zu stärken als auch Risiken für Nutzerinnen und Nutzer sowie für Unternehmen zu minimieren.

4 Die Regelungsstruktur des CRA ist systematisch aufgebaut und gliedert sich in mehrere Kapitel:

- Kapitel I (Allgemeine Bestimmungen) definiert unter anderem Zielsetzung, Anwendungsbereich und zentrale Begriffe.
- Kapitel II (Pflichten für Wirtschaftsakteure) legt die Verantwortlichkeiten der Hersteller, Importeure und Händler fest.
- Kapitel III (Grundlegende Anforderungen und Konformitätsbewertung) enthält die technischen und organisatorischen Anforderungen an Produkte sowie die Verfahren zur Bewertung ihrer Einhaltung.
- Kapitel IV (Marktüberwachung und Durchsetzung) beschreibt die Rolle und Befugnisse der Marktüberwachungsbehörden sowie die Maßnahmen bei Verstößen.
- Kapitel V (Delegierte Rechtsakte und Durchführungsrechtsakte) regelt die Befugnisse der Kommission zur weiteren Ausgestaltung des Rechtsakts.
- Kapitel VI (Übergangs- und Schlussbestimmungen) enthält Regelungen zur Umsetzung und zum Inkrafttreten.

5 Insgesamt schafft der CRA damit einen **kohärenten Rechtsrahmen für einheitliche Cybersicherheitsstandards** im Binnenmarkt der EU.

## B. Schutzgüter und Ziele

### I. Begriffsverständnis Cybersicherheit

6 Der CRA enthält selbst keine Definition zum Begriff der Cybersicherheit, sondern **verweist** gem. Art. 3 Nr. 3 CRA auf die **Definition nach Art. 2 Nr. 1 VO EU 2019/881** (sog. „Rechtsakt zur Cybersicherheit").[1] Auf der einen Seite festigt die EU mit dem Rückgriff auf die bestehende Begrifflichkeit ihre Cyberstrategie. Auf diese Weise vermeidet die EU, dass für elementare Aspekte in diesem Zusammenhang keine unterschiedlichen bzw. divergierenden Begrifflichkeiten begründet und verwendet werden.

7 Daher sind auch im Anwendungsbereich des CRA unter **Cybersicherheit** zunächst „[…] alle Tätigkeiten, die notwendig sind, um Netz und Informationssysteme, die Nutzer solcher Systeme und andere von Cyberbedrohungen betroffene Personen zu schützen", zu verstehen. Insoweit muss im Anwendungsbereich des CRA im Zusammenhang mit Cybersicherheit auch auf die **Definition** von **Cyberbedrohung** zurückgegriffen werden: „Cyberbedrohung bezeichnet einen möglichen Umstand, ein mögliches Ereignis oder eine mögliche Handlung, der/das/die Netz- und Informationssysteme, die Nutzer dieser Systeme und andere Personen schädigen, stören oder anderweitig beeinträchtigen könnte" (Art. 2 Nr. 8 VO (EU) 2019/881). In diesem Zusammenhang stellte der Unionsgesetzgeber in den Erwägungsgründen klar, dass Cybersicherheit keinesfalls nur eine Frage von technischen Vorkehrungen und Sicherheitsmaßnahme sei, sondern auch die menschliche Komponente erfasst werden (müsse), wenn es um Schutzmaßnahmen

1 VO (EU) 2019/881 – Rechtsakt zur Cybersicherheit.

## Stichwortverzeichnis

Die **fetten** Zahlen verweisen auf den Paragrafen (Beitrag), die mageren auf die Randnummer.