

Schröder | Hartl [Hrsg.]

Cyber Resilience Act

Cyberresilienz-Verordnung



NomosKOMMENTAR

Prof. Dr. Meinhard Schröder
Dr. Korbinian Hartl [Hrsg.]

Cyber Resilience Act

Cyberresilienz-Verordnung

RA Dr. Tobias Ackermann, München | RA Dr. Korbinian Hartl, München | RA Stefan Hessel, LL.M., Saarbrücken | ORR Dr. Kai Hofmann, Dresden | Prof. Dr. Lukas Iffländer, Hochschule für Technik und Wirtschaft Dresden | Dr. Jonas Jossen, Mag. rer. publ., Bundesamt für Sicherheit in der Informationstechnik (BSI) | Jan Philip Kühne, Universität Passau | StA Julien Mehnert | SyndikusRA Dr. Christian Piovano, Friedrichshafen | RA Manuel Poncza, Köln | RA Stephan Schmidt, FAIT-Recht, Mainz | RAin Dr. Kristina Schreiber, FAinVerwR, Köln | Prof. Dr. Meinhard Schröder, Universität Passau | RA Dr. Paul Vogel, LL.M. Eur., München | RA Dr. Gerhard Wiebe, Berlin



Nomos

Zitiervorschlag: NK-CRA/Bearbeiter Art ... 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 978-3-7560-0246-7

1. Auflage 2026

© Nomos Verlagsgesellschaft, Baden-Baden 2026. Gesamtverantwortung für Druck und Herstellung bei der Nomos Verlagsgesellschaft mbH & Co. KG. Alle Rechte, auch die des Nachdrucks von Auszügen, der fotomechanischen Wiedergabe und der Übersetzung, vorbehalten.

Vorwort

Sehr geehrte Leserinnen, sehr geehrte Leser,

Cybersicherheit stellt nicht nur eine der größten Herausforderungen für die digitale Gesellschaft dar, sondern hat sich längst als eigenständiges, durchaus vielfältiges und fragmentiertes Rechtsgebiet etabliert. Mit der Cyberresilienz-Verordnung (CRA) hat der europäische Gesetzgeber nun einen Rahmen geschaffen, der bisherige Lücken im Cybersicherheits-Recht schließen soll: Vernetzte Produkte sind allgegenwärtig und werden in Zahl und Vielfalt in den kommenden Jahren nur weiter exponentiell zunehmen. Schwachstellen bergen erhebliche wirtschaftliche und gesellschaftliche Risiken. Inzwischen ist klar, dass die Gewährleistung von Cybersicherheit nicht allein eine Frage der Vertragsgestaltung, sektorspezifischer Sonderregulierung oder des Datenschutzes sein kann.

Mit dem CRA wachsen Produktrecht und Digitalgesetzgebung zusammen, was für die Praxis tiefgreifende Veränderungen bedeutet: Hersteller und andere Wirtschaftsakteure stehen vor neuen Pflichten, die weit über bisherige Anforderungen hinausgehen. Auch bleibt abzuwarten, wie die Rechtsprechung den CRA systematisch in das Gefüge der europäischen Digitalregulierung einordnen wird.

Angesichts dieser Unsicherheiten soll der Kommentar Ihnen eine umfassende Orientierung im CRA bieten. Unser Dank gebührt zunächst den Autorinnen und Autoren, die mit Ihrer Fachkompetenz und praktischen Erfahrung diesen Kommentar ermöglicht haben und tragen. Wir sind froh, dass Experten aus der rechtsanwaltlichen Praxis, „digitalnahen“ Behörden und der Wissenschaft bereit waren, ihr Wissen zu teilen und dieses Werk in Angriff zu nehmen.

Unser besonderer Dank gilt dem Nomos-Verlag für die immer entschlossene Unterstützung dieses Projekts und die verlässliche Begleitung bis zur Publikation. Hervorheben möchten wir insbesondere Herrn Dr. Ganzhorn, der die Konzeption des Kommentars maßgeblich gefördert, die Abstimmung zwischen Herausgebern, Autorinnen und Autoren mitkoordiniert und damit ganz wesentlich zum Gelingen des Werkes beigetragen hat.

Der Kommentar befindet sich auf dem Stand von Dezember 2025. Anregungen und Kritik sind herzlich willkommen.

Passau/München März 2026

Meinhard Schröder und Korbinian Hartl

Inhaltsverzeichnis

Vorwort	5
Autorinnen und Autoren	11
Abkürzungsverzeichnis	13

Verordnung (EU) 2024/2847 des Europäischen Parlaments und des Rates vom 23. Oktober 2024 über horizontale Cybersicherheitsanforderungen für Produkte mit digitalen Elementen und zur Änderung der Verordnungen (EU) Nr. 168/2013 und (EU) 2019/1020 und der Richtlinie (EU) 2020/1828 (Cyberresilienz-Verordnung)

Kapitel I Allgemeine Bestimmungen

Artikel 1	Gegenstand	17
Artikel 2	Anwendungsbereich	23
Artikel 3	Begriffsbestimmungen	38
Artikel 4	Freier Verkehr	103
Artikel 5	Beschaffung oder Nutzung von Produkten mit digitalen Elementen	110
Artikel 6	Anforderungen an Produkte mit digitalen Elementen	115
Artikel 7	Wichtige Produkte mit digitalen Elementen	132
Artikel 8	Kritische Produkte mit digitalen Elementen	143
Artikel 9	Konsultation der Interessenträger	153
Artikel 10	Ausbau der Kompetenzen in einem digitalen Umfeld mit Cyberabwehrfähigkeit	156
Artikel 11	Allgemeine Produktsicherheit	157
Artikel 12	Hochrisiko-KI-Systeme	161

Kapitel II Pflichten der Wirtschaftsakteure und Bestimmungen in Bezug auf freie und quelloffene Software

Artikel 13	Pflichten der Hersteller	167
Artikel 14	Meldepflichten der Hersteller	189
Artikel 15	Freiwillige Meldungen	197
Artikel 16	Einrichtung einer einheitlichen Meldeplattform	199
Artikel 17	Sonstige Bestimmungen im Zusammenhang mit der Berichterstattung	204
Artikel 18	Bevollmächtigte	207
Artikel 19	Pflichten der Einführer	209
Artikel 20	Pflichten der Händler	216
Artikel 21	Fälle, in denen die Pflichten der Hersteller auch für Einführer und Händler gelten	228
Artikel 22	Sonstige Fälle, in denen die Pflichten der Hersteller gelten	231
Artikel 23	Identifizierung der Wirtschaftsakteure	234
Artikel 24	Pflichten der Verwalter quelloffener Software	235
Artikel 25	Sicherheitsbescheinigung für freie und quelloffene Software	246
Artikel 26	Leitlinien	249

Kapitel III Konformität des Produkts mit digitalen Elementen		
Artikel 27	Konformitätsvermutung	254
Artikel 28	EU-Konformitätserklärung	263
Artikel 29	Allgemeine Grundsätze der CE-Kennzeichnung	270
Artikel 30	Vorschriften und Bedingungen für die Anbringung der CE-Kennzeichnung	274
Artikel 31	Technische Dokumentation	283
Artikel 32	Konformitätsbewertungsverfahren für Produkte mit digitalen Elementen	296
Artikel 33	Unterstützungsmaßnahmen für Kleinunternehmen sowie kleine und mittlere Unternehmen, einschließlich Start-up-Unternehmen	303
Artikel 34	Abkommen über die gegenseitige Anerkennung	307
Kapitel IV Notifizierung von Konformitätsbewertungsstellen		
Artikel 35	Notifizierung	308
Artikel 36	Notifizierende Behörden	311
Artikel 37	Anforderungen an notifizierende Behörden	319
Artikel 38	Informationspflichten der notifizierenden Behörden	324
Artikel 39	Anforderungen an notifizierte Stellen	325
Artikel 40	Vermutung der Konformität von notifizierten Stellen	335
Artikel 41	Zweigstellen notifizierter Stellen und Vergabe von Unteraufträgen durch notifizierte Stellen	336
Artikel 42	Antrag auf Notifizierung	340
Artikel 43	Notifizierungsverfahren	342
Artikel 44	Kennnummern und Verzeichnisse notifizierter Stellen	345
Artikel 45	Änderungen der Notifizierungen	346
Artikel 46	Anfechtung der Kompetenz notifizierter Stellen	348
Artikel 47	Operative Pflichten der notifizierten Stellen	350
Artikel 48	Einspruch gegen Entscheidungen notifizierter Stellen	355
Artikel 49	Meldepflichten der notifizierten Stellen	356
Artikel 50	Erfahrungsaustausch	358
Artikel 51	Koordinierung der notifizierten Stellen	359
Kapitel V Marktüberwachung und Durchsetzung		
Artikel 52	Marktüberwachung und Kontrolle von Produkten mit digitalen Elementen auf dem Unionsmarkt	361
Artikel 53	Zugang zu Daten und zur Dokumentation	377
Artikel 54	Nationale Verfahren für Produkte mit digitalen Elementen, die ein erhebliches Cybersicherheitsrisiko bergen	380
Artikel 55	Schutzklauselverfahren der Union	389
Artikel 56	Verfahren auf Unionsebene für Produkte mit digitalen Elementen, die ein erhebliches Cybersicherheitsrisiko bergen	394
Artikel 57	Konforme Produkte mit digitalen Elementen, die ein erhebliches Cybersicherheitsrisiko bergen	399
Artikel 58	Formale Nichtkonformität	404
Artikel 59	Gemeinsame Tätigkeiten der Marktüberwachungsbehörden	407

Artikel 60	Koordinierte Kontrollen (Sweeps)	417
Kapitel VI Übertragene Befugnisse und Ausschussverfahren		
Artikel 61	Ausübung der Befugnisübertragung	424
Artikel 62	Ausschussverfahren	433
Kapitel VII Vertraulichkeit und Sanktionen		
Artikel 63	Vertraulichkeit	440
Artikel 64	Sanktionen	455
Artikel 65	Verbandsklagen	474
Kapitel VIII Übergangs- und Schlussbestimmungen		
Artikel 66	Änderung der Verordnung (EU) 2019/1020	481
Artikel 67	Änderung der Richtlinie (EU) 2020/1828	482
Artikel 68	Änderungen der Verordnung (EU) Nr. 168/2013	482
Artikel 69	Übergangsbestimmungen	483
Artikel 70	Bewertung und Überprüfung	490
Artikel 71	Inkrafttreten und Geltungsbeginn	492
Anhang I	Grundlegende Cybersecurityanforderungen	497
Anhang II	Informationen und Anleitungen für den Nutzer	499
Anhang III	Wichtige Produkte mit digitalen Elementen	502
Anhang IV	Kritische Produkte mit digitalen Elementen	503
Anhang V	EU-Konformitätserklärung	504
Anhang VI	Vereinfachte EU-Konformitätserklärung	505
Anhang VII	Inhalt der technischen Dokumentation	506
Anhang VIII	Konformitätsbewertungsverfahren	511
Erwägungsgründe		521
Durchführungsverordnung (EU) 2025/2392 der Kommission vom 28. November 2025 über die technische Beschreibung der Kategorien von wichtigen und kritischen Produkten mit digitalen Elementen gemäß der Verordnung (EU) 2024/2847 des Europäischen Parlaments und des Rates		565
Delegierte Verordnung (EU) 2026/881 der Kommission vom 11. Dezember 2025 zur Ergänzung der Verordnung (EU) 2024/2847 des Europäischen Parlaments und des Rates durch Festlegung der Modalitäten und Bedingungen für die Geltendmachung von Cybersicherheitsgründen im Zusammenhang mit dem Aufschub der Verbreitung von Meldungen		579
Delegierte Verordnung (EU) 2025/1535 der Kommission vom 29. Juli 2025 zur Ergänzung der Verordnung (EU) 2024/2847 des Europäischen Parlaments und des Rates hinsichtlich einer Ausnahme von der Anwendung der genannten Verordnung für bestimmte Produkte mit digitalen Elementen, die in den Anwendungsbereich der Verordnung (EU) Nr. 168/2013 des Europäischen Parlaments und des Rates fallen		585
Stichwortverzeichnis		589

Autorinnen und Autoren

<i>Dr. Tobias Ackermann</i> Rechtsanwalt, München	Art. 47–50
<i>Dr. Korbinian Hartl</i> Rechtsanwalt, München	Art. 1 (mit <i>Schröder</i>)
<i>Stefan Hessel, LL.M.</i> Rechtsanwalt, Saarbrücken	Art. 3 Nr. 19, 27 Art. 32–34
<i>Dr. Kai Hofmann</i> ORR, Dresden	Art. 2 Art. 3 Nr. 1, 2, 23–25, 32, 34, 35, 47 Art. 3 Nr. 3, 5–11, 39 (mit <i>Iffländer</i>) Art. 4, 5 Art. 6–8 (mit <i>Iffländer</i>) Art. 9–12 Art. 13 Rn. 66–74 (mit <i>Iffländer</i>)
<i>Prof. Dr. Lukas Iffländer</i> Hochschule für Technik und Wirtschaft Dresden	Art. 3 Nr. 3, 5–11, 39 (mit <i>Hofmann</i>) Art. 6–8 (mit <i>Hofmann</i>) Art. 13 Rn. 66–74 (mit <i>Hofmann</i>)
<i>Dr. Jonas Jossen, Mag. rer. publ.</i> Bundesamt für Sicherheit in der Informations- technik (BSI)	Art. 3 Nr. 26, 28 Art. 35–38, 51
<i>Jan Philip Kühne</i> Universität Passau	Art. 3 Nr. 18 Art. 59–71
<i>Julien Mehnert</i> Staatsanwalt	Art. 3 Nr. 12, 13, 15, 16, 20, 21, 40–46, 51 Art. 13 Rn. 1–65 Art. 14–19, 23 Anhang II, VI
<i>Dr. Christian Piovano</i> Syndikusrechtsanwalt, Friedrichshafen	Art. 31 Anhang VII
<i>Manuel Poncza</i> Rechtsanwalt, Köln	Art. 3 Nr. 17, 22, 30 Art. 20–22
<i>Stephan Schmidt</i> Rechtsanwalt, Fachanwalt für IT-Recht, Mainz	Art. 3 Nr. 4, 14, 36, 48 Art. 24–27
<i>Dr. Kristina Schreiber</i> Rechtsanwältin, Fachanwältin für Verwaltungs- recht, Köln	Art. 3 Nr. 33, 37, 38, 49, 50 Art. 52–58
<i>Prof. Dr. Meinhard Schröder</i> Universität Passau	Art. 1 (mit <i>Hartl</i>)
<i>Dr. Paul Vogel, LL.M. Eur.</i> Rechtsanwalt, München	Art. 3 Nr. 29 Art. 39–46
<i>Dr. Gerhard Wiebe</i> Rechtsanwalt, Berlin	Art. 3 Nr. 31 Art. 28–30

Verordnung (EU) 2024/2847 des Europäischen Parlaments und des Rates vom 23. Oktober 2024 über horizontale Cybersicherheitsanforderungen für Produkte mit digitalen Elementen und zur Änderung der Verordnungen (EU) Nr. 168/2013 und (EU) 2019/1020 und der Richtlinie (EU) 2020/1828 (Cyberresilienz-Verordnung)

(Text von Bedeutung für den EWR)

(ABl. L, 2024/2847, 20.11.2024, ELI: <http://data.europa.eu/eli/reg/2024/2847/oj>);

ABl. L, 2025/90555, 2.7.2025; ABl. L, 2025/90828, 17.10.2025

(Celex-Nr. 32024R2847)

zuletzt geändert durch Art. 104 VO (EU) 2025/327 vom 11. Februar 2025

(ABl. L, 2025/327, 5.3.2025, ELI: <http://data.europa.eu/eli/reg/2025/327/oj>)

Kapitel I Allgemeine Bestimmungen

Artikel 1 Gegenstand

Mit dieser Verordnung wird Folgendes festgelegt:

- a) **Vorschriften für die Bereitstellung auf dem Markt von Produkten mit digitalen Elementen, um die Cybersicherheit solcher Produkte zu gewährleisten;**
- b) **grundlegende Cybersicherheitsanforderungen an die Konzeption, Entwicklung und Herstellung von Produkten mit digitalen Elementen sowie Pflichten der Wirtschaftsakteure in Bezug auf diese Produkte hinsichtlich der Cybersicherheit;**
- c) **grundlegende Cybersicherheitsanforderungen an die von den Herstellern festgelegten Verfahren zur Behandlung von Schwachstellen, um die Cybersicherheit von Produkten mit digitalen Elementen während der erwarteten Nutzungsdauer der Produkte zu gewährleisten, sowie Pflichten der Wirtschaftsakteure in Bezug auf diese Verfahren;**
- d) **Vorschriften für die Marktüberwachung, einschließlich Überwachung, und die Durchsetzung der in diesem Artikel genannten Vorschriften und Anforderungen.**

Literatur: Biendl, Cybersicherheitsanforderungen nach dem Cyber Resilience Act der Europäischen Union, DB 2024, 1867; Biendl/Füllsack, Der finale Cyber Resilience Act im Überblick – Anwendungsbereich, Pflichten und Sanktionen, CR 2024, 376; Bressner/Gaden/Riediger, Der Cyber Resilience Act, DuD 2023, 327 ff.; Czychowski/Kroker, Handlungsempfehlungen für den Einsatz von Open Source Software zur Compliance mit dem CRA – Wie der Handlungsbedarf nach CRA optimal genutzt werden kann, CR 2025, 148; Dittrich/Heinelt, Compliance-Pflichten für Hersteller nach dem Cyber Resilience Act, RD 2023, 309; Erdelt, Meldepflichten des Cyber Resilience Acts, ZfPC 2024, 176; Heckmann/Ziegler, Der Cyber Resilience Act: Ein Gesetz „mit digitalen Elementen“, ITRB 2024, 159; Hessel/Callewaert, Der Cyber Resilience Act der EU-Kommission, K&R 2022, 789; Heynike/Taraz, Der Cyber Resilience Act, CCZ 2025, 92; Kreißl, Der Cyber Resilience Act: Neue Cybersicherheitsanforderungen für Produkte mit digitalen Elementen, ZfPC 2025, 223; Paschke/Fellenberg, Einblick in die Regelungsinhalte des Cyber Resilience Act, EuDIR 2025, 198; Piltz/Weiß/Zwerschke, Der Vorschlag für einen Cyber Resilience Act aus Sicht der DS-GVO, CR 2023, 154 und 289; Rennert, Mehr Cybersicherheit für vernetzte Produkte: Der Vorschlag der EU-Kommission für einen „Cyber Resilience Act“. Eine Analyse vor dem Hintergrund jüngster Bedrohungen für die Cybersicherheit, ZfDR 2023, 206; Ruttloff/Wagner/Stilz, Der Entwurf des Cyber Resilience Act (CRA) und seine Auswirkungen auf das Gewährleistungs- und Produkthaftungsrecht, BB 2024, 1603; Scheibenflug/Monschke/Hildebrandt, Cloud-Dienste im Regelungsgeflecht von CRA und NIS2-Richtlinie – Warum Cloud-Dienste den Compliance-Anforderungen von CRA und NIS2-Richtlinie unterfallen, CR 2024, 712; Schöttle, Der Cyber Resilience Act: Hintergrund, Produktkategorien und Sicherheitsanforderungen. Einführung und Anwendungsbereiche der grundlegenden Pflichten, MMR 2024, 741; Schöttle, Der Cyber Resilience Act: Zeitliche Aspekte, Meldepflichten, Akteure und Sanktionen. Definition und die Aufgabe von Open Source Software-Stewards, MMR 2024, 834; Schweinoch/

Meßmer, Vorschlag der EU-Kommission für einen „Cyber Resilience Act“, CR 2022, R112; Siglmüller, Cyber Resilience Act und Digital Operational Resilience Act – Lässt sich IT-Sicherheit rechtlich erzwingen?, ZfPC 2023, 221; Teichmann, Cyber Resilience Act – Produktsicherheit, SBOM und Herstellerhaftung entlang des Lebenszyklus, CCZ 2025, 165; Teichmann, Cybersicherheit als Produkteigenschaft – der Cyber Resilience Act der EU, NJW 2025, 2577; Teichmann, Der Cyber Resilience Act der EU, NVwZ 2025, 1662; Voigt/Falk, Der Cyber Resilience Act, MMR 2023, 88; Wiebe, Cybersicherheitsrecht 2.0 – Vorschlag eines Cyber Resilience Act, ZRP 2023, 73; Wiebe, Das neue Recht der Cyberresilienz, 2025; Wiebe/Daelen, Der Cyber Resilience Act aus produktsicherheitsrechtlicher Perspektive, EuZW 2023, 257; Wiebe/Daelen/Kerger, Der neue Cyber Resilience Act, K&R 2025, 79; Ziegler, Digitale Produktsicherheit: Der Vorschlag des Cyber Resilience Acts der EU-Kommission, jurisPRITR 2/2023; Zirnstein, Better cybersecurity due to increased regulation? The final European Cyber Resilience Act – The first comprehensive, horizontally applicable approach for more cybersecurity in digital products, CRi 2024, 65; Zirnstein, Der Entwurf des Cyber Resilience Act, CR 2022, 707.

Erwägungsgründe: 1–11

A. Allgemeines	1	II. Cybersicherheitsanforderungen bei Konzeption, Entwicklung und Herstellung (lit. b)	16
I. Entstehungsgeschichte	1	III. Schwachstellenbehebung während der erwarteten Nutzungsdauer (lit. c)	23
II. Sinn und Zweck	3	IV. Marktüberwachung und Durchsetzung (lit. d)	27
III. Systematische Einordnung	6	C. Bewertung und Ausblick	30
B. Kommentierung	12		
I. Regelungen zur Bereitstellung von Produkten mit digitalen Elementen auf dem Markt (lit. a)	12		

A. Allgemeines

I. Entstehungsgeschichte

- Art. 1 hat im Vergleich zum **Entwurf der Kommission**¹ im Laufe des Gesetzgebungsverfahrens nur geringfügige Änderungen erfahren. In lit. c wurde die ursprünglich vorgeschlagene Formulierung „um die Cybersicherheit von Produkten mit digitalen Elementen während ihres gesamten Lebenszyklus zu gewährleisten“ durch die schwächere Formulierung „um die Cybersicherheit von Produkten mit digitalen Elementen während der erwarteten Nutzungsdauer der Produkte zu gewährleisten“ ersetzt (→ Rn. 23 ff.). Weiter wurde in lit. d nach dem Begriff der Marktüberwachung – sprachlich in der deutschen Fassung wenig verständlich (→ Rn. 27) – der Zusatz „einschließlich Überwachung“ ergänzt und – rein redaktionell – die ursprüngliche Formulierung „der oben genannten Vorschriften und Anforderungen“ durch die Formulierung „der in diesem Artikel genannten Vorschriften und Anforderungen“ ersetzt.
- In der **Cybersicherheitsstrategie** der Kommission 2020 war erstmals in Erwägung gezogen worden, „neue horizontale Vorschriften zur Verbesserung der Cybersicherheit aller vernetzten Produkte und zugehörigen Dienste im Binnenmarkt“ zu erlassen.² Bis dahin hatte die Union zwar Cybersicherheit zunehmend als horizontales Thema verstanden, verbindliche Cybersicherheitsvorgaben aber vor allem für bestimmte Sektoren erlassen (insbesondere die NIS-Richtlinien). Mit dem CRA werden nun – gestützt auf die Binnenmarktkompetenz des Art. 114 AEUV – nahezu alle „Produkte mit digitalen Elementen“ (→ Art. 3 Rn. 2 ff.), die nicht besonderen Anforderungen in anderen Rechtsakten unterliegen oder außerhalb der Kompetenzen des Unionsgesetzgebers liegen, mit Cybersicherheitsanforderungen belegt.

II. Sinn und Zweck

- Art. 1 beschreibt den Gegenstand des CRA in vier Blöcken (zu den Details → Rn. 12 ff.). Die Bestimmung mag punktuell zur teleologischen Auslegung anderer Vorschriften herangezogen

¹ COM(2022) 454 final.

² „Die Cybersicherheitsstrategie der EU für die digitale Dekade“, JOIN(2020) 18 final.

werden können; ihre eigentliche Bedeutung liegt darin, dem Rechtsanwender einen (sehr groben) **Überblick über die Inhalte** des CRA zu geben. Soweit also ein bestimmtes Thema in den Art. 2 ff. CRA geregelt ist und nach den üblichen Regeln der Normauslegung ein bestimmtes Ergebnis tragfähig ist, dürfte Art. 1 CRA dem im Einzelfall nicht entgegenstehen. Es wäre unlogisch anzunehmen, der Gesetzgeber hätte mit einer notwendig schlank formulierten Übersicht die Anwendung der eigentlich inhaltlichen Regelungen begrenzen wollen. Der argumentative Wert von Art. 1 CRA ist demnach stark eingeschränkt. Ein ähnliches Vorgehen hat der Gesetzgeber auch in anderen Digitalrechtsakten gewählt, zB in Art. 1 DA, der ebenfalls weitgehend eine Inhaltsübersicht enthält.³

Warum der CRA diese Inhalte aufweist, beschreibt der Unionsgesetzgeber in den ersten Erwägungsgründen: „Cybersicherheit bedeutet eine der größten Herausforderungen für die Union. Die Zahl und Vielfalt der vernetzten Geräte wird in den kommenden Jahren exponentiell zunehmen. Cyberangriffe sind ein Thema von öffentlichem Interesse, da sie sich nicht nur auf die Wirtschaft der Union, sondern auch auf die Demokratie sowie die Sicherheit und Gesundheit der Verbraucher kritisch auswirken.“⁴ Dieser Herausforderung stellt sich die Union durch **horizontale Cybersicherheitsvorgaben für Produkte mit digitalen Elementen** für den gesamten Binnenmarkt.⁵ Sie möchte damit zwei Probleme angehen, „die hohe Kosten für die Nutzer und die Gesellschaft verursachen: ein geringes Maß an Cybersicherheit von Produkten mit digitalen Elementen, das sich in weitverbreiteten Schwachstellen und der unzureichenden und inkohärenten Bereitstellung von Sicherheitsaktualisierungen zu deren Behebung zeigt, sowie ein unzureichendes Verständnis und ein mangelnder Informationszugang der Nutzer, wodurch sie daran gehindert werden, Produkte mit angemessenen Cybersicherheitsmerkmalen auszuwählen oder sicher zu verwenden.“⁶

Keine Erwähnung findet in Art. 1 der dem Rechtsakt seine (Kurz-)Bezeichnung gebende Begriff der **Cyberresilienz**. Auch sonst wird er, sieht man von Art. 33 Abs. 2 ab, wo „Reallabore für Cyberresilienz“ geregelt werden, im operativen Teil des CRA nicht verwendet. Lediglich in den Erwägungsgründen ist gelegentlich von (Cyber-)Resilienz die Rede. Der Begriff der Resilienz stammt ursprünglich aus der Werkstoffkunde, fand dann Eingang in die Psychologie und schließlich ins Recht.⁷ Versucht man ausgehend von dem originären Begriffsverständnis einen Unterschied zwischen IT- bzw. Cybersicherheit und Cyberresilienz zu definieren, fällt ins Auge, dass es bei der Resilienz im Unterschied zur Sicherheit nicht um die Abwehr von Gefahren geht, also darum, dass das Schutzgut unversehrt bleibt, sondern um dessen Fähigkeit, trotz etwaiger Störungen wieder in den Ursprungszustand zurückzukehren, zumindest aber seine Funktionsfähigkeit zu behalten. Diese besondere Akzentsetzung kommt im CRA allenfalls punktuell zum Ausdruck: Im Rahmen von „security by design“ müssen mögliche Sicherheitsvorfälle mitbedacht werden, Pflichten zur Aufrechterhaltung der Cybersicherheit sollen über den gesamten Lebenszyklus eines Produkts dessen Brauchbarkeit sicherstellen, und eine Vielzahl von Akteuren wird, teilweise subsidiär, adressiert. Das ist allerdings auch im Bereich der klassischen IT-Sicherheit nichts völlig Neues (wenngleich es nun erstmals gesetzlich angeordnet wird). Anders als im Digital Operations Resilience Act (DORA),⁸ wo die „operationale Resilienz“, also die Aufrechterhaltung der Funktion im Vordergrund steht, wird der Begriff der Resilienz im CRA also weitgehend von seinen Wurzeln gelöst. Die Verwendung eines neuen Begriffs soll wohl vor allem zum Ausdruck bringen, dass mit den weitreichenden Vorgaben des CRA ein **neues Level an IT-Sicherheit** in der Union erreicht werden soll.

³ Vgl. BeckOK DatenschutzR/Veil, Stand 1.2.2025, DA Art. 1 Rn. 1.

⁴ Erwägungsgrund 1.

⁵ Erwägungsgründe 1, 2, 8.

⁶ Erwägungsgrund 1.

⁷ Vgl. zum Begriff etwa Alexander Nat. Hazards Earth Syst. Sci., 13 (2013), 2707 ff.; siehe auch die Beiträge in Karidi/Schneider/Gutwald (Hrsg.), Resilienz, 2018.

⁸ Verordnung (EU) 2022/2554 vom 14.12.2022, ABl. L 333, 1.

III. Systematische Einordnung

- 6 Beim CRA handelt es sich im Kern um **Produktrecht**, hier bezogen auf Produkte mit digitalen Elementen. Für diesen Bereich gilt seit 2008 der sogenannte „Neue Rechtsrahmen“ (New Legislative Framework, NLF), ein Maßnahmenpaket, das aus verschiedenen Rechtsakten besteht. Zu nennen sind insofern zunächst die Verordnung (EG) Nr. 765/2008 mit Vorschriften über die Akkreditierung sowie der Beschluss Nr. 768/2008, der ua ein Muster für künftige Rechtsvorschriften zur Produktharmonisierung enthält. Zahlreiche Vorschriften des CRA orientieren sich an diesem Muster. Die ursprünglich auch in der Verordnung (EG) Nr. 765/2008 geregelte Marktüberwachung wurde zwischenzeitlich in der Verordnung (EU) 2019/1020 (Marktüberwachungsverordnung, MÜVO) separat geregelt; diese Verordnung gilt auch im Anwendungsbereich des CRA, wird allerdings durch diesen nach dem *lex specialis*-Grundsatz ergänzt und punktuell modifiziert. Zu den Details → Art. 52 Rn. 16 ff.
- 7 Der horizontale Ansatz des CRA wird in Art. 2 mithilfe von **Bereichsausnahmen** durchbrochen. Diese Bereichsausnahmen bestehen (bzw. können durch die Kommission im Wege der delegierten Rechtssetzung geschaffen werden, Art. 2 Abs. 5) einerseits, wo in spezielleren Vorschriften des Unionsrechts bereits Cybersicherheitsanforderungen vorgesehen sind (→ Art. 2 Rn. 29 ff.). Damit werden insbesondere im Medizin- und Verkehrsbereich Doppelanforderungen vermieden. Andererseits beachtet der Unionsgesetzgeber in Art. 2 Abs. 7 seine Kompetenzgrenzen: Der CRA gilt nicht für Produkte mit digitalen Elementen, die ausschließlich für Zwecke der nationalen Sicherheit oder für Verteidigungszwecke entwickelt oder geändert wurden, und auch nicht für Produkte, die speziell für die Verarbeitung von Verschlusssachen konzipiert sind. Diese Bereiche erweisen sich auch im Fall von Querschnittsthemen wie der IT-Sicherheit als weitgehend immun gegen einen europarechtlichen Zugriff.
- 8 Das Verhältnis des CRA zum allgemeinen Produktsicherheitsrecht wird in Art. 11 geregelt, der differenziert die Anwendbarkeit der **Allgemeinen Produktsicherheitsverordnung** (General Product Safety Regulation, GPSR⁹) regelt. Für Cybersecurity-Risiken gilt demnach vorrangig der CRA, für Nicht-Cybersecurity-Risiken gelten die (allgemeinen oder besonderen) Produktsicherheitsvorschriften neben dem CRA (vgl. Erwägungsgrund 50).
- 9 Das Verhältnis zur **KI-Verordnung**¹⁰ wird in Art. 12 und Erwägungsgrund 51 beschrieben. Im Grundsatz stehen die Anforderungen beider Rechtsakte nebeneinander. Hinzuweisen ist aber darauf, dass eine Konformitätsbewertung nach dem CRA auch für die Beurteilung der Konformität gem. Art. 15 KI-VO nutzbar gemacht werden kann, sodass eine „Doppelbewertung“ vermieden wird.
- 10 Das Verhältnis zur **NIS-2-Richtlinie**¹¹ wird in Erwägungsgrund 52 beschrieben. Grundsätzlich stehen die Vorgaben nebeneinander, was angesichts der unterschiedlichen Anknüpfungspunkte (einerseits Hersteller von Produkten und nachgelagerte Wirtschaftsakteure, andererseits Betreiber von kritischen Infrastrukturen) auch konsequent ist. Nicht übersehen werden darf aber, dass der CRA zahlreiche Bezugnahmen, auch in institutioneller Hinsicht (CSIRT usw.), auf die NIS-2-Richtlinie und die durch diese sowie durch den **Cybersecurity Act**¹² geschaffenen (Behörden-)Strukturen enthält.
- 11 Das Verhältnis zur **Maschinenverordnung**¹³ wird ausschließlich in Erwägungsgrund 53 beschrieben. Auch hier gilt im Grundsatz (und angesichts der Nicht-Regelung im operativen Teil beider Rechtsakte naheliegend), dass die Anforderungen nebeneinanderstehen. Anders als im Fall der

9 Verordnung (EU) 2023/988 des Europäischen Parlaments und des Rates vom 10.5.2023, ABl. L 135, 1.

10 Verordnung (EU) 2024/1689 des Europäischen Parlaments und des Rates vom 13.6.2024, ABl. L, 2024/1689 vom 12.7.2024.

11 Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates vom 14.12.2022, ABl. L 333, 80.

12 Verordnung (EU) 2019/881 des Europäischen Parlaments und des Rates vom 17.4.2019, ABl. L 151, 15.

13 Verordnung (EU) 2023/1230 des Europäischen Parlaments und des Rates vom 14.6.2023, ABl. L 165, 1.

KI-Verordnung ist die „Doppelverwendung“ einer Konformitätsbewertung nicht ausdrücklich vorgesehen; der Gesetzgeber weist aber darauf hin, dass insbesondere über die Anwendung harmonisierter Normen Synergieeffekte erzielt werden können.

B. Kommentierung

I. Regelungen zur Bereitstellung von Produkten mit digitalen Elementen auf dem Markt (lit. a)

Der CRA knüpft an die Bereitstellung von Produkten auf dem Markt an (Art. 2 Abs. 1 CRA, 12 dazu → Art. 2 Rn. 4, 7 und Art. 3 Nr. 22). Wesentliche Überlegung des Gesetzgebers war wohl, so durch den klaren Anknüpfungspunkt „Marktangebot“ die Geltung der materiellen Anforderungen sicherzustellen.¹⁴

Alternativ hätten etwa auch – im Rahmen einer völlig anderen Gesetzeskonzeption – reine Anforderungen an die Verwender von Produkten mit digitalen Elementen gestellt werden können. Einen solchen im Vollzug dysfunktionalen Weg geht etwa die DS-GVO, die in Art. 32 DS-GVO zwar risikobasiert Anforderungen an die **Sicherheit der Verarbeitung personenbezogener Daten** stellt, dabei aber nicht den Hersteller von Produkten in den Blick nimmt, auch wenn diese eindeutig auf die Verarbeitung personenbezogener Daten ausgelegt sind, sondern den Anwender. 13

Regelungen zur Bereitstellung von **Produkten mit digitalen Elementen** auf dem Markt befinden sich zentral in Kapitel II. Zum Anwendungsbereich des CRA hinsichtlich der auf dem Markt bereitgestellten Produkte mit digitalen Elementen → Art. 2 Rn. 7 ff., zur Bereitstellung auf dem Markt bzw. Inverkehrbringen (als erstmaliger Bereitstellung auf dem Markt) Art. 3 Nr. 21 und 22. 14

Der CRA ist – und dies ist dem Gesetzgeber wichtig – gerade kein zB auf Industrieanlagen bezogenes Recht mit Fokus auf Maschinen und Lieferkettensicherheit. Gerade Verbraucherprodukte (zB Spielzeug, Babyphones, Wearables) sollen sicher sein (Erwägungsgrund 10). Der **Verbraucherschutz** findet sich auch in der Einstufung als „wichtige Produkte mit digitalen Elementen“ wieder (dazu → Art. 2 Rn. 11). 15

II. Cybersicherheitsanforderungen bei Konzeption, Entwicklung und Herstellung (lit. b)

Cyberbedrohungen sind dynamisch, Cybersicherheit muss daher, um effektiv zu sein, „by design“ 16 gedacht werden. Eine nachträgliche „Härtung“ oder der Einsatz ergänzender Sicherheitsprodukte ist nicht immer tauglich. Der Gesetzgeber möchte – insbesondere vor dem Hintergrund umfassend vernetzter Systeme – Cybersicherheit daher von Grund auf berücksichtigt wissen (Erwägungsgrund 10).

Zentrale Norm ist Art. 13 Abs. 1 (→ Art. 13 Rn. 5), demnach müssen Hersteller gewährleisten, dass ein Produkt mit digitalen Elementen gemäß den grundlegenden **Cybersicherheitsanforderungen** in Anhang I Teil I konzipiert, entwickelt und hergestellt worden ist. 17

In der Sache geht es um ein durchgehend hohes Sicherheitsniveau durch sichere Konzeption, fortlaufende Risikobewertung (Art. 13 Abs. 3), Dokumentation und Reaktion auf (erkannte) Schwachstellen. Ein zentraler Faktor bei der Auswahl vernetzter Produkte wird perspektivisch wohl dem sog. **Unterstützungszeitraum** zukommen (→ Art. 13 Rn. 23). 18

Einen ähnlichen herstellerbezogenen „by design“-Ansatz sieht das **Datenrecht** in Art. 3 Datenverordnung (Data Act) vor. Demnach müssen vernetzte Produkte im Sinne der Datenverordnung (Art. 2 Nr. 5 Data Act) so konzipiert und hergestellt sein, dass die relevanten Daten für den Nutzer 19

¹⁴ Vgl. Erwägungsgrund 10.

zugänglich sind. Cybersicherheitsanforderungen ergeben sich auch insoweit aus der Natur der Sache, da der Prozess schon im Eigeninteresse des Herstellers sicher ausgestaltet sein sollte.

- 20 Die KI-VO enthält in Art. 15 Abs. 1 eine ähnliche Vorgabe speziell zu **Hochrisiko-KI-Systemen**. Diese „müssen so konzipiert und entwickelt [sein], dass sie ein angemessenes Maß an Genauigkeit, Robustheit und Cybersicherheit erreichen und in dieser Hinsicht während ihres gesamten Lebenszyklus beständig funktionieren“.
- 21 In der DS-GVO sieht Art. 25 Abs. 1 DS-GVO **Datenschutz durch Technikgestaltung** und damit konzeptionell auch Datensicherheit qua Produktkonzeption vor. Allerdings werden Hersteller in Art. 25 Abs. 1 DS-GVO nicht selbst verpflichtet. Eine rechtlich relevante „Vorfeldwirkung“ auf die Hersteller müsste bislang – über bloße Appelle wie Erwägungsgrund 78 der DS-GVO hinaus – etwa durch zivilrechtliche Mangelbegriffe erzielt werden.¹⁵
- 22 Der Anhang I des CRA sieht in Absatz 2 lit. d–f Anforderungen an den **technischen Datenschutz** vor und steht so in Wechselwirkung mit Art. 32 DS-GVO. Der Grundsatz der Datenminimierung findet sich ausdrücklich in Anhang I Teil I Abs. 2 lit. g CRA.

III. Schwachstellenbehebung während der erwarteten Nutzungsdauer (lit. c)

- 23 Laufende **Sicherheitsupdates** sind für vernetzte Systeme unabdingbar. Gerade im deutschen Kauf- und Werkrecht mit dem Gefahrübergang als zentralem Übergabepunkt der geschuldeten Leistung waren nachlaufende Updatepflichten aber ein Fremdkörper. Die Rechtslage hierzu ist – rein mit Blick auf das BGB – umstritten. Jedenfalls gegenüber Verbrauchern bestehen mit § 327f Abs. 1 S. 2 BGB für digitale Produkte inzwischen Aktualisierungspflichten.
- 24 Der CRA adressiert eine Pflicht zur **Schwachstellenbehebung** speziell in Art. 13, insbesondere Abs. 8, in Verbindung mit Anhang I (Teil 2) (weiterführend → Art. 13 Rn. 21 ff.). In der Sache geht es um sichere, wirksame und zeitnahe Behebung von Schwachstellen nach einem definierten Prozess.
- 25 Art. 14 CRA sieht umfassende (behördliche) **Meldepflichten** (→ Art. 14 Rn. 1 ff.) und Informationen an betroffene Nutzer (→ Art. 14 Rn. 18), vor. Ausgangspunkt sind sog. „aktiv ausgenutzte Schwachstellen“ (→ Art. 14 Rn. 3 und Art. 3 Nr. 42) oder „schwerwiegende Sicherheitsvorfälle“ (→ Art. 14 Rn. 7 ff.).
- 26 Melde- und Informationspflichten können parallel nach der DS-GVO bei einer **Verletzung des Schutzes personenbezogener Daten** bestehen (Art. 4 Nr. 12 und Art. 35, 36 DS-GVO). Gerade bei einer Verletzung des Schutzes personenbezogener Daten und folgenden datenschutzrechtlichen Rechtsstreitigkeiten dürften Pflichten unter dem CRA zur technischen Sicherheit relevant werden. Der EuGH sieht die **Beweislast** für technische Sicherheit der Verarbeitung personenbezogener Daten beim Verantwortlichen im Sinne der DS-GVO.¹⁶

IV. Marktüberwachung und Durchsetzung (lit. d)

- 27 Der CRA enthält weiterhin Regelungen zur „**Marktüberwachung, einschließlich Überwachung**“. Die Formulierung der deutschen Fassung ist so kaum verständlich; in der englischen Fassung ist – etwas klarer – die Rede von „rules on market surveillance, including monitoring“. Da gleichwohl surveillance eine intensivere und finalere Form des monitoring ist, erscheint der Zusatz wenig hilfreich.
- 28 Der CRA enthält schließlich Vorschriften zur Durchsetzung, insbesondere zum Bußgeldrahmen (→ Art. 64 Rn. 31). Hier stand augenscheinlich, wie bei vielen neueren (Digital-)Rechtsakten,

¹⁵ Zu alledem auch weiterführend Kühling/Buchner/Hartung DS-GVO Art. 25 Rn. 13.

¹⁶ EuGH (Dritte Kammer) Urt. v. 25.1.2024 – C-687/21, NZA 2024, 320 (322).

die DS-GVO Pate. Ob die Zurückhaltung deutscher Aufsichtsbehörden bei Bußgeldern auch im Kontext des CRA fortgesetzt wird, bleibt abzuwarten.

Art. 65 CRA sieht die Möglichkeit von **Verbandsklagen** vor (→ Art. 65 Rn. 11).

29

C. Bewertung und Ausblick

Die frühere Strategie, Cybersicherheit (außer in kritischen Bereichen) als Teil der Produktqualität zu verstehen, die „der Markt“ regelt, wird mit dem CRA zu Recht verabschiedet. Cybersicherheitslücken wirken über vertragliche Beziehungen hinaus, wenn etwa vernetzte Geräte zum Teil von Botnetzen werden. Cybersicherheit ist insofern eine **Frage des öffentlichen Interesses**, dessen sich der Gesetzgeber annehmen muss. 30

Ein weiterer positiver Effekt der Regulierung ist, dass die Frage, welche Cybersicherheitsstandards adäquat sind, nun nicht mehr fallweise von Gerichten beantwortet werden, sondern – zumindest im Ansatz – durch den Gesetzgeber. Das verbessert die **demokratische Legitimation** des Cybersicherheitsrechts. 31

Mit dem CRA ist das (Gesetzgebungs-)Programm der **Cybersicherheitsstrategie 2020** weitgehend abgeschlossen. Die wesentliche Aufgabe für die Kommission wird in der nächsten Zeit darin liegen, die im CRA enthaltenen Aufträge zur delegierten und Durchführungs-Rechtsetzung zu erfüllen und die Wirksamkeit des CRA zu evaluieren. 32

Artikel 2 Anwendungsbereich

(1) Diese Verordnung gilt für auf dem Markt bereitgestellte Produkte mit digitalen Elementen, deren bestimmungsgemäßer Zweck oder vernünftigerweise vorhersehbare Verwendung eine direkte oder indirekte logische oder physische Datenverbindung mit einem Gerät oder Netz einschließt.

(2) Diese Verordnung gilt nicht für Produkte mit digitalen Elementen, auf die folgende Rechtsakte der Union Anwendung finden:

- a) Verordnung (EU) 2017/745,
- b) Verordnung (EU) 2017/746,
- c) Verordnung (EU) 2019/2144.

(3) Diese Verordnung gilt nicht für Produkte mit digitalen Elementen, die nach der Verordnung (EU) 2018/1139 zertifiziert worden sind.

(4) Diese Verordnung gilt nicht für Geräte, die in den Anwendungsbereich der Richtlinie 2014/90/EU des Europäischen Parlaments und des Rates¹ fallen.

(5) (1) Die Anwendung dieser Verordnung auf Produkte mit digitalen Elementen, die unter andere Rechtsvorschriften der Union mit Anforderungen für alle oder einige der von den grundlegenden Cybersicherheitsanforderungen in Anhang I abgedeckten Risiken fallen, kann eingeschränkt oder ausgeschlossen werden, wenn

- a) eine solche Einschränkung oder ein solcher Ausschluss mit dem für diese Produkte geltenden allgemeinen Rechtsrahmen vereinbar ist und
- b) mit den sektorspezifischen Vorschriften dasselbe Schutzniveau erreicht wird, wie es diese Verordnung gewährleistet, oder ein höheres.

1 **Amtl. Anm.:** Richtlinie 2014/90/EU des Europäischen Parlaments und des Rates vom 23. Juli 2014 über Schiffsausrüstung und zur Aufhebung der Richtlinie 96/98/EG des Rates (ABl. L 257 vom 28.8.2014, S. 146).

(2) Der Kommission wird die Befugnis übertragen, gemäß Artikel 61 zur Ergänzung dieser Verordnung delegierte Rechtsakte zu erlassen, in denen sie die Notwendigkeit einer solchen Einschränkung oder eines solchen Ausschlusses feststellt und gegebenenfalls die betreffenden Produkte und Vorschriften sowie den Umfang der Einschränkung festlegt.

(6) Diese Verordnung gilt nicht für Ersatzteile, die auf dem Markt bereitgestellt werden, um identische Komponenten in Produkten mit digitalen Elementen zu ersetzen, und die nach denselben Spezifikationen hergestellt werden wie die Bauteile, die sie ersetzen sollen.

(7) Diese Verordnung gilt nicht für Produkte mit digitalen Elementen, die ausschließlich für Zwecke der nationalen Sicherheit oder für Verteidigungszwecke entwickelt oder geändert wurden, und auch nicht für Produkte, die speziell für die Verarbeitung von Verschlusssachen konzipiert sind.

(8) Die in dieser Verordnung festgelegten Verpflichtungen umfassen nicht die Bereitstellung von Informationen, deren Offenlegung wesentlichen Interessen der Mitgliedstaaten im Bereich der nationalen Sicherheit, der öffentlichen Sicherheit oder der Verteidigung zuwiderlaufen würde.

Literatur: Arzt/Fischer/Kreutzer/Scheel/Schneider/Schreiber/Selzer, Der EU Cyber Resilience Act: Ein Überblick aus rechtlicher Sicht, Version 1.0, 2024; Becker, Stellungnahme für den BT-Innenausschuss, 22.10.2012, Ausschussdrucksache 17(4)585 B; BSI, Lage der IT-Sicherheit in Deutschland 2024, 2024; KOM, Commission Staff Working Document, Impact Assessment Report [zum Vorschlag für die CRA], SWD(2022) 282 final, Brüssel 2022 (zitiert: Impact Assessment); Medical Device Coordination Group, MDCG 2019-16 Rev. 1, Guidance on Cybersecurity for medical devices, Juli 2020; Schantz/Wolff, Neues DatenschutzR, 2017; Schöttle, Der Cyber Resilience Act: Hintergrund, Produktkategorien und Sicherheitsanforderungen Einführung und Anwendungsbereiche der grundlegenden Pflichten, MMR 2024, 741.

Erwägungsgründe: 9, 11, 12, 15, 16, 17, 20, 18, 24, 25, 26, 27, 28, 29, 30, 33, 53

A. Allgemeines	1	2. Medizinprodukte und In-vitro-Diagnostika	31
I. Entstehungsgeschichte	1	3. Kraftfahrzeuge	35
II. Sinn und Zweck	3	III. Ausnahme für zertifizierte Luftfahrzeuge (Abs. 3)	40
III. Systematische Einordnung	6	IV. Ausnahme für Schiffsausrüstungen (Abs. 4)	46
B. Kommentierung	7	V. Ausnahmemöglichkeiten (Abs. 5)	48
I. Originärer Anwendungsbereich (Abs. 1) ..	7	VI. Ausnahme für Ersatzteile (Abs. 6)	54
1. Relevante Begriffe	7	VII. Ausnahmen für die nationale Sicherheit (Abs. 7)	60
2. Direkte Verbindung mit einem Netz oder Gerät	10	VIII. Ausnahmen für nationale Sicherheitsinteressen (Abs. 8)	67
3. Verbindung mit einem Netz oder Gerät	11	IX. Im Übrigen: Parallele Anwendung des CRA	73
4. Einzelfragen	18	C. Kritik und Ausblick	75
a) Freie und quelloffene Software	18		
b) Cloud-Computing-Dienste (SaaS, PaaS, IaaS)	25		
c) Legacy Software	27		
II. Ausnahmen für Bereiche mit eigenen Cybersicherheitsanforderungen (Abs. 2) ..	29		
1. Grundlegendes	29		

A. Allgemeines

I. Entstehungsgeschichte

- Der Kern der Regelung zum Anwendungsbereich war bereits im Entwurf der KOM enthalten. Insbesondere das Prinzip der **horizontalen Produktregulierung** blieb im Gesetzgebungsverfahren gleich. Der grundsätzliche Mechanismus (verbindungsfähige PdE) wurde um das Merkmal der Bereitstellung am Markt ergänzt. Diese Klarstellung ist sinnvoll, um die Produkte, die regulär unter den CRA fallen (zB FOSS-Geschäftsmodelle), von jenen zu unterscheiden, für die nur die Pflichten der Verwalter quelloffener Software gelten (Art. 24 CRA, FOSS-Projekte, → Rn. 20).

Im Übrigen wurden im Gesetzgebungsverfahren nur Ausnahmen ergänzt:

2

- Für Schiffsausrüstung (Abs. 4)
- Für Ersatzteile (Abs. 6)
- Für Sicherheitsinteressen (Abs. 8)

II. Sinn und Zweck

Die Norm regelt den Anwendungsbereich des CRA; nur in Bezug auf Produkte, die innerhalb 3 dieses Bereichs liegen, entfalten die Pflichten der CRA ihre Wirkung.

Als horizontale Produktregulierung geht der Gesetzgeber dabei in zwei Schritten vor: Erst öffnet 4 er den Anwendungsbereich maximal, also auf sämtliche PdE zur Verbindung mit einem Netz oder Gerät (→ Rn. 7 ff.). Im zweiten Schritt schränkt er die Anwendbarkeit dann sektorenweise und in Bezug auf einzelne Komponenten wieder ein (→ Rn. 29 ff.). Durch diesen **Opt-out-Ansatz** werden die wichtigsten Abgrenzungsfragen geklärt, ohne dass gleichzeitig Lücken im System der produktbezogenen Cybersicherheitsregulierung entstünden.

Wo keine Ausnahmen greifen, ist der CRA parallel zu der fraglichen Norm anzuwenden, selbst 5 wenn sich dabei thematische Überschneidungen ergeben. Einige dieser Fälle hat der Gesetzgeber in den Erwägungsgründen klargestellt (→ Rn. 73 ff.).

III. Systematische Einordnung

Der Anwendungsbereich gehört zu den allgemeinen Bestimmungen und ist darum für sämtliche 6 Kapitel der CRA von Bedeutung. Für Aspekte, die außerhalb des Anwendungsbereichs in Art. 2 CRA liegen, sind die Vorgaben des CRA schon grundsätzlich nicht von Belang.

B. Kommentierung

I. Originärer Anwendungsbereich (Abs. 1)

1. Relevante Begriffe. Art. 2 Abs. 1 CRA spannt den originären Anwendungsbereich der Norm 7 auf, von dem im weiteren Verlauf Ausnahmen gemacht werden. Die wesentlichen Begriffe für den Anwendungsbereich sind nahezu sämtlich in den Begriffsbestimmungen enthalten. In der Reihenfolge des Art. 2 Abs. 1 CRA:

- Bereitstellen auf dem Markt, Art. 3 Nr. 22
- Produkte mit digitalen Elementen, Art. 3 Nr. 1
- Zweckbestimmung, Art. 3 Nr. 23
- Vernünftigerweise vorhersehbare Verwendung, Art. 3 Nr. 24
- Indirekte Verbindung, Art. 3 Nr. 10
- Logische Verbindung, Art. 3 Nr. 8
- Physische Verbindung, Art. 3 Nr. 9

Für eine detaillierte Beschreibung der jeweils erfassten Produkte und Tätigkeiten sei auf die 8 Kommentierungen zu den einschlägigen Definitionen verwiesen. Folgende Grenzfälle und Klarstellungen sind besonders relevant:

- PdE meint schlicht **Hardware und/oder Software** von und für Computer – in allen Formen und Größen und unabhängig davon, ob sie für Unternehmer oder Verbraucher (Smart Home, Wearables) vorgesehen sind (PdE, Art. 3 Nr. 1).
- **Cloud-Dienste** sind nur insofern erfasst, als sie notwendig sind, eine Funktion des PdE zu unterstützen (Datenfernverarbeitung, Art. 3 Nr. 2).
- Das Lizenzmodell von Software spielt nur eine untergeordnete Rolle. **Freie und quelloffene Software** (→ Rn. 18) ist grundsätzlich ebenso erfasst wie proprietäre Software. Ob das Produkt entgeltlich oder unentgeltlich abgegeben wird, spielt keine Rolle. Ausnahmen gibt es nur, falls

die Abgabe nicht im Rahmen einer Geschäftstätigkeit erfolgt, wie dies bei der öffentlichen Verwaltung oder Non-Profit-Organisationen der Fall sein kann (Art. 3 Nr. 22).

- 9 Für die Kommentierung Art. 2 Abs. 1 CRA bleiben damit nur die Begriffe der direkten Verbindung sowie des Geräts oder Netzes.
- 10 **2. Direkte Verbindung mit einem Netz oder Gerät.** Der Begriff der direkten Verbindung erschließt sich ohne Weiteres aus der Definition der indirekten Verbindung. Dort geht es darum, dass ein PdE auch als Teil eines größeren Systems, das seinerseits mit einem Gerät oder Netz verbunden ist, in den Anwendungsbereich der CRA fällt. Direkt bedeutet also nur, dass dieser Zwischenschritt wegfällt. Es ist im Grunde eine Nicht-Voraussetzung und soll nur verdeutlichen, dass alle denkbaren Verbindungsarten für Art. 2 Abs. 1 CRA zählen.
- 11 **3. Verbindung mit einem Netz oder Gerät.** Der Begriff des Netzes oder Geräts wird im CRA nur über Umwege erläutert. Hauptanwendungsfall für ein Netz ist sicher das Internet. In den Erwägungsgründen zeigt sich das in ErwG 24, der „ein sicheres Internet“ als ein Ziel der NIS-2-RL angibt, wobei die CRA den verantwortlichen Betreibern helfe, wenn diese auf sichere Weise entwickelte PdE einsetzen könnten. Ansonsten spielt das Internet nur für die Einordnung von Produkten als wichtige PdE eine Rolle, weil sich Anhang III Klasse I Nr. 12 auf „Modems für die Internetverbindung“ bezieht und Nr. 18 auf „mit dem Internet verbundenes Spielzeug“.
- 12 Einen weiteren Hinweis auf die **Netze** liefert die Verweiskette aus der Definition der Cybersicherheit (Art. 3 Nr. 3). Sie verweist auf „Netz- und Informationssysteme“ (Art. 2 Nr. 2 CSA), die wiederum in Art. 6 Nr. 1 NIS-2-RL ua definiert werden als ein „elektronisches Kommunikationsnetz“ im Sinne von Art. 2 Nr. 1 RL (EU) 2018/1972. Es liegt darum nahe, den Begriff des Netzes wie in der EECC-Richtlinie (EU) 2018/1972 zu verstehen (Art. 3 Nr. 3, → Art. 3 Rn. 28 f.). Er umfasst sämtliche Übertragungssysteme, die der Signalübertragung dienen, unabhängig von der Art der übertragenen Information: Leitungsnetze, mobile Netze, Netze für Hör- und Fernsehfunk sowie Kabelfernnetze – selbst Stromnetze, soweit sie zur Signalübertragung genutzt werden.
- 13 Legt man das zugrunde, ist der **Netzbegriff der CRA** maximal weit zu verstehen. Er umfasst vor allem auch Netze, die – ua aus Sicherheitsgründen – ggf. nicht mit dem Internet verbunden sind. Dazu zählen zB Netze für industrielle Steuerungssysteme, Kraftwerke² oder die Leit- und Sicherungstechnik der Bahn.³ Selbst Rundfunknetze gehören dazu – wenn das betreffende PdE über eine Möglichkeit verfügt, zu senden.
- 14 Für eine **Einschränkung in Bezug auf rein empfangende Geräte bei Rundfunknetzen** spricht auch der Zweck des weiten Anwendungsbereichs, wie ihn ErwG 9 erläutert. Danach soll auch „als weniger kritisch geltende Hardware und Software“ erfasst sein, weil sie sonst „eine Kompromittierung eines Geräts oder Netzes erleichtern“. Zwar wurde der Vorschlag, den Anwendungsbereich der CRA auf bidirektionale Verbindungen zu beschränken,⁴ nicht aufgegriffen. Für die in ErwG 9 genannte Kompromittierung braucht es aber zumindest eine sendende Verbindung ins Netz, über die Geräte, die als bloße Empfänger fungieren, nicht verfügen.
- 15 Dieser Gedanke lässt sich am Beispiel der Funkrundsteuerung von **Straßenlaternen** oder Photovoltaikanlagen verdeutlichen, zu der auf dem 38C3-Kongress⁵ – durchaus umstrittene⁶ – Sicherheitslücken diskutiert wurden. Das System basiert auf Langwellen; in Deutschland steuern zwei

2 Arzt et al., Der EU Cyber Resilience Act: Ein Überblick aus rechtlicher Sicht, Version 1.0, März 2024, S. 8 f.

3 Davon gehen zB auch die Verbände der Bahnindustrie (UNIFE) und der Bahnbetreiber (CER) aus.

4 ZVEI, Position on the proposal for a Cyber Resilience Act, 2023, https://www.zvei.org/fileadmin/user_upload/Presse_und_Medien/Publikationen/2023/Februar/Cyber_Resilience_ACT/2023-02-09_ZVEI_Position_Paper_Cyber_Resilience_Act_CRA.pdf, S. 4.

5 Vortrag von Bräunlein und Melette auf dem 38C2 vom 28.12.2024, BlinkenCity: Radio-Controlling Street Lamps and Power Plants, <https://media.ccc.de/v/38c3-blinkencity-radio-controlling-street-lamps-and-power-plants>.

6 Spiegel vom 28.12.2024, Könnten Hacker Blackouts über Funk auslösen?; Golem.de vom 29.12.2024, <https://www.golem.de/news/rundsteuerempfaenger-gehackt-laesst-sich-ueber-funksignale-ein-blackout-herbeifuehren-2412-192013.html>.

Stichwortverzeichnis

Die **fetten** Zahlen verweisen auf den Paragraphen, die mageren auf die Randnummer.

Abbildung **Anh. VII 3**

Abgabe **3 127 ff.**, 142

– entgeltliche **3 136**

– entgeltliche oder unentgeltliche **22 8**

– im Zusammenhang mit einer Geschäftstätigkeit **3 143**

– ohne Gewinnerzielungsabsicht **3 148**

– unentgeltliche **3 136**, 143

– Vertrieb **3 137**

– zur Verwendung **3 137**

Abkommen über die gegenseitige Anerkennung **34 1 ff.**

Abschlussbericht

– aktiv ausgenutzte Schwachstelle **14 6**

– schwerwiegender Sicherheitsvorfall **14 12**

Administrative Cooperation Groups (ADCO)
13 70 ff., **52 14**, 32, 74 ff.

Adressangabe **13 46 ff.**

Adressat der Meldung **15 4**

Adressatenkreis **22 3 f.**

– Einführer **22 1**

– Händler **22 1**

– natürliche oder juristische Person **22 1**, 6 ff.

Akkreditierung **36 9 ff.**, **40 3 f.**, **42 5 f.**, **45 4**

– Akkreditierungsverfahren **36 16 ff.**

– Antrag **36 17 f.**

– Begutachtung **36 19 f.**

– Entscheidung **36 21**

– Überwachung **36 22**

Akkreditierungsstelle **36 8 ff.**, **42 5**

– DAkkS **36 12**

Akkreditierungsurkunde **42 5**, 7, **43 7**, 11

Akkreditierungsverfahren **42 8**

Aktiv ausgenutzte Schwachstelle **3 268 f.**

Aktualisierung **6 34 ff.**, **13 29 f.**

Alexa **7 46**

Allgemeine Informationen

– aktiv ausgenutzte Schwachstelle **14 5**

– schwerwiegender Sicherheitsvorfall **14 11**

Amtshilfe **52 34**

Änderung der Zweckbestimmung **21 18**

Änderung zu eigenen Zwecken **22 9**

Anerkennung, Abkommen über gegenseitige
34 1 ff.

Anfechtungsklage **58 14**

Anforderung

– Abschreckung **64 22 ff.**

– Bestimmtheit **64 55**

– Ne bis in idem **64 56 ff.**

– Verbot der Doppelbestrafung **64 56 ff.**

– Verhältnismäßigkeit **64 25 ff.**

– Wirksamkeit **64 21 ff.**

Anleitungen für den Nutzer **Anh. II 1 ff.**

Anonymität **6 53**

Anwendbarkeit

– Verbraucherschützende Vorschrift **65 36 ff.**

– Wirtschaftsakteur **65 29 ff.**

Anwendung, technische **47 4**, **49 20**

Anwendungsbereich **2 1 ff.**, **68 3**

– bidirektionale Verbindung **2 14 f.**

– Cloud-Computing **2 25 f.**

– Eisenbahn **2 13**

– FOSS (freie und quelloffene Software)
2 18 ff.

– industrielle Steuerungssysteme **2 13**

– kooperative intelligente Verkehrssysteme
2 17

– Legacy-Software **2 27 f.**

– Produkte mit digitalen Elementen **52 25**

– PV-Anlagen **2 15**

– Rundfunk **2 14 f.**

– Verbindung mit einem Gerät **2 17**

– Verbindung mit einem Netz **2 11 ff.**

Archiv **13 31**

ATEX-Richtlinie, Übergangszeitraum **69 13**

Aufbau/Stufe der Lieferkette **20 6**

Auffangfunktion **3 110**

Aufgaben des Bevollmächtigten **18 5 f.**

Aufschieben der Meldung **16 12**

Aufzüge **4 36**

Ausfallsicherheit **6 54 f.**

Auskunft

– Auskunftersuchen **49 14**

– falsche **64 47**

– irreführende **64 49**

– Sanktion **64 41 ff.**

– unvollständige **64 48**

Auslegung **21 10 ff.**

Ausnahme **24 14**

Ausnutzbare Schwachstelle **3 267**

Ausschussverfahren **62 3 ff.**

Außergewöhnliche Umstände **16 5 ff.**, **56 5**

Ausstellung **4 16 ff.**

Austausch von Informationen **24 39**

Auswirkungen, negative **49 12**

Authentifizierung **6 38 ff.**, **7 25**

Autorisierung **7 25**

B2B-Vertrieb **20 61 ff.**

B2C-Vertrieb **20 61**, 63 ff.

- Baumusterprüfbescheinigung 32 12
Bedienungsanleitung 13 52 ff.
Befugnis erteilende Behörde 36 23 ff.
Befugniserteilung 45 5
Begleitgesetz, nationales 52 77
Begründetes Verlangen 13 62, 20 48 ff.
Behandeln 13 22 ff.
Behandlung von Schwachstellen 13 17 f., 22 ff.
Behörde, Marktüberwachung 52 18
Behördenzuständigkeit 52 4
Beiladung 52 80
Beinahe-Vorfall 3 272
Beizufügende Informationen und Anleitungen
 Anh. II 2 ff.
Belastungen, unnötige 47 9 f.
Bemessungskriterium
 – Art des Verstoßes 64 64
 – Dauer des Verstoßes 64 66
 – fortdauernder Verstoß 64 67 ff.
 – Größe 64 71
 – Kleinstunternehmen, kleine und mittlere Unternehmen 64 71
 – Kooperation 64 74 f.
 – Leistungsfähigkeit 64 72
 – Schwere des Verstoßes 64 65
 – Wiederholungstat 64 67 ff.
Benachrichtigung der Nutzer 24 47
Benennung der Abnehmer und Lieferanten 23 1 f.
Benutzerverwaltung 7 25
Bereits in den Verkehr gebracht 21 14 ff.
Bereitstellung auf dem Markt 3 104, 108, 124 ff., 140, 20 1 ff., 38, 67 ff., 21 10
 – Abgabe 3 126, 135
 – off-premise 3 135
 – ohne Änderung der Eigenschaften 3 107
 – on-premise 3 135
Bereitstellung im Rahmen einer Geschäftstätigkeit 24 25
Berichtspflicht der ENISA 17 1 ff.
 – Bericht 17 6
Beschaffung 5 1 ff., 7
 – Autonomie 5 10 f.
 – Vergaberecht 5 21 ff.
Beschluss Nr. 768/2008/EG 3 192, 227, 22 4
Beschränkte Meldung 16 7 f.
Beschreibung **Anh. VII** 3
Beschwerde 48 2
Beschwerde- und Einspruchsverfahren 48 2
Beschwerdeverfahren 48 2
Besitzübertragung 3 123
Besonders außergewöhnliche Umstände 16 7 f.
Bestandsschutz 6 9, 69 1 ff., 20 ff.
 – Komponente 69 21
 – wesentliche Änderung 69 25 ff.
Bestimmung des Herstellers 3 83 ff.
Betriebsanleitung 13 52 ff.
Betriebseinstellung 13 64
Betriebsstätigkeit, Einstellung 20 55 ff.
Betroffeneninformation 14 18
Bevollmächtigte 3 91 ff., 13 3, 18 1, 22 7 f.
Beweislast 22 14
Beweismittel 31 5 ff.
Binnenmarkt 3 228
Blue Guide 41 5 ff., 69 29 f.
Browser 7 26
Bundesamt für Sicherheit in der Informationstechnik (BSI) 50 3
Bußgeld 64 1 ff.
 – Auskunft 64 41 ff., 47 ff.
 – Ausnahme 24 52
 – Behörde 64 81 ff.
 – Bußgeldrahmen 64 31 ff.
 – Kumulierbarkeit mit anderen Maßnahmen 64 87 ff.
 – öffentliche Stelle 64 81 ff.
 – Umsatz 64 35
Bußgeldrahmen
 – Kappungsgrenze 64 31
 – Unternehmensbegriff 64 34
CE-Kennzeichnung 3 227 ff., 13 34 ff., 20 17 ff., 24 50, 29 1 ff., 30 1 ff., 32 4 ff.
 – Adressaten 30 2
 – allgemeine Grundsätze 29 4 ff.
 – Anbringung 20 20 ff.
 – Anbringungsbefugnis 29 6 f.
 – Anbringungsort 30 9 ff.
 – Anbringungspflicht 30 7
 – Anbringungsverbot 29 10
 – Anbringungsvoraussetzung 30 15
 – Anbringungsweise 30 12 ff.
 – andere Kennzeichen 29 14 f., 30 17
 – Aufkleber 30 12
 – Ausnahmen 30 16
 – Ausstellungen 30 16
 – Beeinträchtungsverbot 29 16 f.
 – Beschluss Nr. 768/2008/EG 29 2
 – Conformité Européenne 3 227
 – Datenplatte 30 12
 – Dauerhaftigkeit 30 12
 – Deaktivierungsanordnung 30 4
 – Designbeeinträchtigungen 30 10
 – digitale Form 30 11
 – drittstaatliche Konformitätskennzeichen 29 18

- Eintrittskarte 3 228
- Exklusivität 29 13
- gesetzliche Selbstverständlichkeit 30 6
- grafische Abbildung 3 230
- Grundsatz der Singularität 30 23
- gut sichtbar 30 12 f.
- Harmonisierungsvorschriften 30 23 f.
- Herstellerselbsterklärung 3 228
- Herstellerverantwortung 29 11
- Konformitätsbewertungsverfahren 29 2
- Konformitätsvermutung 3 228
- Korrekturmaßnahmen 30 4
- leserlich 30 12 ff.
- Marktüberwachung 30 4
- Marktüberwachungsrecht 29 19
- Marktverhaltensregel 30 6
- Messen 30 16
- Mindesthöhe 30 14
- missbräuchliche Verwendung 30 4
- Nichtkonformität 3 229, 30 4, 58 10
- NLF-Konformitätstrias 3 227, 29 2
- Pflichten 3 230
- Pflichtenträger 30 7 f.
- Produktanforderung 3 229, 29 3
- Produkt- bzw. Produzentenhaftung 30 6
- produktunmittelbar 30 9
- Proportionen 29 9, 30 14
- Prototypen 30 16
- Prüfpflicht 30 8
- Rückruf 30 4
- Sachmangel 30 6
- Sanktionen 29 19, 30 5
- Schriftbild 29 8 f.
- Selbsterklärung 29 3
- Softwareprodukte 30 11
- unfertige Software 30 16
- Unmöglichkeit 30 9
- Unverhältnismäßigkeit 30 10
- Unzerstörbarkeit 30 12
- Verbraucher 30 11
- Verkehrsfähigkeitsvoraussetzung 3 229
- Verkehrsverbot 3 229, 30 4
- Vertriebsverbote 3 229
- Verwechslungsverbot 29 16
- VO (EG) Nr. 765/2008 29 2
- Wahrnehmbarkeit 30 13
- Warenpass 3 228, 29 3
- Warenverkehrsfreiheit 30 2
- Zeitpunkt 30 15
- Zoll 30 4
- Chargennummer 13 40
- Cloud-Computing, Anwendungsbereich 2 25 f.
- CRA Expert Group 50 2 f.
- CSIRT 3 293, 52 49 ff., 54 20
- CVE Respository 6 28
- Cyberbedrohung 3 32 ff., 273
- Cyber Resilience Act Expert Group 25 13
- Cyberresilienz, Begriff 1 5
- Cyber Security Act, Übergangszeitraum 69 19
- Cybersecurity Skills Academy 10 4
- Cybersicherheit 3 22 ff., 20 7 ff., 22 11 ff.
 - angemessenes Maß 20 17 ff.
- Cybersicherheitsanforderungen 3 212, 6 1 ff.
 - grundlegende **Anh. I 1**
 - KI 12 9 f.
- Cybersicherheitsniveau 3 211
- Cybersicherheitsrisiko 3 245 ff., 20 33 ff.
 - Abwendung 20 52
 - Ausmaß 3 248
 - Auswirkung 22 13 ff.
 - Eintrittswahrscheinlichkeit 3 248
 - erhebliches 3 251 ff., 256, 20 35 ff., 45 ff., 54 16
 - konformes Produkt 57 1
 - Meldung 20 36
 - Minderung 57 6
 - Prognoseentscheidung 3 247
 - Stufung 3 255
 - Zusammenarbeit 20 52
- Cybersicherheitsstrategie 1 2, 24 32 ff., 43 f.
- Cybersicherheitszertifizierung 32 21
 - Behörde 52 50
- Datenfernverarbeitung 3 10 ff., 26 11
 - Lösungen 26 10
- Datenrecht, Datenverordnung 1 19
- Datenschutz 15 7, 16 10, 20 62 f.
 - „by design“ 1 21
 - Datensicherheit 1 13, 22
 - Verletzung des Schutzes personenbezogener Daten 1 26
- Datenschutzaufsichtsbehörden 52 54 ff.
- Datensicherheit 15 7, 16 10
- Datenzugang 53 6
- Dauerhafte Unterstützung 24 31
- Delegierter Rechtsakt 26 2, 17, 61 1 ff.
 - Abgrenzung zu Durchführungsrechtsakten 61 15 f.
 - Befugnisübertragung 61 17 ff.
 - Bericht 61 22
 - Dauer der Befugnisübertragung 61 20 ff.
 - Einspruch 61 32 ff.
 - Erlassbefugnis 27 31 f.
 - Konsultation 61 30
 - Mitteilungspflichten 61 31
 - Rechtsgrundlage 61 11 ff.
 - Rechtsschutz 61 37 ff.

- Widerruf der Befugnisübertragung 61 23 ff.
- Delegierte Verordnung 61 1
- DID-Richtlinie 3 282
- Digital Operations Resilience Act 1 5
- DIN 44 300 53 9
- Dokumentation 13 19
- Dokumentationspflicht 13 19, 19 18
- Dokumentationsweise 13 20
- Drittanbieterkomponenten 25 2
- Drittkonformitätsbewertung 32 2 ff.
- Drittstaat 47 6
 - angemessenes Schutzniveau 63 81 ff.
 - sensible Information 63 70 ff.
 - Vertraulichkeitsvereinbarung 63 77 ff.
- DS-GVO 6 49
- Dual Licensing 24 26
- Durchführung des CRA 9 5 f.
- Durchführungsbefugnis, Kommission 62 10
- Durchführungsgesetz, nationales 52 77
- Durchführungsrechtsakt 3 292, 27 17 ff., 25, 62 1 ff.
 - Abgrenzung zu delegierten Rechtsakten 62 14
 - Änderung 27 29
 - Formvorschriften 27 22
 - Gremien 27 23
 - Konsultation 27 24
 - Prüfverfahren 27 20
 - Rechtsschutz 62 33
 - Rückruf 3 286
 - Subsidiarität 27 18
 - Verfahren 27 21
 - Verweise im CRA 62 29 ff.
- Durchführungsverordnung 62 1
- Durchsetzung 20 65, 52 1 ff.
- EHR-Systeme 31 47 ff., 32 36 ff.
- eID 8 53
- eIDAS 2 73
- Eigenbedarf 3 145
- Eigene Marke, Anbringen 21 12
- Eigener Name, Anbringen 21 12
- Eigenkonformitätsbewertung 32 2 ff.
- Einflussbereich, Sachherrschaft 3 129
- Einführer 3 94 f., 13 3, 19 1 ff.
- Einspruch 48 1
- Einspruchsverfahren 48 1 f.
- Einstellung der Betriebstätigkeit 19 20, 20 55 ff.
- Einzelprodukt 3 130
- Eisenbahn 2 13
- Elektronisches Informationssystem 3 43, 59
- Elementare Gefährdungen 3 246
- Empfänger der Meldung 15 4
- Endnutzer 3 109, 141
- Endprodukt 3 52, 20 7
- Endpunkt 3 73 ff.
- ENISA 10 3, 52 49 ff., 56 13
- EN ISO/IEC 17000 3 199
- Entfernt stattfindende Datenfernverarbeitung 24 21
- Entschließungsermessen 58 7
- Entwickler freier und quelloffener Software 26 12
- Entwicklung 6 11 f.
- Entwicklungskosten 24 23
- Erfahrungsaustausch 49 20, 50 1 ff., 52 53
- Erforderlichkeit 20 47 f.
- Erfüllungszeitpunkt 6 5
- Ermessen 47 25
- Ersatzteile 2 54 ff.
- Erteilung der Bevollmächtigung 18 2 ff.
- EU-Baumusterprüfbescheinigung 69 1 ff.
 - Harmonisierungsrechtsvorschriften 69 12 ff.
 - Übergangszeitraum 69 8 ff.
- EU-Baumusterprüfung 32 9 ff.
- EU-CyCLONe 17 2
- EU-Funkanlagenrichtlinie 27 8
- EU-Konformitätsbewertung 13 34 ff.
- EU-Konformitätserklärung 3 227, 13 34 ff., 28 1 ff., Anh. V 1
 - Aktualisierung 28 11
 - Aufbewahrung 28 4
 - Ausstellung 28 10
 - Ausstellungspflicht 28 7 f.
 - Ausstellungsverantwortung 28 24
 - Beifügung 28 4, 12
 - Bevollmächtigter 28 8
 - Deaktivierungsanordnung 28 5
 - Einführer 28 9
 - Form 28 16
 - formelle Nichtkonformität 28 5
 - formelle Verkehrsfähigkeitsvoraussetzung 28 11
 - Geldbuße 28 5
 - Geltungsbeginn 28 11
 - gesetzliches Verkehrsverbot 28 5
 - Grundsatz der Singularität 28 21 f.
 - Händler 28 9
 - Harmonisierungsrechtsvorschriften 28 22
 - Hersteller 28 7
 - Inhalt 28 13 ff., 17
 - Konformitätsverantwortung 28 23 f.
 - Konformitätsvermutung 28 2
 - Marktüberwachung 28 5
 - Marktverhaltensregel 28 6
 - Mindestangaben 28 25

- Muster 28 17
- NLF-Konformitätstrias 28 1
- Produkthaftung 28 6
- Rechtssetzungsbefugnis 28 25
- Rückruf 28 5
- sachlicher Geltungsbereich 28 14
- Sachmangel 28 6
- Selbsterklärung 28 2
- Sprache 28 15
- Unterzeichnung 28 10
- vereinfachte 28 20, **Anh. VI 1**
- vollständige 28 17
- weitere Angaben 28 19
- Zoll 28 5
- Europäische Schwachstellendatenbank 17 8
- Europäisches Kompetenzzentrum für Cybersicherheit 10 5
- Europäisches Schema für die Cybersicherheitszertifizierung 25 9
- European Cybersecurity Skills Framework (ECSF) 10 3
- EU-Typengenehmigung 68 1 ff.
- EU-Wirtschaftsakteur 3 77
- Evaluation des CRA 70 1 ff.
- Konsultation 70 9
- Meldeplattform 70 12 ff.
- regelmäßige Überprüfung 70 8 ff.
- Veröffentlichung 70 10
- Zurückhaltung von Meldungen 70 12 ff.
- Expertengruppe 50 2 f.
- Exploit Mitigation Techniques 6 65
- Fachkräftemangel 35 14
- Fachkunde 20 12
- Fahrzeuge 68 1 ff.
- Fahrzeugklasse L 68 2
- Fehlanwendung 3 186 ff., 216
- Fehlfunktion 3 266
- Feldinformation 14 18
- Feldmaßnahme 13 60 ff., 14 18, 19 13 f.
- Fernabsatz 3 141
- Fertigungskontrolle 32 15
- Fertigungsprozess 47 11
- Finanzbestimmungen 52 35
- Finanzielle Unterstützung 33 18
- Förderung 33 2
- Form der Meldung 14 22
- Formelle
 - Prüfpflicht 20 22 ff., 30
 - Prüfung 20 13 ff.
 - Überprüfung 20 22 ff.
- FOSS *siehe* Freie und quelloffene Software (FOSS)
- Fotografie 31 14
- Foundations 24 4
- Freier Verkehr 4 1 ff.
- produktbezogen 4 11
- Reichweite 4 9 f.
- Voraussetzungen 4 13 ff.
- Freie und quelloffene Software (FOSS) 3 280, 13 16, 24 1 f., 4, 28 f., 25 1, 4, 26 3
- Anwendungsbereich 2 18 ff.
- copyleft 3 280 f.
- Geschäftstätigkeit 2 20 ff.
- Komponenten 25 3
- Freiwillige Meldung 15 1 ff.
- Beinahe-Vorfall 15 3 ff.
- Cyberbedrohung 15 3 ff.
- Rechtsfolgen 15 8
- Schwachstelle 15 3 ff.
- Sicherheitsvorfall 15 3 ff.
- Frühwarnung
 - aktiv ausgenutzte Schwachstelle 14 4
 - schwerwiegender Sicherheitsvorfall 14 10
- Fulfilment-Dienstleister 3 77
- Funkanlage (RED) 2 73
- Funktionsaktualisierungen 3 223
- Gebotene Sorgfalt 13 15
- Gebühr 3 144
- Gebührende Sorgfalt 20 26 ff.
- Gegenseitige Anerkennung, Abkommen über 34 1 ff.
- Geldbuße 47 3, 64 1 ff.
- Vertraulichkeit 63 87 ff.
- Geltungsbeginn 14 2, 71 1 ff.
- Ausnahme 71 10 ff.
- Gemeinsame Spezifikation
 - Meldeverfahren 27 28
 - Vorlagepflicht 27 34
- Gerät 2 17
- Geschäftsmodelle 24 26
- Geschäftstätigkeit 3 146, 24 7 f., 24
 - unternehmensbezogener Kontext 3 142
- Gewerbliche Tätigkeit 24 17
- Gewinnabsicht 3 143
- GPSR *siehe* Produktsicherheitsverordnung
- Grundlegende Cybersecurityanforderungen **Anh. I 1**
- Grundschutz 6 21
- Haftung 17 1, 7, 20 65 ff.
- Deliktsrecht 20 68
- verschuldensabhängige 20 68
- Händler 3 97 ff., 105 ff.
- Tatbestandsvoraussetzungen 3 101
- Wirtschaftsakteur 3 96 ff.
- Händlergemeinschaft 3 103 ff.
- Händlerpflicht 20 4, 31

- Hardware 3 44 ff.
- Hardware Security Module 8 45
- Harmonisierte Norm 3 239, 26 2, 27 3 ff., 9 ff., 31 17, **Anh. VII** 7 f.
 - Bewertung 27 27
 - Fundstelle 27 26
 - Nichtbeachten 27 15
- Harmonisierungsvorschrift 3 231 ff., 11 11
 - Übergangszeitraum 69 12 ff.
- Hauptniederlassung 14 15 ff.
- Helpdesk 17 1, 9
- Hersteller 3 80 ff., 107, 109, 13 1 ff., 21 3, 7, 22 10 ff., 24 30
 - Identifikation 21 12
 - Software 3 82
- Herstellerfiktion 21 7, 22 2
- Herstellerkennzeichnung 13 46 ff.
- Herstellerpflicht 13 1 ff., 21 1 ff., 22 1 ff., 24 5
- Herstellervermutung 21 5
- Herstellung 6 11 f.
- Herstellungsprozess 3 138, 226
- Hochrisiko-KI 52 71
- Hochrisiko-KI-System 12 5, 31 47 ff., 35 12
- Hoheitsgebiet 47 6
- Horizontaler Ansatz 2 4, 11 5
- Identifikationskennzeichnung 13 39
- Identitätsverwaltung 6 38 ff.
- IEC 62443 6 18 ff.
- Industriedienstleister 47 9
- Industrielle Steuerungssysteme 2 13
- Information der Nutzer 14 18 ff.
- Information der Öffentlichkeit 17 1, 4 f.
- Informationen für den Nutzer **Anh. II** 1 ff.
- Informationsaustausch 49 20
 - Drittstaat 63 67 ff., 77 ff., 81 ff.
- Informationspflicht 13 39 ff.
 - der Wirtschaftsakteure 23 3
 - des Einführers 19 11 f., 14 ff.
 - Umfang 20 58 f.
- Informationssystem, elektronisches 3 59 ff.
- Informations- und Erfahrungsaustausch 49 20
- Inkrafttreten 71 1 ff.
- Instandhaltungspflicht 13 21 ff.
- Integrierte Schaltung 7 40 ff.
- Interesse, öffentliches 47 9
- Interessenkonflikt 49 17
- Interessenträger 9 7
- Interinstitutionelle Vereinbarung 61 10
- Internationale Zusammenarbeit 52 34
- Internes Kontrollverfahren 32 8 ff.
- Inverkehrbringen 3 122 ff., 6 6 f., 21 10
 - unter eigenem Namen 21 2 ff., 6 ff.
 - unter eigener Marke 21 2 ff., 6 ff.
- In-vitro-Diagnostika 2 34 ff.
- Kennnummer 30 19 ff.
 - Anweisungsrecht 30 21
 - formelle Produktanforderung 30 20
 - Gestaltungsanforderungen 30 22
 - Verkehrsfähigkeitsvoraussetzung 30 20
- Kennzeichnung 21 7
- Kennzeichnungspflicht 13 39 ff., 18 7
 - des Einführers 19 15 ff.
- Kernfunktion 7 9 ff.
- Kleine und mittlere Unternehmen (KMU) 39 36 f., 47 12
 - Unterstützungsmaßnahmen 33 1 ff.
- Kleinstunternehmen 47 12
 - Unterstützungsmaßnahmen 33 1 ff.
- Kollektiver Rechtsschutz 65 1 ff.
- Komitologie-Verordnung 62 2 ff.
 - Ausschuss 62 15 ff.
 - Prüfverfahren 62 18 ff., 25 ff., 31
- Kommerzielle Nutzung 24 26 f.
- Kommerzielles Unternehmen 24 8
- Komponente 3 49 ff., 13 15 ff., 23
- Konformität 13 37 f., 20 29 ff., 21 16, 52 31, 57 1
 - beeinflussende Änderung 21 17
- Konformitätsbescheinigung 47 16 ff., 25
 - Aufhebung 49 10
 - Aussetzung 47 21 f., 27, 49 8
 - Einschränkung 47 26, 49 7
 - Verweigerung 49 6
 - Widerruf 47 21, 23, 28, 49 10
- Konformitätsbewertung 13 33 ff., 32 1 ff.
 - Nichtkonformität 58 10
 - Rangfolge 56 10 f.
- Konformitätsbewertungsstelle 3 198 ff., 204 ff., 39 1 ff., 10 ff., 40 1 ff., 41 1 ff., 42 1 ff., 43 2 ff., 45 5, 7
 - Akkreditierungsstelle 3 203
 - notifizierte Stellen 3 202
 - Prüflabor 3 200
 - Unterauftragnehmer 3 201
 - VO (EG) Nr. 765/2008 3 198
 - Zertifizierungsstelle 3 200
- Konformitätsbewertungsverfahren 3 210, 217, 227, 13 33 ff., 28 11, 32 1 ff., 39 3, 45 8, 54 19, **Anh. VIII** 1
 - Konformitätsvermutung 27 35 f.
- Konformitätserklärung 13 34 ff., **Anh. V** 1
 - vereinfachte **Anh. VI** 1
- Konformitätsnachweis 31 1
- Konformitätspflicht 13 5 f., 19 3
- Konformitätsvermutung 27 1 ff., 9 ff., 13, 25
 - Cybersicherheitszertifikat 27 30, 33
 - EU-Konformitätserklärung 27 30

- gesetzliche Vermutung 27 7
- Produktsicherheitsrecht 27 2 ff.
- Konsultation 9 1 ff., 57 8
- Kontrolle, stichprobenartige 20 24 ff.
- Konzeption 6 11 f.
- Kooperationspflicht 20 35 ff., 46 ff., 53 ff.
- Koordinator 3 293, 54 22
- Koordinierte Kontrollen (Sweeps)
 - Cyberangriffe 60 13
 - Rechtsschutz 60 38
- Koordinierte Offenlegung von Schwachstellen 16 6
- Koordinierungsgruppe 39 34
- Korrekturmaßnahme 13 61 ff., 20 38 ff., 47 18, 20, 52 28, 54 24, 33, 58 13
 - angemessene 47 20
 - Nichtkonformität 52 40
 - risikounabhängige 58 5 ff.
- Kraftfahrzeuge 2 35 ff., 48 ff.
- Kraftwerke 2 13
- Kritisches Produkt mit digitalen Elementen 32 32 ff., **Anh. IV 1**
- Künstliche Intelligenz 52 71
 - KI-Verordnung 1 20, 12 1 ff., 52 71 f.
- Leicht verständliche Sprache 24 43
- Leitlinien 26 1 ff., 5 f.
 - für Kleinstunternehmen 33 17
 - Konsultationspflicht 26 18
 - Mindestinhalte 26 9
 - Unterstützungszeiträume 26 13
 - Veröffentlichungspflicht 26 7
- Lieferant 13 15
- Lieferkette 3 103 f., 284, 20 1 ff., 5 ff., 22 5
 - Integrität 6 13
 - Rücknahme 3 289
- Lieferung durch karitative Organisationen 3 148
- Luftfahrzeuge 2 40 ff.
- Mängel
 - Cybersicherheitszertifizierungen, Schema 55 27
 - harmonisierte Normen 55 26
 - Spezifikationen 55 28
- Manipulation 6 46
- Marktbeobachtungspflicht 13 60 ff.
- Marktmaßnahme 13 60 ff., 19 13 f.
- Marktüberwachung 3 97, 52 1 ff., 83
 - Behördenzuständigkeit 52 18
 - Maßnahmen 52 21
 - ultima ratio 52 21
 - Vertraulichkeit 63 1 ff.
- Marktüberwachungsbehörde 3 233 ff., 20 33 ff., 46 ff., 51, 57, 59 f., 24 40 ff., 27 7, 53 1 ff.
 - Befugnis 52 33, 38, 57 16
 - Bericht an die Kommission 52 70
 - Bindungswirkung 52 81
 - Datenzugang 53 6
 - Ermittlungsbefugnisse 60 32 ff.
 - geeignete 20 67 f.
 - koordinierte Kontrollen (Sweeps) 60 1 ff.
 - Ressourcen 52 57
 - unabhängig, unparteiisch, unvoreingenommen 52 29
 - Untersuchungsgrundsatz 52 41
 - Verbindungsstelle 3 234, 52 27
 - Verbraucher 52 67 ff.
 - Zusammenarbeit 59 1 ff., 6, 9, 12, 15, 18, 22, 27, 29, 33, 36, 38, 41 f., 48, 51, 60 28
 - Zusammenarbeit mit anderen Behörden 52 47 ff.
- Marktüberwachungsrechtlich 20 66 ff.
- Marktüberwachungs-Verordnung (MÜ-VO) 1 6, 3 233, 283 f., 52 19 ff., 25 ff., 66 1 ff.
 - Änderung 66 1
 - Rücknahme 3 287 f.
- Marktüberwachung und Durchsetzung
 - koordinierte Kontrollen (Sweeps) 60 1 ff., 13, 38
 - Produkterwerb unter verdeckter Identität 60 18 ff.
 - Zusammenarbeit 59 1 ff., 7
- Marktzugang 35 14
- Marktzugangsverbot 49 9
- Maschinenverordnung 2 39, 73, 4 36
 - Anwendbarkeit 69 15
 - Übergangszeitraum 69 14 f.
- Massenfertigung 47 11
- Massive Cybersicherheitsvorfälle 17 2
- Medizinprodukte 2 31 ff.
- Meldepflicht 14 1 ff., 20 34 ff., 49 2 ff.
 - aktiv ausgenutzte Schwachstelle 14 1 ff.
 - ausgenutzte Schwachstelle 24 47
 - schwerwiegender Sicherheitsvorfall 14 1 ff., 24 47
- Meldeplattform 14 14 ff., 16 1 f., 11, 24 48
- Meldung 20 43 ff.
 - durch Dritte 15 6
 - informieren 20 43
 - unverzüglich 20 43
 - von Schwachstellen 13 59
- Messe 4 16 ff.
- Militär 2 62
 - Fahrzeuge 2 38
- Mindestanforderungen 6 40

Stichwortverzeichnis

- Mindestaufgaben eines Bevollmächtigten **18 6**
- Missverständnis **21 8 ff.**
- Mitteilungspflicht
 - Kommission **64 77 ff.**
 - Marktüberwachungsbehörde **64 80**
- Musterbedingungen **22 4**
- Musterbestimmungen
 - des Beschlusses Nr. 768/2008/EG **21 4**
 - Selbstverpflichtung **3 99**
- Nachmarktpflichten **20 37**
- Nachweis **20 26 ff.**
- Namensangabe **13 46 ff.**
- Namens- und Adressangabe **19 16 f.**
- NANDO **43 6, 9, 44 2, 5 f., 45 6**
- Nationale Normenwerke der EU-Mitgliedstaaten **3 243**
- Nationale Sicherheit **2 63**
- Negative Auswirkungen **49 12**
- Netz **2 11 ff.**
- Netzwerkgerät **7 36 ff.**
- Netzwerkkarte **7 34**
- Netzwerksicherheit **7 55**
- New Legislative Framework **3 227, 30 3, 32 3 ff., 39 2 f., 46 8**
- Nicht auf einen Bevollmächtigten übertragbare Aufgaben **18 3 f.**
- Nichtkonformität **13 60 ff., 19 7 ff., 55 24**
 - risikounabhängige **58 1 ff.**
- NIS-2-RL **5 12 ff., 8 37, 42, 55**
- NIS-Richtlinien **1 2**
- NLF **35 1 f.**
 - Konformitätstrias **3 227, 28 1, 30 3**
- Non-Konformität **20 28, 37 ff.**
- Norm
 - europäische **3 236 ff.**
 - internationale **3 236 ff.**
- Normungsorganisation **3 240, 27 10, 12**
 - Auftrag **27 11**
- Normungstätigkeiten **39 34 f.**
- Notifizierende Behörde **3 192 ff., 39 8, 43 3 ff., 45 1 ff., 46 3**
 - Akkreditierungsstelle **36 8 ff.**
 - Anforderungen **37 1 ff.**
 - Aufgabe **3 194 f.**
 - Benennung **36 2 ff.**
 - Bewertung und Überwachung **3 194**
 - „eine“ Behörde **36 6**
 - Erteilung der Befugnis **3 195**
 - Hochrisiko-KI-Systeme **36 6**
 - Informationspflichten **38 1 ff.**
 - Interessenkonflikte **37 4 ff.**
 - Kompetenz **37 15 f.**
 - Mitarbeiter **37 28 ff.**
 - Objektivität **37 7 ff.**
 - personelle Trennung **37 10 ff.**
 - Unparteilichkeit **37 7 ff.**
 - Vertraulichkeit **37 25 ff.**
 - Wettbewerbsverbot **37 17 ff.**
- Notifizierte Stelle **3 202, 204 ff., 39 1 ff., 40 1 ff., 41 1 ff., 42 1 ff., 44 1 ff., 45 1 ff., 46 1 ff.**
 - Kennnummer **30 19 ff.**
 - Koordinierung **51 1 ff.**
- Notifizierung **35 1 ff., 39 10 ff., 42 1 ff., 43 4 ff., 45 1 ff.**
 - BSI **36 39**
 - Informationen **54 40**
 - Koordinierungsstelle für die Notifizierung **35 7**
 - NANDO-Informationssystem **35 5 f.**
 - nichtstaatliche Stellen **36 33 ff.**
 - notifizierende Behörde **35 3 ff.**
 - notifizierte Stelle **35 4**
 - Verantwortung **36 36 ff.**
 - Verzicht auf Akkreditierung **36 30 ff.**
- Notifizierungsverfahren **3 192, 42 2 ff., 43 2, 6, 13, 46 5**
- Nutzer **20 60 ff.**
- Nutzungsdauer **13 24**
- Nutzungsmöglichkeit **3 134**
- Offene Archive **3 147**
- Offenlegung
 - Aufschiebung **6 92**
 - Methode **6 91**
 - Pflicht **6 90**
- Offenlegung von Schwachstellen **16 12**
- Öffentliches Interesse **47 9**
- Öffentliche Verwaltung **3 144**
- Öffentliche Verwaltungseinrichtung **3 145**
- Open Source **52 7**
 - -Foundations **24 3, 10**
 - -Initiative **24 11**
 - -Komponente **24 23**
 - -Projekte **24 20**
 - -Repositories **24 16**
 - software steward **3 86, 24 1**
- Open-Source-Software **3 89**
 - Marktüberwachung **52 42 ff.**
- Opt-out **6 69**
- Personenbezogene Daten **3 274 ff.**
- Pflicht
 - zum Einschreiten **47 30**
 - zur Meldung **49 2 ff.**
 - zur Selbstanzeige **49 12**
- Pflichtdokumentation **25 2**
- Pflichten
 - CE-Kennzeichen **3 130**

- Erfüllung 22 12
- Pflichten bei Nichtkonformität 13 60 ff., 19 10 ff.
- Pflichten des Händlers 20 1 ff.
- Betriebstätigkeit 20 2 ff.
- gebührende Sorgfalt 20 2 ff.
- Nichtkonformität 20 2 ff.
- Produktkonformität 20 2 f.
- Überprüfungspflichten 20 2 ff.
- Pflichten des Herstellers 13 1 ff.
- Pflichtenkatalog, Erweiterung 21 1
- PKI 7 33
- Polizei 2 66
- Privatverkauf 22 9
- Privilegierung
 - Kleinunternehmen, kleine und mittlere Unternehmen 64 91 ff.
 - OSS 64 93
 - Verwalter quelloffener Software 64 93 ff.
- Produkt
 - Komponente 3 55 ff.
 - Lebenszyklus 20 19
 - Verwendungszeitraum 20 19
- Produkt, End- 3 52
- Produktanforderung, formelle 28 3, 30 2
- Produkthaftung 31 4 ff.
- Produkthaftungsrecht 11 8
- Produkthaftungsrichtlinie 24 15
- Produktmissbrauch 3 174 ff., 191
- Produkt mit digitalen Elementen 3 2 ff., 105 ff., 124 ff., 136, 209, 24 13, 24
- Änderung 3 210 f., 216 f., 226
- Endprodukt 3 140
- Reparatur 3 218, 220
- wesentliche Änderung 3 212 f., 218, 223 ff.
- Zweckänderung 3 214 f., 220
- Produktrechtliche Verantwortung 13 15
- Produktsicherheitsausschuss 62 17
- Produktsicherheitsrecht 11 1 ff.
- Produktsicherheitsregulierung 52 83
- Produktsicherheitsverordnung 52 22, 69 18
- Produktwarnung 54 38
- Prognose 56 9
- Prototyp 4 21
- Prüfbericht, Konformität 52 31
- Prüfpflichten des Einführers 19 4
- CE-Kennzeichnung 19 5
- EU-Konformitätserklärung 19 5
- Konformität 19 5 ff.
- technische Dokumentation 19 5
- Typen-, Chargin- oder Seriennummer 19 5
- Prüfsumme 6 47
- Prüf- und Kontrollpflichten 3 110
- Prüfung 31 18
 - des CRA 70 1 ff.
- Prüfverfahren
 - Berufungsausschuss 62 25
 - schriftliches Verfahren 62 31 f.
 - Stellungnahme 62 21
- PV-Anlagen 2 15
- Qualitätssicherung 13 15, 32 16 ff.
- Quasi-Hersteller 3 81, 22 3 ff.
- Quellcode 24 22, 29
- Quelloffene Software 32 35 ff., 52 7
 - Marktüberwachung 52 42 ff.
- Quelloffene Softwarekomponenten, Open-Source-Software 3 146
- Radio Equipment Directive (RED), Übergangszeitraum 69 16
- Rangfolge der Inanspruchnahme 19 13
- Reallabor 33 8 ff.
- Rechtsfolge 21 11 f., 20, 22 10
- Rechtsträger 3 126
- Redundanz 6 54 f., 64
- Reparatur 21 19
- Ressourcenbereitstellung 52 9
- Risiko 13 61 ff.
- Risikoanalyse 6 4
- Risikobasierter Ansatz 6 15 f.
- Risikobewertung 6 77, 13 8 ff., 31 20 f.
- Risikofaktoren
 - internationale 54 31
 - koordinierte Risikobewertung 56 18
 - nichttechnische 3 252, 54 30, 56 17
- Risikoniveau 3 220
- Risikostufung 24 5
- Rücknahme 3 287
- Rückruf 3 283
- Rückverfolgung 13 39 ff.
- Rundfunk 2 14
- Sachherrschaft 3 123, 131
 - Besitzfähigkeit 3 133
- Sanktion 20 66 ff., 64 1 ff.
 - Amtshaftung 63 89
 - Anforderung 64 19 ff., 55 f.
 - Behörde 64 81 ff.
 - Bemessungskriterium 64 63 ff., 71 ff.
 - Bußgeld 64 31
 - Dänemark und Estland 64 84 ff.
 - Ermessen 64 28
 - Kumulierbarkeit mit anderen Maßnahmen 64 87 ff.
 - Milderung 64 69, 74 f.
 - Mitteilungspflicht 64 77 ff.
 - öffentliche Stelle 64 81 ff.

Stichwortverzeichnis

- OWiG 64 76
- Prävention 64 8
- Privilegierung 64 91 ff.
- Rechtsschutz 64 96 ff.
- Regelungsverpflichtung 64 17 ff.
- Umsetzungsermessen 64 19
- Umstände im Einzelfall 64 61 ff.
- Verjährung 64 30
- Zuständigkeit 64 18
- SBOM 3 257 ff., 13 66 ff., 70 ff.
- Format 3 260
- maschinenlesbar 3 260 ff.
- Schadensersatzanspruch 48 4
- Schiffsausrüstung 2 46 ff.
- Schlüsselverwaltung 7 33
- Schnittstelle 3 51, 6 60
- Schriftform 18 2
- Schutzklauselverfahren 55 1
- Schutzniveau 47 14 f.
- Schwachstelle 3 266, 6 27, 13 17 ff., 20 43 ff., 24 37 f.
- Behandlung 6 9
- CVE Repository 6 28
- koordinierte Offenlegung 2 68
- Zeitpunkt der Behebung 6 30
- Schwachstellendatenbank 17 8
- Schwachstellenmanagement 31 30 f.
- Schwerwiegend 14 8 f.
- Schwerwiegender Sicherheitsvorfall 24 49
- Security by design 24 35
- Security Level 6 18 ff.
- Security und Safety 7 17
- Seilbahn 4 36
- Sektorübergreifende Gruppe 51 4 ff.
- benannte Vertreter 51 9
- Ergebnisse 51 7
- Kooperationspflicht 51 11 f.
- Mitglieder 51 5
- Organisation 51 6
- Selbstanzeige 49 12
- Selbsterklärung 30 2
- Selbstverpflichtung 13 13
- Selbstzertifizierung 47 2
- Sensibilisierung der Öffentlichkeit 17 4 f.
- Separierung 6 64
- Serienfertigung 47 11
- Serienherstellung 13 37 f.
- Seriennummer 13 40
- Sicherheit
- des Binnenmarktes 16 8
- nationale 2 63, 5 17
- öffentliche 2 65
- Sicherheitsaktualisierung 3 223 f., 6 9, 13 29 f.
- Sicherheitsbauteil 12 2
- Sicherheitsbescheinigung 25 8
- Sicherheitsbescheinigungsprogramm 25 5, 7, 10 ff., 14
- Sponsoring 25 15
- Sicherheitsinteressen, nationale 2 67 ff.
- Sicherheitspatch 13 29 f.
- Sicherheitsrisiko, erhebliches 20 45
- Sicherheitsupdate 31 27
- Sicherheitsvorfall 3 246, 270
- mit Auswirkungen auf die Sicherheit des Produkts mit digitalen Elementen 3 271
- Signatur 6 47
- Siri 7 46
- Smartcard 8 52
- Smartwatch 7 52
- Sofortvollzug 54 48
- Software
- Alpha-Version 4 26
- Beta-Version 4 26
- Repositories 4 27
- Software-Produkt 3 43 f.
- Vorab-Version 4 26
- wesentliche Änderung 3 221 f.
- Softwareabhängigkeiten 13 70 ff.
- Softwarearchiv 13 31
- Softwareprodukt 3 133 f.
- Software-Stückliste 3 257 ff., 6 78, 13 70 ff., 31 19, 32 ff., **Anh. II** 10
- Softwareupdate 21 19
- Softwareversionen **Anh. VII** 3
- Sorgfaltsmaßstab 20 32
- gebührende Sorgfalt 20 9 ff.
- Spezifikationen **Anh. VII** 7 f.
- Sprache, leicht verständliche 20 50 ff.
- Standardisierungsorganisationen 27 3
- Standardkonfiguration 6 32 ff.
- Start-up, Unterstützungsmaßnahmen 33 1 ff.
- Stichproben 52 30
- Störungen 6 58
- Streckengeschäft 3 129
- Stromzähler 8 48
- Stückliste, Software 13 70 ff.
- Stufenweiser Aufbau 20 7
- Sub-Group Conformity Assessment and Accreditation 50 5
- Sweeps 52 2
- Technische Anwendung 47 4, 49 20
- Technische Dokumentation 13 14, 32, 28 12
- Nichtkonformität 58 10
- Vereinfachung 33 19 f.
- Technischer Consultant 3 241
- Technische Unterlagen 21 21
- Tertiäre Rechtsetzung 62 10 ff.

- Tertiäres Unionsrecht 61 11
- Testberichte 31 22, **Anh. VII** 9
- Testbetrieb 3 139
- Testzwecke 4 25 ff.
 - Sicherheitsbauteil 4 34
- Ticketing 6 98
- Tracking 13 41
- Traffic Light Protocol 2 71
- Transparenz 63 14 f.
 - Informationsfreiheitsverordnung 63 18
- Trennung Safety und Security 6 86
- Trusted Execution Environment 7 59
- Typennummer 13 40
- Übergabe 3 130
- Übergangszeitraum 69 1 ff.
 - EU-Baumusterprüfbescheinigung 69 8 ff.
- Übermittlung von Informationen 13 62 f.
- Überprüfung, Umfang 20 25 ff.
- Überprüfungspflicht 20 16 ff.
- Überschreiben 6 74
- Übertragungsfehler 6 46
- Überwachung 6 67
- UKlaG 65 26 ff.
- Ultima ratio 56 1
- Umgang mit Meldungen 16 3 ff.
- Umlabeln 21 9 f.
- Unbefugte Zugriffe, Überwachung 6 38 ff.
- Ungenauigkeit 21 8 f.
- Unionsmarkt 3 140
- Unnötige Belastungen 47 9 f.
- Unteraufträge 49 16
- Unterlassungsklagerichtlinie 65 11
- Unternehmen, kleine und mittlere 47 12
- Unterrichtungspflicht 20 55 ff.
- Unterstützungsmaßnahmen 33 1 ff.
- Unterstützungszeitraum 3 121, 13 10, 23 ff., 29, 54 ff., 20 18 ff.
 - Beginn 13 25 ff.
 - EU-Konformitätserklärung 13 35
 - Festlegung 52 76
 - technische Dokumentation 13 32
- Untersuchungsgrundsatz 52 41
- Update 6 34 ff., 83 ff., 13 21 ff., 29 f.
- Updatepflicht 13 21 ff.
- VDuG
 - Abhilfe 65 16 ff.
 - Abhilfeendurteil 65 17
 - Abhilfegrundurteil 65 17
 - Anwendungsbereich 65 19 ff.
 - Gerichtszuständigkeit 65 25
 - Klageberechtigung 65 22 ff.
 - Verbraucher 65 20 f.
- Verbandsklage 65 1 ff.
 - Anwendbarkeit 65 8, 29, 36
 - UKlaG 65 2
 - VDuG 65 2
 - VRUG 65 9 f.
- Verbandsklagerichtlinie 65 11, 67 1 ff.
 - Abhilfe 65 12
 - Änderung 67 1 ff.
 - Umsetzung 65 13 ff.
 - Unterlassung 65 12
 - VRUG 65 13 ff.
- Verbindung
 - indirekte 3 67 f.
 - logische 3 71 f.
 - physische 3 70
- Verbindungsstelle 52 27
- Verbot des Marktzugangs 49 9
- Verbraucher 3 115 ff.
 - Verbandsklage 65 1 ff.
- Verbraucherbeschwerde 52 67 ff., 82
- Verbraucherprodukt 3 249
- Verbraucherschutz 115, 65 6
- Verdachtsmeldungen 49 13
- Vereinfachte EU-Konformitätserklärung 13 36, **Anh. VI** 1
- Vereinfachte technische Dokumentation 33 19 f.
- Vergabe 5 21 ff.
 - von Unteraufträgen 49 16
- Verhältnismäßigkeit 47 8, 11
 - ultima ratio 54 24
- Verhältnismäßigkeitsgrundsatz 22 12, 47 8, 13, 21
- Verkehrsfähigkeitsvoraussetzung, formelle 28 3, 30 2
- Verkehrssysteme, kooperative intelligente 2 17
- Vermarketingsstopp 58 12
- Vernünftigerweise vorhersehbare Verwendung 6 8
- Verordnung (EU) 2017/745 22 5
- Verordnung (EU) 2023/988 22 5
- Verordnungsermächtigung 14 21 f.
- Verschlüsselung 6 41 f.
 - Verfahren 6 42
- Verschlussachen 2 64
- Verstoß 47 3
 - gegen die grundlegenden Cybersicherheitsanforderungen 13 29
- Verteidigung 2 62, 5 17
- Vertraulichkeit 15 7, 63 1 ff.
 - Ausnahmen 63 62 ff.
 - DS-GVO 63 20
 - Einwilligungsvorbehalt 63 57 ff.
 - geistiges Eigentum 63 42

Stichwortverzeichnis

- Geschäftsgeheimnisse **63** 43 ff.
- Marktüberwachungsgesetz **63** 16
- nationale/öffentliche Sicherheitsinteressen **63** 50 ff.
- Quellcode **63** 45
- Sanktion **63** 87 ff.
- Schutzziele **63** 38
- Strafverfahren **63** 56
- Umfang **63** 32 ff.
- Verpflichtung der Akteure **63** 21 ff.
- vertrauliche Geschäftsinformation **63** 47
- Verwaltungsverfahren **63** 56
- verwandte Vorschriften **63** 15
- wirksame Durchführung **63** 48 f.
- Verwalter quelloffener Software **3** 86 ff., **24** 1, 12, 28
- juristische Person **3** 88
- systematische und nachhaltige Unterstützung **3** 90
- Verwaltungsakt **52** 78 f.
- Verwaltungsrechtsweg **52** 78 f., **58** 14
- Verwendung **5** 8
- bestimmungsgemäße **3** 152, 191
- Fehlanwendung **3** 186 ff.
- rechtmäßige **3** 178
- vernünftigerweise vorhersehbare **3** 167 ff., 191
- zweckbestimmungswidrige **3** 174
- Verzögerung **14** 21
- Virens Scanner **7** 28
- Virtualisierung **7** 34
- VM **7** 53
- Vollharmonisierung **4** 3
- Vollzug **52** 3 ff.
- Vorbedingungen **20** 67 f.
- Vorführung **4** 16 ff.
- Vorlagepflicht, Umfang **20** 48 ff.
- Vormarktpflicht **20** 28, 45 ff.
- VRUG, VDuG **65** 16 ff.
- Wahlrecht **47** 7
- Weiterleitung von Informationen an Marktüberwachungsbehörden **16** 9
- Weiterverarbeitung **3** 138
- Werbekampagne **3** 130
- Wesentliche Änderung **3** 107, 209 ff., **21** 2 ff., 13 ff., 18, **22** 1 ff., 6 ff., **26** 16, **28** 11
- Bestandsschutz **69** 25 ff.
- Meldepflicht **69** 31
- ursprüngliche Leistung **3** 219
- Wesentlich geänderte Version **13** 30
- Wichtige Produkte mit digitalen Elementen **32** 22 ff., **Anh. III** 1
- Widerruf der Befugnisübertragung, Teilwider-ruf **61** 26
- Wiederherstellung der Konformität **13** 61
- Wirtschaftsakteur **3** 77 ff., **22** 4 ff.
- Produktsicherheitspflichten **20** 4 ff.
- Verwalter quelloffener Software **3** 78
- Zahlen mit Daten **24** 18
- Zentrale Anlaufstelle **13** 59
- Zivilrechtliche Folgen **14** 20
- Zivilrechtliches Verfahren **52** 81
- Zugangsdaten **7** 27
- Zugangsrecht **53** 6
- Zugangsverwaltung **6** 38 ff.
- Zugelassene Sprache **31** 56
- Zugriffsmöglichkeit **3** 139
- Zulieferer **13** 15
- Zurückhaltung **16** 4 ff.
- Zurverfügungstellung erforderlicher Dokumente **20** 23
- Zur Verfügung zu stellende Dokumente **20** 27
- Zusammenarbeit **24** 41
- Behörden **59** 12
- ENISA **56** 15, **59** 2, 33 ff., **60** 28 ff.
- Ermessen **59** 29 ff., 36 f.
- fairer Wettbewerb **59** 41
- Gewährleistung guter Verwaltung **59** 2, 42 ff.
- gewonnene Informationen **59** 2, 48 ff.
- interbehördliche **59** 22 ff.
- Interessenträger **59** 12 f., 27 ff.
- Kommission **56** 15, **59** 2, 33 ff.
- Pflicht zur Kooperation **59** 6
- Sorgetragungspflicht **59** 38 ff.
- Vereinbarung über gemeinsame Tätigkeiten **59** 1 ff., 15, 18 ff.
- Veröffentlichungspflicht **59** 2, 9, 51 ff.
- zwischen notifizierten Stellen **49** 20
- Zuständigkeit der Marktüberwachungsbehör-de **24** 42
- Zweckbestimmung **3** 149 ff., **6** 8, **52**
- Definitionsrecht **3** 157
- Einschränkungen **3** 159
- Kontext **3** 158
- Quellen **3** 161 ff.
- übliche Verwendung **3** 165 f.
- Zwischenberichte, schwerwiegender Sicher-heitsvorfall **14** 13