Mandanteninformation

Mai 2026

Der **Cyber Resilience** Act: weitreichende Pflichten für Produkte mit digitalen Elementen

Der Cyber Resilience Act (CRA)[1] schafft erstmals EU-weit ein horizontales Regelwerk für die Cybersicherheit von Produkten mit digitalen Elementen. Die Verordnung setzt bereits beim Produktdesign an und begleitet Produkte durch den gesamten Lebenszyklus - von der Risikobewertung bei der Herstellung über die Konformitätsbewertung und CE-Kennzeichnung vor dem Inverkehrbringen bis zur Meldung von Sicherheitsvorfällen und der Vornahme von Korrekturmaßnahmen bei bereits auf dem Markt befindlichen Produkten.

Für Hersteller, Einführer und Händler bedeutet dies spürbaren Umsetzungsdruck. Wer Produkte mit digitalen Elementen in Verkehr bringt oder bereitstellt, muss technische, organisatorische und dokumentarische Prozesse rechtzeitig auf den CRA ausrichten; besonders praxisrelevant ist die Erstellung der sog. Software-Stückliste (SBOM), die eine umfangreiche Dokumentation der im Produkt verbauten Softwarekomponenten erfordert.

I. Hintergrund und Ziel des Rechtsaktes

Der CRA bezweckt eine unionsweite Harmonisierung der Cybersicherheitsanforderungen für Produkte mit digitalen Elementen. Er soll einerseits das Sicherheitsniveau vernetzter Produkte anheben und andererseits den Binnenmarkt stärken, indem ein einheitlicher Mindeststandard für Produkte mit digitalen Elementen geschaffen wird. Anders als sektorale IT-Sicherheitsregime (z.B. die NIS-2 Richtlinie[2]) adressiert der CRA nicht den Betrieb von Unternehmen als solchen, sondern die Produkte selbst und deren Cybersicherheitsanforderungen über den gesamten Produktlebenszyklus.

[1] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=OJ:L_202402847.

[2] https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32022L2555.

Der CRA folgt – wie etwa auch die KI-Verordnung – dem sog. New Legislative Framework. Das bedeutet, dass Produkte vor dem Inverkehrbringen die einschlägigen Cybersicherheitsanforderungen und Dokumentationspflichten erfüllen, ein Konformitätsbewertungsverfahren durchlaufen und mit einer CE-Kennzeichnung versehen werden müssen. Werden später Sicherheitsmängel bekannt, bestehen Melde- und Abhilfepflichten. Die Kommission hat hierzu einen nicht bindenden Leitlinienentwurf veröffentlicht, der insbesondere kleine und mittlere Unternehmen bei der Umsetzung ihrer Pflichten unterstützen soll.[3]

II. Anwendungsbereich

Der CRA erfasst Produkte mit **digitalen Elementen**, die **auf dem Unionsmarkt** bereitgestellt werden (Art. 2 Abs. 1 CRA). Ein solches Produkt ist ein Software- oder Hardwareprodukt inklusive seiner Datenfernverarbeitungslösungen; erfasst sind auch getrennt in Verkehr gebrachte Komponenten, sofern sie Teil eines Produkts mit digitalen Elementen sind (Art. 3 Nr. 1 CRA). Entscheidend ist, dass die beabsichtigte oder vernünftigerweise vorhersehbare Verwendung eine **direkte oder indirekte logische oder physische Datenverbindung zu einem Gerät oder Netzwerk** einschließt. Dies umfasst grundsätzlich jede kabellose oder kabelgebundene Schnittstelle zwischen zwei entfernten Produkten, die dem beidseitigen Datenaustausch dient und für die Funktionalität des Produkts erforderlich ist.

Praxishinweis: Der sachliche Anwendungsbereich des CRA ist deshalb weit. Typischerweise fallen darunter insbesondere:

(i) Stand-alone-Software, Apps und Computerprogramme;

(ii) Hardware mit eingebetteter Software, etwa IoT-Geräte;

(iii) Hardwarekomponenten wie Router, Firewalls, Motherboards oder integrierte Schaltkreise;

(iv) Eine Kombination von Hard- und Software, bei der die Software erforderlich ist, damit das Produkt seine bestimmungsgemäße Funktion erfüllen kann.

Für die Praxis bedeutsam ist die Abgrenzung zur reinen Dienstleistung: Software-as-a-Service ist nicht ohne Weiteres ein CRA-Produkt, kann aber erfasst sein, wenn die erbrachte Datenverarbeitung Teil des Produkts ist (Ewgr. 11. 12 CRA). Maßgeblich ist stets das konkrete Produkt mit seiner vorgesehenen Funktion und Nutzung.

Praxishinweis: Zu beachten ist, dass für Software-as-a-Service-Dienstleistungen die Anforderungen der NIS2-Richtlinie gelten können, die in Deutschland durch das BSIG umgesetzt wurde.[4]

Pflichten treffen vor allem den **Hersteller**, also denjenigen, der das Produkt unter eigenem Namen oder eigener Marke vermarktet (Art. 3 Nr. 13 CRA). Hinzu treten Pflichten für **Einführer** (Art. 3 Nr. 16 CRA), **Händler** (Art. 3 Nr. 17 CRA) und **Verwalter quelloffener Software** (Art. 3 Nr. 14 CRA).

III. Pflichten

1. Herstellerpflichten

a. Cybersicherheits- und Dokumentationspflichten, Art. 13 CRA i.V.m. Anhang I, II CRA

Hersteller müssen **Produkte so entwerfen, entwickeln und herstellen,** dass sie ein dem Risiko

[3] https://digital-strategy.ec.europa.eu/de/news/commission-publishes-feedback-draft-guidance-assist-companies-applying-cyber-resilience-act

[4] Siehe hierzu die Mandanteninformation zur Umsetzung der NIS2-Richtlinie (unter https://www.sza.de/de/thinktank/cybersicherheit-nis2-richtlinie-deutschland-cyber-resilience-act).

angemessenes Maß an Cybersicherheit gewährleisten. Kernpflicht ist eine dokumentierte **Cybersecurity-Risikobewertung**, die sich am bestimmungsgemäßen Zweck und an der vernünftigerweise vorhersehbaren Verwendung orientiert und während des Unterstützungszeitraums aktuell gehalten werden muss.

Die Produkte müssen insbesondere die folgenden Anforderungen erfüllen:

- sichere Standardkonfiguration und Schutz vor unbefugtem Zugriff;
- Wahrung von Vertraulichkeit, Integrität und Verfügbarkeit;
- möglichst geringe Angriffsfläche und geeignete Protokollierung;
- sichere Lösch- und Zurücksetzungsfunktionen;
- Behandlung von Schwachstellen und Bereitstellung von Sicherheitsaktualisierungen während des Unterstützungszeitraums.

Der **Unterstützungszeitraum** ist vom Hersteller festzulegen und muss sich an der voraussichtlichen Nutzung des Produkts orientieren; er beträgt grundsätzlich mindestens fünf Jahre, es sei denn das Produkt hat voraussichtlich eine kürzere Nutzungsdauer (Art. 13 Abs. 8 CRA). Die Mitteilung des Unterstützungszeitraums ist Teil der gegenüber dem Nutzer bestehenden Pflichtangaben nach Anhang II CRA.

Die **Cybersicherheitsbewertung** ist in die technische Dokumentation aufzunehmen, die den zuständigen Marktüberwachungsbehörden auf Anfrage zur Verfügung zu stellen ist. Besondere Bedeutung kommt dabei der **SBOM** zu (Anhang I Teil II Nr. 1 CRA). Die SBOM ist eine Dokumentation der in einem Produkt enthaltenen Komponenten und beinhaltet auch von Dritten bezogene Software (Art. 3 Nr. 39 CRA). Damit wird im Ergebnis eine Verpflichtung zur Dokumentation der Software-Lieferkette etabliert, jedenfalls mit Blick auf die direkt im Produkt verbauten Komponenten. Hiermit dürfte regelmäßig ein erheblicher Dokumentationsaufwand verbunden sein. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat bereits eine technische Richtlinie erlassen, an der sich Anbieter von Produkten mit digitalen Elementen orientieren können.[5]

Zur Erfüllung der Pflichten des CRA nehmen die harmonisierten Normen, deren Fundstellen im Amtsblatt der Europäischen Union veröffentlicht werden, eine entscheidende Rolle ein. Sofern ein Produkt die Anforderungen der einschlägigen Normen erfüllt, wird die Konformität mit den grundlegenden Cybersicherheitsanforderungen nach Art. 27 Abs. 1 CRA vermutet.

b. Konformitätsbewertung (Art. 32 CRA), Konformitätserklärung (Art. 28 CRA) und CE-Kennzeichnung (Art. 30 CRA)

Vor dem Inverkehrbringen muss das Produkt **eine Konformitätsbewertung** durchlaufen. Die Produktkategorie und das damit einhergehende Risiko des Produkts bestimmen, ob eine interne Kontrolle genügt oder ob eine notifizierte Stelle einzuschalten ist. Die Einordnung richtet sich nach der Funktion und Zweckbestimmung des Produkts, wie sie sich insbesondere aus den Kategorien der Anhänge III und IV ergibt.

- Unkritische Produkte: interne Kontrolle genügt;
- wichtige Produkte nach Anhang III Klasse I CRA (z.B. Passwortmanager, Produkte mit VPN-Funktion, Software für die Suche, Entfernung und Quarantäne von Schadsoftware): interne Kontrolle ist möglich, soweit alle anwendbaren Anforderungen durch einen relevanten harmonisierten Standard, eine gemeinsame Spezifikation oder ein einschlägiges Zertifizierungsschema abgedeckt sind; andernfalls ist eine Prüfung durch eine notifizierte Stelle erforderlich;
- wichtige Produkte nach Anhang III Klasse II CRA (z.B. Firewalls, Intrusion-Detection-Systeme

[5] Abrufbar unter https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03183/BSI-TR-03183-2.pdf?__blob=publicationFile&v=3

und Intrusion-Prevention-Systeme) und kritische Produkte nach Anhang IV CRA (Chipkarten oder ähnliche Geräte): Prüfung durch eine notifizierte Stelle ist grundsätzlich zwingend.

Die Konformität des Produkts mit den Anforderungen des CRA wird durch die **Konformitätserklärung** dokumentiert (Art. 28 CRA), durch die der Hersteller Verantwortung für die Konformität des Produkts übernimmt. Zudem ist auf den Produkten grundsätzlich eine **CE-Kennzeichnung** anzubringen (Art. 30 CRA)

c. Melde- und Informationspflichten

Nach Art. 14 CRA muss der Hersteller aktiv ausgenutzte Schwachstellen und schwerwiegende Sicherheitsvorfälle an das sog. Computer-Notfallteam (CSIRT) und die Cybersicherheitsagentur ENISA melden. Nach dem Referentenentwurf zum CRA-Umsetzungsgesetz soll die Rolle des CSIRT in Deutschland vom BSI wahrgenommen werden.[6] Der CRA sieht ein gestuftes Meldesystem vor.

- Frühwarnung innerhalb von 24 Stunden nach Kenntniserlangung;
- weitergehende Informationen innerhalb von 72 Stunden;
- Abschlussbericht binnen 14 Tagen nach Verfügbarkeit einer Korrektur- oder Risikominderungsmaßnahme bei aktiv ausgenutzten Schwachstellen bzw. binnen eines Monats bei schwerwiegenden Vorfällen.

Neben der behördlichen Meldepflicht bestehen im Fall von aktiv ausgenutzten Schwachstellen und erheblichen Sicherheitsvorfällen auch Informationspflichten gegenüber den Nutzern (Art. 14 Abs. 8 CRA). Dies umfasst auch die Mitteilung von Risikominderungs- und Korrekturmaßnahmen. Außerdem müssen ggf. auch die vorgelagerten Anbieter von Software-Komponenten informiert werden, wenn die jeweiligen Komponenten Schwachstellen enthalten (Art. 13 Abs. 6 CRA).

> **Praxishinweis:** Für betroffene Unternehmen ist entscheidend, die Meldewege, Zuständigkeiten und Freigabeprozesse vorab festzulegen. Die Fristen sind so knapp, dass sie nur mit einer vorbereiteten Incident-Response-Organisation eingehalten werden können.

2. Pflichten von Einführern, Händlern und Verwalter quelloffener Software

Einführer müssen vor dem Inverkehrbringen prüfen, ob das Produkt die CRA-Anforderungen erfüllt. Dies umfasst insbesondere die Prüfung, ob die Konformitätsbewertung erfolgt ist, die technische Dokumentation erstellt wurde und eine CE-Kennzeichnung sowie Konformitätserklärung vorliegen (Art. 19 Abs. 1 CRA). Händler haben ähnliche, aber etwas weniger weitreichende Prüfpflichten (Art. 20 CRA). Sofern Anhaltspunkte für Nichtkonformität bestehen, dürfen Einführer und Händler die Produkte nicht in den Verkehr bringen bzw. auf dem Markt bereitstellen. Bringen sie das Produkt unter eigenem Namen oder eigener Marke in Verkehr, gelten sie selbst als Hersteller (Art. 21 CRA).

Verwalter quelloffener Software werden nur unter engen Voraussetzungen vom CRA adressiert. Erfasst ist eine juristische Person, die nicht selbst Hersteller ist, spezifische freie und quelloffene Software für kommerzielle Verwendungen nachhaltig unterstützt und deren Fortbestand sichert (Art. 3 Nr. 14 CRA). Die Verwalter quelloffener Software müssen insbesondere eine Cybersicherheitsstrategie entwickeln und dokumentieren sowie mit den Marktüberwachungsbehörden zusammenarbeiten. Sie trifft zudem eine Meldepflicht zu schwerwiegenden Vorfällen und aktiv ausgenutzten Schwachstellen (Art. 24 CRA).

[6] https://www.bmi.bund.de/SharedDocs/gesetzgebungsverfahren/DE/Downloads/referentenentwuerfe/CI3/vo-entwurf-cyberresilienz.pdf?__blob=publicationFile&v=1.

IV. Durchsetzung

Der CRA wird durch die Marktüberwachungsbehörden der Mitgliedstaaten durchgesetzt. Nach dem Referentenentwurf zum CRA-Umsetzungsgesetz soll das BSI als zuständige Marktüberwachungsbehörde ernannt werden.[7] Den Marktüberwachungsbehörden stehen umfangreiche Befugnisse zu, insbesondere Auskunftsrechte (Art. 53 CRA), Kontrollbefugnisse (Art. 60 CRA), Anordnung von Korrekturmaßnahmen sowie Rücknahme- und Rückrufmaßnahmen (Art. 54 Abs. 1 CRA). Die Verordnung ist damit als klassisches Produktaufsichtsregime mit spürbaren behördlichen Eingriffsbefugnissen ausgestaltet.

Bei Verstößen drohen erhebliche Geldbußen. Die Verordnung sieht als Obergrenze - je nach Art des Verstoßes - bis zu 15 Mio. EUR oder bis zu 2,5 % des weltweiten Jahresumsatzes vor (Art. 64 Abs. 2 CRA). Dies gilt jedoch nicht für Verwalter quelloffener Software, die der Sanktionsvorschrift des Art. 64 CRA nicht unterliegen (Art. 64 Abs. 10 b CRA). Der CRA kann zudem Auswirkungen auf den zivilrechtlichen Sorgfaltsmaßstab haben. Die Nichteinhaltung des CRA kann daher zu einer privatrechtlichen Haftung führen.

V. Geltungsbeginn

Der CRA ist bereits am 10. Dezember 2024 in Kraft getreten, die volle Anwendung folgt jedoch gestaffelt (Art. 71 CRA):

- 11. Juni 2026: Geltungsbeginn der Vorschriften über die Notifizierung von Konformitätsbewertungsstellen;
- 11. September 2026: Geltungsbeginn der Meldepflichten für aktiv ausgenutzte Schwachstellen und schwerwiegende Vorfälle (Art. 14 CRA);
- **11. Dezember 2027**: vollumfängliche Anwendung der materiellen Pflichten des CRA.

Produkte, die vor dem 11. Dezember 2027 bereits auf dem Markt sind, unterfallen dem CRA nur, wenn sie ab diesem Zeitpunkt erheblich modifiziert wurden (Art. 69 Abs. 2 CRA).

VI. Praxisfolgen

Für Unternehmen, die digitale Produkte vertreiben, besteht eine hohe Wahrscheinlichkeit, dass sie vom CRA betroffen sein werden. Cybersicherheit muss in diesem Fall schon vom Entwurf des Produktes an mitgedacht werden. Besondere Bedeutung hat in diesem Fall die SBOM, d.h. die Pflicht, die in ein Produkt integrierten Komponenten (insbesondere Software) zu dokumentieren.

Die Nichteinhaltung des CRA kann empfindliche Bußgelder und zivilrechtliche Haftung auslösen. Aufgrund der komplexen regulativen und technischen Anforderungen raten wir betroffenen Unternehmen, unverzüglich mit der Implementierung geeigneter Sicherheits- und Meldekonzepte zu starten. Hierbei unterstützen wir Sie gerne.

[7] https://www.bmi.bund.de/SharedDocs/gesetzgebungsverfahren/DE/Downloads/referentenentwuerfe/CI3/vo-entwurf-cyberresilienz.pdf?__blob=publicationFile&v=1

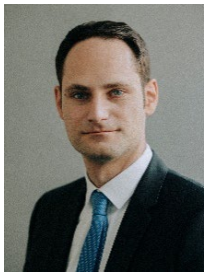
Diese Mandanteninformation beinhaltet lediglich eine unverbindliche Übersicht über das in ihr adressierte Themengebiet. Sie ersetzt keine rechtliche Beratung. Als Ansprechpartner zu dieser Mandanteninformation und zu Ihrer Beratung stehen gerne zur Verfügung:

Dr. Thomas Nägele
Rechtsanwalt | Partner
Compliance, Interne Untersuchungen | Datenschutz und Datensicherheit| Gewerblicher Rechtsschutz | IT-Recht | Prozessführung und Schiedsverfahren

T +49 621 4257 222
E Thomas.Naegele@sza.de

Dr. Simon Apel
Rechtsanwalt | Partner
Gewerblicher Rechtsschutz | Datenschutz und Datensicherheit

T +49 621 4257 386
E Simon.Apel@sza.de



Alexander Stolz, LL.M. (Dresden / Exeter)
Rechtsanwalt | Counsel
Commercial | Datenschutz und Datensicherheit| Gewerblicher Rechtsschutz | IT-Recht

T +49 621 4257 222
E Alexander.Stolz@sza.de

Hannah Bräunche
Rechtsanwältin | Associate
Gewerblicher Rechtsschutz | Datenschutz und Datensicherheit | Commercial

T +49 621 4257 386
E Hannah.Braeunche@sza.de

Serpil Dilbaz, LL.B.
Rechtsanwältin | Associate
Datenschutz und Datensicherheit| Gewerblicher Rechtsschutz | IT-Recht

T +49 621 4257 222
E Serpil.Dilbaz@sza.de