Cyber Resilience Act (CRA)

- Ein Cheatsheet aus der DORA-Werkstatt -

DISCLAIMER: Das Cheatsheet dient als Orientierungshilfe für einen ersten Überblick über die Inhalte und Anforderungen des Cyber Resilience Act. Das Cheatsheet ist nicht rechtsverbindlich und ersetzt keine juristische Prüfung.

LEGENDE:

relevant für Händler | relevant für Betreiber | relevant für Verwalter quelloffener Software

relevant für kritische Produkte | relevant für wichtige Produkte | relevant für „Standard-Produkte“

Bezug	Titel	Beschreibung	Datum	Produkte	Relevant für		
Kap. I	ALLGEMEINE BESTIMMUNGEN						
Art. 1	*Art. 1 (Gegenstand) enthält den Gegenstand der Verordnung. Die Vorschriften gelten für Produkte mit digitalen Elementen.*		*11.12.27*				
Art. 2	Anwendungsbereich	**Art. 2 enthält den Anwendungsbereich der Verordnung.** • CRA gilt für Software- & Hardwareprodukte, die eine Datenverbindung mit Netzen oder Geräten herstellen • Erfasst sind „Standard-Produkte“, wichtige Produkte sowie kritische Produkte • Es gibt umfangreiche Ausnahmen, z.B. für Medizinprodukte, KFZ-Produkte, etc.	11.12.27	+ +	X	X	X
Art. 3	Begriffsbestimmungen	**Art. 3 enthält die Begriffsdefinitionen des CRA. Besonders wichtig dabei die Wirtschaftsakteure** • „Hersteller“ = Unternehmen, dass „[…] Produkte mit digitalen Elementen entwickelt oder herstellt oder […] konzipieren, entwickeln oder herstellen lässt und sie unter ihrem Namen oder ihrer Marke vermarktet […]“ • „Händler“ = Unternehmen, dass „[…] ein Produkt mit digitalen Elementen ohne Änderung seiner Eigenschaften auf dem Unionsmarkt bereitstellt […]“	11.12.27		X	X	X
Art. 4	Freier Verkehr	**Art. 4 enthält Regelungen zum freien Verkehr in der EU.** • CRA-konforme Produkte dürfen EU-weit in Verkehr gebracht werden • Nichtkonforme Produkte und Software dürfen lediglich auf Messen oder Ausstellungen gezeigt bzw. zu Testzwecken bereitgestellt werden (Wichtig: Kennzeichnungspflicht)	11.12.27		X	X	
Art. 5	*Art. 5 (Beschaffung oder Nutzung von Produkten mit digitalen Elementen) enthält Regelungen und Kriterien, gemäß derer die EU befugt ist zusätzliche Cybersicherheitsanforderungen stellen*		*11.12.27*				
Art. 6	Anforderungen an Produkte mit digitalen Elementen	**Art. 6 enthält Anforderungen an Produkte mit digitalen Elementen.** Die Bereitstellung ist nur zulässig bei… • Umsetzung der Cybersicherheitsanforderungen aus Anhang I – Teil 1 (Cybersicherheitsanforderungen) • Umsetzung der Verfahren aus Anhang I – Teil 2 (Anforderungen an die Behandlung von Schwachstellen)	11.12.27	+ +	X	X	
Art. 7	Wichtige Produkte mit digitalen Elementen	**Art. 7 enthält Regeln zu wichtigen Produkten mit digitalen Elementen.** • Wichtige Produkte sind in Anhang III gelistet. Es erfolgt eine Unterscheidung zwischen Klasse 1 & 2 • Die Integration eines wichtigen Produkts macht das Gesamtprodukt nicht automatisch bewertungspflichtig • Konkretisierung zu wichtigen Produkten ist über die Durchführungsverordnung 2025/2392 erfolgt • Wichtige Produkte müssen das Konformitätsbewertungsverfahren aus Artikel 32, Abs. 2 und 3 umsetzen	11.12.27		X	X	
Art. 8	Kritische Produkte mit digitalen Elementen	**Art. 8 enthält Regeln zu kritischen Produkten mit digitalen Elementen.** • Kritische Produkte sind in Anhang IV gelistet (insb. Hardwaregeräte mit Sicherheitsboxen, Smart-Meter-Gateways und Chipkarten, einschließlich Sicherheitselemente) • Kritische Produkte brauchen ein EU-Cybersicherheitszertifikat als Nachweis für die Einhaltung der grundlegenden Cybersicherheitsanforderungen gemäß Anhang I	11.12.27		X	X	

Legende: Händler von Produkten | Hersteller von Produkten | Kritische Produkte | Wichtige Produkte | Sonstige Produkte

Bezug	Titel	Beschreibung	Datum	Produkte	Relevant für		
Art. 9	*Art. 9 (Konsultation der Interessenträger) enthält Regelungen auf EU-Ebene zur Einbindung von Stakeholdern bei der Vorbereitung von Maßnahmen zur Änderung und Durchführung des CRA*		*11.12.27*				
Art. 10	*Art. 10 (Ausbau der Kompetenzen in einem digitalen Umfeld mit Cyberabwehrfähigkeit) enthält Vorgaben für EU-Mitgliedsstaaten zur Förderung von Cybersicherheitskompetenzen zur Qualifizierung von Fachkräften*		*11.12.27*				
Art. 11	Allgemeine Produktsicherheit	**Art. 11 enthält Vorgaben für Produkte mit digitalen Elementen, die nicht von CRA erfasst werden.** • Für alle Sicherheitsaspekte, die CRA nicht abdeckt, greift die allgemeine Produktsicherheitsverordnung (Verordnung (EU) 2023/988)	11.12.27	⚠	X	X	
Art. 12	Hochrisiko-KI-Systeme	**Art. 12 enthält Vorgaben zu Wechselwirkungen zwischen CRA & KI-VO bei Hochrisiko-KI-Systemen.** • Standard-Produkte, die gleichzeitig Hochrisiko-KI-Systeme sind, gelten als konform mit Artikel 15 der KI-VO, wenn sie die Anforderungen des CRA aus Anhang I Teil 1 und 2 erfüllen und den Nachweis des Cybersicherheitsniveaus über die EU-Konformitätserklärung nach CRA erbringen • Für wichtige und kritische Produkte, die gleichzeitig Hochrisiko-KI-Systeme sind, müssen zwei Konformitätsbewertungen nach CRA und KI-VO gemacht werden.	11.12.27	⚠+⚠+⚠	X	X	
Kap. II	PFLICHTEN DER WIRTSCHAFTSAKTEURE UND BESTIMMUNGEN IN BEZUG AUF FREIE UND QUELLOFFENE SOFTWARE						

Art. 13	Pflichten der Hersteller	**Art. 13 enthält die Pflichten der Hersteller**
		• Hersteller müssen Produkte müssen gemäß Anhang I Teil 1 (Cybersicherheitsanforderungen) entwickeln
		• Hersteller müssen die Produkte einer Cybersicherheitsrisikoanalyse unterziehen
		  • Die Ergebnisse sind zu dokumentieren und regelmäßig zu aktualisieren
		  • Die Ergebnisse sind während des gesamten Produktlebenszyklus zu berücksichtigen.
		  • In der Risikoanalyse ist zu dokumentieren, welche Anforderungen aus Anhang I Teil 1 (Grundlegende Cybersicherheitsanforderungen) auf das Produkt anwenderbar sind und wie sie umgesetzt wurden
		  • In der Risikoanalyse ist zu dokumentieren, welche Anforderungen aus Anhang I Teil 2 (Schwachstellenmanagement) festgelegt sind
		  • In der Risikoanalyse ist zu dokumentieren, welche Maßnahmen ergriffen werden, damit das Produkt ein angemessenes Cybersicherheitsniveau erreicht
		  • Die Cybersicherheitsrisikoanalyse muss Teil der der technischen Dokumentation sein
		• Der Hersteller …
		  • trägt bei der Einbindung von Drittkomponenten, inkl. Open-Source-Software die Verantwortung, dass die Cybersicherheit des
		  • meldet Schwachstellen in Drittkomponenten dem jeweiligen Anbieter und sorgt für deren Behebung
		  • dokumentiert alle sicherheitsrelevanten Informationen und Schwachstellen seines Produkts und bezieht diese bei der Cybersicherheitsrisikoanalyse ein
		  • sorgt für ein angemessenes Schwachstellen- und Patchmanagement während der Produktlebensdauer
		  • fixiert den Support-Zeitraum in der technischen Dokumentation zum Produkt. Die Mindestsupportzeit beträgt 5 Jahre
		  • legt eine Strategie und Maßnahmen zur Kommunikation von Schwachstellen fest
		  • stellt sicher, dass Sicherheitsupdates mindestens 10 Jahre verfügbar bleiben
		  • kann ältere Versionen seines Produktes in einem Software-Archiv bereitstellen, sofern er über Risiken informiert
		  • muss eine Konformitätsbewertung durchführen und die CE-Kennzeichnung anbringen
		  • muss eine technische Dokumentation zu seinem Produkt erstellen
			11.12.27	⚠+⚠+⚠		X	

Legende: Händler von Produkten | Hersteller von Produkten | Kritische Produkte | Wichtige Produkte | Sonstige Produkte

Bezug	Titel	Beschreibung	Datum	Produkte	Relevant für		
		• muss technische Dokumentation und Konformitätsbewertung für mindestens 10 Jahre aufbewahren • stellt sicher, dass bei der Serienfertigung von Produkten die Konformität mit den Vorgaben des CRA gewahrt bleibt • stellt sicher, dass Produkte durch eine Produktkennzeichnung identifiziert werden können • stellt Kontaktinformationen bereit und richtet eine zentrale, leicht zugängliche Anlaufstelle für Nutzer und Schwachstellenmeldungen ein • stellt verständliche Anleitungen für sein Produkt bereit, die Informationen zu sicherer Installation, Betrieb und Verwendung Aufschluss geben und hält diese 10 Jahre verfügbar • stellt sicher, dass das Ende des Supportzeitraums transparent vor dem Kauf ersichtlich ist und der Nutzer bei Ablauf darüber unterrichtet wird • legt dem Produkt die EU-Konformitätserklärung oder vereinfachte Erklärung bei • ergreift bei Nicht-Konformität seines Produkts sofort Korrekturmaßnahmen • stellt die Zusammenarbeit mit Marktüberwachungsbehörden sicher und übermittelt alle relevanten Informationen					

Art. 14	Meldepflichten der Hersteller	**Art. 14 enthält die Meldepflichten zu Vorfällen mit Bezug zum Produkt.**
		• Aktive ausgenutzte Schwachstellen müssen dem zuständigen CSIRT und der ENISA gemeldet werden.
		  • Die Meldung erfolgt über eine einheitliche Meldeplattform
		  • Die Meldungen müssen die festgelegten Mindestinhalte des CRA enthalten
		  • Die Erstmeldung muss innerhalb von 24 h erfolgen
		  • Die vollständige Schwachstellenmeldung muss innerhalb von 72 h erfolgen
		  • Der Abschlussbericht muss spätestens 14 Tage nach Bereitstellung der Korrekturmaßnahmen vorliegen
		• Schwerwiegende Sicherheitsvorfälle müssen ebenfalls dem zuständigen CSIRT und der ENSIA gemeldet werden
		  • Schwerwiegende Sicherheitsvorfälle liegen vor, wenn Verfügbarkeit, Integrität, Authentizität oder Vertraulichkeit von sensiblen Daten oder wichtigen Funktionen betroffen sind oder es sich um einen böswilligen Angriff in Verbindung mit Schadcode handelt.
		  • Die Meldung erfolgt über eine einheitliche Meldeplattform
		  • Die Meldungen müssen die festgelegten Mindestinhalte des CRA enthalten
		  • Die Erstmeldung muss unverzüglich, spätestens nach 24 h erfolgen
		  • Die vollständige Schwachstellenmeldung muss innerhalb von 72 h erfolgen
		  • Der Abschlussbericht muss spätestens nach 1 Monat vorliegen
		• Hersteller müssen betroffene Nutzer über ausgenutzte Schwachstellen, schwerwiegende Sicherheitsvorfälle und über zu ergreifende Maßnahmen informieren
			Achtung, abweichendes Datum:
			
			11.09.26
				+ +		X	

Art. 15	Freiwillige Meldungen	**Art. 15 enthält Regeln zu freiwilligen Meldungen.** • Schwachstellen, Cyberbedrohungen, Beinahe-Vorfälle und Sicherheitsvorfälle können freiwillig gemeldet werden • Meldung erfolgt an ein CSIRT oder die ENISA • Es entstehen keine zusätzlichen Pflichten durch freiwillige Meldung	11.12.27	+ +	X	X	
Art. 16	*Art. 16 (Einrichtung einer einheitlichen Meldeplattform) enthält Regeln zur Einrichtung einer einheitlichen Meldeplattform durch die ENISA*		*11.12.27*				

Legende: Händler von Produkten | Hersteller von Produkten | Kritische Produkte | Wichtige Produkte | Sonstige Produkte

Bezug	Titel	Beschreibung	Datum	Produkte	Relevant für		
					Händler	Hersteller	
Art. 17	*Art. 17 (Sonstige Bestimmungen im Zusammenhang mit der Berichterstattung) enthält weitere Bestimmungen zur Berichterstattung durch ENISA und CSIRTS sowie zur Schwachstellendatenbank*		*11.12.27*				
Art. 18	Bevollmächtigte	**Art. 18 enthält Regeln zu Bevollmächtigten.** • Hersteller können für ausgewählte Aufgaben aus CRA, einen Bevollmächtigten benennen • Einzelne Kernpflichten aus Art. 13 (1–11, 12(1) und 14) können nicht übertragen werden	11.12.27	+ +	X	X	
Art. 19	*Art. 19 (Pflichten der Einführer) regelt die Pflichten der Einführer für das Inverkehrbringen und die Marktüberwachung für Produkte aus Nicht-EU-Ländern*		*11.12.27*				

Art. 20	Pflichten der Händler	**Art. 20 enthält Pflichten der Händler.**
		• Händler stellen Produkte nur mit gebührender Sorgfalt unter Berücksichtigung der Anforderungen des CRA bereit
		• Der Händler …
		  • prüft, ob folgende Informationen zum Produkt und alle erforderlichen Dokumente vorliegen
		  • CE-Kennzeichnung
		  • Identifikationskennzeichen (Typ-/Seriennummer)
		  • Herstellerangaben (Name, Adresse, Kontakt)
		  • Nutzerinformationen/Anleitungen (Anhang II)
		  • Support-Enddatum
		  • EU-Konformitätserklärung
		  • Ggf. Einführerangaben (Name, Adresse, Kontakt)
		  • prüft, ob alle grundlegenden Cybersicherheitsanforderungen und Anforderungen an das Schwachstellenmanagement gemäß Anhang I erfüllt sind, bevor er das Produkt auf dem Markt bereitstellt
		  • meldet erhebliche Cybersicherheitsrisiken an Hersteller und Marktüberwachungsbehörde
		  • sorgt dafür, dass Korrekturmaßnahmen ergriffen werden, oder nimmt das Produkt vom Markt
		  • informiert Hersteller und ggf. Marktüberwachungsbehörde über Schwachstellen im Produkt
		  • arbeitet mit der Marktüberwachungsbehörde zusammen
		  • informiert bei Erforderlichkeit die Nutzer des Produkts über die Einstellung der Betriebstätigkeit des Herstellers
			11.12.27	+ +	X		

Art. 21	Fälle, in denen die Pflichten der Hersteller auch für Einführer und Händler gelten	**Art. 21 legt fest, wann Händler und Einführer als Hersteller gelten.** Sie gelten als Hersteller, • wenn sie Produkte unter eigener Marke in Verkehr bringen • wenn sie Produkte wesentlich ändern.	11.12.27	+ +	X	X	
Art. 22	*Art. 22 (Sonstige Fälle, in denen die Pflichten der Hersteller gelten) erweitert die Fälle, in denen Herstellerpflichten gelten: Jede natürliche oder juristische Person, die ein Produkt wesentlich ändert und bereitstellt, gilt als Hersteller*		*11.12.27*				
Art. 23	Identifizierung der Wirtschaftsakteure	**Art. 23 enthält Regeln zur Identifizierung von Wirtschaftsakteuren.** • Hersteller, Händler, Einführer, etc. müssen auf behördliche Anfrage ihre Liefer- und Abgabekette benennen • Informationen über Bezugs- und Abgabewege sind mindestens 10 Jahre vorzuhalten	11.12.27	+ +	X	X	
Art. 24	Pflichten der Verwalter quelloffener Software	**Art. 24 enthält Pflichten der Verwalter quelloffener Software.** Sie müssen … • eine dokumentierte Cybersicherheitsstrategie erstellen • ein angemessenes Schwachstellen- und Patchmanagement implementieren • mit Marktüberwachungsbehörden zur Risikominderung zusammenarbeiten • auf Verlangen Unterlagen bereitstellen und ggf. die Meldepflichten aus Art. 14 umsetzen	11.12.27	+ +			X

Legende: Händler von Produkten | Hersteller von Produkten | Kritische Produkte | Wichtige Produkte | Sonstige Produkte

Bezug	Titel	Beschreibung	Datum	Produkte	Relevant für		
Art. 25	*Art. 25 (Sicherheitsbescheinigung für freie und quelloffene Software) enthält Vorgaben, die die Kommission dazu berechtigen, freiwillige Sicherheits-zertifizierungsprogramme einzuführen, die es erleichtern, die Konformität zu Cybersicherheitsanforderungen bewerten*		*11.12.27*				
Art. 26	*Art. 26 (Leitlinien) enthält Regeln und Vorgaben zur Erstellung weiterer Leitlinien zur Umsetzung des CRA durch die EU*		*11.12.27*				
Kap. III	KONFORMITÄT DES PRODUKTS MIT DIGITALEN ELEMENTEN						
Art. 27	Konformitätsvermutung	**Art. 27 regelt die Konformitätsvermutung für CRA-relevante Produkte.** • Produkte gelten als konform mit den Cybersicherheitsanforderungen aus Anhang I, wenn sie harmonisierten EU-Normen oder veröffentlichten technischen Spezifikationen entsprechen • Die EU legt Normen und technische Spezifikationen per Durchführungsrechtsakt fest • EU-Konformitätserklärungen oder EU-Cybersicherheitszertifikate können die CRA-Konformität ebenfalls nachweisen	11.12.27	+ +		X	
Art. 28	EU-Konformitätserklärung	**Art. 28 regelt die EU-Konformitätserklärung für CRA-relevante Produkte.** • Der Hersteller stellt die EU-Konformitätserklärung gemäß Art. 13 (12) und bestätigt damit die Erfüllung der Cybersicherheitsanforderungen aus Anhang I • Die EU-Konformitätserklärung folgt den Vorgaben aus Anhang V bzw. VI für die vereinfachte Version und enthält die Konformitätsbewertung nach Anhang VIII	11.12.27	+ +		X	
Art. 29	*Artikel 29 (Allgemeine Grundsätze der CE-Kennzeichnung) beschreibt die allgemeinen Grundsätze der CE-Kennzeichnung gemäß Artikel 30 der Verordnung (EG) Nr. 765/2008.*		*11.12.27*				
Art. 30	Vorschriften und Bedingungen für die Anbringung der CE-Kennzeichnung	**Art. 30 regelt die Vorgaben für die CE-Kennzeichnung von CRA-Produkten.** • Die CE-Kennzeichnung muss sichtbar, lesbar und dauerhaft angebracht sein (auf Produkt und Verpackung oder auf der EU-Konformitätserklärung oder Website)	11.12.27	+ +		X	
Art. 31	Technische Dokumentation	**Art. 31 regelt die technische Dokumentation für CRA-Produkte.** • Hersteller müssen eine technische Dokumentation gemäß Anhang VII erstellen und fortlaufend aktualisieren • Die technische Dokumentation weist nach, wie die Anforderungen aus Anhang I erfüllt werden • Unterliegt das Produkt mehreren EU-Rechtsakten, reicht eine gemeinsame technische Dokumentation aus, die die jeweiligen Mindestinhalte vorweist.	11.12.27	+ +		X	
Art. 32	Konformitätsbewertungsverfahren für Produkte mit digitalen Elementen	**Art. 32 regelt die Konformitätsbewertung für CRA-Produkte.** • Hersteller müssen eine Konformitätsbewertung ihres Produktes durchführen, um festzustellen, ob alle grundlegenden Cybersicherheitsanforderungen aus Anhang I erfüllt sind • Dafür stehen verschiedene Verfahren zur Auswahl: interne Kontrolle, EU-Baumusterprüfung mit Fertigungs-kontrolle, umfassende Qualitätssicherung oder ein europäisches Cybersicherheitszertifikat • Für wichtige Produkte (Klasse I/II) und kritische Produkte gelten strengere Verfahren mit verpflichtender Prüfung durch Dritte bzw. Zertifizierung • Open-Source-Produkte können die Verfahren nutzen, wenn die technische Dokumentation öffentlich zu-gänglich ist.	11.12.27	+ +		X	
Art. 33	*Art. 33 (Unterstützungsmaßnahmen für Kleinstunternehmen sowie kleine und mittlere Unternehmen, einschließlich Start-up-Unternehmen) enthält Regelungen für die Mitgliedsstaaten, wie sie KMU bei Schulung, Beratung und Konformitätsbewertung unterstützen können.*		*11.12.27*				
Art. 34	*Art. 34 (Abkommen über die gegenseitige Anerkennung) enthalt Regelungen wie die EU Konformitätsbewertungen aus Drittländern anerkennen kann*		*11.12.27*				
Kap. IV	NOTIFIZIERUNG VON KONFORMITÄTSBEWERTUNGSSTELLEN						
Art. 35 – Art. 51	*Art. 35 – Art. 51 enthalten Vorgaben für die Mitgliedsstaaten zur Benennung der notifizierenden Stellen und Anforderungen an die Konformitätsbewer-tungsstellen*		*11.06.26*				
Kap. V	MARKTÜBERWACHUNG UND DURCHSETZUNG						

Legende: Händler von Produkten | Hersteller von Produkten | Kritische Produkte | Wichtige Produkte | Sonstige Produkte

Bezug	Titel	Beschreibung	Datum	Produkte	Relevant für		
Art. 52	*Art. 52 (Marktüberwachung und Kontrolle von Produkten mit digitalen Elementen auf dem Unionsmarkt) enthält Vorgaben für die Mitgliedsstaaten zur Benennung der Marktüberwachungsbehörden sowie an deren Arbeitsweise*		*11.12.27*				
Art. 53	*Art. 53 (Zugang zu Daten und zur Dokumentation) regelt den behördlichen Zugriff auf Daten für die Konformitätsbewertung.*		*11.12.27*				
Art. 54	Nationale Verfahren für Produkte mit digitalen Elementen, die ein erhebliches Cybersicherheitsrisiko bergen	**Art. 54 regelt das nationale Verfahren, wenn ein Produkt ein erhebliches Cybersicherheitsrisiko birgt** • Stellt eine Marktüberwachungsbehörde ein mögliches erhebliches Cybersicherheitsrisiko fest, führt sie eine Konformitätsprüfung durch und kann Korrekturmaßnahmen verlangen • Wirtschaftsakteure (Hersteller, Händler, Einführer, etc.) müssen dann innerhalb einer vorgegebenen Frist die Konformität herstellen oder das Produkt zurückrufen • Erfolgen keine Korrekturen, können nationale Behörden Beschränkungen oder Verbote aussprechen und das Produkt vom Markt nehmen	11.12.27	+ +	X	X	
Art. 55	*Art. 55 (Schutzklauselverfahren der Union) regelt, wie in Europa vorzugehen ist, wenn einzelne Mitgliedstaaten Maßnahmen gegen ein Produkt ergreifen, die Auswirkungen auch auf andere europäische Länder haben.*		*11.12.27*				
Art. 56	*Art. 56 (Verfahren auf Unionsebene für Produkte mit digitalen Elementen, die ein erhebliches Cybersicherheitsrisiko bergen) regelt das unionsweite Verfahren und den Umgang mit Produkten, die ein erhebliches Cybersicherheitsrisiko bergen. Die Handlungsoptionen der Europäischen Kommission werden konkretisiert.*		*11.12.27*				
Art. 57	Konforme Produkte mit digitalen Elementen, die ein erhebliches Cybersicherheitsrisiko bergen	**Art. 57 enthält Vorgaben für den Umgang mit konformen Produkten, die dennoch erhebliche Cybersicherheitsrisiken bergen.** • Für CRA-konforme Produkte, die erhebliche Risiken für Gesundheit, Grundrechte, kritische IKT-Dienste oder Aspekte des Schutzes öffentlicher Interessen aufweisen, können weitere Maßnahmen angeordnet werden • Die jeweiligen Wirtschaftsakteure (Hersteller, Händler, etc.) müssen innerhalb der vorgegebenen Frist geeignete Korrekturmaßnahmen umsetzen • Bei fortbestehenden Risiken kann die Europäische Kommission selbst eingreifen.	11.12.27	+ +	X	X	
Art. 58	Formale Nichtkonformität	**Art. 58 enthält Regeln zum Umgang mit Non-Compliance** • CE-Kennzeichnung fehlt/ wurde nicht korrekt angebracht • EU-Konformitätserklärung fehlt/ wurde nicht ordnungsgemäß erstellt • Technische Dokumentation fehlt oder ist nicht vollständig • Kennnummer der notifizierenden Stelle fehlt • Werden diese Mängel nicht behoben, kann der Mitgliedstaat das Produkt vom Markt nehmen, zurückrufen oder seine Bereitstellung untersagen.	11.12.27	+ +	X	X	X
Art. 59	*Art. 59 (Gemeinsame Tätigkeiten der Marktüberwachungsbehörden) regelt gemeinsame Aktivitäten der Marktüberwachungsbehörden und Zusammenarbeitsbedingungen*		*11.12.27*				
Art. 60	*Art. 60 (Koordinierte Kontrollen (Sweeps)) regelt koordinierte Kontrollen („Sweeps“) durch Marktüberwachungsbehörden. Dabei führen die Behörden zeitgleiche, koordinierte Kontrollen durch, ggf. auch mit Testkäufen unter falscher Identität.*		*11.12.27*				
Kap. VI	ÜBERTRAGENE BEFUGNISSE UND AUSSCHUSSVERFAHREN						
Art. 61/ Art. 62	*Art. 61 und 62 (Ausübung der Befugnisübertragung + Ausschussverfahren) regelen die Bedingungen und Verfahren, unter denen weitere delegierte Rechtsakte zum CRA erlassen dürfen*		*11.12.27*				
Kap. VII	VERTRAULICHKEIT UND SANKTIONEN						
Art. 63	*Art. 63 (Vertraulichkeit) enthält Vorgaben, dass alle beteiligten Stellen vertrauliche Informationen schützen müssen, insbesondere Geschäftsgeheimnisse, geistiges Eigentum, Ermittlungen und Sicherheitsinteressen*		*11.12.27*				

Legende: Händler von Produkten | Hersteller von Produkten | Kritische Produkte | Wichtige Produkte | Sonstige Produkte

Bezug	Titel	Beschreibung	Datum	Produkte	Relevant für		
Art. 64	Sanktionen	**Art. 64 enthält die Grundsätze zur Sanktionierung von Verstößen gegen den CRA.** • Schwere Verstöße (insb. gegen Anhang I sowie gegen Herstellerpflichten nach Art. 13 und 14): Bußgelder bis zu 15 Mio. EUR oder 2,5 % des weltweiten Jahresumsatzes • Weitere Pflichtverstöße: bis zu 10 Mio. EUR oder 2 % des weltweiten Jahresumsatzes geahndet werden. • Falsche oder irreführende Angaben gegenüber Behörden: 5 Mio. EUR oder 1 % des Umsatzes kosten. • Ausnahmen gelten für Kleinst- und Kleinunternehmen bei bestimmten Meldefristen (Art. 14 Abs. 2a/4a) sowie für Verwalter quelloffener Software	11.12.27	+ +	X	X	X
Art. 65	*Art. 65 (Verbandsklagen) regelt die Möglichkeit von Verbandsklagen gegen CRA-Zuwiderhandlungen.*		*11.12.27*				
Kap. VIII	ÜBERGANGS- UND SCHLUSSBESTIMMUNGEN						
66 - 68	*Art. 66 – 68 enthalten Änderungen der Verordnung (EU) 2019/1020, der Richtlinie (EU) 2020/1828, und der Verordnung (EU) Nr. 168/2013*		*11.12.27*				
Art.69	Übergangsbestimmungen	Art. 69 regelt die Übergangsbestimmungen des CRA. • Bestehende EU-Baumusterprüfbescheinigungen bleiben bis 11. Juni 2028 gültig. • Produkte, die vor dem 11. Dezember 2027 in Verkehr gebracht wurden, müssen den CRA nur bei wesentlichen Änderungen erfüllen. • Die Meldepflichten aus Art. 14 gelten für alle bestehenden Produkte ab dem 11. Dezember 2027.	11.12.27	+ +	X	X	X
Art. 70	*Art. 70 (Bewertung und Überprüfung Inkrafttreten und Geltungsbeginn) regelt die Bewertung und Überprüfung des CRA ab 2030*		*11.12.27*				
Art. 71	Inkrafttreten und Geltungsbeginn	Art. 71 regelt das Inkrafttreten und den Geltungsbeginn des CRA. • Die Verordnung gilt ab 11. Dezember 2027. • Art. 14 gilt bereits ab 11. September 2026, • Kapitel IV (Art. 35–51) gilt ab 11. Juni 2026.	11.12.27	+ +	X	X	X
• Anhänge							
Anh. I	GRUNDLEGENDE CYBERSECURITYANFORDERUNGEN Teil 1: • (1) Angemessenes Cybersicherheitsniveau über den gesamten Produktlebenszyklus • (2a) Keine bekannten ausnutzbaren Schwachstellen beim Inverkehrbringen • (2b) Sichere Standardkonfiguration und Möglichkeit zum Zurücksetzen • (2c) Regelmäßige und sichere Sicherheitsupdates (auch automatisiert möglich) • (2d) Schutz vor unbefugtem Zugriff und Erkennung von Zugriffen • (2e) Schutz der Vertraulichkeit von Daten (z. B. durch Verschlüsselung) • (2f) Schutz der Integrität von Daten, Programmen und Konfigurationen • (2g) Verarbeitung nur notwendiger Daten (Datenminimierung) • (2h) Sicherstellung der Verfügbarkeit wesentlicher Funktionen • (2i) Keine Beeinträchtigung anderer Systeme oder Netze • (2j) Möglichst geringe Angriffsfläche durch sicheres Design • (2k) Begrenzung der Auswirkungen von Sicherheitsvorfällen • (2l) Protokollierung und Überwachung sicherheitsrelevanter Vorgänge • (2m) Sichere und vollständige Löschung von Daten und Einstellungen					

Legende: Händler von Produkten | Hersteller von Produkten | Kritische Produkte | Wichtige Produkte | Sonstige Produkte

Bezug	Titel	Beschreibung	Datum	Produkte	Relevant für
	Teil 2	• (1) Ermittlung und Dokumentation von Configuration Items (Software-Stückliste, Abhängigkeiten sowie Schwachstellen • (2) Schnelle Behebung von Schwachstellen durch Bereitstellung von Sicherheitsupdates • (3) Regelmäßige Sicherheitsprüfung der Produkte • (4) Veröffentlichung von Informationen zu behobenen Schwachstellen zu Art, Auswirkung und Schwere • (5) Koordinierte Offenlegung von Schwachstellen • (6) Einrichtung einer Kontaktstelle für Schwachstellenmeldungen • (7) Bereitstellung von Mechanismen zur Verteilung von Sicherheitspatches • (8) Kostenlose und zeitnahe Bereitstellung von Sicherheitsupdates			
Anh. II		INFORMATIONEN UND ANLEITUNGEN FÜR DEN NUTZER • Herstelleridentität und Kontaktinformationen • Zentrale Meldestelle für Schwachstellen • Eindeutige Identifikation des Produkts • Zweckbestimmung und Sicherheitsmerkmale des Produkts • Hinweise zu vorhersehbaren Nutzungs- und Sicherheitsrisiken • Zugang zur EU-Konformitätserklärung • Art der Sicherheitsunterstützung und Unterstützungszeitraum • Anleitungen zur sicheren Nutzung über den gesamten Produktlebenszyklus • Zugriff auf die Software-Stückliste			
Anh. III		WICHTIGE PRODUKTE MIT DIGITALEN ELEMENTEN • IAM- & PAM-Tools inkl. ZuKo-Tools • Browser • Passwort-Manager • Tools für Malware-Detection • VPM-Tools • Netzmanagementsysteme • SIEM-Systeme • Bootmanager • PKI und Tools für Zertifikateerstellugn • API (physische und logische) • Betriebssysteme • Router, Modems und Switches • Prozessoren • Mikrocontroller • Sicherheitsrelevante Schaltsysteme • Virtuelle Assistenten (KI) • Sicherheitsrelevante Smart Home Produkte • Spielzeug mit Internetverbindung • Wearables für Gesundheitsüberwachung			

Bezug	Titel	Beschreibung	Datum	Produkte	Relevant für

		• Wichtige Produkte gemäß Anhang III (Klasse 2) sind:
		  • Virtualisierungs-Systeme
		  • Firewall, IDS- und IPS-Systeme
		  • Manipulationssichere Prozessoren
		  • Manipulationssichere Mikrocontroller			

Anh. IV		KRITISCHE PRODUKTE MIT DIGITALEN ELEMENTEN • Hardwaregeräte mit Sicherheitsboxen • Smart-Meter-Gateways • Chipkarten oder ähnliche Geräte, einschließlich Sicherheitselemente			
Anh. V		EU-KONFORMITÄTSERKLÄRUNG			
Anh. VI		VEREINFACHTE EU-KONFORMITÄTSERKLÄRUNG			
Anh. VII		INHALT DER TECHNISCHEN DOKUMENTATION • Allgemeine Produktbeschreibung und Nutzerinformationen • Beschreibung von Konzeption, Entwicklung, Herstellung und Schwachstellenmanagement • Dokumentierte Cybersicherheitsrisikobewertung über den gesamten Lebenszyklus • Begründung und Herleitung des Unterstützungszeitraums • Nachweis der angewandten Normen, Spezifikationen oder Zertifizierungsschemata • Test- und Prüfberichte zur Cybersicherheitskonformität • EU-Konformitätserklärung • Software-Stückliste auf Anforderung der Marktüberwachung			
Anh. VIII		KONFORMITÄTSBEWERTUNGSVERFAHREN • Teil I: Internes Kontrollverfahren (Modul A): Eigenverantwortliche Konformitätsbewertung durch den Hersteller • Teil II: EU-Baumusterprüfung (Modul B): Externe Prüfung der technischen Konzeption durch eine notifizierte Stelle • Teil III: Konformität mit dem Baumuster (Modul C): Interne Fertigungskontrolle nach erfolgreicher Baumusterprüfung • Teil IV: Umfassende Qualitätssicherung (Modul H): Ganzheitliches Qualitätssicherungssystem mit externer Überwachung			