2026 CAMPUS TAGE

DSN Akademie

10 Jahre DSGVO

Und jetzt?
Gemeinsam weiterdenken!

DSN Akademie

CRA – Cybersicherheit als Rechtspflicht

Falko Klages / Dominik Bleckmann

www.dsn-group.de

DSN Akademie

Falko Klages, Volljurist
Senior Berater

Dominik Bleckmann, Volljurist
Prokurist | Leiter Compliance

datenschutz nord Gruppe
T +49(0)421 69 66 32 329 / 349
E-Mail fklages@datenschutz-nord.de

www.dsn-group.de

Agenda

DSN Akademie

1. Einordnung
2. Wer ist wie betroffen?
3. Sinn, Zweck & Erwägungsgründe
4. Produkthaftung trifft Cybersicherheit
5. Handlungsfelder & Vorgehen

1. Einordnung

Der digitale Rechtskatalog der EU

Schnellübersicht

Inhalt CRA

„Alle Produkte, die in der EU verkauft werden und „digitale Elemente" enthalten, müssen den Anforderungen des CRA entsprechen."
- BSI

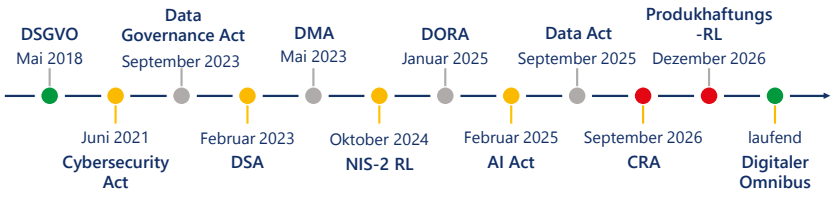
CE-Kennzeichnungspflicht für digitale Produkte

(Quelle: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Cyber_Resilience_Act/cyber_resilience_act_node.html)

- Was umfasst „alle Produkte"?
- Was heißt „verkauft"?
- Was sind „digitale Elemente"?
- Was sind die Anforderungen des CRA?

Zeitstrahl (Auswahl)

Sortiert nach erster Geltung



Systematik der Regelungen

Welle 1 (2016-19) *„Wer darf was?"*	**Welle 2 (2022-23)** *„Wie funktioniert der digitale Markt?"*	**Welle 3 (2024-27)** *„Was muss ein digitales Produkt?"*
DSGVO	NIS-2	CRA
Cybersecurity Act	DORA	AI Act
(eIDAS 1.0)	CER	Produkthaftungs-RL
	DSA / DMA	MaschinenVO
	Data Act	(Digitaler Omnibus)

Systematik der Regelungen

- Durchsetzung digitaler Rechte ohne direkte Handhabe erschwert
- Welle 3 schließt die Lücke zwischen Verkäufer & Käufer / Bereitsteller & Verwender
- CRA anders strukturiert als die (meisten) bisherigen Gesetze:
- Hersteller haftet für gesamten Produktzyklus

Vergleichstabelle

	DSGVO	NIS-2	CRA
Adressat	Datenverarbeiter	Betreiber	Hersteller
Gegenstand	Daten	Organisation	Produkt
Schwellenwert	Nein	50 MA/10 Mio. €	**Nein**
Branchenfilter	Nein	Ja (Sektoren)	**Nein**
Lebenszyklus	Nein	Nein	**Ja**

Hersteller haftet für (auch digitale) Produkte von Herstellung bis zum End-of-Support!

2. Wer ist wie betroffen?

Persönlicher Anwendungsbereich

Das Produkt entscheidet

Beispiele für Betroffenheit

- Softwarehersteller, insb. auch von On-Premise-Produkten
- Maschinenbauer mit vernetzten Produkten (z.B. SPS/SCADA)
- IT-Dienstleister mit Produktvertrieb im eigenen Namen
- EU-Importeure vernetzter Produkte
- Händler, die Produkte wesentlich modifizieren oder unter eigener Marke verkaufen

Das Produkt entscheidet

Beispiele für betroffene Produktarten

- **vernetzte Verbraucherprodukte:** Smartphones, Laptops, Smart-Home-Geräte, Smartwatches, Router und vernetztes Spielzeug, aber auch Wärmepumpen, Photovoltaik-Anlagen und Pumpensteuerungen
- **Industrielle und B2B-Software:** Betriebssysteme, industrielle Automatisierungssoftware, Passworthager, Firewalls und Mikroprozessoren
- **Kritische Infrastrukturen:** Produkte der Klasse I und II wie Smart-Meter-Gateways oder IIoT-Anwendungen (Industrial Internet of Things).
- **Ausnahmen**: Medizintechnik, Luftfahrt und Kraftfahrzeuge u. a. (s. u.)

Rollenbestimmung

Wer sind sie für ihr Produkt?

- Private Label:

volle Herstellerpflichten (Art. 13 CRA)

- Wesentliche Modifikation:

ebenfalls volle Herstellerpflichten (Art. 21 CRA)

- Konzerninterne Lieferung an rechtlich selbstständige Tochtergesellschaft:

volle Herstellerpflichten (Erwägungsgrund 15)

Ausnahmen (lex specialis derogat legi generali)

- Medizinprodukte (MDR / IVDR), EU 2017/ 745
Nur für **Kernprodukt.**
Nicht: Begleit-Apps, Cloud-Dienste, Diagnostik

- In-vitro-Diagnostika, EU 2017/ 746
- Luftfahrtprodukte, EU 2018/ 1139
- Marineausrüstung, EU 2014/ 90

- Kraftfahrzeuge und Automotive (UN WP.29), EU 2019/ 2144
Nur für **typengenehmigte Komponenten.**
Nicht: Aftermarket-Produkte, Diagnose, Flottenmanagement

- Dual-Use / Verteidigung
Nur bei **ausschließlicher Verteidigungswidmung.**

- Reine SaaS
Nur ohne **installierbare Komponenten.**
Nicht: Clients, Agenten, zusätzliche Downloads

Risikoklassen

1. Standardprodukte (Default / Geringes Risiko)

Diese Kategorie umfasst den **Großteil (ca. 90 %) aller digitalen Produkte** auf dem Markt. [ ]
Regelung: Der Hersteller führt die Konformitätsbewertung eigenständig durch (**Selbstzertifizierung**) und bringt das CE-Kennzeichen an.
Produktbeispiele: Smart-Home-Geräte (z. B. smarte Lampen, Kühlschränke), Smart-TVs, Spielekonsolen, Fitness-Tracker, Textverarbeitungs-Software, PC-Spiele, Fotobearbeitungs-Apps und einfache IoT-Sensoren.

2. Wichtige Produkte – Klasse I (Mittleres Risiko)

Hierbei handelt es sich um Produkte mit funktionaler Relevanz für die allgemeine Cybersicherheit, deren Kompromittierung bereits spürbare Schäden anrichten kann.
Regelung: Eine Selbstzertifizierung ist **nur dann zulässig**, wenn der Hersteller bestehende harmonisierte EU-Normen vollständig anwendet. Fehlen diese Standards, muss eine benannte externe Stelle (Notified Body) die Prüfung übernehmen.
Produktbeispiele: Standalone-Browser, Passwortmanager, VPN-Software, Router und Netzwerk-Switches für den Heimgebrauch sowie Identitäts- und Zugangskontrollsysteme.

Risikoklassen

3. Wichtige Produkte – Klasse II (Höheres Risiko)

Diese Klasse enthält Produkte, die eine kritische Sicherheitsfunktion erfüllen oder tief im System verankert sind. Sicherheitsvorfälle in dieser Klasse haben weitreichende, potenziell kritische Auswirkungen.
Regelung: Eine reine Selbstzertifizierung ist ausgeschlossen. Es ist **zwingend eine externe Konformitätsbewertung** durch eine unabhängige Prüfstelle erforderlich.
Produktbeispiele: Betriebssysteme (für PCs, Server und Smartphones), industrielle Firewalls, Router für den industriellen Einsatz, Hypervisoren und Container-Runtime-Systeme sowie manipulationssichere Mikroprozessoren.

4. Kritische Produkte (Hochkritisch / Anhang IV)

Diese Produkte sind für die Aufrechterhaltung essenzieller gesellschaftlicher Funktionen und hochsensibler Infrastrukturen von zentraler Bedeutung.
Regelung: Es gelten die **strengsten Zertifizierungsauflagen** des gesamten CRA. Eine lückenlose Überwachung durch staatlich benannte Stellen ist Pflicht.
Produktbeispiele: Smart-Meter-Gateways (intelligente Stromzähler), Hardware-Sicherheitsmodule (HSM), elektronische Identitätsausweise (Smartcards/Secure Elements) und zentrale Steuerungskomponenten für kritische Infrastrukturen (KRITIS).

3. Sinn, Zweck & Erwägungsgründe

Sachlicher Anwendungsbereich & Auswahl an Einzelanforderungen

Grundsätzliche Anwendung

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.

- Auf dem Markt bereitgestellt
- Produkt mit digitalen Elementen
- Gerichtet auf/ verwendbar für eine Datenverbindung

Horizont der Herstellerhaftung

Art. 13 Abs. 3 CRA

(3) Die Bewertung des Cybersicherheitsrisikos wird während eines gemäß Absatz 8 festzulegenden Unterstützungszeitraums dokumentiert und gegebenenfalls aktualisiert. Diese Bewertung des Cybersicherheitsrisikos umfasst mindestens eine Analyse der Cybersicherheitsrisiken auf der Grundlage der Zweckbestimmung und der vernünftigerweise vorhersehbaren Verwendung des Produkts mit digitalen Elementen, wie der Betriebsumgebung oder der zu schützenden Anlagen, wobei die voraussichtliche Nutzungsdauer des Produkts berücksichtigt wird. In der Bewertung des Cybersicherheitsrisikos wird angegeben, ob und gegebenenfalls in welcher Weise die Sicherheitsanforderungen gemäß Anhang I Teil I Nummer 2 auf das einschlägige Produkt mit digitalen Elementen anwendbar sind und wie diese Anforderungen auf der Grundlage der Bewertung des Cybersicherheitsrisikos umgesetzt werden. Ferner ist anzugeben, wie der Hersteller Anhang I Teil I Nummer 1 anzuwenden hat und welche Anforderungen an die Behandlung von Schwachstellen in Anhang I Teil II festgelegt sind.

- Risikoanalyse muss die „**vernünftigerweise vorhersehbare Verwendung**“ berücksichtigen!
- Risikoanalyse bezogen nur auf die beabsichtigte Verwendung ist **unzureichend!**

Kostenlose Updates als Rechtspflicht

Art. 13 Abs. 8 CRA:

> (8) Wenn sie ein Produkt mit digitalen Elementen in den Verkehr bringen und während der erwarteten Produktlebensdauer und des Unterstützungszeitraums stellen die Hersteller sicher, dass Schwachstellen dieses Produkts, einschließlich seiner Komponenten, wirksam und im Einklang mit den grundlegenden Cybersicherheitsanforderungen in Anhang I Teil II behandelt werden.

- Verantwortung für Produkt endet nicht bei on-premise Einrichtung beim Endkunden
- Bestimmung des Unterstützungszeitraums vollständig produktabhängig, **aber mindestens 5 Jahre,** sofern das Produkt nicht nach allgemeiner Erwartung weniger lang verwendet wird**.**
- Notwendige Updates müssen bereitgestellt werden, um dauerhaft Sicherheitsanforderungen des Anhangs zu gewährleisten
- Bei Schwachstellen ist eine Nachbesserung **unverzüglich** bereitzustellen (Art. 13 Abs. 6 CRA i.V.m. Anhang 1 Teil 2 Nr. 2)

Wesentliche Änderung als Dauerprozess

Art. 3 Abs. Nr. 30 CRA:

> 30. „wesentliche Änderung" eine Änderung des Produkts mit digitalen Elementen n
> auf die Konformität des Produkts mit den grundlegenden Cybersicherheitsanfor
> oder zu einer Änderung des bestimmungsgemäßen Zwecks, für den das Produk

Leitlinien darüber, was eine wesentliche Softwareänderung darstellt, werden von der EU-Kommission werden erwartet!

Erwägungsgrund 39:
- Digitale Produkte können durch Softwareupdates wesentlich geändert werden, insb. neue Funktionen
- Ausnahme: Sicherheitsupdates (die Sicherheit erhöhen), Barrierefreiheit

Fazit: Bei **jeglicher Einwirkung** auf Produkt muss auf Quellcode-Ebene die Risikoanalyse **aktualisiert** werden!

4.

Produkthaftung trifft Cybersicherheit

Interdisziplinäre Anforderungen & die neue Produkthaftungsrichtlinie

Produkthaftung: Hardware zu Software

Amtsblatt der Europäischen Union — DE — Reihe L

2024/2853 — 18.11.2024

RICHTLINIE (EU) 2024/2853 DES EUROPÄISCHEN PARLAMENTS UND DES RATES

vom 23. Oktober 2024

über die Haftung für fehlerhafte Produkte und zur Aufhebung der Richtlinie 85/374/EWG des Rates

(Text von Bedeutung für den EWR)

- Bislang: Produkthaftungsrichtlinie von 1985
- Umstritten, ob Software überhaupt „Produkt" im Sinne des Haftungsrechts („bewegliche Sache")
- (Fast) zeitgleich mit CRA Veröffentlichung der neuen EU-Produkhaftungsrichtlinie
- Zivilrechtliche Sanktionierung von Verstößen gegen Pflichtenkatalog des CRA
- Umsetzung bis 09. Dezember 2026

Definition „Produkt“
Inklusion jeglicher Software

- Art. 4 Nr. 1 & Erwägungsgrund 13 nennen: Betriebssysteme, Firmware, Computerprogramme, Apps, KI-Systeme
- Erfasst sind: verkaufte, kostenlose, heruntergeladene und als SaaS bereitgestellte Software
- Auch fehlerhafte Softwareupdates nach Inverkehrbringen begründen Haftung

- Gleichzeitige Haftung möglich insb. bei KI-Produkten nach CRA, Produkthaftungsrichtlinie & AI Act

- Ausnahme: **reine** Dienstleistungen (Abgrenzung!)

Fehlerbegriff
CRA-Verstoß als Produktfehler

Art. 7 Abs. 1: Verstoß gegen unionsrechtliche Sicherheitsanforderung (= CRA) erfüllt unmittelbar Tatbestand eines „Fehlers“ (s. auch Art. 7 Abs. 2)

Beispiele:
- Fehlende Sicherheitsupdates
- unzureichendes Schwachstellenmanagement
- Fehlende Secure-by-Default-Konfiguration
- Cybersicherheitsmängel nach Inverkehrbringen

Fazit: Erfüllung Anforderungen CRA ist stärkster verfügbarer Schutz vor Haftung

Beweislast
Offenlegungspflichten & Tatsachenvermutung

Art. 10 Abs. 1: Kläger muss Fehler, Schaden & Kausalzusammenhang beweisen.

Aber: Art. 10 Abs. 2 sieht **gesetzliche Tatsachenvermutung** vor!
- Vermutung eines Fehlers bei Verstoß gegen Produktsicherheitsanforderungen (CRA)!
- Art. 9 beinhaltet Verpflichtungsmöglichkeit des Herstellers auf Offenlegung interner Unterlagen (insb. technische Dokumentation, Risikoanalysen, Schwachstellenberichte); Verweigerung führt unmittelbar zur Annahme der Fehlerhaftigkeit
- Kommt in der Praxis einer Beweislastumkehr nahezu gleich.

Fazit: Prozessuales Unterliegen bei fehlender CRA-Dokumentation noch vor Eröffnung der Beweisaufnahme absehbar.

Haftungsadressat
Erweiterter Kreis

Analog zur persönlichen Anwendbarkeit des CRA, jedoch mit Erweiterung:
- Hersteller haften primär (Softwareentwickler ausdrücklich betroffen)
- Akteure, die Produkte wesentlich verändern

Subsidiäre Haftung:
- Importeur
- EU-Bevollmächtigte
- Fulfillment-Dienstleister

Haftungsumfang

§ 10 ProdHaftG (a.F.): Höchstbetrag 85 Mio.

EU-Produkthaftungsrichtlinie:
- Kein Haftungshöchstbetrag (Zivilrecht)
- Selbstbehalt iHv. 500€ entfällt

Risikolandschaft

Ebene 1 – Behördlich (CRA):
Bußgeld bis 15 Mio. € oder 2,5 % Jahresumsatz (Konzern)

Ebene 2 – Zivilrechtlich (EU-Produkthaftungsrichtlinie):
Schadensersatz für jeden Betroffenen unbegrenzt der Höhe nach

Ebene 3 – gute Nachrichten:
Keine eigene persönliche Haftung der Geschäftsführung vorgesehen (vgl. § 38 Abs. 1 BSIG); Durchgriffshaftung nur in Ausnahmefällen nach allgemeinen Grundsätzen.

5. Handlungsfelder & Vorgehen

Best Practices

Dringender Handlungsbedarf

Priorisierung

Priorität 1: Meldefristen ab 11.09.2026 beachten
- Incident-Response-Prozess aufbauen
- Verantwortliche Personen benennen
- ENISA-Meldeplattform anbinden

Priorität 2: Betroffenheit abschließend klären (Ende 2026)
- Produktportfolio analysieren
- Rolle & Klassifizierung bestimmen
- Ausnahmen prüfen

Priorität 3: Vollständige Konformität (Dezember 2027)
- SBOM
- Risikoanalyse(n)
- Technische Dokumentation
- Konformitätsbewertung
- CE-Kennzeichnung

Cybersecurity Versicherung

- Mittlerweile umfassende Risikoprüfungen: intensive Due Diligence (ISO27001 Standard)
- Deckungssumme orientiert an diversen Merkmalen. Bußgeld-Bemessungsgrenzen von DSGVO & weiteren Gesetzen relevant (z.B. 2-4% des Jahresumsatzes)
- Aber: steigender Trend wegen hoher Lösungsgeldforderungen!
- Mittlerweile nur noch selten eine realistische Option: stark gewachsene Prämien

heise online > Malware > Ransomware > Versicherer zu Cyberangriffen: Schäden "im Cyberspace nicht mehr versicherbar"

Versicherer zu Cyberangriffen: Schäden "im Cyberspace nicht mehr versicherbar"

Versicherungsgesellschaften müssen immer mehr Geld zur Regulierung von Schäden durch Cyberattacken ausgeben. Solche Verträge seien bald nicht mehr finanzierbar.

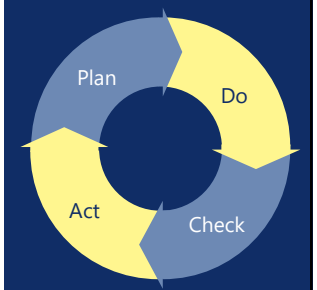
181

Compliance Management System

Standardisiertes Vorgehen möglich (ISO 27001 & 37301, etc.)!
Kombination diverser Anforderungen!
CMS als Nachweis für Erfüllung der Organisationspflichten!

Schnelle Amortisierung (ROSI) der Kosten für CO, IKS, etc.
(Kosten für eine durchschnittliche Betriebsunterbrechung bei ca. 5000-7000€ pro Minute; **Quellen**: IBM, statista, Veeam)

Klare Abläufe und Ausführungsvorgaben!
Lösung von uns: DSN Port: Compliance



Prüfungsschema
Schritt 1 - Produktbetroffenheit

VORPRÜFUNG
Ist das Produkt ein „Produkt mit digitalen Elementen" (Soft-/Hardware mit direkter oder indirekter Datenverbindung)?
Wird es auf dem EU-Markt in Verkehr gebracht / bereitgestellt?
Greift eine Ausnahme (Medizinprodukte, Kfz, Luftfahrt, bestimmte Marine-/Sektorregelungen, reine SaaS ohne Fernverarbeitungskomponente etc.)?
Handelt es sich um ausgenommene freie/Open-Source-Software ohne kommerzielle Tätigkeit?
Produktklasse bestimmt: Standardprodukt / wichtig Klasse I / wichtig Klasse II / kritisch?
Rolle korrekt eingeordnet (Hersteller vs. Einführer/Händler; ggf. Herstellerpflichten durch wesentliche Änderung / Eigenmarke ausgelöst)?

Prüfungsschema
Schritt 2 - Produktbetroffenheit

Cybersicherheitsrisikobewertung
Cybersicherheitsrisikobewertung durchgeführt und dokumentiert?
Bewertung über den gesamten Lebenszyklus (Planung, Design, Entwicklung, Produktion, Lieferung, Wartung) berücksichtigt?
Ergebnis der Risikobewertung in die technische Doku aufgenommen und aktuell gehalten?
Sorgfaltspflicht bei integrierten Drittkomponenten (inkl. Open Source) erfüllt?

Prüfungsschema
Schritt 3 - Produkt

Produkteigenschaft, Anhang I, Teil 1
Auslieferung ohne bekannte ausnutzbare Schwachstellen
Sichere Standardkonfiguration + Rücksetzmöglichkeit auf Werkszustand
Schwachstellen durch Sicherheitsupdates behebbar (ggf. automatisch, mit Opt-out & Benachrichtigung)
Schutz vor unbefugtem Zugriff (Authentifizierung, Identitäts-/Zugriffsverwaltung, Meldung unbefugter Zugriffe)
Vertraulichkeit gespeicherter/übertragener Daten (Verschlüsselung „at rest" / „in transit", State of the Art)
Integrität von Daten, Befehlen, Programmen, Konfiguration (Schutz vor Manipulation, Meldung von Korruption)
Datenminimierung – nur zwecknotwendige Daten
Verfügbarkeit wesentlicher Funktionen, auch nach Vorfall (DoS-Resilienz)
Minimierung negativer Auswirkungen auf andere Geräte/Netze
Angriffsflächen begrenzt (inkl. externer Schnittstellen)
Exploit-Mitigation-Techniken umgesetzt
Sicherheitsrelevantes Logging/Monitoring interner Aktivität (mit Opt-out)
Sicheres & dauerhaftes Löschen von Daten/Einstellungen; sichere Datenübertragung

Prüfungsschema
Schritt 4 - Produkt

Schwachstellenbehandlung, Anhang I, Teil II
SBOM (maschinenlesbar, gängiges Format – z. B. CycloneDX/SPDX), mind. Top-Level-Abhängigkeiten, gepflegt
Schwachstellen unverzüglich behandelt/behoben; Security- ggf. getrennt von Feature-Updates
Regelmäßige Sicherheitstests & Reviews
Nach Fix: öffentliche Offenlegung behobener Schwachstellen (Beschreibung, betroffene Produkte, Impact, Abhilfe)
Coordinated-Vulnerability-Disclosure-Policy vorhanden und angewandt
Meldekanal/Kontaktadresse für Schwachstellen (eigenes Produkt + Drittkomponenten)
Sichere Verteilmechanismen für Updates (ggf. automatisch)
Sicherheitsupdates unverzüglich, i. d. R. kostenlos, mit Advisory verteilt

Prüfungsschema
Schritt 5 - Dokumentation

Support Period
Unterstützungszeitraum festgelegt (mind. 5 Jahre, außer kürzere erwartete Nutzungsdauer)
Zeitraum spiegelt erwartete Nutzungsdauer wider und ist begründet
Unterstützungszeitraum für Nutzer klar ausgewiesen
Umgang mit Schwachstellen während des gesamten Zeitraums sichergestellt

Prüfungsschema
Schritt 6 - Dokumentation

Technische Dokumenation, Anhang VIII
Allgemeine Produktbeschreibung, Zweckbestimmung, Versionen
Design-/Entwicklungs-/Produktionsdoku inkl. Architektur
Nachweis der Erfüllung der grundlegenden Anforderungen (Anhang I)
Risikobewertung enthalten
Angewandte (harmonisierte) Normen / gemeinsame Spezifikationen / Zertifizierungen
Bericht über Sicherheitstests
SBOM referenziert/enthalten
Kopie der EU-Konformitätserklärung
Doku aktuell und für mind. 10 Jahre ab Inverkehrbringen aufbewahrt

Prüfungsschema

Schritt 7 – Konformitätsbewertung und CE-Kennzeichnung

Klasse	Zulässiges Verfahren
Standardprodukt	Modul A – interne Kontrolle (Selbstbewertung)
Wichtig Klasse I	Modul A nur bei vollständiger Anwendung einschlägiger harmonisierter Normen / gemeinsamer Spezifikationen / Zertifizierung; sonst Drittstelle (Modul B+C oder H)
Wichtig Klasse II	Verpflichtend Drittstelle: EU-Baumusterprüfung (B+C) oder umfassende QS (H)
Kritisch	Ggf. verpflichtende europäische Cybersicherheitszertifizierung (per Durchführungsrechtsakt)

Korrektes Konformitätsbewertungsverfahren gewählt und durchgeführt
Ggf. notifizierte Stelle eingebunden (bei Klasse II / fehlenden Normen)
CE-Kennzeichnung ordnungsgemäß angebracht
Konformität vor Inverkehrbringen sichergestellt

Prüfungsschema

Schritt 8 - Dokumentation

EU-Konformitätsbewertung, Anhang V
EU-Konformitätserklärung ausgestellt, Struktur nach Anhang V
Verweis auf CRA + ggf. weitere anwendbare Unionsrechtsakte
Produktidentifikation, Herstellerangaben, angewandte Normen enthalten
Mit Produkt bereitgestellt oder unter URL zugänglich

Prüfungsschema

Schritt 9 - Dokumentation

Informations- und Nutzerpflichten, Anhang II
Name, Anschrift, zentrale Anlaufstelle des Herstellers angegeben
Produktidentifikation (Typ, Charge, Serien-Nr. o. Ä.)
Zweckbestimmung + wesentliche Sicherheitseigenschaften beschrieben
Bekannte/absehbare Umstände mit erheblichem Cyberrisiko benannt
Kontaktstelle & Ort der CVD-Policy für Schwachstellenmeldungen angegeben
Hinweis auf SBOM-Verfügbarkeit (soweit einschlägig)
Ende des Unterstützungszeitraums klar kommuniziert
Anleitung zu sicherer Inbetriebnahme, Nutzung, Update, Außerbetriebnahme/Datenlöschung
Informationen mind. für die Dauer des Unterstützungszeitraums verfügbar

Prüfungsschema

Schritt 10 - Dokumentation

Melde- und Vorfallpflichten, Art. 14
Interner Prozess zur Erkennung/Bewertung aktiv ausgenutzter Schwachstellen und schwerwiegender Vorfälle vorhanden
Frühwarnung ≤ 24 h an zuständiges CSIRT (Koordinator) und ENISA über zentrale Meldeplattform
Meldung ≤ 72 h mit näheren Angaben
Abschlussbericht (Schwachstelle: 14 Tage nach Verfügbarkeit einer Abhilfe; Vorfall: 1 Monat nach Meldung)
Benachrichtigung der Nutzer über Vorfall/Schwachstelle + ggf. Abhilfemaßnahmen
24h-/72h-Referenzpunkte vor erstem Ernstfall getestet

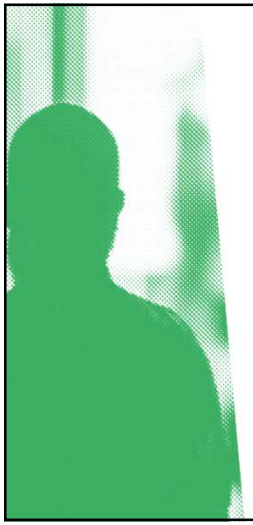
Prüfungsschema
Schritt 11 - Dokumentation

Weitere Herstellerpflichten & Sorgfalt
Bei Nichtkonformität: Korrekturmaßnahmen, ggf. Rücknahme/Rückruf
Kooperation mit Marktüberwachungsbehörden, Bereitstellung von Infos/Doku (in verständlicher Sprache)
Prozesse für Serienkonformität sichergestellt
Bei Einstellung des Betriebs/Support: Information der Behörden & Nutzer, ggf. Übergabe
Bevollmächtigter benannt, falls Hersteller außerhalb der EU

Prüfungsschema
Schritt 12 - Dokumentation

Fristen, Check und Selbstverortung
Meldepflichten (Art. 14) verbindlich — auch für Bestandsprodukte im Feld
Ausreichende Zahl notifizierter Stellen soll bestehen
Vollständige Geltung: grundlegende Anforderungen, Konformitätsbewertung, CE, techn. Doku
Bestandsprodukte (vor 11.12.2027 in Verkehr): CRA greift erst bei wesentlicher Änderung ab 11.12.2027 (Art. 69/Art. 3 Nr. 30)

Fragen?



Vielen Dank
für Ihre
Aufmerksamkeit!