TeleTrusT
Pioneers in IT security.
Bundesverband IT-Sicherheit e.V.

IT-Sicherheitsrechtstag 2026

Berlin, 24.09.2026

Der CRA im Produktlebenszyklus: Von Security by Design bis zu Meldepflichten

Dr. Carsten Brodersen, HK2 Rechtsanwälte

HK2 Rechtsanwälte

Agenda

1. Überblick
2. Anwendungsbereich des CRA
3. Pflichten entlang des Produktlebenszyklus
4. Marktaufsicht und Sanktionen

HK2 Rechtsanwälte

Agenda

1. **Überblick**
2. Anwendungsbereich des CRA
3. Pflichten entlang des Produktlebenszyklus
4. Marktaufsicht und Sanktionen

HK2 Rechtsanwälte

EU - Cybersicherheitsstrategie

Physische Sicherheit	IT-Sicherheit		
CER-Richtlinie	NIS-2-Richtlinie	Cyber Resilience Act (CRA)	Digital Operational Resilience Act (DORA)
KRITIS-Dachgesetz	BSIG	Unmittelbare Geltung	

HK2
Rechtsanwälte

Überblick zum CRA

- Erhöhung des Cyber-Sicherheitsniveaus von Produkten mit digitalen Elementen
- Zugang zum EU-Markt nur bei Einhaltung grundlegender Cyber-Sicherheitsanforderungen (Erweiterung CE-Kennzeichen)
- Produktsicherheitsrecht
- EU-Verordnung = Gilt unmittelbar in den Mitgliedstaaten
- CRA-Durchführungsgesetz (im Gesetzgebungsverfahren)
- Seit 10.12.2024 in Kraft
  - Seit **11.09.2026** greifen Meldepflichten
  - Ab **11.12.2027** voll anwendbar

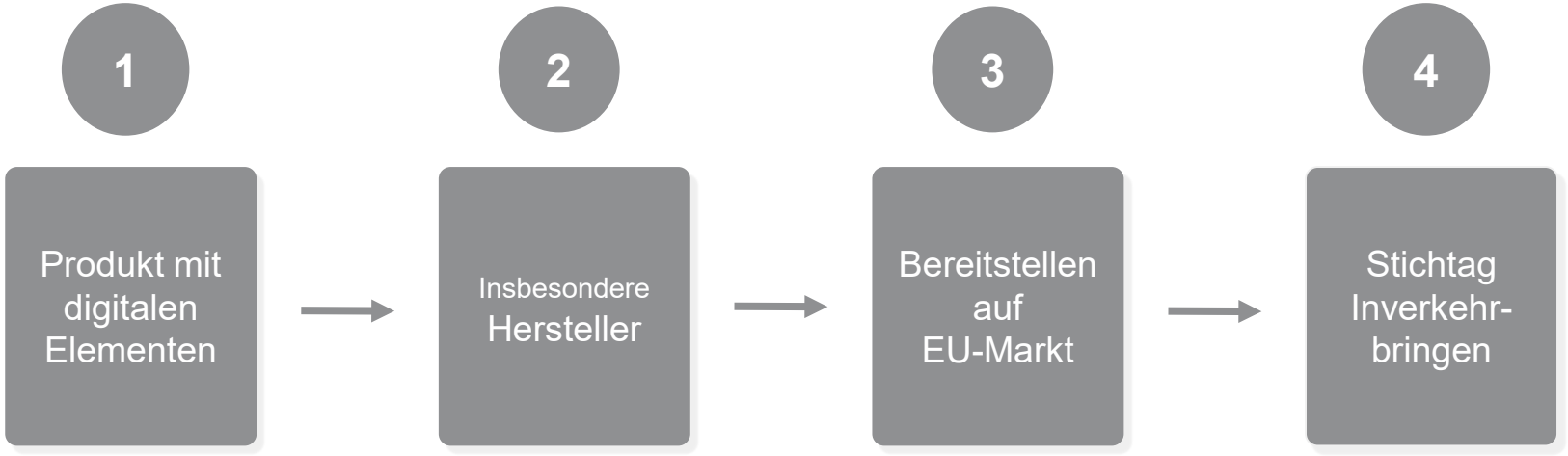
HK2 Rechtsanwälte

Agenda

1. Überblick
2. **Anwendungsbereich des CRA**
3. Pflichten entlang des Produktlebenszyklus
4. Marktaufsicht und Sanktionen

Anwendbarkeit des CRA

Art. 2 CRA: *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****.*



HK2
Rechtsanwälte

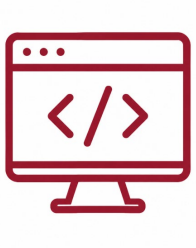
Produkte mit digitalen Elementen

HK2 Rechtsanwälte

Produkte mit digitalen Elementen, Art. 3 Nr. 1 CRA

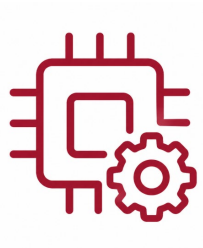
*„Produkt mit digitalen Elementen“ [bezeichnet] ein **Software-** oder **Hardwareprodukt** und dessen **Datenfernverarbeitungslösungen**, einschließlich Software- oder Hardware**komponenten**, die getrennt in den Verkehr gebracht werden*

1. Hardware



2. Software

3. Komponenten



4. Datenfernverarbeitung

HK2 Rechtsanwälte

Hardware, Art. 3 Nr. 5 CRA

*„Hardware“ [bezeichnet] ein physisches elektronisches Informationssystem, das digitale **Daten verarbeiten, speichern oder übertragen** kann, oder Teile eines solchen Systems*

Produkt muss via *Schnittstelle* Daten übertragen können („Konnektivität“)

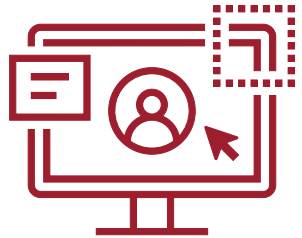
- Vernetzte Verbrauchergeräte
- Vernetzte Industriemaschinen
- Klassische IT-Hardware

HK2 Rechtsanwälte

Software, Art. 3 Nr. 4 CRA

„Software“ [bezeichnet] *den Teil eines elektronischen Informationssystems, der aus* ***Computercode*** *besteht*

- Computercode = Maschinen- und Quellcode
- Stand-alone Software
- Embedded Software
- Hardware-Software-Kombinationen



HK2 Rechtsanwälte

Free and Open-Source-Software, Art. 3 Nr. 48 CRA

*„**Freie und quelloffene Software**“* [bezeichnet] *eine Software, deren **Quellcode offen geteilt** wird und die im Rahmen einer **kostenlosen Open-Source-Lizenz** zur Verfügung gestellt wird, die alle Rechte vorsieht, um sie **frei zugänglich, nutzbar, veränderbar und** weiterverteilbar zu machen*

- FOSS kann Sonderfall von Software-Produkt mit digitalen Elementen sein
- Nur erfasst, soweit (als Komponente) ***kommerziell*** auf dem Markt bereitgestellt

HK2 Rechtsanwälte

Datenfernverarbeitung, Art. 3 Nr. 2 CRA

„Datenfernverarbeitung“ [bezeichnet] ***entfernt stattfindende Datenverarbeitung****, für die eine* ***Software*** *vom Hersteller selbst oder unter dessen Verantwortung konzipiert und entwickelt wird und* ***ohne die das Produkt*** *mit digitalen Elementen* ***eine seiner Funktionen nicht erfüllen könnte***

1. Entfernt stattfindende Datenverarbeitung
2. ohne die das Produkt mindestens eine seiner Funktionen nicht erfüllen könnte **und**
3. vom Hersteller oder unter seiner Verantwortung konzipiert wurde.

HK2 Rechtsanwälte

Software as a Service (SaaS)

- Cloudlösungen/ XaaS als „Remote Data Processing Solution“?
- Daten*fern*verarbeitung maßgeblich
  - Muss Datenübertragung zu (Hardware-)Produkt mit digitalen Elementen ermöglichen
  - Produktbezogen anhand Notwendigkeit für Funktionsumfang bestimmen

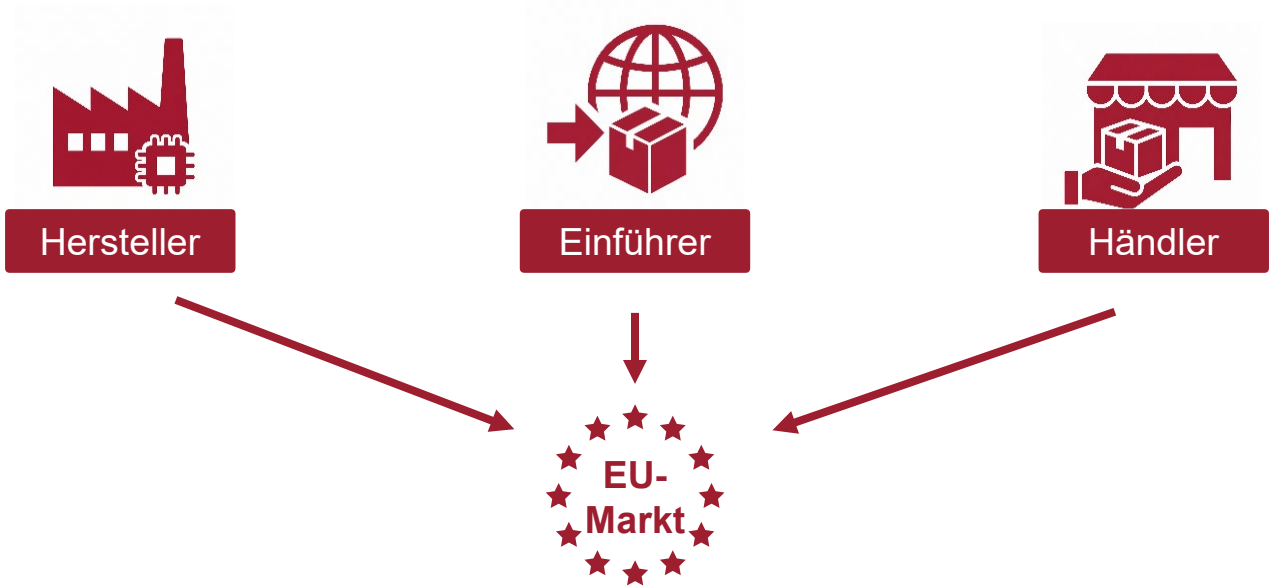
SaaS-Anbieter können in den Anwendungsbereich von **NIS-2**/ **BSIG** fallen!

HK2
Rechtsanwälte

Marktakteure

HK2
Rechtsanwälte

Adressierte Akteure



Sitz in der EU ist nicht erforderlich

Hersteller, Art. 3 Nr. 13 CRA

„Hersteller“ [bezeichnet] *eine natürliche oder juristische Person, die Produkte mit digitalen Elementen* ***entwickelt oder herstellt*** *oder die Produkte mit digitalen Elementen* ***konzipieren, entwickeln oder herstellen lässt*** *und sie* ***unter ihrem Namen oder ihrer Marke vermarktet****, sei es gegen Bezahlung, zur Monetarisierung oder unentgeltlich*

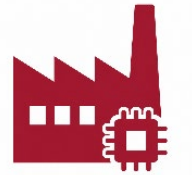
entwickeln / herstellen
oder
konzipieren, entwickeln oder herstellen *lassen*

+

In eigenem Namen vermarkten

- Klassische Hersteller/ Entwickler
- Auftraggeber von Fremdentwicklung
- White-Label-Anbieter
- Einführer, Händler oder sonstige Personen nach wesentlicher Änderung

- Produkt im eigenen Namen oder unter eigener Marke auf den Markt bringen



Zeitliche Anwendbarkeit

HK2
Rechtsanwälte

Wann gelten welche Pflichten?

HK2
Rechtsanwälte

Wann gelten welche Pflichten?

Risikoanalyse

EU-
Konformitätserklärung

CE-Kennzeichnung

Schwachstellen-
Management

Aktualisierungspflichten

Informations- und
Meldepflichten

Inverkehrbringen
nach 11.12.2027

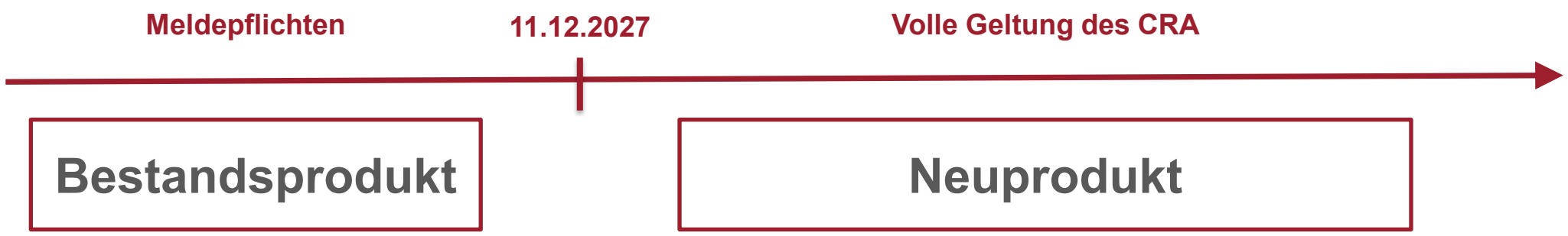
Konzeption, Entwicklung, Herstellung

Unterstützung
≥ 5 Jahre

HK2 Rechtsanwälte

Was ist mit Bestandsprodukten?

- **Einzelstückprinzip:**
  - erfasst sind **ab 11.12.2027** in Verkehr gebrachte *Einheiten*
  - maßgeblich ist nicht die Produkt*reihe*
- **Bestandsprodukte:**
  - Einheiten, die **vor** dem **11.12.2027** in Verkehr gebracht wurden, sind grds. nicht erfasst
  - es sei denn, sie werden danach **wesentlich geändert**
  - **Ausnahme: Meldepflichten** auch für Bestandsprodukte **seit 11.09.2026**



HK2 Rechtsanwälte

Wesentliche Änderungen

Art. 3 Nr. 30: *„Wesentliche Änderung“* [bezeichnet] *eine Änderung des Produkts mit digitalen Elementen* ***nach dessen Inverkehrbringen****, die sich auf die* ***Konformität des Produkts*** *mit den grundlegenden Cybersicherheitsanforderungen in Anhang I Teil I auswirkt oder zu einer* ***Änderung des bestimmungsgemäßen Zwecks****, für die das Produkt geprüft wurde, führt.*

- **Bestandsprodukte:** Werden Anforderungen des CRA unterworfen (Art. 69 Abs. 2 CRA)
- **Rollenwechsel:** Einführer, Händler, sonstige Personen, die wesentliche Änderungen vornehmen und auf Markt bereitstellen, gelten als ***Hersteller*** (Art. 21, 22 CRA)

HK2 Rechtsanwälte

Agenda

1. Überblick
2. Anwendungsbereich des CRA
3. **Pflichten entlang des Produktlebenszyklus**
4. Marktaufsicht und Sanktionen

HK2 Rechtsanwälte

Pflichten entlang des Produktlebenszyklus

HK2
Rechtsanwälte

Wann gelten welche Pflichten?

Risikoanalyse

EU-
Konformitätserklärung

CE-Kennzeichnung

Schwachstellen-
Management

Aktualisierungspflichten

Informations- und
Meldepflichten

Inverkehrbringen
nach 11.12.2027

Konzeption, Entwicklung, Herstellung

Unterstützung
≥ 5 Jahre

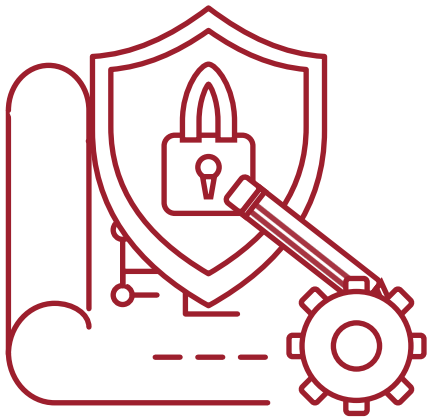
HK2
Rechtsanwälte

Vor Inverkehrbringen: Security by Design

Security by Design/ by Default, Art. 13 Abs. 1 i. V. m. Anhang I Teil I

Produkte müssen nach grundlegenden Cybersicherheits-Anforderungen des CRA **konzipiert, entwickelt** und **hergestellt** werden (Art. 13 Abs. 1 CRA)

- Abhängig von **Cybersicherheits-Risikoanalyse** (Art. 13 Abs. 2 CRA)
- Katalog technischer Anforderungen:
  1. Keine bekannten und ausnutzbaren Schwachstellen
  2. Sichere Standardkonfiguration („**security by default**“)
  3. Möglichkeit eines Factory-Resets
  4. Möglichkeit von Sicherheitsaktualisierungen
  5. Rechte- und Zugriffsbeschränkungen
  6. Produkt erkennt und meldet unbefugte Zugriffe etc.



HK2
Rechtsanwälte

Produktkategorisierung und CE-Kennzeichnung

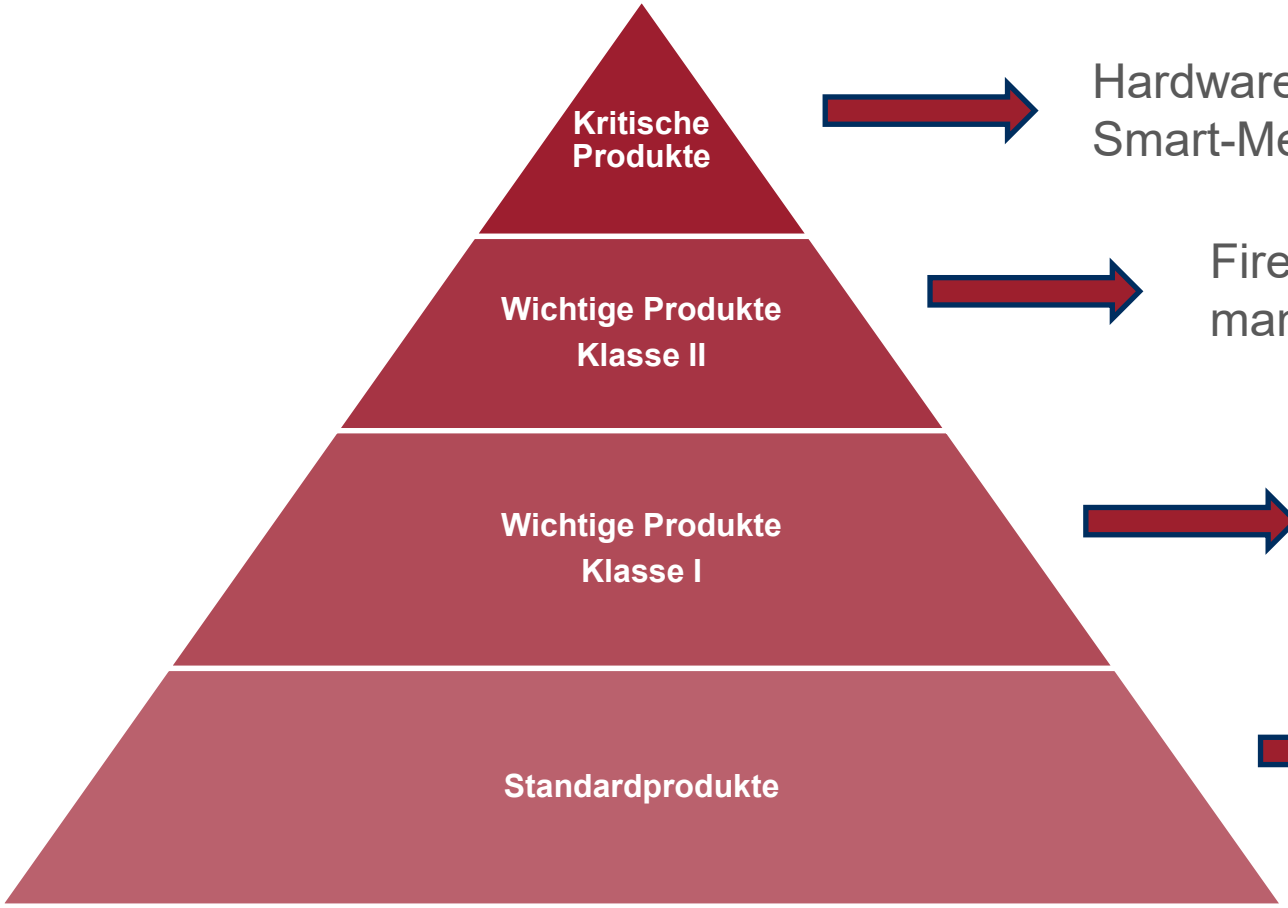
CE-Kennzeichnung

CE-Kennzeichen ist **Marktzugangsvoraussetzung** und **Herstellerpflicht**

- Ergebnis eines **Konformitätsbewertungsprozesses**
- Voraussetzung für **Konformitätserklärung** ist Dokumentation der Pflichtinhalte nach Anhang I Teil I (Art 31 Abs. 1 und 32 Abs. 1 CRA):
- **CE-Kennzeichnung** anschließend vom Hersteller gut sichtbar, leserlich und dauerhaft anzubringen (Art. 30 Abs. 1 CRA)

HK2
Rechtsanwälte

Produktklassen



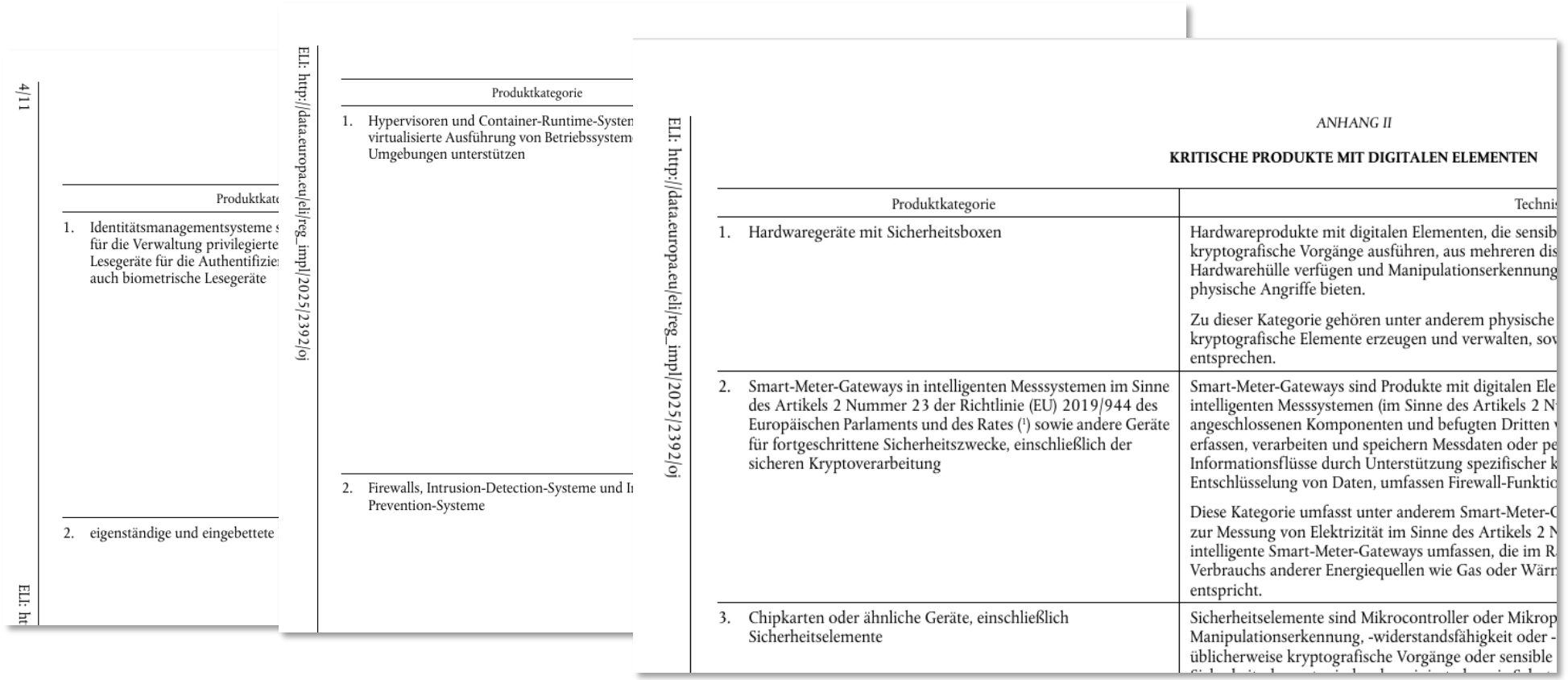
Hardwaregeräte mit Sicherheitsboxen, Smart-Meter-Gateways, Smartcards

Firewalls, manipulationssichere Mikroprozessoren

Passwortmanager, Spielzeug mit Internetverbindung, Wearables

Smartphones, Steuererklärungssoftware oder Saugroboter

Durchführungsakt als Orientierungshilfe



4/11

ELI: http://data.europa.eu/eli/reg_impl/2025/2392/oj

Produktkate
1. Identitätsmanagementsysteme s für die Verwaltung privilegierte Lesegeräte für die Authentifizie auch biometrische Lesegeräte
2. eigenständige und eingebettete

Produktkategorie
1. Hypervisoren und Container-Runtime-Systen virtualisierte Ausführung von Betriebssystem Umgebungen unterstützen
2. Firewalls, Intrusion-Detection-Systeme und I Prevention-Systeme

ELI: http://data.europa.eu/eli/reg_impl/2025/2392/oj

ANHANG II

KRITISCHE PRODUKTE MIT DIGITALEN ELEMENTEN

Produktkategorie	Techni
1. Hardwaregeräte mit Sicherheitsboxen	Hardwareprodukte mit digitalen Elementen, die sensib kryptografische Vorgänge ausführen, aus mehreren dis Hardwarehülle verfügen und Manipulationserkennung physische Angriffe bieten. Zu dieser Kategorie gehören unter anderem physische kryptografische Elemente erzeugen und verwalten, sov entsprechen.
2. Smart-Meter-Gateways in intelligenten Messsystemen im Sinne des Artikels 2 Nummer 23 der Richtlinie (EU) 2019/944 des Europäischen Parlaments und des Rates [1] sowie andere Geräte für fortgeschrittene Sicherheitszwecke, einschließlich der sicheren Kryptoverarbeitung	Smart-Meter-Gateways sind Produkte mit digitalen Ele intelligenten Messsystemen (im Sinne des Artikels 2 N angeschlossenen Komponenten und befugten Dritten erfassen, verarbeiten und speichern Messdaten oder pe Informationsflüsse durch Unterstützung spezifischer k Entschlüsselung von Daten, umfassen Firewall-Funktio Diese Kategorie umfasst unter anderem Smart-Meter-C zur Messung von Elektrizität im Sinne des Artikels 2 N intelligente Smart-Meter-Gateways umfassen, die im R Verbrauchs anderer Energiequellen wie Gas oder Wärr entspricht.
3. Chipkarten oder ähnliche Geräte, einschließlich Sicherheitselemente	Sicherheitselemente sind Mikrocontroller oder Mikrop Manipulationserkennung, -widerstandsfähigkeit oder - üblicherweise kryptografische Vorgänge oder sensible

https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=OJ:L_202502392

HK2 Rechtsanwälte

Das Konformitätsbewertungsverfahren

Schritt 1: Produktkategorie bestimmen

- Standardprodukte
- Wichtiges Produkt Klasse II
- Wichtiges Produkt Klasse I
- Kritisches Produkt

Schritt 2: Bewertungsverfahren auswählen

- Internes Kontrollverfahren (Modul A)
- Umfassende Qualitätssicherung (Modul H)
- EU-Baumusterprüfverfahren (Modul B)

  Interne Fertigungskontrolle (Modul C)
- Zertifizierung nach Cybersecurity-Act-Schema

Konformitätsbewertung im CRA

Modul A: Interne Fertigungsprotokolle
Standardprodukte: Selbsterklärung
Wichtige Produkte der Klasse 1: Selbsterklärung anhand harmonisierter Europäischer Normen (hEN) (falls vorhanden)

Modul B: Baumusterprüfung + **Modul C: Interne Fertigungskontrolle**
Wichtige Produkte der Klasse 2: Baumuster wird von der KBS[1] geprüft und abgenommen
Wichtige Produkte der Klasse 1: falls hEN nicht verfügbar
Selbsterklärung anhand des nach Modul B abgenommenen Baumusters

Modul H: Umfassende Qualitätssicherung
Wichtige Produkte der Klasse 2: Qualitätssicherungssystem wird von der KBS[1] geprüft und abgenommen
Wichtige Produkte der Klasse 1: falls hEN nicht verfügbar

Zertifizierung nach einem Cybersecurity-Act-Schema
Konformitätsvermutung über Nachweis der Zertifizierung.
Die Zertifizierung für jedes kritische Produkt muss erst über nachgelagerte Rechtsakte in Kraft gesetzt werden, um die Anforderungen an die Zertifizierung festzulegen.[2]

Hinweis:
Eine Konformitätsbewertung mittels Modul B+C oder Modul H ist auch möglich, wenn harmonisierte Europäische Normen vorhanden sind oder Standardprodukte unter die Selbsterklärung fallen.

[1] Konformitätsbewertungsstelle.
[2] Bis dahin fallen die kritischen Produkte in die Gruppe der wichtigen Produkte der Klasse 2.

https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/CRA/CRA_Flyer-2_Produktklassen_Konformitaet.pdf?__blob=publicationFile&v=2

HK2
Rechtsanwälte

Nach Inverkehrbringen: Schwachstellenmanagement

HK2
Rechtsanwälte

Wann gelten welche Pflichten?

Risikoanalyse

EU-
Konformitätserklärung

CE-Kennzeichnung

Schwachstellen-
Management

Aktualisierungspflichten

Informations- und
Meldepflichten

Inverkehrbringen
nach 11.12.2027

Konzeption, Entwicklung, Herstellung

Unterstützung
≥ 5 Jahre

HK2 Rechtsanwälte

Unterstützungszeitraum

Zeitrahmen für **Schwachstellenmanagement *nach* Inverkehrbringen** (Anhang I Teil II)

- Entspricht voraussichtlicher Nutzungsdauer
  - Vernünftige Nutzererwartungen
  - Art und Zweck des Produkts
  - Support vergleichbarer Produkte und zentraler Drittkomponenten
- Gesetzliches Leitbild:
  - **mindestens 5 Jahre**
  - sofern die zu erwartende Produktnutzungszeit nicht kürzer ist
- Wesentliche Änderungen können neuen Unterstützungszeitraum auslösen

Anforderungen an die Behandlung von Schwachstellen (Anhang I Teil II CRA)

HK2 Rechtsanwälte

1.	**Identifikation und Dokumentation**	Schwachstellen und Betroffenheit ermitteln und dokumentieren
2.	**Behebung und Updates**	Schwachstellen unverzüglich behandeln und beheben, u. a. durch Bereitstellung von Sicherheitsaktualisierungen
3.	**Tests und Überprüfung**	Sicherheit des Produkts regelmäßig und wirksam testen und überprüfen
4.	**Offenlegung und Transparenz**	Umfassende Informationen über beseitigte Schwachstellen teilen, einschließlich Beschreibung der Schwachstellen (Auswirkungen, Erkennbarkeit, Hinweise zur Behebung)

Anforderungen an die Behandlung von Schwachstellen (Anhang I Teil II CRA)

HK2 Rechtsanwälte

5.	**Koordinierte Offenlegung**	Strategie für eine koordinierte Offenlegung der Schwachstellen aufstellen und umsetzen
6.	**Austausch von Informationen**	Maßnahmen zum Austausch von Informationen über mögliche Schwachstellen ergreifen
7.	**Mechanismen für Aktualisierung**	Mechanismen für eine sichere Verbreitung von Aktualisierungen bereitstellen
8.	**Verbreitung von Aktualisierungen**	Vorhandene Sicherheitsaktualisierungen unverzüglich und grundsätzlich kostenlos verbreiten, zusammen mit Hinweisen und einschlägigen Informationen

HK2
Rechtsanwälte

Due Dilligence

Anforderungen an die Behandlung von Schwachstellen (Anhang I Teil II CRA)

HK2 Rechtsanwälte

1.	**Identifikation und Dokumentation**	Schwachstellen und Betroffenheit ermitteln und dokumentieren
2.	**Behebung und Updates**	Schwachstellen unverzüglich behandeln und beheben, u. a. durch Bereitstellung von Sicherheitsaktualisierungen
3.	**Tests und Überprüfung**	Sicherheit des Produkts regelmäßig und wirksam testen und überprüfen
4.	**Offenlegung und Transparenz**	Umfassende Informationen über beseitigte Schwachstellen teilen, einschließlich Beschreibung der Schwachstellen (Auswirkungen, Erkennbarkeit, Hinweise zur Behebung)

Identifikation und Dokumentation: Due Diligence von Komponenten

HK2 Rechtsanwälte

Lieferkette: Hersteller ist verantwortlich für *alle* verwendeten Komponenten

- **SBOM** als Dokumentationspflicht für jedes Produkt
  - Verzeichnis aller Software-Komponenten (Drittanbieter-Bibliotheken, FOSS etc.)
  - Mitsamt Versionen und Abhängigkeiten
  - Auf Anfrage gegenüber Marktaufsichtsbehörde offenzulegen (nicht Kunden)
- **Verträge** mit Drittanbietern anpassen
  - Updates über gesamten Unterstützungszeitraum
  - Meldekette innerhalb 24h
  - Dokumentation/ SBOM
  - Mitwirkung etc.

HK2
Rechtsanwälte

Sicherheitsupdates

Anforderungen an die Behandlung von Schwachstellen (Anhang I Teil II CRA)

HK2 Rechtsanwälte

1. 	**Identifikation und Dokumentation**	Schwachstellen und Betroffenheit ermitteln und dokumentieren
2. 	**Behebung und Updates**	Schwachstellen unverzüglich behandeln und beheben, u. a. durch Bereitstellung von Sicherheitsaktualisierungen
3. 	**Tests und Überprüfung**	Sicherheit des Produkts regelmäßig und wirksam testen und überprüfen
4. 	**Offenlegung und Transparenz**	Umfassende Informationen über beseitigte Schwachstellen teilen, einschließlich Beschreibung der Schwachstellen (Auswirkungen, Erkennbarkeit, Hinweise zur Behebung)

HK2
Rechtsanwälte

Updates und Upgrades: Was muss kostenlos sein?

Sicherheitsupdates

kostenlos

(Pflicht)

im Unterstützungszeitraum
i. d. R. **mind. 5 Jahre**

1. **Funktionsupdates**
2. **Zusatzleistungen**
3. **Sicherheitsupdates**

nach Ablauf des Unterstützungszeitraums
oder Individualsoftware im B2B

vergütungsfähig

HK2
Rechtsanwälte

Meldepflichten

HK2 Rechtsanwälte

Meldepflichten, Art. 14 CRA

Aktiv ausgenutzte Schwachstelle

Schwerwiegender Sicherheitsvorfall

Kenntnis

- Pflicht zur Ermittlung von Schwachstellen nach Inverkehrbringen am 11.12.2027

Aktive Ausnutzung

- Bloße Vermutung genügt nicht
- Unverzüglich angemessene Aufklärungsmaßnahmen

24 h
Frühwarnung

72 h
Ausführliche Meldung

14 Tage / 1 Monat
Abschlussbericht

ENISA Single Reporting Platform
verfügbar seit 11.09.2026

Nutzerinformation
“nachdem” Kenntnis erlangt wurde

Agenda

1. Überblick
2. Anwendungsbereich des CRA
3. Pflichten entlang des Produktlebenszyklus
4. **Marktaufsicht und Sanktionen**

HK2 Rechtsanwälte

Mögliche Folgen bei einem CRA-Verstoß

BSI als Marktüberwachungsbehörde (CRA-Durchführungsgesetz-E)

- Anordnung von „Korrekturmaßnahmen“ für Herstellung von Konformität
- Nachgelagert:
  - Vertriebseinschränkung
  - Vertriebsverbot
  - Rückruf
- Bußgeld

Bußgeldrahmen (Art. 64 CRA)

- Verstoß gegen **grundlegende Cybersicherheitsanforderungen**: Bis **EUR 15 Mio**. oder **2,5 % des Jahresumsatzes**
- **Falsche Angaben gegenüber Behörden**: bis EUR 5 Mio. oder 1 % des Jahresumsatzes

HK2 Rechtsanwälte

Modernisierung des Produkthaftungsgesetzes

Zivilrechtliche Produkthaftung nach ProdHaftG n. F.

- Wegen EU-Produkthaftungsrichtlinie bis **09.12.2026** in DE umzusetzen
- Gilt im Verhältnis **B2C**
- „Produkt“ umfasst künftig auch **Software**
- Nichteinhaltung der CRA-Anforderungen kann Produkt**fehler** begründen
- **Verschuldensunabhängig Herstellerhaftung** für kausale Verbraucherschäden
- Auch „Bagatellschäden“ erfasst und verbandsklagenfähig

Verschuldensunabhängige Haftung für Verbraucherschäden

Praxisumsetzung des CRA

HK2 Rechtsanwälte

Konkrete Schritte zur Umsetzung

1 Anwendbarkeit prüfen

- **Produktinventur**: Ist das Produkt vom CRA erfasst?
- **Rolle prüfen**: Hersteller, oder anderer Akteur entlang der Lieferkette?
- **Wann** wurde das Produkt in den Verkehr gebracht?

2 Risikoanalyse

- Für jedes individuelle Produkt
- Technische Sicherheitslücken
- Prozesslücken (z. B. in Lieferkette)
- Dokumentationslücken
- Budget für CRA-Compliance bestimmen

3 Prozess-anpassung

- Bedrohungsmodellierungen und -tests
- Festlegung der Coding-Standards
- Schwachstellenmanagement/ Incident-Response veranlassen
- Unterstützungszeitraum definieren
- Meldewege etablieren

Konkrete Schritte zur Umsetzung

4 Dokumentieren

- Technische Dokumentation jedes Produktes
- Erstellen der SBOM
- Erstellen von Nutzerinformationen

5 CE-Verfahren

- Risikoklasse bestimmen
- Konformitätsbewertungs-verfahren durchlaufen
- Ggf. Einbindung einer externen Prüfstelle
- Entwurf & Anbringen des CE-Kennzeichens

6 Fortlaufende Compliance

- Schwachstellen-Monitoring (Audits)
- Produktupdates prüfen
- Dokumentation

Kontakt

brodersen@hk2.eu

HK2
Rechtsanwälte

Rechtsanwalt
Dr. Carsten Brodersen

Hausvogteiplatz 11 A
10117 Berlin

Telefon +49 (0)30 27 89 00-0
Telefax +49 (0)30 27 89 00-10
E-Mail brodersen@hk2.eu

www.hk2.eu

www.hk2.eu

linkedin.com/in/cbbrodersen/