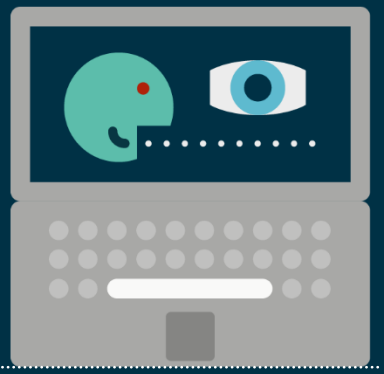
Cyber Resilience Act (CRA)

Bedeutung für den Softwarevertrieb und FOSS

25. September 2024

Inhalt

01 Timeline und Grundlagen



Die xz-Hintertür: Das verborgene Oster-Drama der IT

Mit einer Hintertür in einer unbekannten Kompressionsbibliothek hätten Unbekannte beinahe große Teile des Internets übernehmen können. Leider kein Scherz.

(Bild: BeeBright / Shutterstock.com)

02.04.2024, 17:10 Uhr Lesezeit: 8 Min. | Security

Ziele des CRA

Cybersicherheit

- Einheitlicher EU-Rechtsrahmen
- *Cybersecurity by Design:* Cyberreslilienz während des gesamten Lebenszyklusses

Transparenz

- Aufklärung von Nutzer:innen
- Information über Sicherheitseigenschaften und Schwachstellen

Sicherheits-aktualisierungen

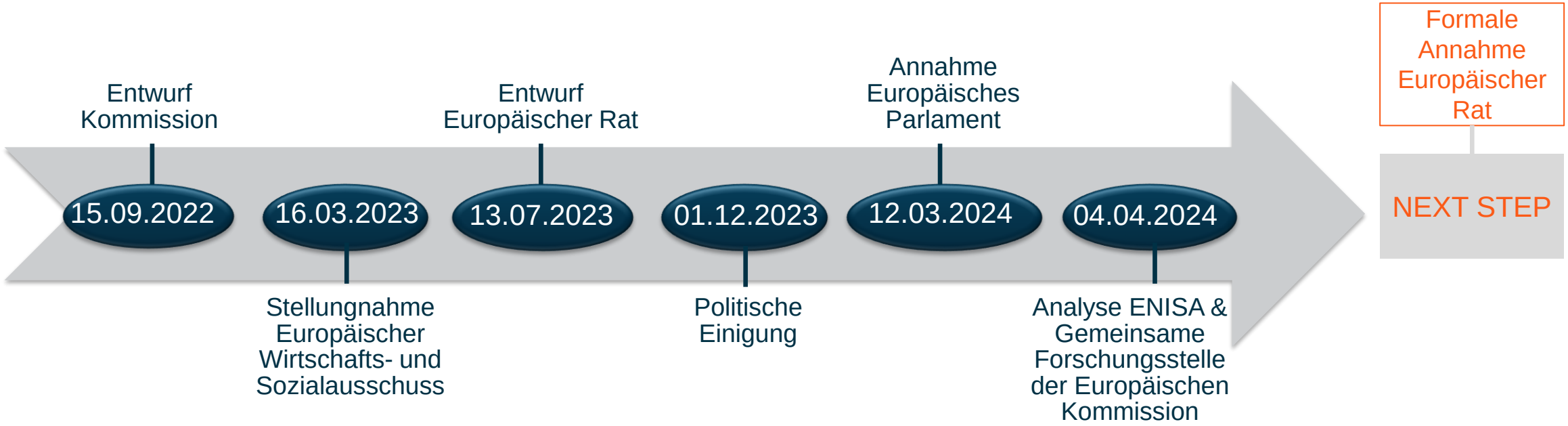
- Lebenslange/fortlaufende Updates

Eindämmung von Schwachstellen

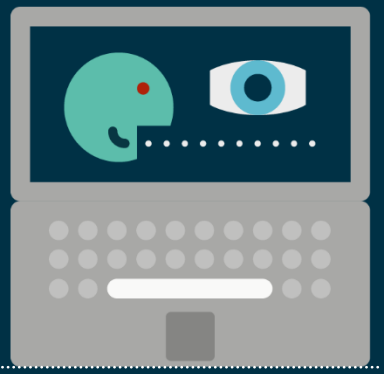
- Kohärente Bereitstellung

Stand der Gesetzgebung

Bislang kein Unionsrechtsakt zur sektorübergreifenden Cybersicherheit digitaler Produkte.



02 Anwendungsbereich



Persönlicher Anwendungsbereich

- „Wirtschaftsakteure” (Art. 13 ff, Art. 3 Nr. 12 ff. CRA-E)
  Hersteller:innen, deren Bevollmächtigte, Einführer:innen, Händler:innen, natürliche oder juristische Personen als Quasi-Hersteller:innen

  → eigenständige Pflichten für alle Wirtschaftsakteur:innen
- Open Source Stewards („Verwalter quelloffener Software“) mit Sonderrolle bzw. als “Verpflichteter light“ ohne eigenes Vermarktungsinteresse, Art. 3 Nr. 14 i. V. m. Art. 24

Räumlicher Anwendungsbereich

- Alle **innerhalb des Unionsmarkts** in Verkehr gebrachten Produkte mit digitalen Elementen, ungeachtet des Herstellungsorts
- **Akteure außerhalb** der EU sind verpflichtet, wenn sie Produkte mit digitalen Elementen **im Unionsmarkt in Verkehr bringen**
- Adressat:innen der Norm müssen sicherstellen, dass beim Import von Produkten mit digitalen Elementen schon bei der Herstellung und über den **Lebenszyklus der Produkte** die Pflichten eingehalten werden

Sachlicher Anwendungsbereich

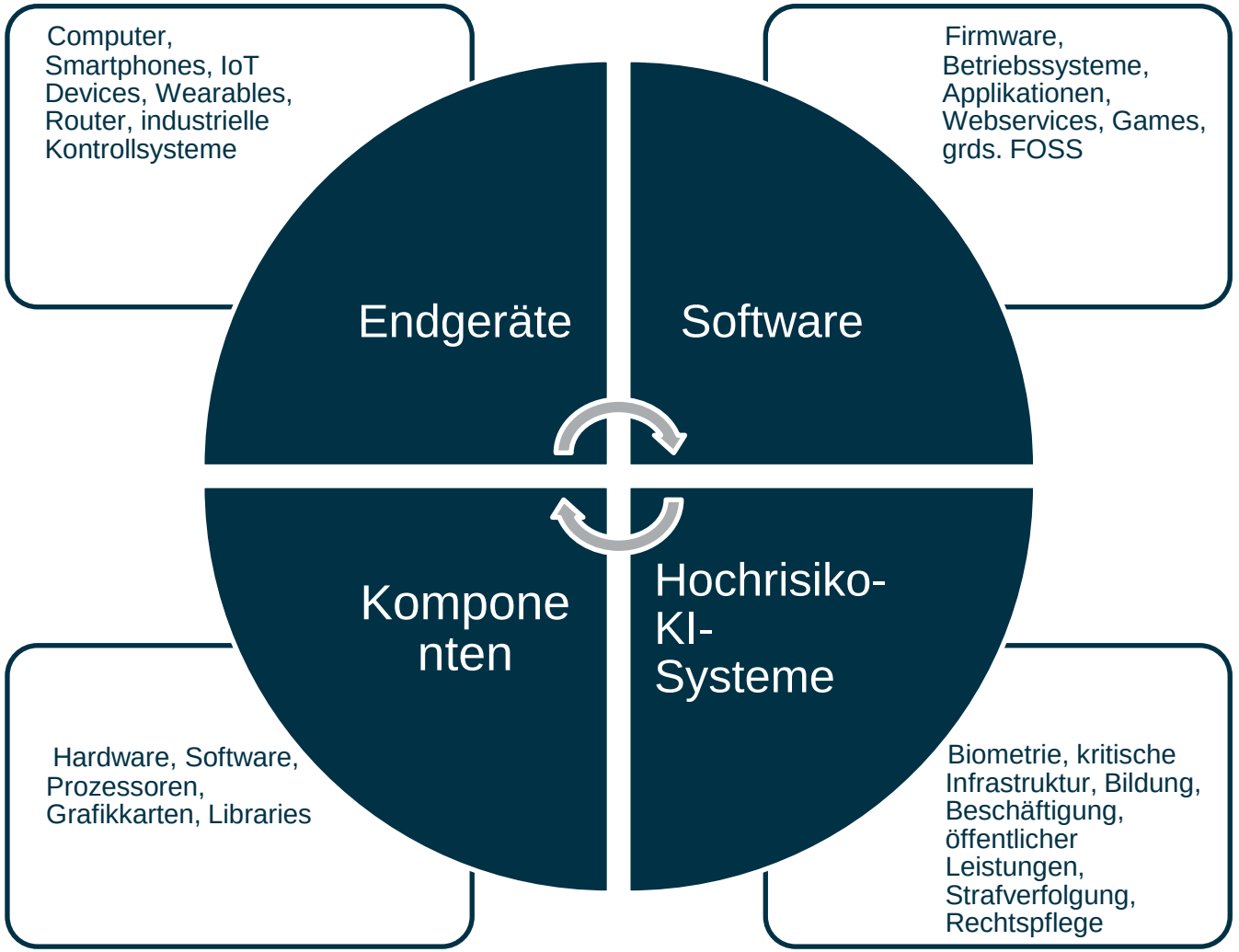
- „Produkt mit digitalen Elementen", Art. 3 Nr. 1 (vgl. §§ 327 ff. BGB)

  „**Software- oder Hardwareprodukt** und dessen Datenfernverarbeitungslösungen, **einschließlich** Software- oder Hardwarekomponenten, die getrennt in Verkehr gebracht werden sollen."

  → explizit Software (*Standalone*-Vertrieb oder eingebaut in *Hardware*)

- VO gilt für Produkte mit digitalen Elementen, deren bestimmungsgemäße oder vernünftigerweise vorhersehbare Verwendung eine **direkte oder indirekte Datenverbindung** mit einem **Gerät oder Netz** einschließt

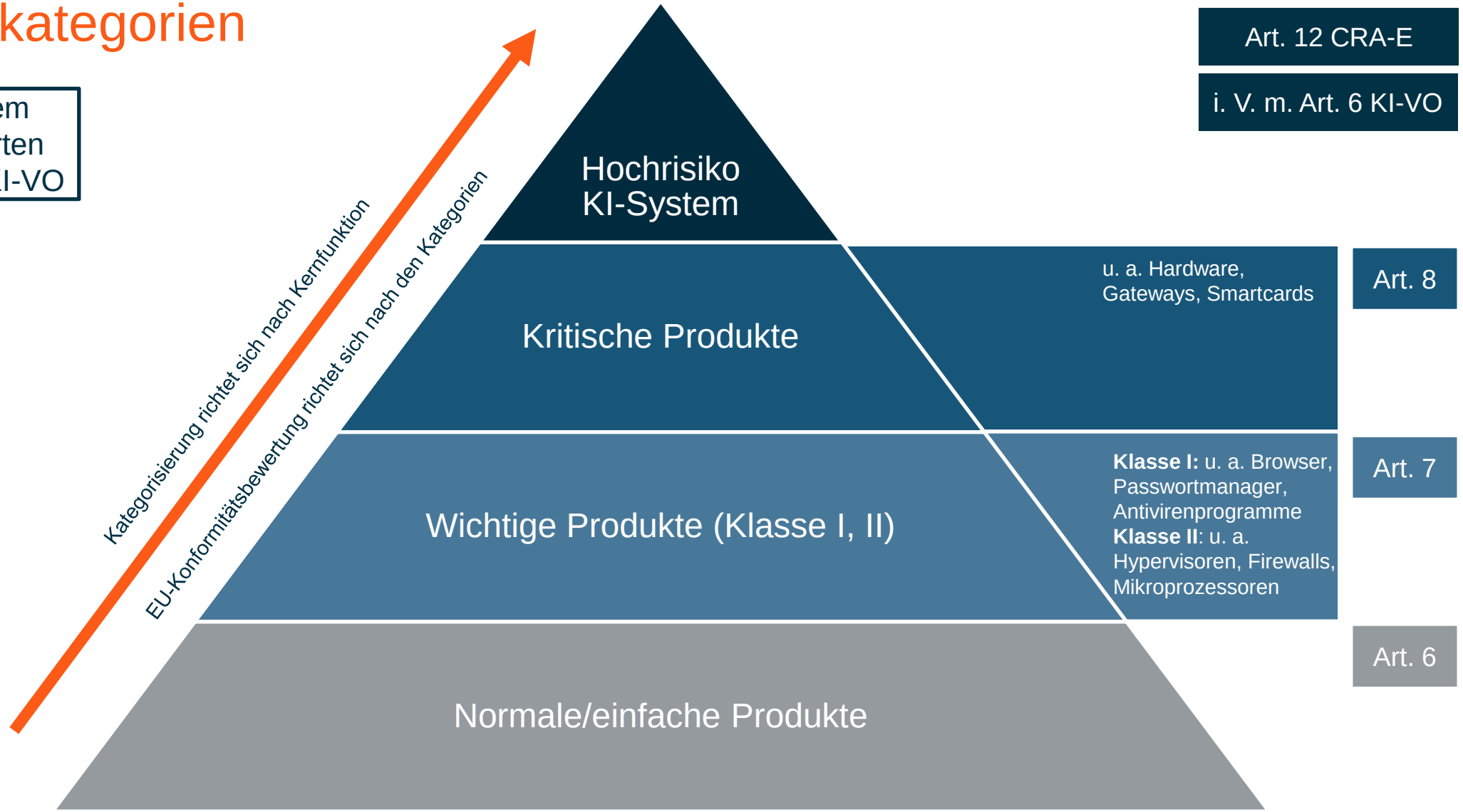
Sachlicher Anwendungsbereich



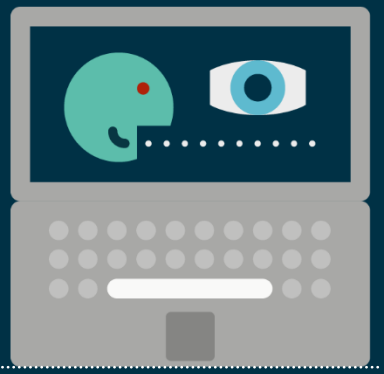
Ausgenommen sind reine Service-Leistungen wie SaaS/PaaS/IaaS
EG 12 (→ NIS-2-RL)

Produktkategorien

Ähnlich dem risikobasierten Ansatz der KI-VO



03 Verpflichtungen



Pflichtensystem des CRA

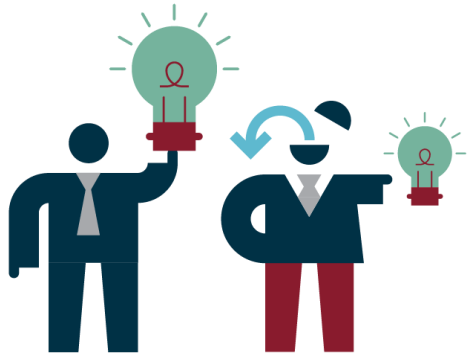
- Umfassende Pflichten für Hersteller:innen, Importeur:innen, Händler:innen z. B.
  - Produkthaftungspflichten
  - Prozess- und Dokumentations- und Updatepflichten
  - Informations- und Meldepflichten
  - Konformitätsbewertungspflichten
  - CE-Kennzeichnung für „Produkte mit digitalen Elementen“
- Abgestufte Verantwortlichkeit innerhalb der Lieferkette

Pflichten von Hersteller:innen

- Anfertigung technischer Dokumentationen Art. 31 Anh. VII
  - Umfangreiche Beschreibungen & Abbildungen des Produkts mit digitalen Elementen
  - Bewertung und Dokumentation des Cybersicherheitsrisikos und etwaiger Schwachstellen
  - Aktualisierung technischer Dokumentationen über die gesamte Lebensdauer inkl. Drittkomponenten (auch FOSS Art. 13 Abs. 5)
- Erfassung von Komponenten in einer „Software-Stückliste“ (Art. 13 Abs. 24, Art. 3 Nr. 39 i. V. m. Anh. I Teil II Abs. 1)

Pflichten der Hersteller:innen

- Melde- und Informationspflichten zu Schwachstellen (Art. 14) über eine einheitliche Meldeplattform (Art. 16)
- Durchführung von Konformitätsverfahren (Art. 32 i. V. m. Anh. VIII) bei notifizierten Stellen (Artt. 35 ff.), Ausstellung von EU-Konformitätserklärungen (Art. 28), CE-Kennzeichnung (Art. 30)



Pflichten für Importeur:innen/Händler:innen

- Importeur:innen beim/Händler:innen nach dem Inverkehrbringen
- Kontrollpflichten, Sicherstellen von Korrekturmaßnahmen (Art. 19, 20)
    1. Durchgeführtes Konformitätsbewertungsverfahren
    2. Erstellte erforderliche (z. B. technische) Unterlagen
    3. Beigefügte CE-Kennzeichnung und EU-Konformitätserklärung
- Kooperations-, Melde-, Kontaktangabe-, Aufbewahrungs-, und Nachweispflichten

„Aufwertung“ zur Herstellereigenschaft (Art. 21), wenn

- Inverkehrbringen unter eigenem Namen/eigener Marke
- Wesentliche Änderung an bereits in Verkehr gebrachtem Produkt

Pflichten für Importeur:innen/Händler:innen

Importeur:innen (Art. 19)

Abs. 1, 3: Sicherstellung CRA-Anforderungen

Abs. 2: Kontroll- und Nachweispflicht

1. Konformitätsbewertungsverfahren
2. Erstellte **technische Dokumentation**
3. Beigefügte CE-Kennzeichnung & EU-Konformitätserklärung
4. Prüfung Pflichten Hersteller:innen Art. 13 Abs. 15, 16, 19

Abs. 3, 8: Informations- und Meldepflicht

Abs. 4: Kontaktangabepflicht

Abs. 5: Verpflichtung zu Korrekturmaßnahmen

Abs. 6: Aufbewahrungs- und Nachweispflicht

Abs. 7: Kooperationspflicht

Händler:innen (Art. 20)

Abs. 1, 3: Sicherstellung CRA-Anforderungen (Sorgfaltsverpflichtung)

Abs. 2: Kontrollpflicht

1. CE-Kennzeichnung
2. Prüfung Pflichten Hersteller- und Importeur:innen Art. 13 Abs. 15, 16, 18, 19, 20 und Abs. 19 Abs. 4
3. Erstellte **erforderliche Dokumente**

Abs. 3, 4, 6: Informations- und Meldepflicht

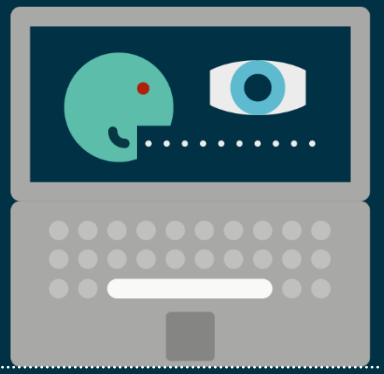
Abs. 4: Verpflichtung zu Korrekturmaßnahmen

Abs. 5: Kooperationspflicht (Aufbewahrungs- und Nachweispflicht)

„Aufwertung“ zur Herstellereigenschaft (Art. 21), wenn

- Inverkehrbringen unter eigenem Namen/eigener Marke
- Wesentliche Änderung an bereits in Verkehr gebrachtem Produkt

04 EU-Gesetzgebungskontext



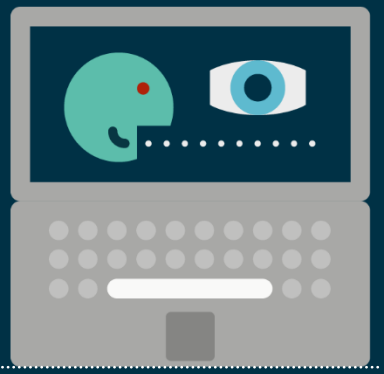
EU-Gesetzgebungskontext - Übersicht

*	Gesetz	Wesentlicher Inhalt und Anwendungsbereich
1	**PLD**	Erweiterte verschuldensunabhängige Haftung von Hersteller:innen für fehlerhafte Produkte; zivilrechtliche Ansprüche bei Verstoß
2	**CRA**	Einheitliche Cybersicherheitsanforderungen für Produkte mit digitalen Elementen, haftungsunabhängiges Sanktionsregime
3	**NIS-2**	Cybersicherheitsanforderungen für Dienstleistungen
4	**KI-Verordnung**	Einheitliche Zulässigkeitsanforderungen beim Vertrieb von KI-Systemen, u. a. Cybersicherheitsanforderungen (Art. 15)

Bislang keine „Feinabstimmung“ zwischen den Produkthaftungsregelungen, lediglich einfache Verzahnung.

* “Ebene” des Produktzyklus

05 FOSS im CRA



FOSS im CRA - Allgemeines

- Zahlreiche Sonderregelungen für FOSS (EG 17-22) als Resultat intensiven Lobbyings der FOSS-Community
    - Anerkennung der Bedeutung von FOSS und den Besonderheiten
    - Regelung von Bereichsausnahmen für die Entwicklung und Bereitstellung von FOSS
    - Konsultation der „FOSS“-Community im Zuge von Umsetzungsmaßnahmen der VO, Art. 9
- Meldepflicht für FOSS-Schwachstellen, Art. 14
- Evtl. Freiwillige Sicherheitsbescheinigungen zur Erleichterung der Integration von FOSS-Komponenten, Art. 25 i. V. m. Art. 13 Abs. 5 i. V. m. EG 21

FOSS im CRA – FOSS-Begriff

Art. 3 (48):

„„freie und quelloffene Software“ 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 im CRA - FOSS-Begriff

Anforderungen an die Open-Source-Lizenz

- **Verfügbarkeit** des Source-Codes erforderlich?
  - Quellcode „offen geteilt“, Lizenz zur Verfügung gestellt → Zurverfügungstellung des Quellcodes nicht explizit gefordert
  - BSD-Lizenz und MIT-Lizenz verlangen dies nicht
- **Freie Lizenz:** Kostenlosigkeit oder Freiheit?
  - Wortlaut: deutsch „kostenlos“; „frei“ zugänglich / englisch “free” (nicht definiert)
  - Telos: Nutzungsfreiheit, nicht Kostenlosigkeit, deshalb sind entgeltliche Dienstleistungen möglich → “free as in free speech, not as in free beer”

FOSS im CRA - Bereichsausnahme

ErwG. 18:

*„(…) In Bezug auf Wirtschaftsakteure, die in den Anwendungsbereich dieser Verordnung fallen, sollte nur freie und quelloffene Software, die **auf dem Markt bereitgestellt** und somit zum Vertrieb oder zur Nutzung im Rahmen einer **Geschäftstätigkeit** verfügbar gemacht wird, in den Anwendungsbereich dieser Verordnung fallen. Die bloßen Umstände, unter denen das Produkt mit digitalen Elementen entwickelt wurde, oder die Art und Weise, wie die Entwicklung finanziert wurde, sollten daher bei der Bestimmung des kommerziellen oder nichtkommerziellen Charakters der entsprechenden Tätigkeit nicht berücksichtigt werden. Insbesondere sollte für die Zwecke dieser Verordnung und in Bezug auf die Wirtschaftsakteure, die in ihren Anwendungsbereich fallen, die Bereitstellung von Produkten mit digitalen Elementen, die als freie und quelloffene Software eingestuft und von ihren Herstellern nicht zu Geld gemacht werden, nicht als Geschäftstätigkeit betrachtet werden, damit sichergestellt ist, dass **klar zwischen der Entwicklungs- und der Lieferphase unterschieden** wird. Darüber hinaus sollte die Lieferung von Produkten mit digitalen Elementen, die als freie und quelloffene Softwarekomponenten eingestuft werden und zur Integration durch andere Hersteller in ihre eigenen Produkte mit digitalen Elementen bestimmt sind, nur dann als Bereitstellung auf dem Markt betrachtet werden, wenn die entsprechende Komponente von ihrem ursprünglichen Hersteller zu Geld gemacht wird.(…)“*

FOSS im CRA - Bereichsausnahme

- Grundsatz: Gesetzgeberische Intention die Entwicklung und allgemeine Bereitstellung von FOSS von der Regulierung im CRA auszunehmen
- Aber: Privilegierungen (mit Ausnahme der Regelungen für Stewards) weiterhin nur im Erwägungsgrund verankert
- Unterstützung von FOSS-Organisationen („not-for-profit organisations“)
- Pflichten greifen erst, wenn FOSS (isoliert oder als Teil eines Produkts oder Dienstes) mit **direkter Gewinnerzielungsabsicht auf den Markt gebracht** wird z. B. operatives Einsetzen, keine bloße Bereitstellung in offenen Archiven über Paketverwaltung/Plattformen

FOSS im CRA - FOSS-Begriff

Anforderungen an das Open Source Produkt

- **Quellcode als Softwareprodukt?**
  - Software besteht nach Art. 3 Nr. 4 nur aus Computercode
  - Nach EG 31 i. V. m. EG 12 PLD ist der reine Quellcode von Software kein Produkt (da für sich genommen nicht funktionsfähig)
- **Umfang der Open Source-Bereichsausnahme**
  - Nur abtrennbare Open-Source-Bestandteile oder das vollständige Produkt?
  - Hersteller:innen haften für Open-Source-Bestandteile

    → Im Zweifel in vollem Umfang

FOSS im CRA - Bereichsausnahme

- Problem: **Herstellereigenschaft** bei FOSS
- Nur Softwareurheber:in oder auch Contributor / Distributor?
  - Z. B. Contributions im Arbeitsverhältnis, § 69b UrhG
  - Natürliche oder juristische Personen, die mit Quellcode zu FOSS-Produkten beitragen und nicht selbst lizenziert, sind von den Verpflichtungen ausgenommen
- Vielzahl an potenziellen Hersteller:innen durch jeden „Branch“ und „Clones“ unter eigenem Namen

➡ Jede Person, die im eigenen Namen FOSS bereitstellt, muss Cyberresilienz beachten

FOSS im CRA - Bereichsausnahme

- Voraussetzung ist die **Geschäftstätigkeit** des:der Herstellers:in und eine Bereitstellung auf dem Markt, unmittelbare Gewinnerzielung, für sich genommen genügt nicht:
    - Bloße finanzielle Unterstützung
    - Beiträge von Hersteller:innen in der Entwicklung
    - Regelmäßige Veröffentlichung von Versionen

    ➡ „Klare“ Unterscheidung zwischen Entwicklungs- und Lieferphase
- Tätigkeiten gemeinnütziger Organisationen nicht kommerziell, wenn alle Einnahmen nach Kostenabzug zur Verwirklichung **gemeinnütziger Zwecke** verwendet werden

FOSS im CRA – Rolle der FOSS-Stewards

Art 3 (14):

„„Verwalter quelloffener Software“ eine juristische Person, bei der es sich nicht um einen Hersteller handelt, die den Zweck oder das Ziel hat, die Entwicklung spezifischer Produkte mit digitalen Elementen, die als freie und quelloffene Software gelten und für kommerzielle Tätigkeiten bestimmt sind, systematisch und nachhaltig zu unterstützen, und die die Vermarktbarkeit dieser Produkte sicherstellt;“

FOSS im CRA – Rolle der FOSS-Stewards

- Systematische und nachhaltige Unterstützung der FOSS-Entwicklung, Art. 3 Nr. 14 i. V. m. EG 19
    - Ist die Einzelentwicklerin, die regelmäßig released umfasst? Eher nicht, da ausdrücklich Stiftung/Einrichtung gefordert
    - Problem: Dual-Licensing-Modelle: wohl keine Doppelfunktion (Art. 3 Nr. 14: Juristische Person ist nicht Hersteller:in), Abgrenzung Commercial Edition / Community Edition
- Problem: Abgrenzung zu gemeinnützigen Organisationen (i. d. R. FOSS-Stiftungen u. ä. Institutionen)
- Eingeschränkte Nachweis- und Meldepflichten, Art. 24
    - Entwicklung und Dokumentation von Cybersicherheitsstrategien zur Unterstützung von Entwickler:innen → Initiative großer Foundations (u. a. Apache, Eclipse Foundation) zur gemeinsamen Entwicklung von Sicherheitsstandards und –strategien
    - Zusammenarbeit mit Marktüberwachungsbehörden bei Sicherheitslücken
    - „Detailgrad“ der Informationen orientiert sich an der Intensität des Vorfalls
- Befreiung von den Sanktionen, vgl. Art. 64 Nr. 10 (b)

FOSS im CRA – Hauptkritik zur Regulierung

- Fortbestehende Herausforderung bei der Entwicklung von „kommerzieller“ FOSS
  - Keine bloße „Garagenbastelei“ durch „Hobby“-Entwickler:innen
  - FOSS wird in weiten Teilen von Unternehmen mit kommerziellen Interessen entwickelt, die ein anderes wirtschaftliches Setup besitzen als kommerzielle Softwareanbieter:innen
- Wirtschaftliche Sinnhaftigkeit wird in der Umsetzung der Anforderungen aus dem CRA in Frage gestellt
  - Größere Anzahl von nicht-zahlenden Nutzer:innen bei OSS-Geschäftsmodellen → Finanzierung erfolgt gerade nicht im Verhältnis zu Nutzerzahlen über skalierende Lizenzverkäufe, sondern über Services, Beratung und andere nicht-skalierende Leistungen
  - Regelmäßig 1:1-Verhältnis von Lizenzerlösen je Softwarekopie bei kommerzieller Software

Noch Fragen?

Lina Böcker
Partner
Germany

+49 30 72621 8095
lina.boecker@osborneclarke.com

Tim Schmetzer
Associate
Germany

+49 30 72621 8159
tim.schmetzer@osborneclarke.com

Vielen Dank

Osborne Clarke ist der Firmenname für ein internationales Rechtsanwaltsbüro und die damit verbundenen Abteilungen. Alle Einzelheiten dazu hier: osborneclarke.com/verein

Diese Materialien werden nur zu allgemeinen Informationszwecken geschrieben und bereitgestellt. Sie sind nicht vorgesehen und sollten nicht als Ersatz für Rechtsberatung verwendet werden. Bevor Sie sich mit einem der folgenden Themen befassen, sollten Sie sich rechtlich beraten lassen.