Der Cyber Resilience Act: Ein Gesetz „mit digitalen Elementen“

Prof. Dr. Dirk Heckmann
Lehrstuhl für Recht und Sicherheit der Digitalisierung, Technische Universität München

11. Deutscher IT-Rechtstag
25.04.– 26.04.2024 in Berlin

Die Bedrohungslage

Mehr als **2.000** **Schwachstellen** in Softwareprodukten **(15 % davon kritisch)** wurden im Berichtszeitraum durchschnittlich im Monat bekannt. Das ist ein **Zuwachs von 24 %.**

Bundesamt für Sicherheit in der Informationstechnik

Bitkom legt Zahlen vor

tagesschau

206 Milliarden Euro Schaden durch Cyberkriminalität

Stand: 01.09.2023 13:35 Uhr

„Wenn alles miteinander vernetzt ist, kann auch alles gehackt werden“

Ursula von der Leyen, State of the Union Rede, 2021

CRA in a nutshell

Was?

Art. 3 Nr. 1 CRA

Ein Produkt mit digitalen Elementen ist „ein Software- oder Hardwareprodukt und dessen Datenfernverarbeitungslösungen, einschließlich Software- und Hardwarekomponenten, die getrennt in Verkehr gebracht werden sollen“

Wer?

Alle Wirtschaftsteilnehmer der Lieferkette

(Hersteller, Importeur, Händler)

Wann?

2026: Meldepflichten

2027: restliche Verpflichtungen des CRA

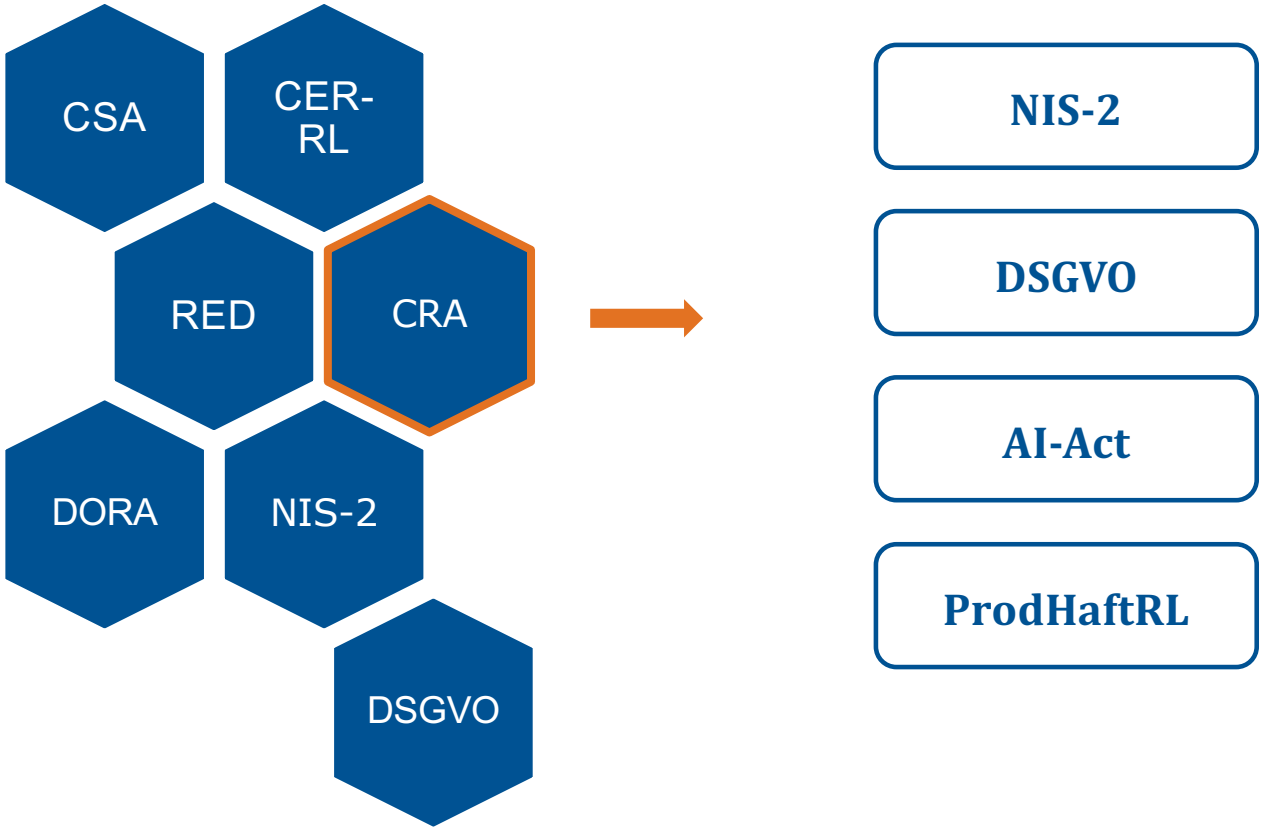
CRA in a nutshell

Pflichten der Hersteller

CE

- Angemessenes Cybersicherheitsniveau („Security by Design“) Anhang I, Teil 1
- fortlaufende Produktüberwachung und Updatepflicht für Schwachstellen
- Melde-, Informations- und Dokumentationspflichten

CRA als Teil der europäischen Cybersicherheitsregulierung



CRA als Gesetz „mit digitalen Elementen“

1 Open Source Software

2 CRA und AI-Act

3 CRA und das digitale Schuldrecht

1 CRA und OSS – Entwurfsfassung

Interessensverband warnt

NETZPOLITIK.ORG

Cyber Resilience Act gefährdet Open Source

> Um die Innovation oder die Forschung nicht zu behindern, sollte freie und quelloffene Software, die **außerhalb einer Geschäftstätigkeit** entwickelt oder bereitgestellt wird, nicht unter diese Verordnung fallen.

ErwGr 10
CRA-E

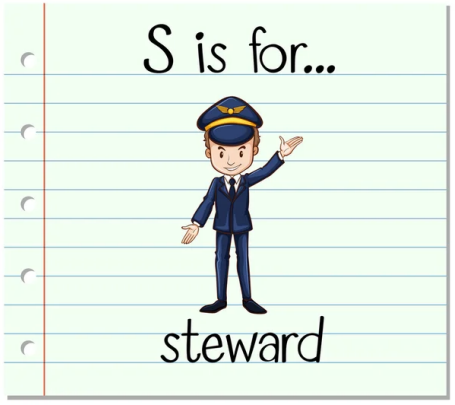
1 CRA und OSS – nach dem Trilog

ErwGr 18

ErwGr 19

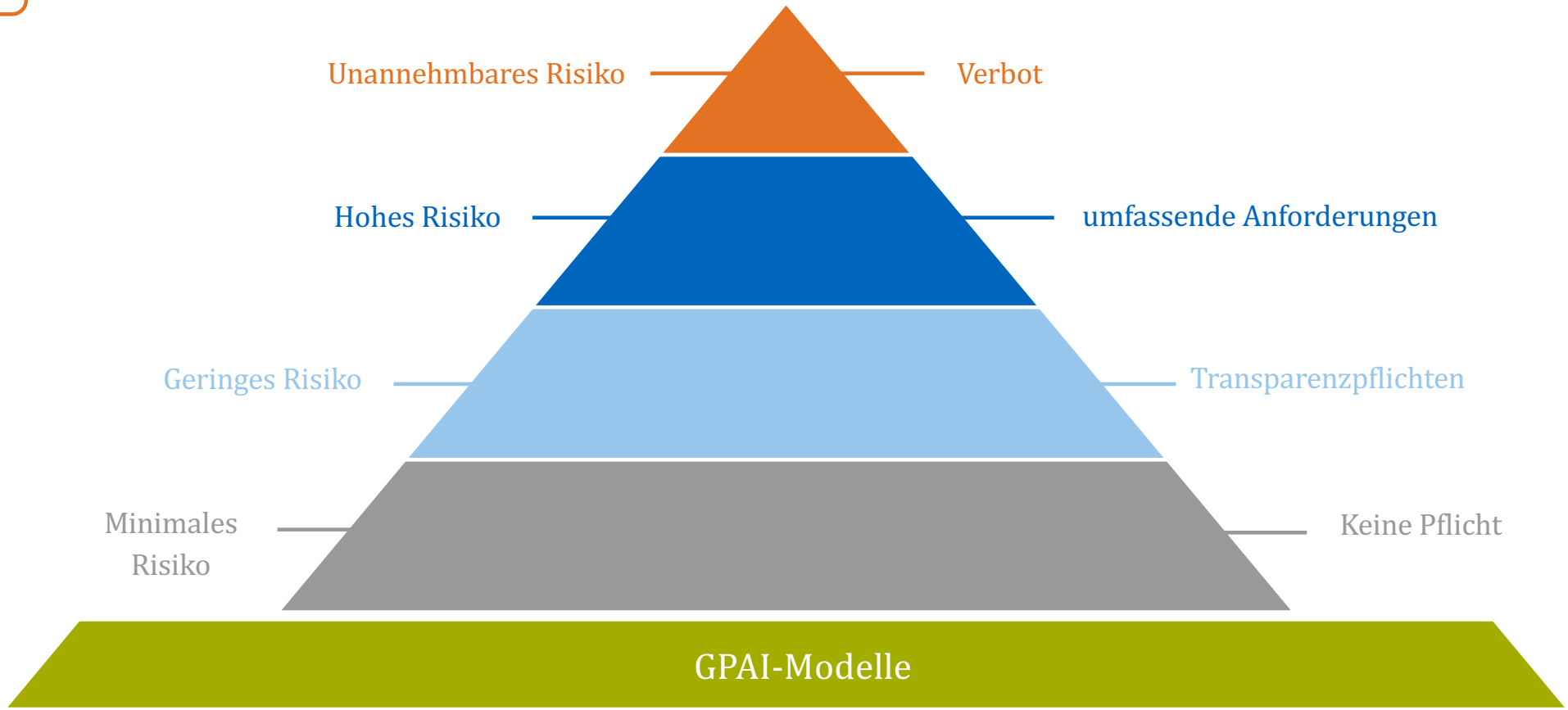
- Nur noch sehr wenige OSS-Projekte zukünftig betroffen
- OSS-Community mit Änderungen zufrieden

neu:

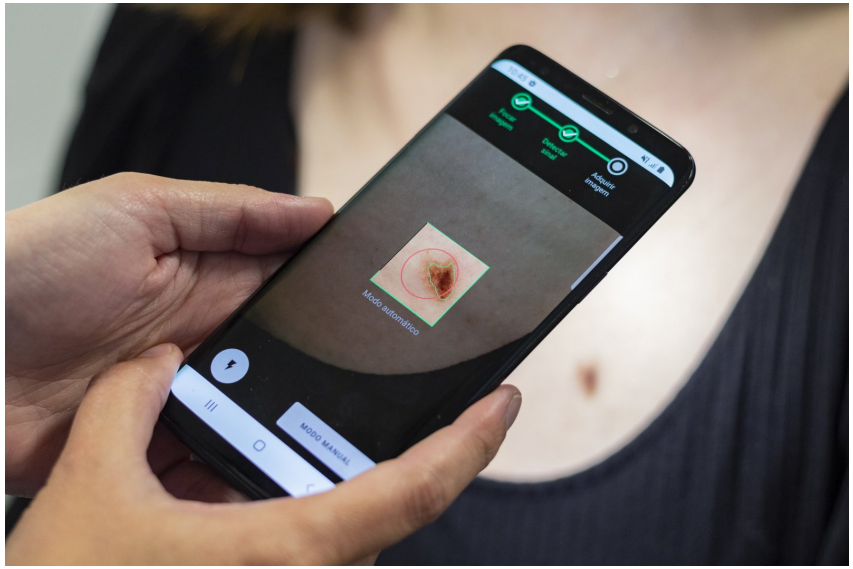


„OSS-Verwalter“ / „OSS-Steward“

2 CRA und der AI-Act



2 CRA und der AI-Act



© Fraunhofer AICOS

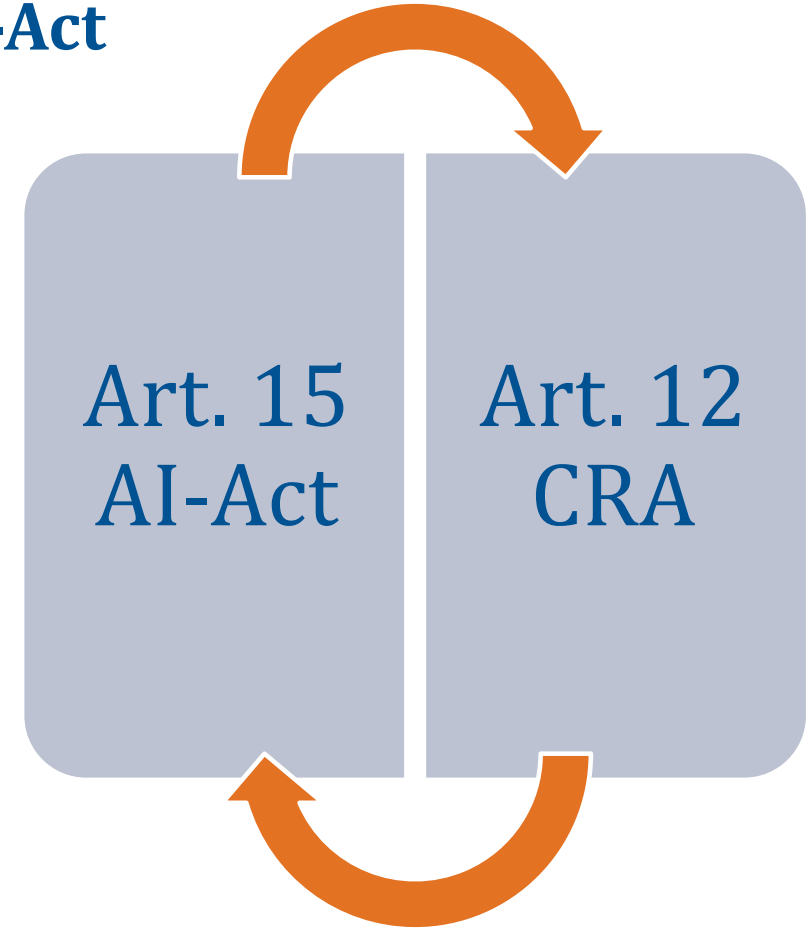
2 CRA und der AI-Act

„so widerstandsfähig wie möglich“

TOMs

Robustheit durch technische Redundanz

Schutz vor „Datenvergiftung“ und “Modellvergiftung“



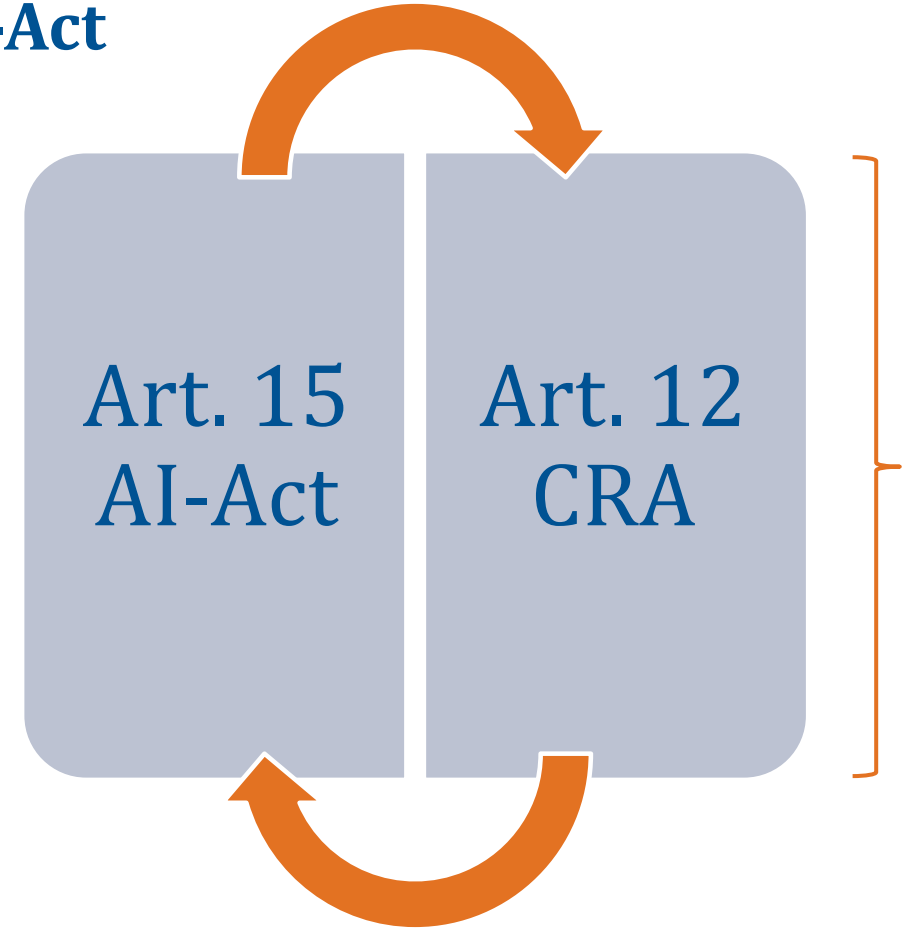
Überschneidung im Anwendungsbereich

Cybersicherheitsanforderungen des Art. 15 AI-Act gelten als erfüllt, wenn Anforderungen des CRA erfüllt werden

2 CRA und der AI-Act

ohne ausnutzbaren Schwachstellen

Datenminimierung bei KI



beide Rechtsakte zusammen denken!

3 CRA und das digitale Schuldrecht

Der CRA wird auch Auswirkungen auf vertraglicher Eben haben!

§ 327 ff. BGB

Umsetzung der Digitale-Inhalte-RL

Anwendungsbereich

- B2C
- dem Kaufrecht vorrangig

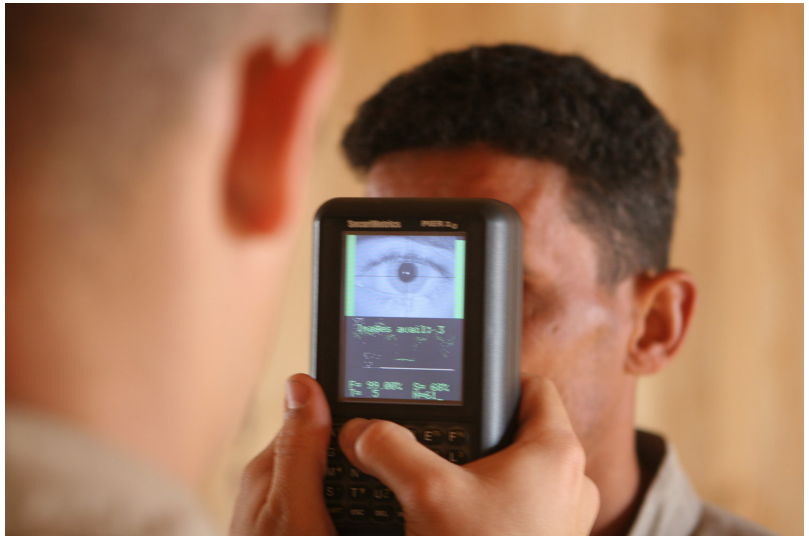
Digitale Produkte
iSv § 327 Abs. 1 BGB

nicht verwechseln mit den Produkten mit digitalen Inhalten

Produktmangel
iSv § 327e BGB

Einfallstor für den CRA?

3 CRA und das digitale Schuldrecht



3 CRA und das digitale Schuldrecht

§ 327e BGB – Produktmangel

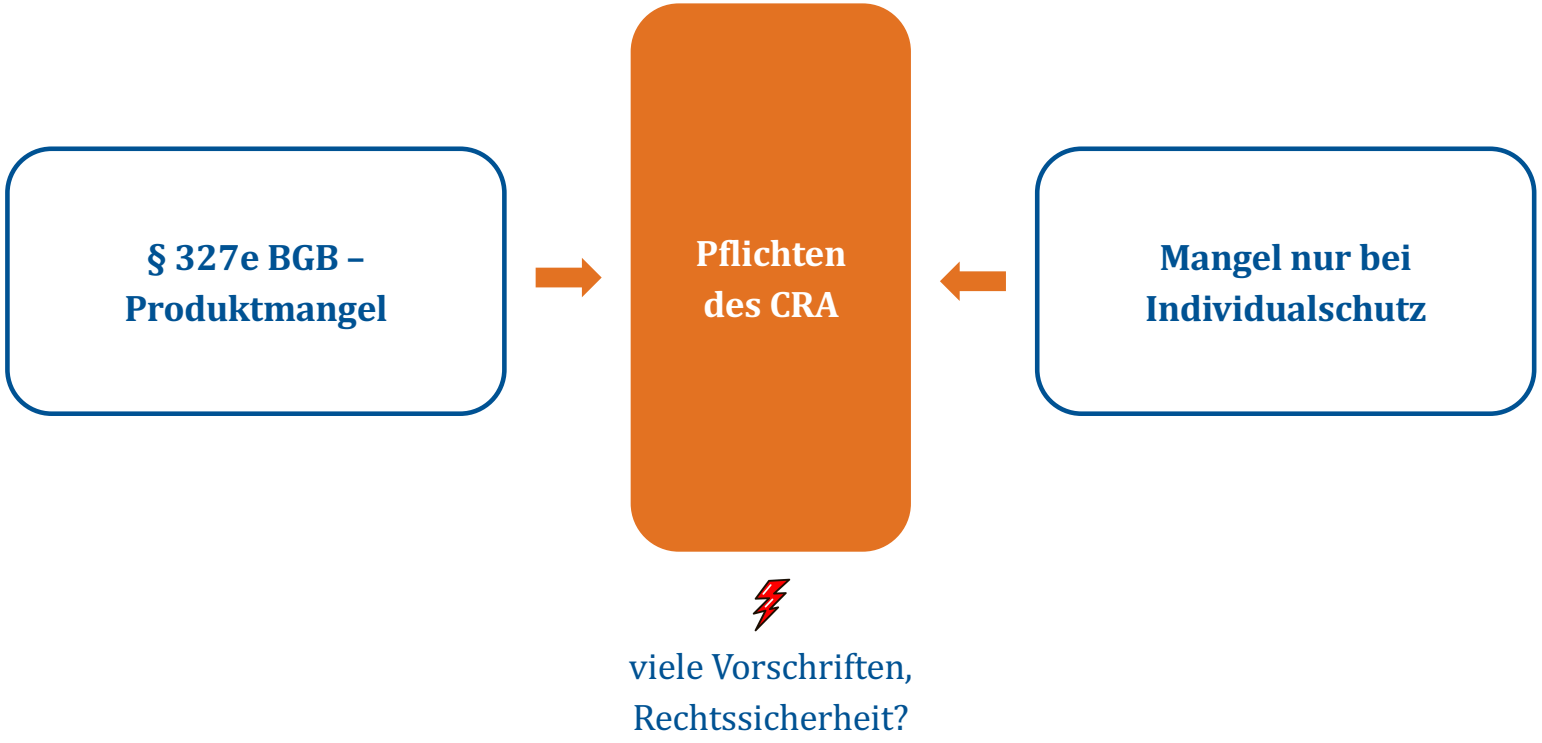
(3) [1]Das digitale Produkt entspricht den objektiven Anforderungen, wenn
1.es sich für die **gewöhnliche Verwendung** eignet,
2.es eine Beschaffenheit, einschließlich der Menge, der Funktionalität, der Kompatibilität, der Zugänglichkeit, der Kontinuität und der **Sicherheit** aufweist, die bei digitalen Produkten derselben Art üblich ist und die der **Verbraucher** unter Berücksichtigung der Art des digitalen Produkts **erwarten kann**

↓ produktspezifische Vorgaben

↓ europäisches Sekundärrecht

DSGVO-Verstöße als Produktmangel

3 CRA und das digitale Schuldrecht



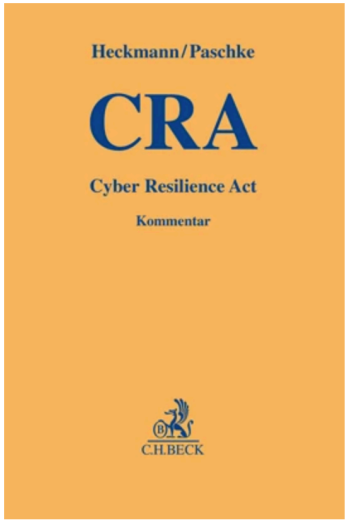
Happy to discuss!

Dirk-Heckmann

dirk.heckmann@tum.de

@elawprof
@TumCdps

Das Buch zum Film:



Ankündigung

Heckmann / Paschke

Cyber Resilience Act • CRA

Kommentar
Buch. Hardcover
2025
Rund 650 S.
C.H.BECK. ISBN 978-3-406-82441-8
Format (B x L): 12,8 x 19,4 cm

Das Werk ist Teil der Reihe: › **Gelbe Erläuterungsbücher**