

TeleTrust-"IT-Sicherheitsrechtstag" 2024

Berlin, 25.09.2024

Cyber Resilience Act – Haftungsrechtliche Konsequenzen

Prof. Dr. Laura Schulte, Hochschule Bielefeld



Cyber Resilience Act – Haftungsrechtliche Konsequenzen

Prof. Dr. Laura Schulte

ÜBERBLICK

II Ziele & Verfahrensstand

II Anwendungsbereich

II Rechtspflichten

II Sanktionen

II Fazit

ÜBERBLICK

II Ziele & Verfahrensstand

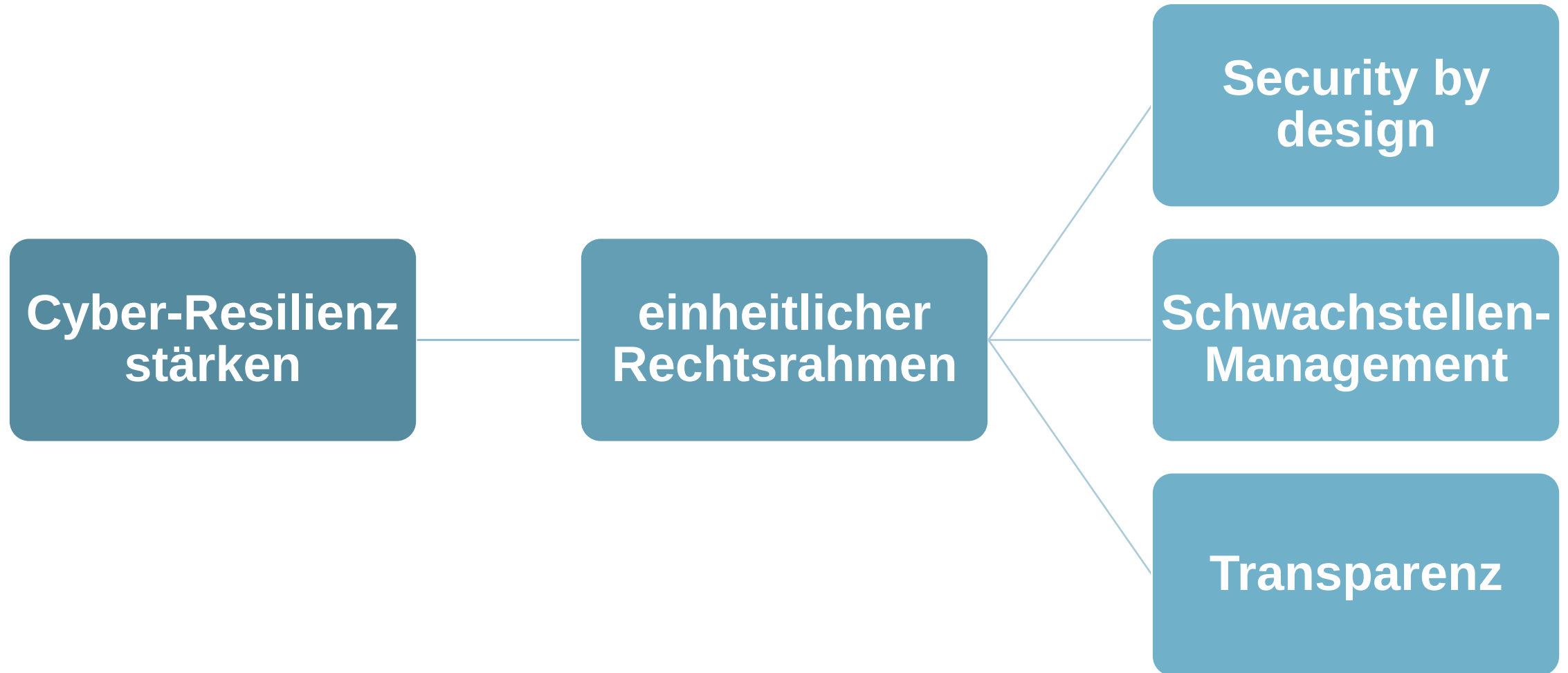
II Anwendungsbereich

II Rechtspflichten

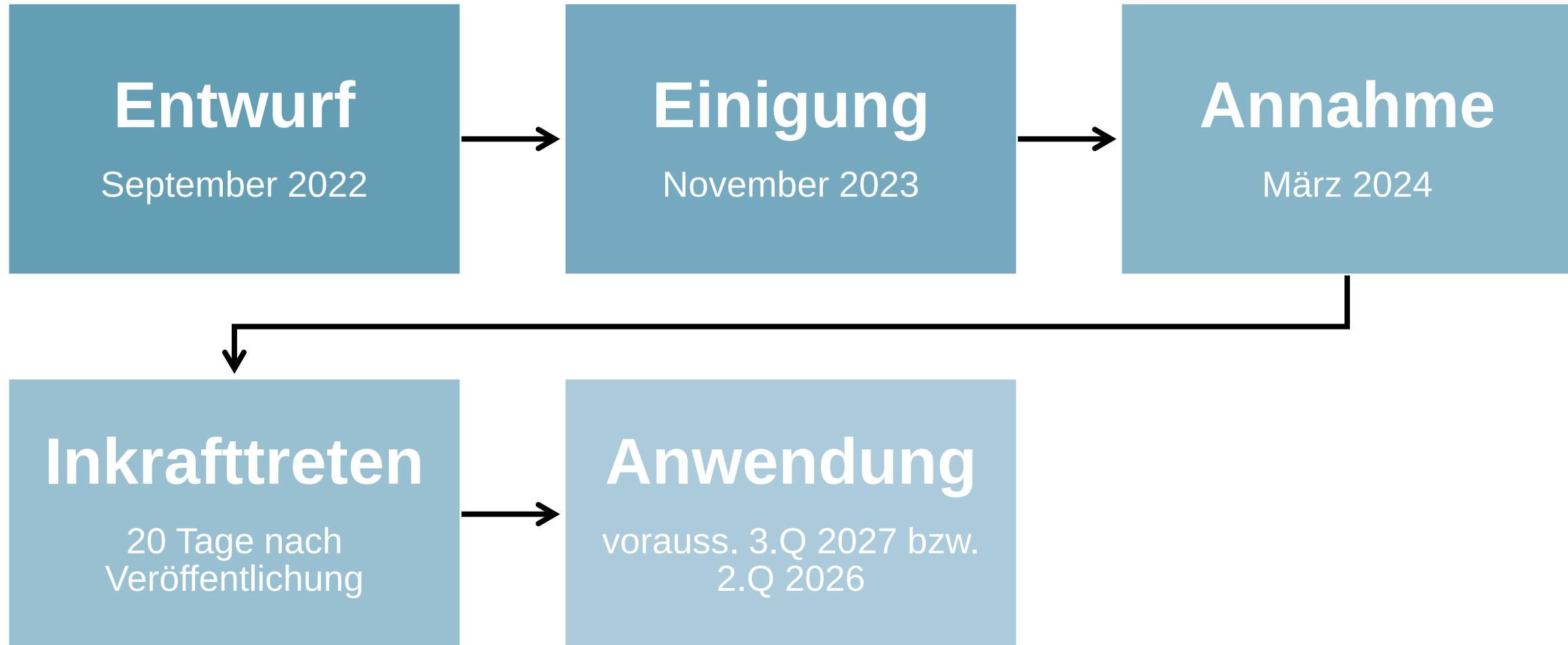
II **Sanktionen**

II Fazit

ZIELE

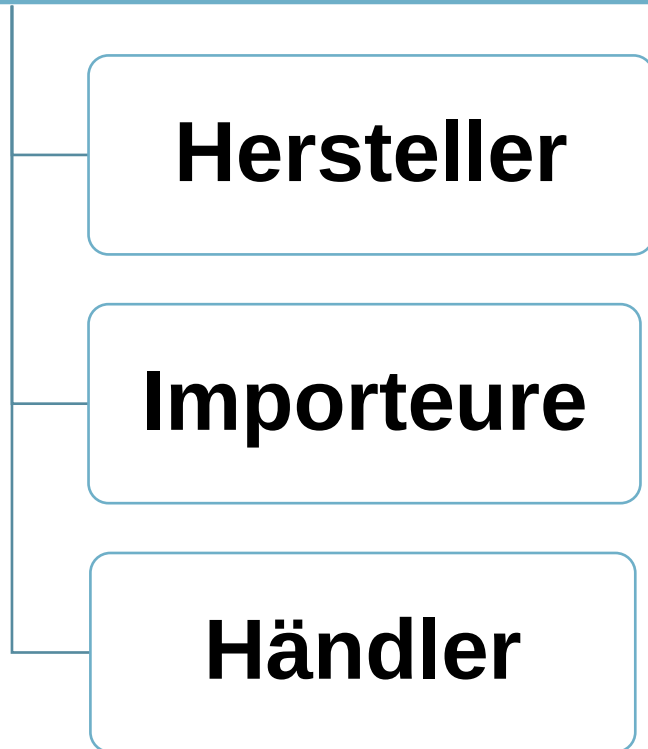


VERFAHRENSSTAND



ANWENDUNGSBEREICH

persönlich



sachlich



RECHTSPFLICHTEN

II Verpflichtungen für Hersteller

- grundlegende **Cybersicherheitsanforderungen**
- obligatorische Prozesse zur **Behandlung von Schwachstellen**
- **Konformitätsbewertung**
- **Informations- und Transparenzpflicht**

II Importeure und Händler

- Handeln nur mit Produkten, die erforderliche **Kennzeichnung** tragen und **wesentliche Cybersicherheitsanforderungen** erfüllen

SANKTIONEN – ALLGEMEINES

Artikel 64 Sanktionen

- (1) ¹Die Mitgliedstaaten erlassen Vorschriften über Sanktionen, die bei Verstößen der Wirtschaftsakteure gegen diese Verordnung zu verhängen sind, und treffen alle für die Umsetzung der Sanktionen erforderlichen Maßnahmen. **²Die vorgesehenen Sanktionen müssen wirksam, verhältnismäßig und abschreckend sein.** ³Die Mitgliedstaaten teilen der Kommission diese Vorschriften und Maßnahmen unverzüglich mit und melden ihr unverzüglich alle diesbezüglichen Änderungen.

SANKTIONEN – ALLGEMEINES

- II Wirtschaftsakteure sollen sich während des **gesamten Lebenszyklus** um Sicherheit bemühen
- II **Mitgliedstaaten** sollen Sanktionsvorschriften erlassen und durchsetzen
- II Norm setzt engen Rahmen für Ausfüllung des Regelungsauftrages
 - **maximale Bußgeldhöhe**
 - **Bemessungskriterien**
- II **Privilegierung** von Kleinstunternehmen und kleinen / mittleren Unternehmen sowie für Verwalter quelloffener Software

SANKTIONEN – ALLGEMEINES

Artikel 64 Sanktionen

- (2) Bei **Nichteinhaltung der grundlegenden Anforderungen in Anhang I oder Verstößen gegen die in den Artikeln 13 und 14** festgelegten Pflichten, werden Geldbußen von **bis zu 15 000 000 EUR oder** – im Falle von Unternehmen – von bis zu **2,5 %** des gesamten weltweiten **Jahresumsatzes** des vorangegangenen Geschäftsjahres verhängt, je nachdem, welcher Betrag höher ist.

SANKTIONEN – ALLGEMEINES

- || nahezu jeder Verstoß gegen CRA kann mit einem Bußgeld geahndet werden
- || Bußgeldrahmen hängt von dem jeweils begangenen Verstoß ab
- || Verstöße gegen Vorgaben, die **direkten Bezug zur Cybersicherheit** haben, wiegen schwerer als Verstöße gegen formale Vorgaben:
 - Verstöße gegen **Art. 13 und Art. 14** sowie
 - Verstöße gegen die **Vorgaben in Anhang I**

SANKTIONEN – ALLGEMEINES

Artikel 64 Sanktionen

- (5) *Bei der Festsetzung der Geldbuße werden in jedem Einzelfall alle **relevanten Umstände der konkreten Situation** sowie Folgendes gebührend berücksichtigt:*
- a) ***Art, Schwere und Dauer des Verstoßes** und dessen Folgen,*
 - b) *ob bereits dieselbe oder andere Marktüberwachungsbehörden demselben Wirtschaftsakteur **für einen ähnlichen Verstoß Geldbußen auferlegt** haben,*
 - c) ***Größe**, insbesondere im Hinblick auf Kleinunternehmen sowie kleine und mittlere Unternehmen, einschließlich Start-up-Unternehmen, **und Marktanteil des Wirtschaftsakteurs**, der den Verstoß begangen hat.*

SANKTIONEN – BEMESSUNGSKRITERIEN

- II ausdrücklich **benannter Kriterien + Einzelfallumständen = Wirksamkeit, Verhältnismäßigkeit und Abschreckung**
- II in § 17 Abs. 3 OWiG genannte Kriterien können keine Berücksichtigung finden
 - **Autonomie des Unionsrechts**
 - **einheitlichen Anwendung des CRA**
- II einheitliche **Leitlinien zur Bemessung von Bußgeldern** werden sich frühestens mittelfristig herausbilden

SANKTIONEN – BEMESSUNGSKRITERIEN

|| Art, Schwere und Dauer des Verstoßes und dessen Folgen (lit. a)

- **Vorsatz oder Fahrlässigkeit?**
- cybersicherheitsrelevante Vorgaben oder „bloß“ formale Anforderung?
- systematische Zuwiderhandlung?
- Tateinheit oder Tatmehrheit?
- **Schwere des Verstoßes:** leichter, schwerer oder besonders schwerer Verstoß?
- **eingetretener Schaden bzw. mit Verstoß verbundene Gefahr:** Leib und Leben und/oder Vermögensschäden?
- **Dauer des Verstoßes:** kurz, mittel- und langfristige Dauer?

SANKTIONEN – BEMESSUNGSKRITERIEN

II Bereits verhängte Geldbußen (lit. b)

- **Hat sich** mit Bußgeld verfolgter **Zweck** angesichts eines im Wesentlichen vergleichbaren Verstoßes **bereits realisiert**?
- im Wesentlichen gleichartiger Verstoß siehe insbes. Abs. 5 lit. a)
- **Vergleichbarkeit** von **Verletzungshandlung und -erfolg** unter Berücksichtigung eines **zeitlichen und sachlichen Zusammenhangs**

SANKTIONEN – BEMESSUNGSKRITERIEN

II Bereits verhängte Geldbußen (lit. b)

- bereits verhängte Sanktion kann sowohl erschwerend als auch mildernd wirken
- **erschwerend:** wenn Verstoß in einem anderen Mitgliedstaat weiter andauert (Spezialprävention)
- **Gefahr paralleler Bußgeldverfahren:** Soweit jeweils verletzter Rechtsakt unterschiedliche Zwecke verfolgt und andere Umstände würdigt keine mildernde Wirkung

SANKTIONEN – BEMESSUNGSKRITERIEN

II Größe und Marktanteil des Akteurs (lit. c)

- Indikatoren für Leistungsfähigkeit des Bußgeldadressaten
- Größe des Akteurs wohl unabhängig von dem jeweiligen Verstoß (Leistungsfähigkeit) und **Marktanteil – soweit möglich – produktbezogen** (Schaden)
- potenzielle Geldbußen sollen nicht „eingepreist“ werden
- Privilegierung von Kleinstunternehmen sowie kleinen und mittleren Unternehmen inkl. Start-up-Unternehmen

SANKTIONEN – BEMESSUNGSKRITERIEN

|| Einzelfallumstände und sonstige Kriterien

- **Art der Zumessungskriterien und konkrete Gewichtung sind in jedem Bußgeldverfahren gesondert zu bewerten**
- allgemeine Grundsätze: Gleichbehandlung und Effektivität
- Wie lang liegt Verstoß zurück?
- Wie ist Verstoß bekannt geworden?
- Verhalten des Wirtschaftsakteurs vor und nach Verstoß

FAZIT

|| Haftungsrisiko im Bereich IT-Sicherheit wird durch CRA steigen

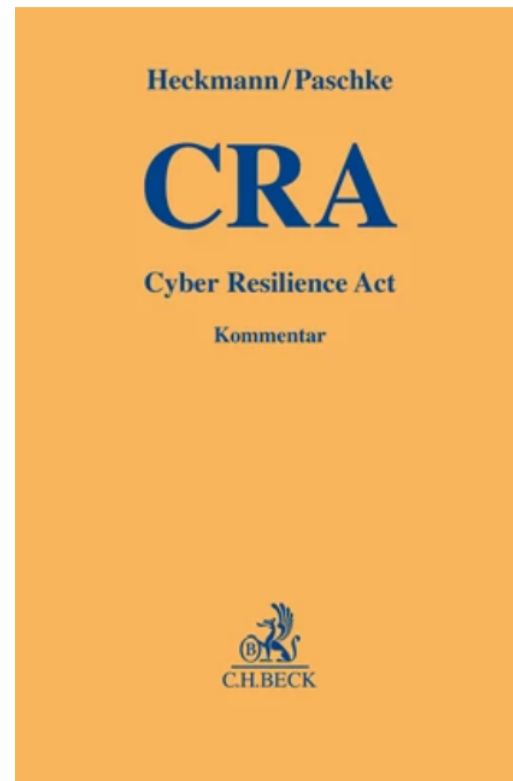
- bis zur Herausbildung einheitlicher Leitlinien / Rechtsprechung erhebliche Rechtsunsicherheit
- bei Auslegung und Anwendung des CRA werden sich Gerichte und Behörden voraussichtlich an Erfahrungen aus Datenschutz- und Produktsicherheitsrecht orientieren

|| Wirtschaftsakteure sollten sich frühzeitig mit CRA auseinandersetzen

- um komplexe Anforderungen zu ermitteln und Prozesse umzusetzen

FAZIT

**Umsetzung rechtlicher
Vorgaben des CRA
sowie
haftungsreduzierender
Vereinbarungen
bedürfen spezieller
juristischer Expertise**



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**

KONTAKT

Prof. Dr. jur.
Laura Schulte

Hochschule Bielefeld
Interaktion 1
33619 Bielefeld

laura.schulte@hsbi.de





Vielen Dank für Ihre Aufmerksamkeit