Change Rules

100% Know-How. 0% Nonsense.

04. April 2025

reusch law

Cyber Resilience Act: Neue Anforderungen an die Cybersicherheit von Produkten

04.04.2025

RAin Christina Kiefer, LL.M.
Senior Associate Digital Business

Agenda

1. Einführung
2. Anwendungsbereich des CRA
3. Vorgaben an die Cybersicherheit
4. CRA und die MedTech-Branche
5. Cybersicherheit in der Lieferkette
6. Praktische Umsetzung

Einführung

Cybersicherheitsrecht

Status Quo: Dynamische Bedrohungslage – Statische Rechtslage

Zunehmende

Digitalisierung und Vernetzung von Produkten und Unternehmen

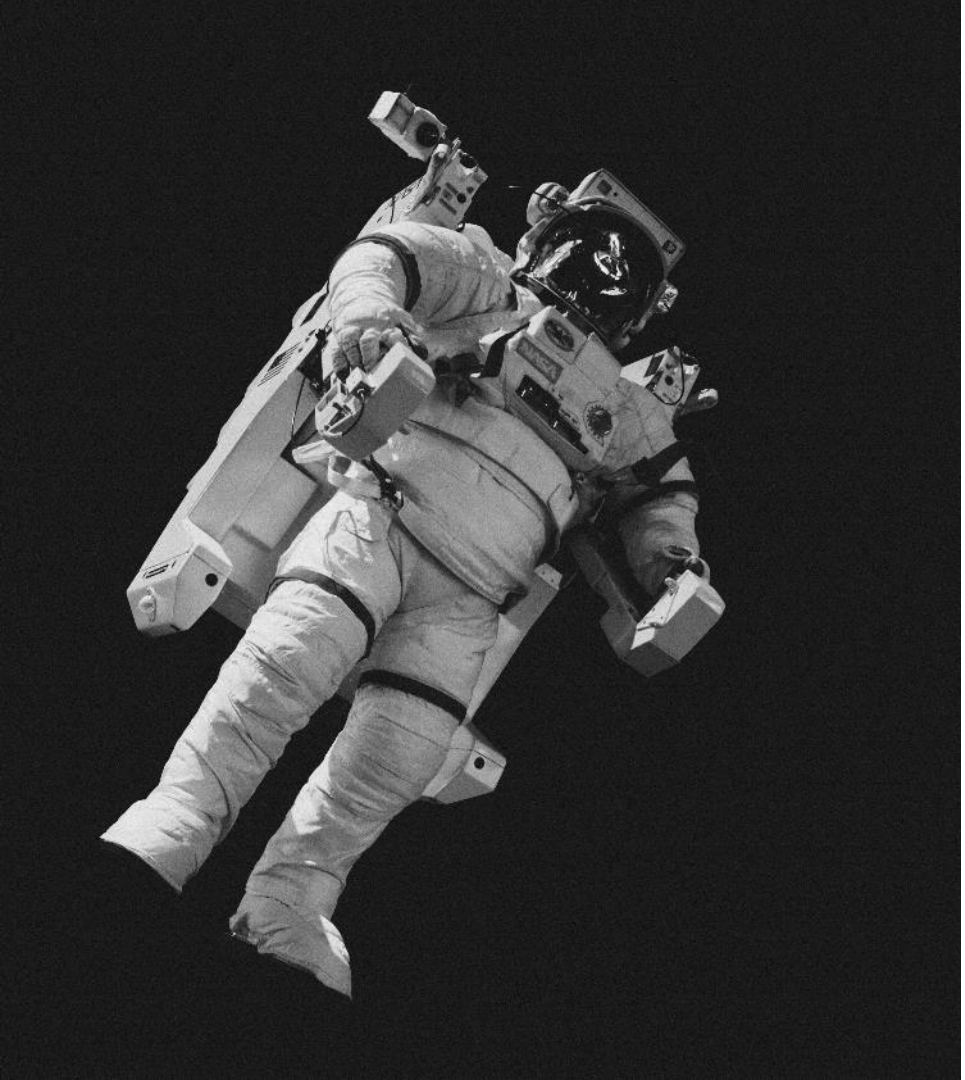
78

neue Schwachstellen pro Tag im Jahr 2023
= 14 % mehr als im Jahr 2022*

0

Allgemeine Gesetze zur Cybersicherheit für Unternehmen und Produkte

*BSI, Die Lage der IT-Sicherheit in Deutschland 2024



EU-Digitalrecht: Cybersicherheit im Fokus

- **Legislative Train**: “A Europe Fit for the Digital Age”
  - 114 Projekte mit digitalem Schwerpunkt
  - 89 davon legislativer Natur
- Schwerpunkt auf **Cybersicherheit**
  - Digitalisierung
  - Innovationsgeschwindigkeit vs. regulatorische Belastung

NIS-2 und CRA als Bausteine einer neuen europäischen Cybersicherheitsarchitektur

NIS-2

Unternehmensbezogene Richtlinie

Status: In Kraft getreten am 16.01.2023 → Umsetzung durch die Mitgliedstaaten

CRA

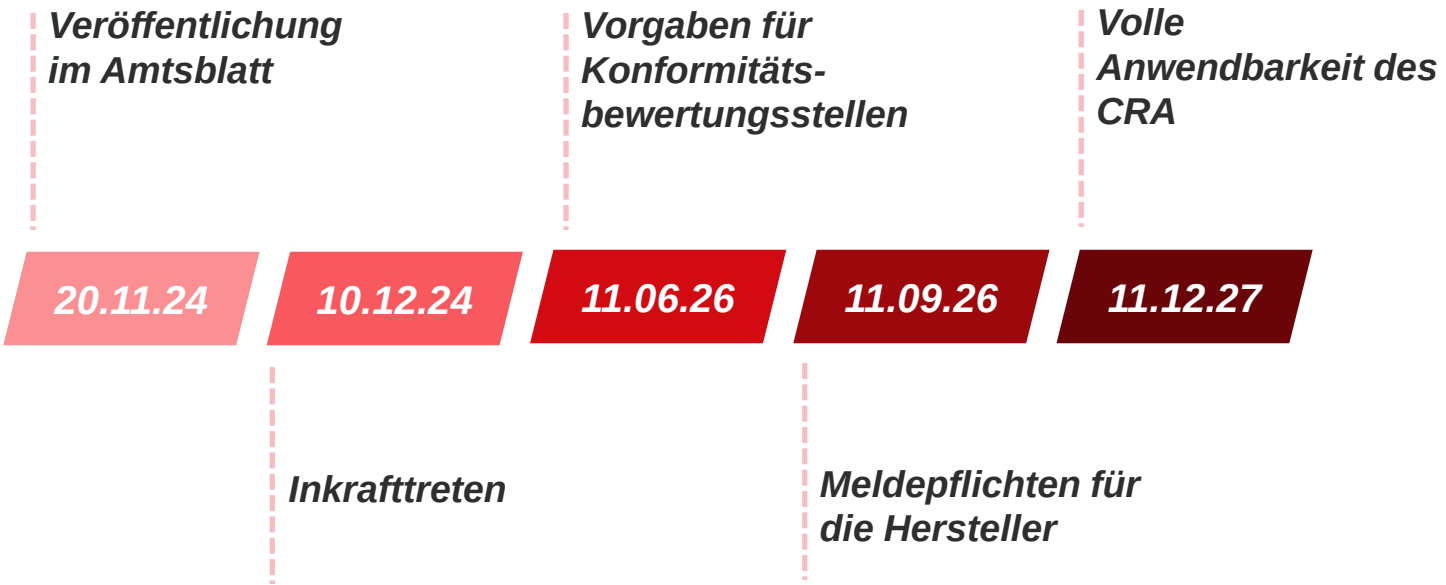
Produktbezogene Verordnung

Status: In Kraft getreten am 10.12.2024→ Schrittweise Anwendung bis 11.12.2027

CRA: Überblick und aktueller Stand

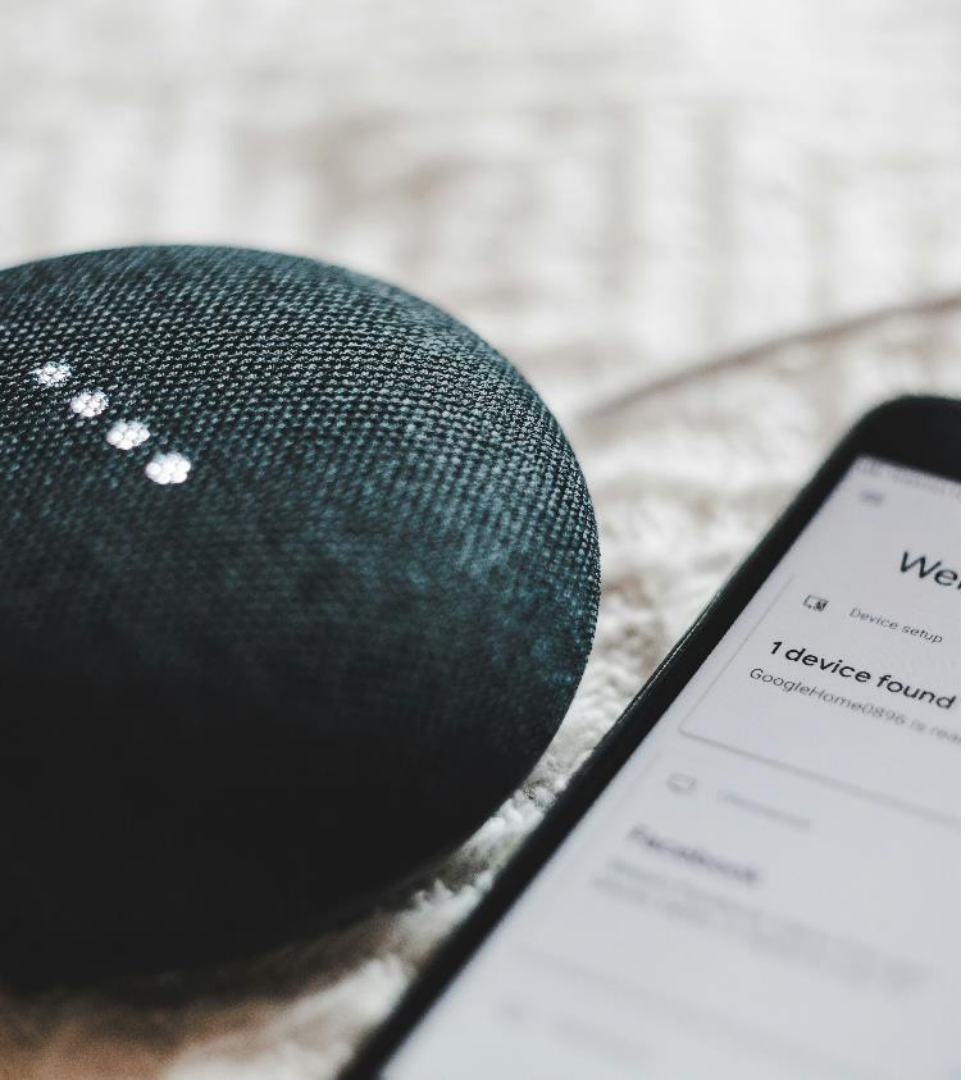
- Verordnung (EU) 2024/2847
- Horizontale, produktbezogene Verordnung
- Unmittelbar anwendbare Anforderungen an die Cybersicherheit für Produkte mit digitalen Elementen
- Keine nationale Umsetzung erforderlich
- Inkrafttreten: 10.12.2024
- Übergangsfrist von bis zu drei Jahren
- Beachte: Wechselwirkungen mit anderen Regelungen des EU-(Digital-)Rechts, wie z.B. KI-Verordnung und Datenschutz-Grundverordnung

Timeline


Veröffentlichung im Amtsblatt
Vorgaben für Konformitäts-bewertungsstellen
Volle Anwendbarkeit des CRA
20.11.24
10.12.24
11.06.26
11.09.26
11.12.27
Inkrafttreten
Meldepflichten für die Hersteller

Anwendungsbereich des CRA

„Produkte mit digitalen Elementen“



Anwendungsbereich

- Sachlich: **Produkte mit digitalen Elementen**
  - Softwareprodukte
  - Hardwareprodukte mit Datenfernverarbeitungslösungen
  - Software- oder Hardwarekomponenten, die getrennt in Verkehr gebracht werden
- Ausnahmen für bestimmte regulierte Produkte
- **Räumlich**: Entgeltliche oder unentgeltliche Bereitstellung auf dem Unionsmarkt im Rahmen einer Geschäftstätigkeit → Marktortprinzip
- Kostenloser Quick-Check: https://cra-check.de

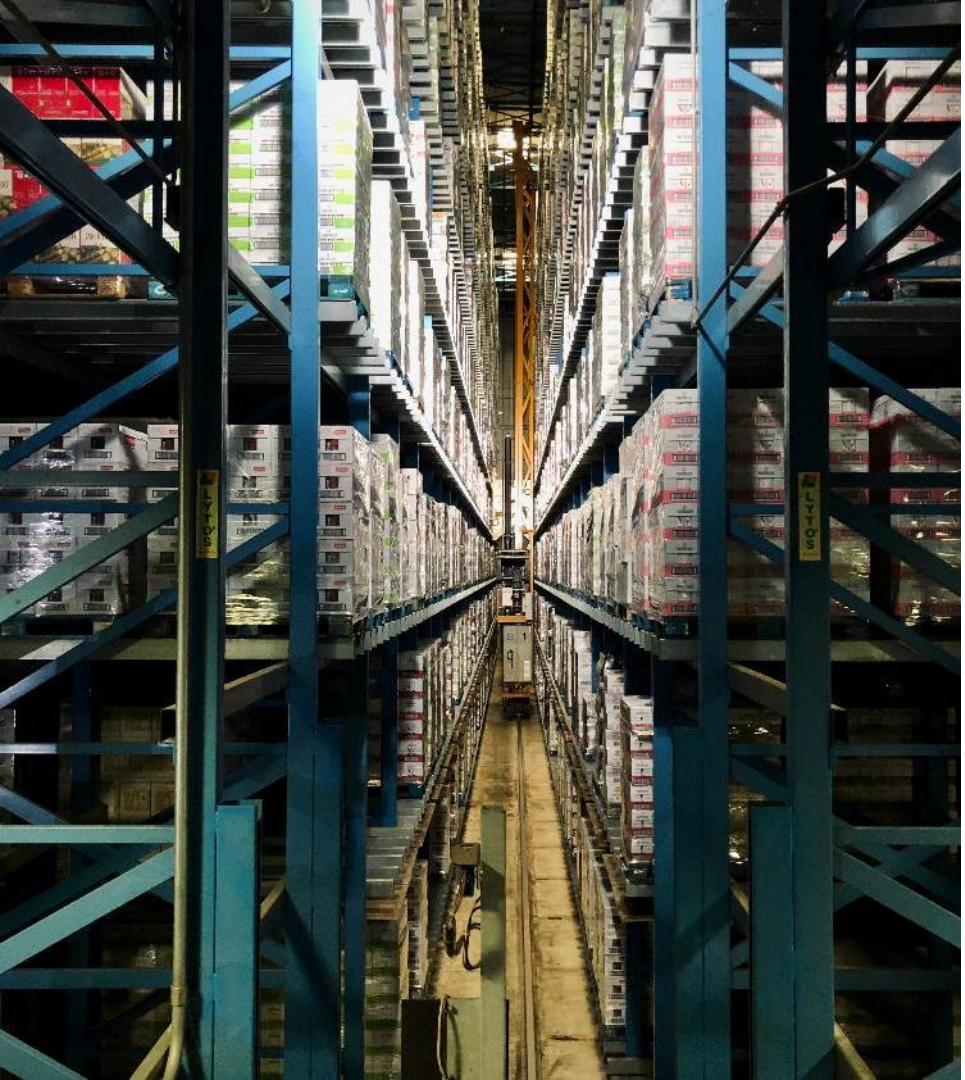
Ausnahmen vom Anwendungsbereich

- **Medizinprodukte und IVD**
- Kraftfahrzeuge
- Produkte der Zivilluftfahrt
- Schiffsausrüstung
- Ersatzteile, die identische Komponenten auf dem Markt ersetzen
- Nationale Sicherheit und Verteidigungszwecke
- **Im Einzelfall**: Produkte, die unter Rechtsvorschriften fallen, die die Risiken aus Anhang I CRA regulieren

Kategorien von Produkten mit digitalen Elementen

90 % der Produkte	10 % der Produkte		
Standard Konformitätsbewertung durch den Hersteller (Art. 32 Abs. 1 CRA)	**Wichtige Produkte "Klasse I„** Anwendung harmonisierter Normen oder Konformitätsbewertung durch eine dritte Partei (Art. 32 Abs. 2 CRA)	**Wichtige Produkte "Klasse II„** Konformitäts-bewertung durch eine dritte Partei (Art. 32 Abs. 3 CRA)	**Kritische Produkte** Europäisches Zertifizierungssystem für Cybersicherheit (Schema nach Cyber Security Act, bisher nur: EUCC-Schema) oder, solange kein Schema vorhanden ist: Bewertung durch dritte Partei nach Abs. 3
Kriterien: Software- oder Hardwareprodukt und seine Datenfern-verarbeitungslösungen	Kriterien: Funktionalität (z.B. kritische Software), Verwendungszweck (z.B. Industrieanlage, NIS-2), sonstige Kriterien (z.B. mögliche negative Auswirkungen)		Kriterien: Kernfunktionalität einer in Anhang IV aufgeführten Kategorie
Beispiele: Bild- und Textverarbeitung, Lautsprecher, Festplatten, Computerspiele	Beispiele (**Anhang III**): Browser, Passwortmanager, VPN und Netzwerk, Bootmanager, Router, Smart Home, Spielzeug, Wearables	Beispiele (**Anhang III**): Virtualisierungssoftware, Firewalls, IDS, manipulations-sichere Mikroprozessoren und -controller	Beispiele (**Anhang IV**): HSM, Smart-Meter-Gateways, Smartcards und vergleichbare Geräte

Konkretisierung durch die EU-Kommission: Befugnis zum Erlass von delegierten Rechtsakten



Adressaten

- Wirtschaftsakteure:
  - **Hersteller** = Person, die Produkte mit digitalen Elementen herstellt oder herstellen lässt oder unter ihrem Namen oder ihrer Marke vermarktet
  - **Bevollmächtigte**
  - **Einführer**
  - **Händler**
  - **Quasi-Hersteller** = Person, die eine wesentliche Änderung am Produkt vornimmt und auf den Markt bringt
- Sonderfall: **Verwalter quelloffener Software**

Vorgaben an die Cybersicherheit

Wer muss was beachten?

Wesentliche Pflichten für Hersteller

1.	2.	3.	4.	5.
Konformität der Produkte mit den Anforderungen nach Anhang I	Bewertung von Cyberrisiken	Bereitstellung von (kostenlosen) Sicherheitsupdates	Meldepflichten bei Sicherheitslücken	Technische Dokumentation

Konformität mit den Anforderungen nach Anhang I

Cybersicherheitsanforderungen

- Keine bekannten Schwachstellen
- Sichere Standardkonfiguration und Updatability
- Schutz vor unbefugtem Zugriff
- Vertraulichkeit, Integrität und Verfügbarkeit
- **Schutz personenbezogener Daten**
- Minimierung potenzieller Angriffsflächen und Eindämmung von Angriffen
- Protokollierung
- Sichere Löschung und Export von Nutzerdaten

Anforderungen an den Umgang mit Schwachstellen

- Schwachstellenmanagement, u.a. durch **SBOM**
- Bereitstellung von kostenlosen Sicherheitsaktualisierungen
- Tests und Überprüfungen der Cybersicherheit
- Bereitstellung von Informationen über behobene Schwachstellen
- Prozess für Responsible Disclosure
- Meldeweg für Schwachstellen

Bewertung von Cyberrisiken

- Grundlage:
  - Verwendungszweck des Produkts
  - Vorhersehbarer Fehlgebrauch
  - Betriebsumgebung
  - Schützende Vermögenswerte
  - Lebensdauer des Produkts
- Mindestinhalt:
  - Anwendbarkeit und Umsetzung der Sicherheitsanforderungen nach Anhang I
  - Einsatz von Drittanbieterkomponenten (auch Open Source)
- Berücksichtigung während des Lebenszyklus

Bereitstellung von Sicherheitsupdates

Festlegung eines Supportzeitraums

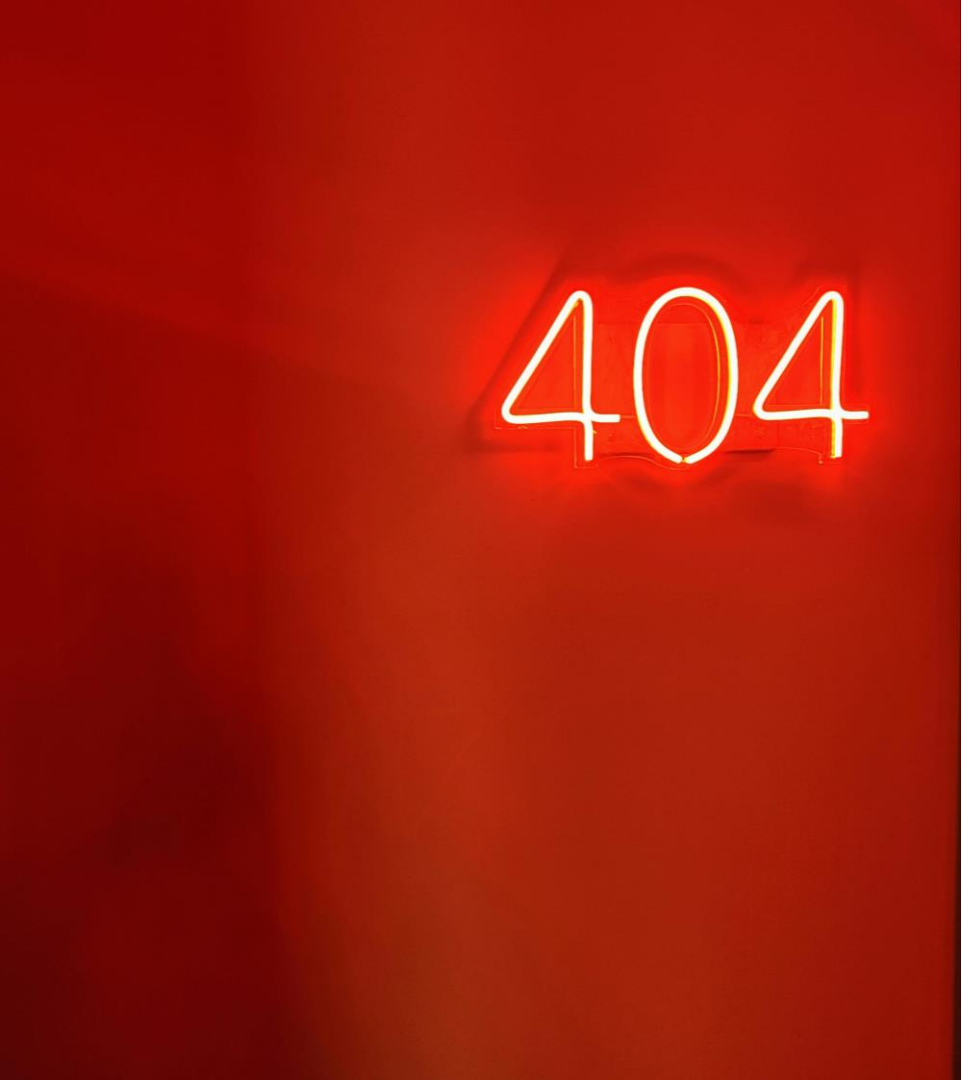
- Erwartung der Nutzer, Art des Produkts, Zweckbestimmung
- Unionsrechtliche Verpflichtungen zur Lebensdauer von Produkten
- Mindestens **fünf Jahre**, sofern Nutzungsdauer nicht kürzer

Anforderungen während des Supportzeitraums

- Updates müssen unverzüglich und in der Regel **kostenlos** zur Verfügung gestellt werden (Ausnahme: maßgeschneiderte Produkte im B2B-Bereich)
- Updates müssen **zehn Jahre** nach dem Inverkehrbringen oder für den Unterstützungszeitraum verfügbar bleiben, je nachdem welcher Zeitraum länger ist
- Bereitstellung **nur** für die zuletzt in Verkehr gebrachte Version der Software, sofern kostenloser Zugang zur letzten Version besteht und der Nutzer keine zusätzlichen Kosten für die Implementierung hat

Pflicht zur Meldung von aktiv ausgenutzten Sicherheitslücken, Art. 14 Abs. 1 CRA

- **Aktiv ausgenutzte Schwachstelle**
  - Schwachstelle (Art. 3 Nr. 40 CRA)
  - Aktiv ausgenutzt: Verlässliche Nachweise für Ausnutzung durch einen böswilligen Akteur (Art. 3 Nr. 42 CRA)
- **Mehrstufiger Meldeprozess**
  - **24 Stunden**: Frühwarnung
  - **72 Stunden**: Meldung
  - **14 Tage** nach Korrektur- oder Abhilfemaßnahme: Abschlussbericht
- Meldung über einheitliche Meldeplattform der ENISA (Art. 16 CRA) → soll zum 11.09.26 eingeführt werden
- Meldepflichten nach anderen Gesetzen bleiben unberührt



Meldepflichten bei schwerwiegenden Vorfällen, Art. 14 Abs. 3 CRA

- **Schwerwiegender Vorfall:**
  - Wirkt sich negativ auf die Fähigkeit eines Produkts aus, die Verfügbarkeit, Authentizität, Integrität oder Vertraulichkeit von Daten/Funktionen zu schützen
  - Einführung oder Ausführung von böswilligem Code in ein Produkt oder im Netzwerk des Produkts
- **Mehrstufiger Meldeprozess:**
  - **Frühwarnung** innerhalb von 24 Stunden
  - **Meldung** innerhalb von 72 Stunden
  - **Abschlussbericht** 1 Monat nach der Meldung
- Meldung über einheitliche Meldeplattform, Art. 16 CRA

Informationspflicht

- Nach Kenntnis einer aktiv ausgenutzten Schwachstelle oder einem schwerwiegenden Vorfall
- Information gegenüber
  - Betroffenen Nutzern des Produktes
  - Ggf. allen Nutzern
- Informationen über
  - Schwachstelle / Vorfall
  - Ggf. Risikominderungsmaßnahmen und Korrekturmaßnahmen, die die Nutzer ergreifen können

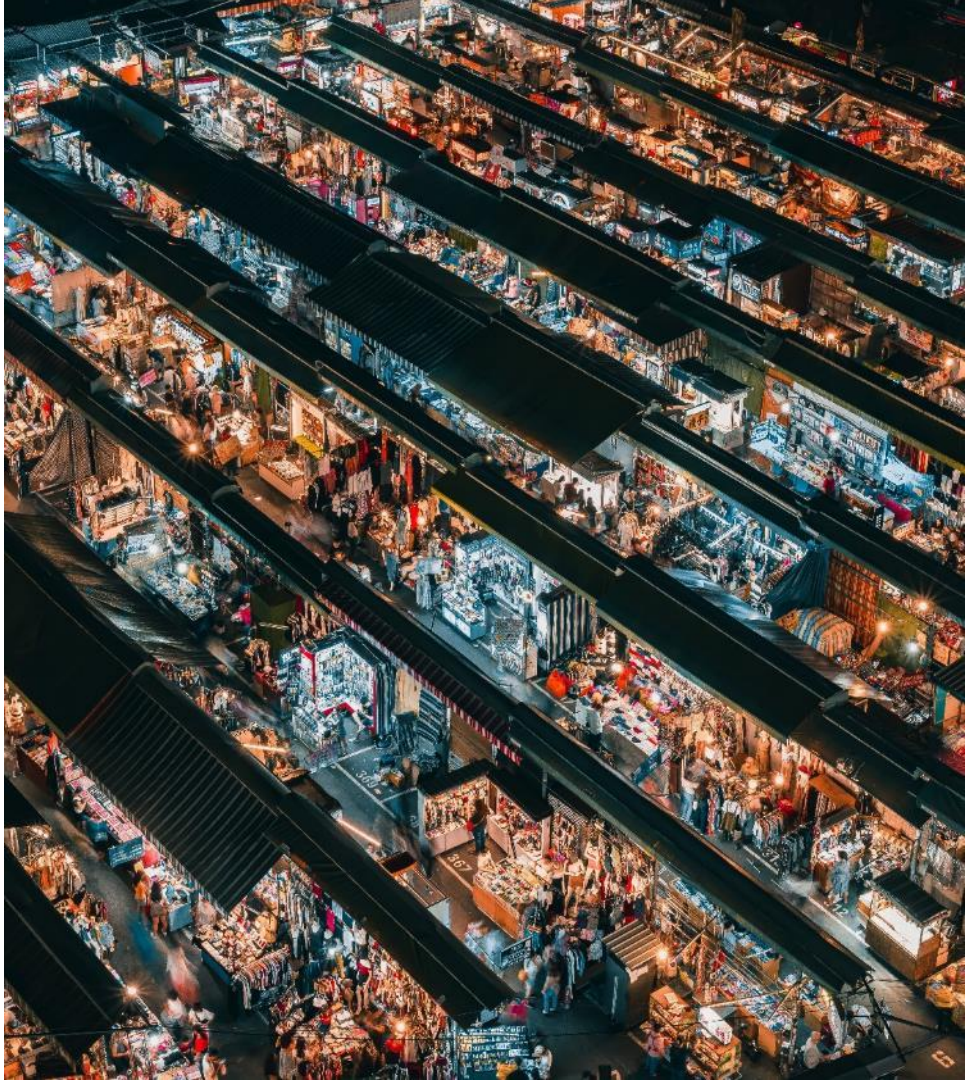
Wesentliche Pflichten für Einführer

- Pflicht zur Prüfung der CRA-Konformität
- Pflicht zur Kontrolle der Angaben und des Konformitätsbewertungsverfahrens des Herstellers
- Ergreifen von **eigenen Korrekturmaßnahmen** bei Nichtkonformität oder ggf. Rücknahme oder Rückruf des Produkts
- **Melde- und Informationspflichten**
- Pflichten des Herstellers anwendbar, wenn
  - Produkt unter eigenem Namen/eigener Marke in Verkehr gebracht oder
  - wesentliche Änderung vorgenommen

  → (**Quasi-Hersteller**)

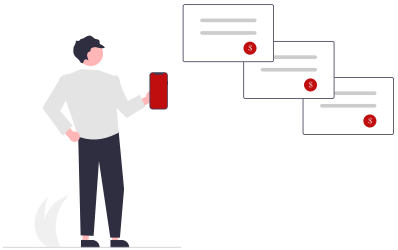
Wesentliche Pflichten für Händler

- Überprüfung der Einhaltung der Pflichten durch Hersteller und Einführer
- **Veranlassung** von Korrekturmaßnahmen bei Nichtkonformität oder ggf. Rücknahme oder Rückruf des Produkts
- **Information des Herstellers** über erkannte Schwachstellen
- Meldepflichten
- Pflichten des Herstellers anwendbar, wenn „Quasi-Hersteller“



Befugnisse und Sanktionen der Aufsichtsbehörden

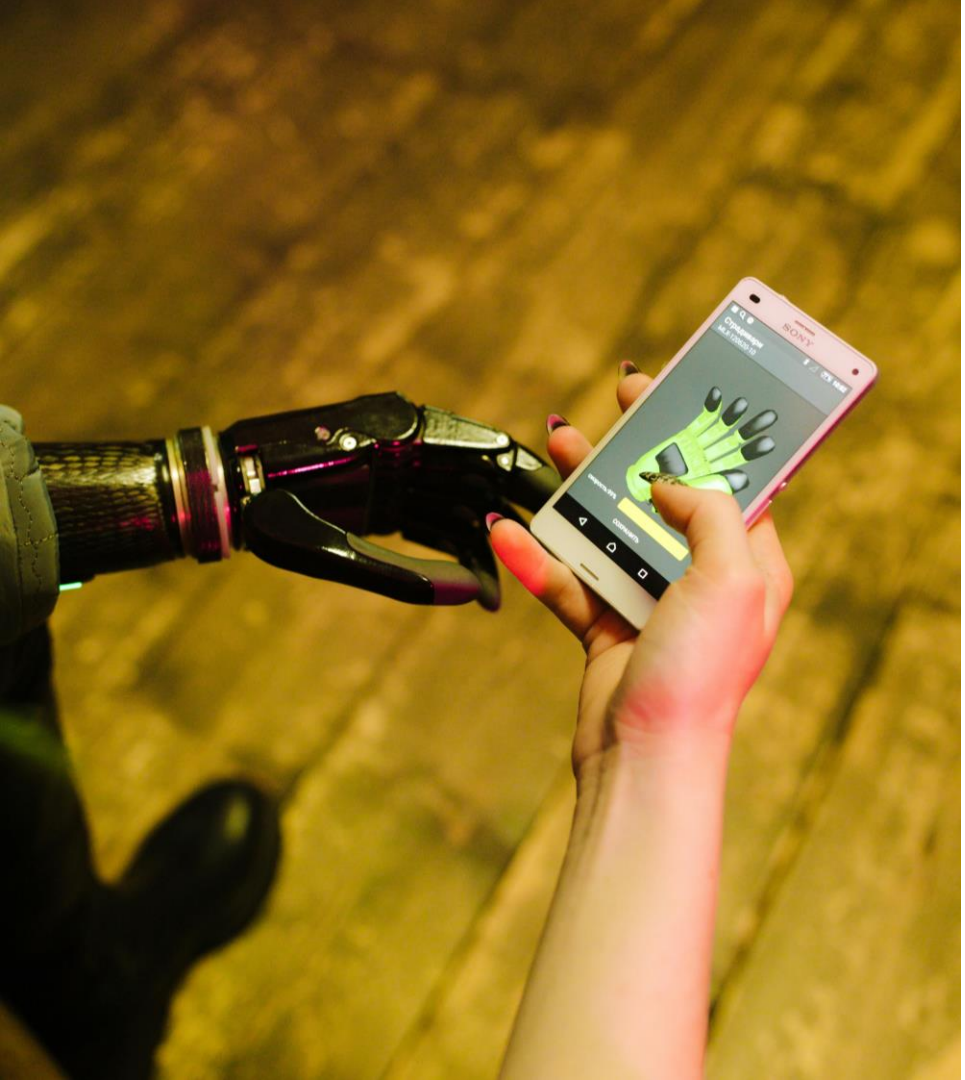
- **Überwachung der Einhaltung durch Marktüberwachungsbehörden:**
  - Zugang zu Daten und zur Dokumentation
  - Überprüfung von Produkten
  - Anweisung und Umsetzung von Korrekturmaßnahmen
  - Entfernung vom Markt oder Produktrückrufe



- **Abgestufte Geldbußen**:
  - bis zu 15 Mio. EUR oder 2,5 % des weltweiten Jahresumsatzes bei Verstößen gegen Anhang I oder **Herstellerpflichten**
  - bis zu 10 Mio. EUR oder 2 % des weltweiten Jahresumsatzes bei Verstößen gegen **sonstige Pflichten** (andere Wirtschaftsakteure, CE-Kennzeichnung und Konformität, Dokumentation)
  - Bis zu 5 Mio. EUR oder 1 % des weltweiten Jahresumsatzes bei **falschen Auskünften**

CRA und die MedTech-Branche

Besondere Herausforderungen



CRA und die MedTech-Branche

- Medizinprodukte und IVD sind vom Anwendungsbereich ausgeschlossen
- Aber anwendbar auf:
  - Produkte, die kein echtes Medizinprodukt darstellen
  - Gesundheitsanwendungen (auch reine Software erfasst)
  - In Verkehr gebrachte Komponenten (Geräte oder Apps) von Medizinprodukten

→ CRA ergänzt bestehende Regelungen für Produkte im Gesundheitssektor

MDR/IVDR und CRA

	MDR / IVDR	CRA
Ziel	Patientensicherheit und Wirksamkeit von Medizinprodukten	Cybersicherheit von Produkten mit digitalen Elementen
Geltungsbereich	Medizinprodukte und In-vitro-Diagnostika	Produkte mit digitalen Elementen (Hardware oder Software), die kein Medizinprodukt oder IVD sind
Adressaten	Hersteller, bevollmächtigte Vertreter, Importeure, Händler, Quasi-Hersteller, Personen, die Systeme oder Behandlungseinheiten in Verkehr bringen oder sterilisiert	Hersteller, Bevollmächtigte, Einführer, Händler, Quasi-Hersteller
Hauptanforderungen	Grundlegende Sicherheits- und Leistungsanforderungen, Technische Dokumentation (klinische Bewertung, weitere Nachweise)	Cybersecurity-by-Design, Updates, Schwachstellenmanagement und Meldung
Zuständige Behörden	Nationale Marktüberwachungsbehörden	Nationale Marktüberwachungsbehörden, ENISA

Herausforderungen für die MedTech-Branche

- Unklare Abgrenzung: Manche Produkte fallen in eine Grauzone zwischen MDR und CRA
- Dokumentationsanforderungen: Hersteller müssen zusätzliche Sicherheitsnachweise für digitale Komponenten erbringen
- Cybersicherheitsstrategie: Sicherheitsupdates sind über den gesamten Lebenszyklus nach dem CRA erforderlich
- Meldungen von Schwachstellen an Behörden und in der Lieferkette

Cybersicherheit in der Lieferkette

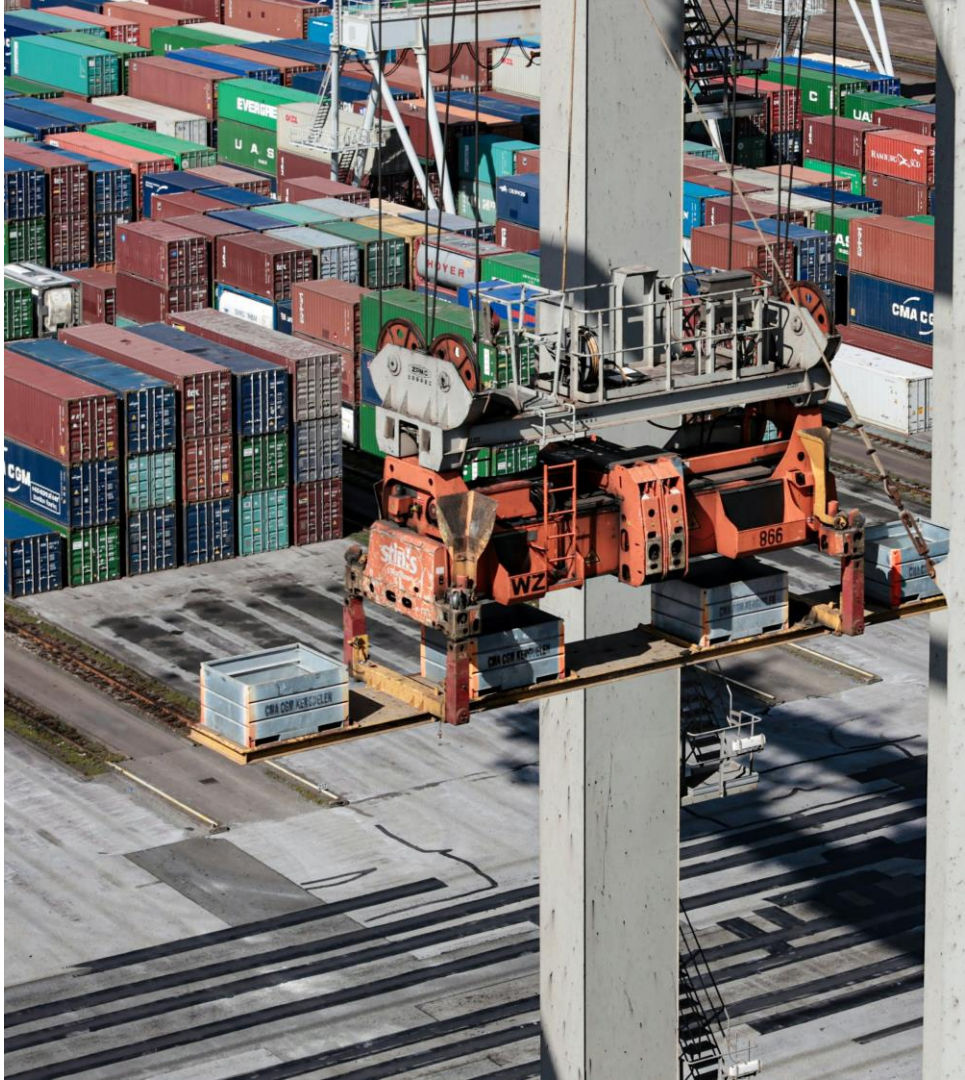
Neue Pflichten und deren Auswirkungen in der Praxis

Cybersicherheit in der Lieferkette – Wirtschaftliche Relevanz

- Gesetzliche Pflicht zur Cybersicherheit von Produkten in der Lieferkette
- Pflicht zur Behandlung von Schwachstellen umfasst auch Drittanbieterkomponenten (inkl. Open Source)
- Kostenlose Bereitstellung von Cybersicherheitsupdates während des Supportzeitraums (Ausnahme: individuelles Produkt im B2B-Bereich)
- Verpflichtung des Herstellers zur Bereitstellung einer SBOM
- Verpflichtung des Herstellers zur Meldung von Sicherheitsverstößen, auch in der Lieferkette

Anforderungen an die Lieferkette nach EU-Digitalrecht

- **NIS-2-Richtlinie:**
  - Verpflichtung zur Gewährleistung und Überwachung der Cybersicherheit in der Lieferkette
- **AI:**
  - Pflichten für Händler als Person in der Lieferkette
  - Risikomanagementmaßnahmen
  - Marktüberwachung: Ursprung und Lieferkette des KI-Systems relevant

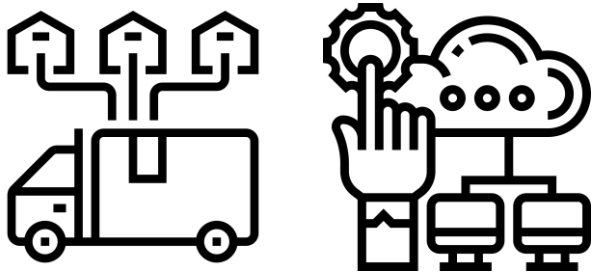


Auswirkungen auf die Lieferkette

Innenverhältnis: Prozesse und Organisation

(Un)mittelbare Verpflichtung nach dem CRA

Außenverhältnis: Vertragliche Vereinbarungen



Produkte

Unternehmen

Zulieferer und Dienstleister

Cybersicherheit in der Lieferkette: Vertragsrahmen

- Bewertung von Cyberrisiken
- Risikomanagement
- Datensicherung und Wiederherstellung
- Einsatz von Subunternehmern
- Bereitstellung von Sicherheitsupdates
- Durchführung von Krisenübungen
- Incident Response
- Kooperation mit Aufsichtsbehörden

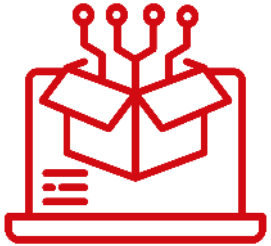
→ **Vertragliche Kontrollbefugnisse sowie Durchsetzung der Pflichten**

Praktische Umsetzung

Risikomanagement und Vertragsgestaltung

Best Practice

Betroffenheit prüfen → Rolle klären → Anforderungen umsetzen → Monitoring



Produkt mit digitalen Elementen

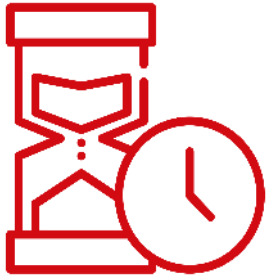
Hersteller, Händler oder Einführer

Technische Maßnahmen

Gap-Analyse

Rechtliche Maßnahmen

Vertrags-gestaltung



Produkte & interne Prozesse, Rechtsfortbildung

Rechtliche Umsetzung: Vertragsrahmen für die Cybersicherheit

Ermittlung der gesetzlichen Anforderungen

Prüfung, inwieweit und in welcher Rolle das Unternehmen gesetzlichen Cybersicherheitsanforderungen unterliegt. Die Ergebnisse werden in einer detaillierten Anforderungsmatrix dargestellt, aus der sich die erforderlichen Regelungen für den Vertragsrahmen ableiten lassen.

Ermittlung der vertraglichen Anforderungen

Prüfung von bestehenden Verträgen zwischen dem Unternehmen und der Lieferkette und Identifizierung der relevanten Regelungen zur Cybersicherheit. Die Ergebnisse werden ebenfalls in einer detaillierten Anforderungsmatrix dargestellt.

Erstellung eines Vertragsrahmens für die Cybersicherheit

Erstellung eines Vertragsrahmens, der die Cybersicherheitsanforderungen für das Unternehmen regelt. Der Schwerpunkt der Vertragsgestaltung liegt in der Regelung der Anforderungen an Zulieferer und Dienstleister.

Bewertung von Cyberrisken

„Der Auftragnehmer ist verpflichtet, dem Auftraggeber sämtliche Informationen zur Verfügung zu stellen, die dieser zur Risikobewertung im Zusammenhang mit [dem Produkt] benötigt. Zur Verfügung gestellt werden mindestens folgende Informationen: […].“

Risikominimierung in der Lieferkette

„Während der Laufzeit dieses Vertrages wird der Auftragnehmer bekannt gewordene Schwachstellen des Produkts beseitigen und alle zumutbaren Maßnahmen zur Risikominimierung treffen und den Auftraggeber fortlaufend informieren. Dies gilt auch für eingesetzte Open Source Software.“

Incident Response Readiness

„Bei Cybersicherheitsvorfällen wird der Auftragnehmer den Auftraggeber unverzüglich in elektronischer Form informieren und fortlaufend weitere Informationen über Aufklärungs- und Abhilfemaßnahmen bereitstellen. [Angaben zum Mindestumfang der Information].

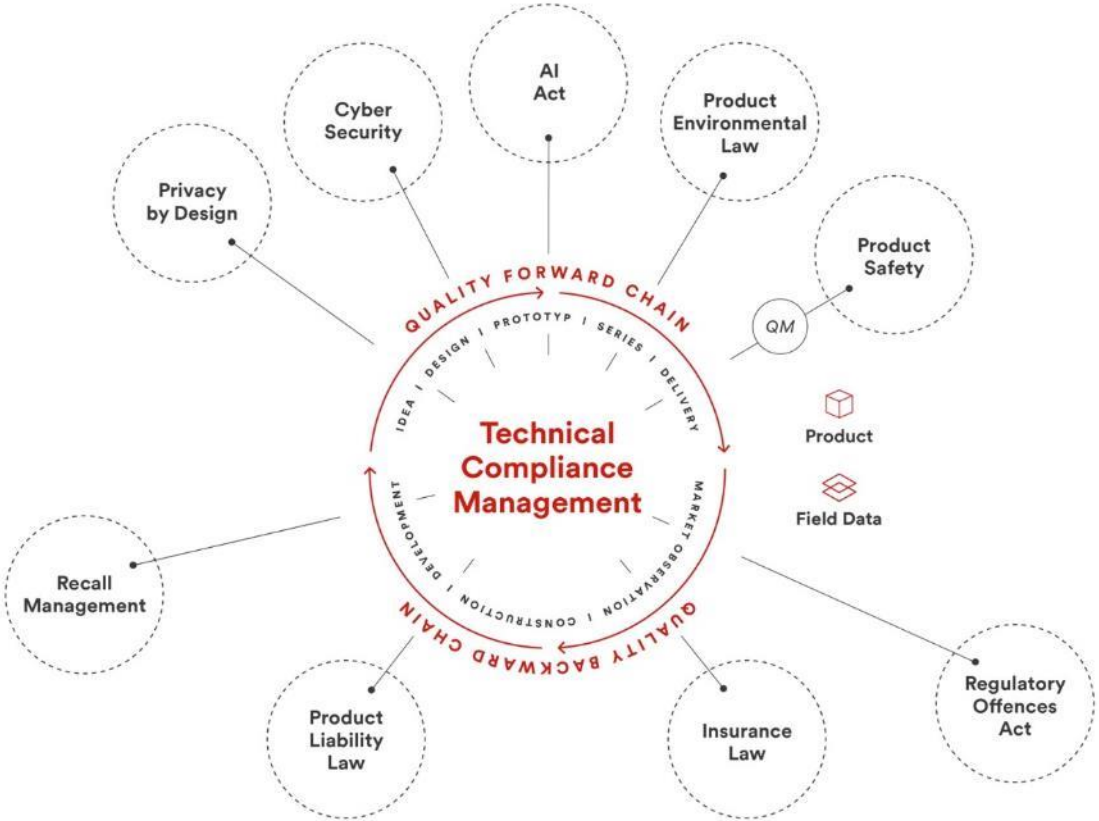
Liegt ein Notfall vor erfolgt die Kommunikation über die vom Auftraggeber bereitgestellte Lösung [Beschreibung der Notfallkommunikation].

Der Auftragnehmer wird mit den für den Auftraggeber zuständigen Aufsichtsbehörden kooperieren.“

Q&A

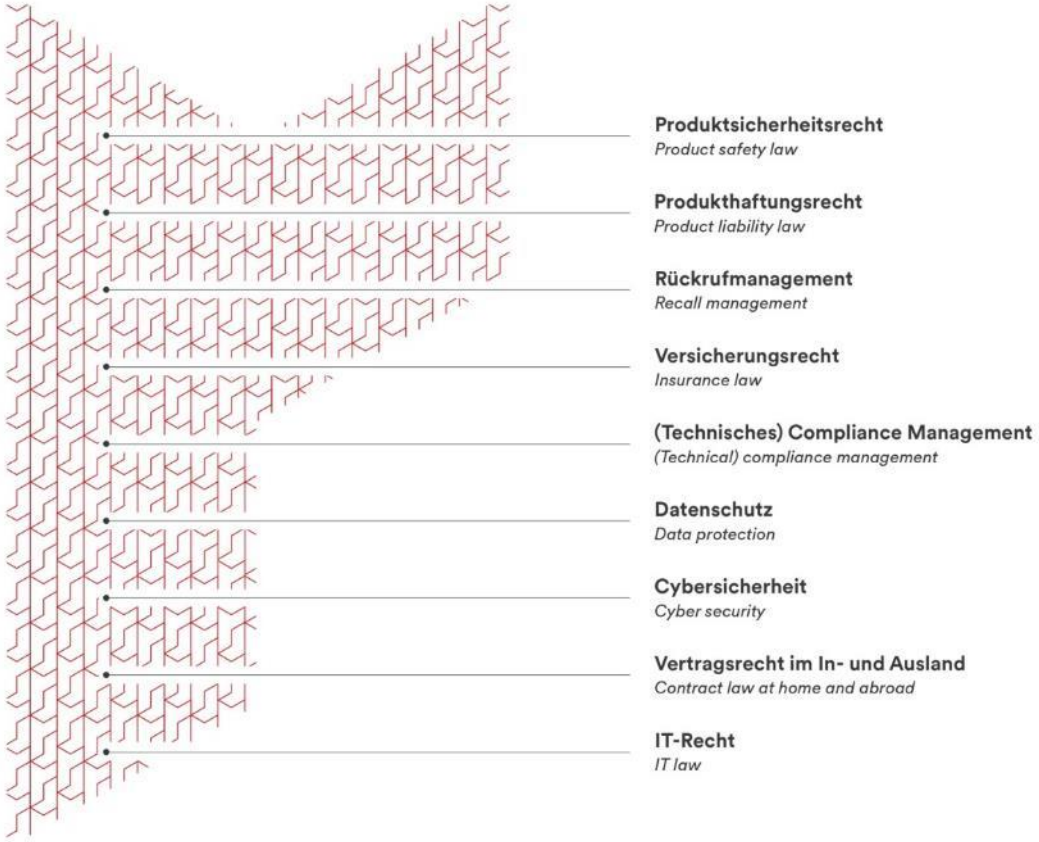
Was wir machen

Spezialisierte Services, Lösungen & Beratung.



Was wir machen

Effektivität ist nicht verhandelbar.



Was uns auszeichnet

International aktiv. In Deutschland daheim.

Dank unseres weltweiten Partnernetzwerks – vertreten in allen relevanten Industrienationen – können wir in vielen Ländern umfassende Beratung aus einer Hand anbieten.

Get in touch with us!

reusch law

Berlin
Joachimsthaler Straße 34
10719 Berlin

T + 49 30 / 2332 895 0
F + 49 30 / 2332 895 11
E info@reuschlaw.de

Saarbrücken
Stengelstraße 1
66117 Saarbrücken

T + 49 681 / 859 160 0
F + 49 681 / 859 160 11
E info@reuschlaw.de