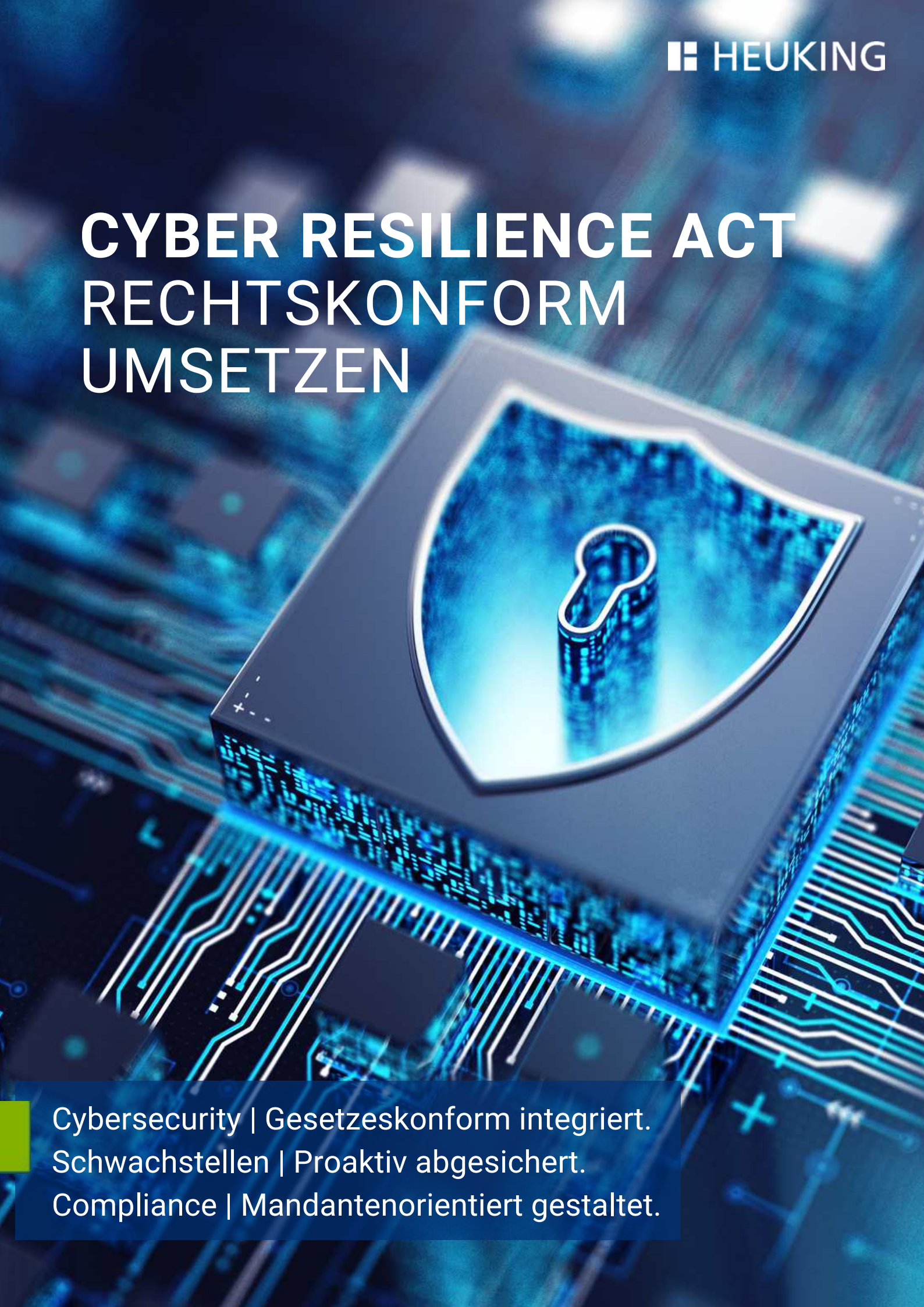
HEUKING

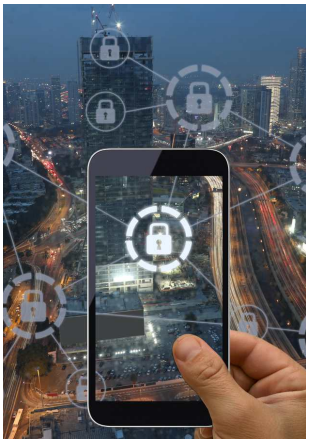
CYBER RESILIENCE ACT RECHTSKONFORM UMSETZEN

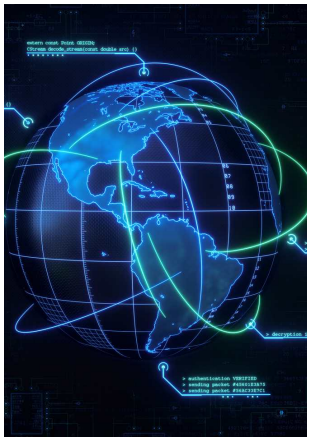


Cybersecurity | Gesetzeskonform integriert.
Schwachstellen | Proaktiv abgesichert.
Compliance | Mandantenorientiert gestaltet.

Überblick

Der Cyber Resilience Act normiert erstmals umfassende Sicherheitsanforderungen für Produkte mit digitalen Elementen – von IoT-Geräten bis zu Softwarelösungen. Die EU reagiert damit auf die wachsende Bedrohungslage durch Cyberrisiken. Der CRA schafft einen einheitlichen Rechtsrahmen für Cybersicherheit, Schwachstellenmanagement und Produktverantwortung. Hersteller müssen Risiken systematisch bewerten, Schutzmaßnahmen implementieren und über den gesamten Produktlebenszyklus hinweg Sicherheitsupdates bereitstellen. Die zunehmende Vernetzung erfordert klare rechtliche Vorgaben und technische Standards.





Betroffene Unternehmen

Produkthersteller

Hersteller, die vernetzte Hardware oder Software mit digitalen Funktionen anbieten (z. B. Fahrzeuge, Maschinen, Medizintechnik), müssen Sicherheitsanforderungen wie „secure by design“ umsetzen.

Einführer

Unternehmen, die Produkte mit digitalen Elementen aus Drittstaaten in die EU importieren, müssen sicherstellen, dass diese den Anforderungen des CRA entsprechen. Dazu gehören Sicherheitsbewertungen, technische Dokumentation und CE-Kennzeichnung.

Händler

Firmen, die Produkte mit digitalen Elementen innerhalb der EU vertreiben, sind verpflichtet, die Konformität der Produkte zu prüfen und sicherzustellen, dass die Herstellerpflichten erfüllt wurden.

Unternehmensgröße

Der CRA gilt unabhängig von der Größe des Unternehmens, also auch für kleine und mittlere Unternehmen sowie Start-ups, sofern sie Produkte mit digitalen Elementen in der EU entwickeln, vertreiben oder importieren.

Geografische Reichweite

Die Verordnung betrifft alle Unternehmen, deren Produkte mit digitalen Elementen in der EU in Verkehr gebracht oder bereitgestellt werden – auch wenn das Unternehmen seinen Sitz außerhalb der EU hat.

Ausnahmen

Nicht betroffen sind ausschließlich private, nicht-kommerzielle Open-Source-Software sowie bestimmte sicherheitsbezogene oder hoheitliche Anwendungen, etwa im militärischen oder behördlichen Bereich.

Sanktionen

Bei Verstößen gegen den Cyber Resilience Act drohen erhebliche Sanktionen bis zu EUR 15 Mio. Die Verordnung verpflichtet die Mitgliedstaaten, wirksame, verhältnismäßige und abschreckende Maßnahmen zu erlassen. Je nach Schwere des Verstoßes können Bußgelder verhängt werden etwa bei fehlender Sicherheitsbewertung, mangelhafter Schwachstellenbehandlung oder unzureichende Updates. Auch falsche oder irreführende Angaben zur Produktsicherheit oder CE-Kennzeichnung können geahndet werden. Zusätzlich sind nationale Maßnahmen wie Verwarnungen, Anordnungen zur Beseitigung von Verstößen oder Marktverbote möglich.

Umsetzungsfristen

- **11. Juni 2026**: Beginn der Notifizierung von Konformitätsbewertungsstellen durch die Mitgliedstaaten.
- **11. September 2026**: Meldepflicht für Hersteller bei aktiv ausgenutzten Schwachstellen in digitalen Produkten.
- **11. Dezember 2027**: Vollständige Anwendung des CRA. Alle Produkte mit digitalen Elementen müssen den Sicherheitsanforderungen entsprechen.

Neue Pflichten (Auszug)

Produkthersteller – Allgemeine Pflichten

- Sicherheitsanforderungen „secure by design“ und „secure by default“ umsetzen
- Technische Dokumentation und CE-Kennzeichnung bereitstellen
- Konformitätsbewertung vor Inverkehrbringen durchführen
- Schwachstellenmanagement und Update-Pflichten etablieren
- Software-Stückliste (SBOM) erstellen und pflegen
- Sicherheitsinformationen für Nutzer klar kommunizieren
- Verantwortlichkeiten entlang der Lieferkette definieren

Produkthersteller – Laufender Betrieb

- Meldung aktiv ausgenutzter Schwachstellen an Behörden
- Bereitstellung von Sicherheitsupdates über den gesamten Produktlebenszyklus
- Pflege der technischen Unterlagen und Nachweise zur Konformität
- Überwachung der Produktsicherheit im Feld
- Vertragliche Absicherung von Pflichten gegenüber Einführern und Händlern
- Zusammenarbeit mit Marktaufsichtsbehörden bei Vorfällen

Unsere Beratung zur CRA-Compliance

Initialanalyse und Bestandsaufnahme

- Prüfung, ob und welche Produkte mit digitalen Elementen unter den CRA fallen.
- Identifikation von Sicherheitsanforderungen und Dokumentationspflichten.
- GAP-Analyse

Sicherheitsbewertung und Konformität

- Unterstützung bei der Risikobewertung und CE-Kennzeichnung.
- Beratung zur Durchführung von Konformitätsverfahren und Schwachstellenmanagement.

Governance und technische Umsetzung

- Entwicklung interner Prozesse zur Cybersicherheit und Update-Strategie.
- Begleitung bei der Einführung sicherer Standardkonfigurationen („secure by default“).

Informationspflichten und Transparenz

- Unterstützung bei der Erstellung der technischen Dokumentation und Software-Stücklisten (SBOM).
- Begleitung der Kommunikation sicherheitsrelevanter Informationen gegenüber Nutzern.
- Schulung von Geschäftsleitung und Mitarbeitern

Meldung und Behördenkommunikation

- Unterstützung bei der Meldung aktiv ausgenutzter Schwachstellen.
- Begleitung bei Anfragen von Marktaufsichtsbehörden und Rückrufmaßnahmen.

Lieferkette und Verantwortung

- Prüfung vertraglicher Pflichten gegenüber Einführern und Händlern.
- Beratung zur Absicherung von Sicherheitsanforderungen entlang der Lieferkette.

HEUKING

Vertrauen Sie auf unsere Expertise – als starker Partner für rechtssichere und praxisnahe Lösungen rund um das Thema Informationssicherheit.

Dr. Hans Markus Wulf
Rechtsanwalt | Partner
Fachanwalt für IT-Recht
ISO/IEC 27001 Auditor (TÜV)
CIPP/E, Datenschutzauditor (TÜV)

m.wulf@heuking.de

Berlin
Chemnitz
Düsseldorf
Frankfurt
Hamburg
Köln
München
Stuttgart

JUVE Handbuch 2024/2025 Wirtschaftskanzleien

FÜHRENDE KANZLEI Legal500 DEUTSCHLAND 2025

Chambers TOP RANKED Germany 2025 HEUKING

heuking.de