HEUKING

CYBER RESILIENCE ACT
PRODUCT COMPLIANCE RECHTSKONFORM UMSETZEN

Cybersecurity | Rechtskonform umgesetzt.

Schwachstellen | Proaktiv abgesichert.

Product Compliance | Mandantenorientiert gestaltet.

Überblick

Der Cyber Resilience Act normiert erstmals umfassende Mindestanforderungen an die Cybersicherheit von Produkten mit digitalen Elementen – von IoT-Geräten bis zu Softwareapplikationen und schafft einen einheitlichen Rechtsrahmen für Cybersicherheit, Schwachstellenmanagement und Product Compliance Prozesse.

Betroffene Wirtschaftsakteure müssen etwa Cybersicherheitsrisiken bewerten, Konformitätsbewertungs-verfahren durchführen, Dokumentationsanforderungen erfüllen und Maßnahmen einführen, um die Cybersicherheit über den gesamten Produktlebenszyklus hinweg zu gewährleisten. Die zunehmende Vernetzung erfordert klare rechtliche Vorgaben und technische Standards.

Betroffene Wirtschaftsakteure und Produkte

Hersteller

Jeder, der Produkte mit digitalen Elementen entwickelt oder herstellt oder die Produkte mit digitalen Elementen konzipieren, entwickeln oder herstellen lässt und sie unter ihrem Namen oder ihrer Marke vermarktet)

Einführer

Jede in der EU ansässige oder niedergelassene natürliche oder juristische Person, die ein Produkt mit digitalen Elementen unter dem Namen oder der Marke einer außerhalb der Union ansässigen oder niedergelassenen natürlichen oder juristischen Person in der Union in den Verkehr bringt.

Händler

Jedes Glied einer Lieferkette, das ein Produkt mit digitalen Elementen ohne Änderung seiner Eigenschaften auf dem Unionsmarkt bereitstellt, mit Ausnahme des Herstellers oder des Einführers.

Produkte mit digitalen Elementen

Jedes vernetzte Software- oder Hardwareprodukt, einschließlich Software- oder Hardwarekomponenten, die getrennt in den Verkehr gebracht werden. Dies umfasst zahlreiche Produkte, wie IoT-Geräte, Softwareapplikationen, Netzschnittstellen, Router, Mikroprozessoren, u.v.m.

Geografische Reichweite

Die Verordnung betrifft alle Unternehmen, die Produkte mit digitalen Elementen in der EU in Verkehr bringen oder auf dem EU-Markt bereitstellen – auch wenn ein Unternehmen seinen Sitz außerhalb der EU hat.

Ausnahmen

Nicht betroffen sind ausschließlich nicht kommerzielle Open-Source-Software sowie Produkte, die unter vorrangige branchenspezifische Produktsicherheitsvorgaben fallen.

Sanktionen

Bei Verstößen gegen den Cyber Resilience Act drohen erhebliche Sanktionen. Diese können je nach Verstoß bis zu EUR 15 Mio. oder 2,5 % des gesamten weltweiten Jahresumsatzes des vorangegangenen Geschäftsjahres betragen.

Zudem können die Marktüberwachungsbehörden Maßnahmen, wie Vertriebsverbote, Produktvernichtungen oder Produktrückrufe anordnen.

Umsetzungsfristen

- **11. September 2026**: Beginn der Geltung der Meldepflichten für Hersteller für Schwachstellen und Sicherheitsvorfälle.
- **11. Dezember 2027**: Alle Anforderungen des CRA sind bei neuen Produkten mit digitalen Elementen einzuhalten.

CRA-Pflichten (Auszug)

Hersteller

- Berücksichtigung der grundlegenden Cybersicherheits-anforderungen in die Produktentwicklung
- Konformitätsbewertung und CE-Kennzeichnung
- Software-Stückliste (SBOM) erstellen und pflegen
- Produktinformationen für Nutzer erstellen
- Verantwortlichkeiten entlang der Lieferkette definieren und kontrollieren
- Schwachstellenmanagement und Update-Pflichten etablieren (inkl. Meldeverfahren

Einführer und Händler

- Durchführung der Konformitätsbewertung überprüfen
- CE-Kennzeichnung und Technische Dokumentation prüfen
- Anbringen von Firma & Kontaktinformationen des Einführers am Produkt
- Prozesse für Pflichten bei Non-Konformität implementieren
- Verantwortlichkeiten entlang der Lieferkette definieren und kontrollieren

Unsere Beratung zur CRA-Compliance

Initialanalyse und Bestandsaufnahme

- Anwendbarkeit des CRA (ggf. auf spezifische Produkte) prüfen
- Identifikation von Cybersicherheitsanforderungen und Dokumentationspflichten
- GAP-Analyse

Risiko- und Konformitätsbewertung

- Unterstützung bei der Risikobewertung und Konformitätsbewertung
- Begleitung bei der Konformitätsbewertung unter Einbeziehung notifizierter Stellen

Governance und technische Umsetzung

- Entwicklung interner Prozesse zur Einhaltung der Cybersicherheitsanforderungen und Meldepflichten
- Schulung von Geschäftsleitung und Mitarbeitern

Informationspflichten und Kommunikation

- Unterstützung bei der Erstellung der technischen Dokumentation und Software-Stücklisten (SBOM)
- Begleitung der Kommunikation sicherheitsrelevanter Informationen gegenüber Nutzern

Meldung und Behördenkommunikation

- Unterstützung bei der Meldung von Schwachstellen und Sicherheitsvorfällen
- Begleitung und Vertretung bei Anfragen und Anordnungen von Marktaufsichtsbehörden

Lieferkette und Verantwortung

- Prüfung und Verhandlung vertraglicher Vereinbarungen zur Gewährleistung der Cybersicherheitsanforderungen in der Lieferkette

HEUKING

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

Berlin
Chemnitz
Düsseldorf
Frankfurt
Hamburg
Köln
München
Stuttgart

FÜHRENDE KANZLEI Legal500 DEUTSCHLAND 2025

TOP KANZLEI Legal500 DEUTSCHLAND 2025

JUVE TOP 50 Wirtschaftskanzlei Deutschland 2024|2025

Handelsblatt Deutschlands BESTE Anwälte 2025 HEUKING

Chambers TOP RANKED Germany 2025 HEUKING

RANKED FIRM 2025 LEADERS LEAGUE

HEUKING RECOGNIZED BY Best Lawyers 2026