Cybersicherheit wird Pflicht

Gesetzentwurf zur Durchführung des Cyber Resilience Act in Deutschland

11. Juni 2026

Mit der Ende 2024 beschlossenen Verordnung (EU) 2024/2847, auch Cyber Resilience Act (CRA), legt die Europäische Union weitere **verbindliche Standards für die Cybersicherheit** fest. Während es bei der Umsetzung der NIS-2-Richtlinie vor allem die Cybersicherheit von Unternehmen und kritischen Infrastrukturen adressiert, steht beim CRA die **Produktsicherheit im Fokus**.

Ab 11. Juni 2026 treten erste Pflichten aus dem CRA in Kraft. Vor diesem Hintergrund hat die Bundesregierung im Mai 2026 einen Entwurf für ein Durchführungsgesetz zum CRA beschlossen. Ziel des Vorhabens ist es, die organisatorischen und behördlichen Voraussetzungen für die Anwendung des CRA in Deutschland zu schaffen. Der Entwurf bietet auch eine Gelegenheit, die Pflichten in den Blick zu nehmen, die sich für betroffene Unternehmen unmittelbar aus dem CRA ergeben.

Pflichten aus dem CRA

Durch den CRA werden erstmals **Anforderungen an die Cybersicherheit für Produkte mit digitalen Elementen** festlegt. Adressiert werden dabei insbesondere **digital vernetzte Soft- und Hardware** wie Smart Devices, Betriebssysteme und Cloud-Lösungen.

Ziel ist es, **Cybersicherheit als grundlegende Produkteigenschaft** zu etablieren und damit den Zugang zum EU-Binnenmarkt an verbindliche Sicherheitsstandards zu knüpfen, die in allen Mitgliedstaaten gelten:

- Zu diesem Zweck müssen Hersteller von Produkten mit digitalen Elementen ab dem 11. September 2026 **aktiv ausgenutzte Schwachstellen sowie schwerwiegende Sicherheitsvorfälle melden**. Diese Meldepflichten erfordern den **Aufbau interner Prozesse** zur strukturierten **Erkennung, Bewertung und Meldung** von Schwachstellen und Sicherheitsvorfällen.

- Ab dem 11. Dezember 2027 tritt der CRA vollständig in Kraft. Ab diesem Zeitpunkt müssen Cybersicherheitsmaßnahmen in allen Schritten von der Entwicklung über die Produktion bis zum Support **während der gesamten Produktlebensdauer** umgesetzt und nachgewiesen werden. Bestehende **Compliance-Systeme**, etwa mit Blick auf die Einhaltung der NIS-2-Richtlinie, müssen um die Pflichten aus dem CRA erweitert werden. Hersteller müssen die **Cybersicherheitsrisiken ihrer Produkte** bewerten und berücksichtigen. Vernetzte Produkte sind von Beginn an sicher zu konzipieren, etwa durch **Verschlüsselung von Daten** und eine **möglichst**

geringe Angriffsfläche. Durch sichere Voreinstellungen, etwa das **Verbot schwacher Standardpasswörter** und **automatische Updates**, wird das Sicherheitsniveau zusätzlich erhöht. Auch die systematische Behandlung von Schwachstellen ist bereits in der Entwicklungsphase vorzusehen. Während des gesamten Supportzeitraum müssen für den Endanwender **Sicherheitsupdates** zur Verfügung gestellt und die Behandlung von Schwachstellen angeboten werden. Dieser **Supportzeitraum** muss vom Hersteller kommuniziert werden und beträgt in der Regel **fünf Jahre.**

- Ein zentraler Hebel des CRA ist die **Erweiterung der so genannten CE-Kennzeichnung** um den Aspekt der Cybersicherheit. Mit der CE-Kennzeichnung erklärt ein Hersteller oder sein Bevollmächtigter, dass das betroffene Produkt den Standards des EU-Binnenmarkts entspricht. Diese Erklärung wird auch als „**Konformitätserklärung**" bezeichnet und wird sich mit dem CRA auch auf **Aspekte der Cybersicherheit** beziehen.

Durchsetzung des CRA in Deutschland

Bereits ab dem 11. Juni 2026 sind die Mitgliedsstaaten verpflichtet, Strukturen zur Implementierung und Durchsetzung des CRA zu schaffen:

- Mit dem Entwurf eines CRA-Durchführungsgesetzes wird das **Bundesamt für Sicherheit in der Informationstechnik (BSI)** zur zentralen **Aufsichts- und Koordinierungsstelle** bei der Anwendung des CRA in Deutschland. Es überwacht die **Einhaltung der im CRA festgelegten Standards** und prüft die **Konformität von Produkten mit den neuen Cybersicherheits-Standards**.

- Der Entwurf sieht **Beratungs- und Beschwerdemöglichkeiten** für betroffene kleine und mittlere Unternehmen vor.

- Darüber hinaus werden auch **Bußgeld- und Sanktionsvorschriften** an die Regelungen des CRA angepasst, sodass ein Verstoß gegen die Pflichten aus dem CRA empfindliche Folgen haben kann.

***

BLOMSTEIN wird Sie über die weiteren Entwicklungen auf dem Laufenden halten. Bei Beratungsbedarf und anderen Fragen zum Thema Cybersicherheit Ihnen Dr. Christopher Wolters, Konstantin Kuhle, Dr. Nils-Hendrik Grohmann, Hanna Sophie Vetter sowie Dr. Moritz Schuchert und das gesamte Team jederzeit gerne zur Verfügung.

BLOMSTEIN | Wir beraten unsere internationalen Mandanten in den Gebieten Kartell-, Vergabe-, Außenwirtschafts- und Beihilferecht sowie ESG in Deutschland, Europa und – über unser globales Netzwerk – weltweit.