



September 2026

Der EU Cyber Resilience Act (CRA) und Software: Neue Cybersicherheitspflichten und CE- Kennzeichnung

Der EU Cyber Resilience Act (CRA) erhebt Cybersicherheit zur Voraussetzung für den EU-Marktzugang und zwar nicht nur für Hardware-Produkte mit digitalen Elementen, sondern auch für eigenständig auf den Markt gebrachte Software. Die zentralen Neuerungen umfassen Konformitätsbewertungen, CE-Kennzeichnungen und die Pflicht zur kostenlosen Bereitstellung von Sicherheits-Updates während eines festgelegten Unterstützungszeitraums. Das kann einige Anbieter vor die Herausforderung stellen, bestehende Go-To-Market-Prozesse und auch Preiskalkulationen grundlegend neu zu überdenken.

Das Thema ist jetzt besonders aktuell: Zwar müssen Software und andere Produkte mit digitalen Elementen die Pflichten erst ab dem 11. Dezember 2027 erfüllen, doch kann der für eine erste CE-Konformitätsbewertung erforderliche Prozess erheblichen zeitlichen Vorlauf beanspruchen. Zum anderen treffen die Anforderungen auch Produkte, die vor dem 11. Dezember 2027 entwickelt und hergestellt wurden, wenn sie nach diesem Datum auf den Markt gebracht werden. Darüber hinaus greifen bereits heute Meldepflichten für aktiv ausgenutzte Schwachstellen und schwerwiegende Sicherheitsvorfälle.

Welche Software fällt in den Anwendungsbereich des CRA?

Der CRA gilt für sogenannte „Produkten mit digitalen Elementen“. Dazu zählen:

- Softwareprodukte, die eigenständig auf dem Markt bereitgestellt werden, wie on-premises Software, einschließlich herunterladbarer Tools, Apps, Agents, SDKs und Client Libraries;
- eingebettete Software, Firmware und möglicherweise vernetzte Systeme;
- Hardwareprodukte mit digitalen Elementen (vor allem IoT-Produkte), einschließlich separat angebotener Hardware- oder Softwarekomponenten (z.B. (und siehe oben) eingebettete Software, Firmware);
- bestimmte Cloud-Lösungen, die vom Hersteller selbst oder unter dessen Verantwortung konzipiert und entwickelt wurden und ohne die das Produkt mit digitalen Elementen eine seiner Funktionen nicht erfüllen könnte;
- kostenfreie und quelloffene Software („Free“ und „Open-Source Software“), wobei sich die regulatorischen Anforderungen hier von denen für gewöhnliche Software unterscheiden (siehe unten).

Dieser weite Anwendungsbereich ist gewollt: Die Europäische Kommission beschreibt den CRA als horizontalen Rahmen für Hardware- und Softwareprodukte, die auf dem Unionsmarkt bereitgestellt werden.

SaaS, Cloud und installierbare Komponenten: Wo der CRA relevant wird

Reine SaaS oder andere Cloud-Dienste fallen grundsätzlich nicht in den Anwendungsbereich des CRA, da sie typischerweise als „Dienstleistung“ und nicht als „Produkt“ auf dem Markt bereitgestellt werden. Anders verhält es sich jedoch, wenn eine Cloud- oder SaaS-Lösung für die Erfüllung einer Funktion eines Produkts mit digitalen Elementen erforderlich ist und vom Hersteller selbst oder unter dessen Verantwortung konzipiert sowie entwickelt wurde (sog. Datenfernverarbeitungslösung).

Zur Veranschaulichung mag folgendes Praxisbeispiel dienen: Eine intelligente Sicherheitskamera zeichnet lokal Bild- und Videomaterial auf, ihre eigentliche Kernfunktionalität ist die KI-gestützte Erkennung von Personen, Fahrzeugen oder sicherheitsrelevanten Ereignissen über eine vom Hersteller betriebene Cloud-Anwendung. Da diese Analyse- und Alarmierungsfunktionen ohne die Cloud-Anbindung nicht zur Verfügung stehen und damit einen Funktionsbestandteil des Produkts darstellen, wird neben der Sicherheitskamera auch die betreffende Cloud-Anwendung als Datenfernverarbeitungslösung vom CRA erfasst.

Wer unterliegt den Verpflichtungen unter dem CRA?

Hauptadressat ist der Hersteller, also derjenige, der Produkte mit digitalen Elementen entwickelt oder herstellt und unter eigenem Namen oder eigener Marke auf dem EU-Markt bereitstellt. Die Hersteller-Pflichten gelten ebenso für jede Person, die eine wesentliche Änderung an dem regulierten Produkt vornimmt und das geänderte Produkt auf dem Markt bereitstellt. Importeure und Händler unterliegen gesonderten Verifizierungs-, Sorgfalts- und Compliance-Verpflichtungen. Der CRA schafft zudem eine eigene Regelung für „Verwalter quelloffener Software“ (Open Source Software), die unter anderem verpflichtet sind, eine Cybersicherheitsstrategie zu entwickeln und zu dokumentieren, mit den Marktüberwachungsbehörden zusammenzuarbeiten und bestimmte Meldepflichten zu erfüllen.

Intern betrifft der CRA mehrere Bereiche gleichzeitig:

- Product, Engineering und DevSecOps müssen Secure-by-Design-Anforderungen operationalisieren und in den Entwicklungsprozess integrieren.
- Legal und Compliance müssen Herstellerstatus, Risikokategorie und Konformitätsprozess bewerten.
- Management und Go-To-Market-Teams müssen sicherstellen, dass die erforderliche Konformitätsbewertung (in der Regel die CE-Konformitätsbewertung) abgeschlossen wurde, die erforderlichen technischen Unterlagen und die EU-Konformitätserklärung vorliegen und die CE-Kennzeichnung angebracht wurde, bevor das Produkt auf dem EU Markt vertrieben wird.

Welche konkreten Maßnahmen müssen Verpflichtete unter dem CRA umsetzen?

Secure by Design

Bereits in der Konzeption und der Produktentwicklung müssen Risikobewertungen, sichere Standardeinstellungen und Zugriffskontrollen, eine nachvollziehbare Sicherheitsarchitektur sowie ein strukturiertes Vulnerability-Handling über den gesamten Produktlebenszyklus hinweg berücksichtigt und adressiert werden.

Sobald einschlägige harmonisierte europäische Normen verfügbar sind, können Hersteller diese nutzen, um in den Genuss einer Konformitätsvermutung in Bezug auf die einschlägigen Anforderungen des CRA zu kommen. Bis dahin können bestehende europäische und internationale Cybersicherheitsnormen zwar nützliche technische Orientierung bieten, begründen aber für sich genommen keine Konformitätsvermutung im Hinblick auf den CRA.

Kostenlose Sicherheitsupdates werden Pflicht

Hersteller sind verpflichtet, Schwachstellen während des festgelegten Unterstützungszeitraums durch Sicherheitsaktualisierungen kostenfrei zu beheben und entsprechende Updates für einen Zeitraum von mindestens zehn Jahre nach Bereitstellung oder für die verbleibende Dauer des Unterstützungszeitraums, je nachdem, welcher Zeitraum länger ist, verfügbar zu halten. Dieser Unterstützungszeitraum bemisst sich in erster Linie nach der erwarteten Nutzungsdauer des Produkts und beträgt in der Regel mindestens fünf Jahre.

Reporting

Bereits seit dem 11. September 2026 müssen Hersteller aktiv ausgenutzte Schwachstellen und schwerwiegende Vorfälle über die CRA-Plattform für die zentrale Meldung („Single Reporting Platform“) der Agentur der Europäischen Union für Cybersicherheit (ENISA) melden. Eine Frühwarnung ist innerhalb von 24 Stunden nach Kenntniserlangung von der Schwachstelle oder dem Vorfall abzugeben, gefolgt von einer Schwachstellen- oder Vorfallsmeldung innerhalb von 72 Stunden. Bei aktiv ausgenutzten Schwachstellen ist der Abschlussbericht spätestens 14 Tage nach Verfügbarkeit einer Abhilfemaßnahme und bei schwerwiegenden Vorfällen innerhalb eines Monats nach Übermittlung der 72-Stunden-Vorfallsmeldung fällig.

Technische Dokumentation, Software Bill of Materials (SBOM) und Nachweispflichten

Fehlende oder unzureichende technische Dokumentation birgt erhebliche Risiken. Hersteller müssen die vom CRA geforderte Dokumentation erstellen und pflegen, einschließlich der Cybersicherheits-

Risikobewertung des Produkts und der technischen Dokumentation, die das jeweils anwendbare Konformitätsbewertungsverfahren stützt. Der CRA verpflichtet Hersteller ferner, Schwachstellen und Produktbestandteile zu ermitteln und zu dokumentieren. Hierzu zählt insbesondere die Erstellung einer Software Bill of Materials (SBOM) in einem gängigen maschinenlesbaren Format, die zumindest die Abhängigkeiten auf oberster Ebene des Produkts erfasst. Unternehmen sollten zudem erwägen, robuste Prozesse für die Meldung von Schwachstellen, für Sicherheitsupdates und für behördliche Anfragen vorzuhalten.

Ausnahme für maßgeschneiderte Software und Test-Versionen

Der CRA lässt eine (begrenzte) Flexibilität für maßgeschneiderte Produkte zu. Wird ein Produkt für einen bestimmten gewerblichen Nutzer für dessen besonderen Zweck entwickelt und vereinbaren Hersteller und Nutzer ausdrücklich abweichende Vertragsbedingungen, so dürfen sie von zwei konkreten Anforderungen abweichen: Der Anforderung an eine standardmäßig sichere Konfiguration und der Anforderung an kostenlose Sicherheitsupdates. Begrenzte Ausnahmen gelten außerdem für „unfertige Software“, die zu Testzwecken bereitgestellt wird, sowie für Produkte, die auf Messen, Ausstellungen und ähnlichen Veranstaltungen präsentiert werden. In allen Fällen knüpft der CRA daran bestimmte Bedingungen, darunter geeignete Hinweise, dass das Produkt noch nicht dem CRA entspricht, sowie Beschränkungen der Bereitstellung, bis die Konformität erreicht ist.

Besonderheiten für KMU

Für Kleinstunternehmen sowie kleine und mittlere Unternehmen (KMU) sieht der CRA eine Reihe gezielter Unterstützungsmaßnahmen vor: Initiativen der Mitgliedstaaten in den Bereichen Schulung, Awareness, Informationen sowie Testmöglichkeiten, Drittbewertung und Regulatory Sandboxes. Kleinstunternehmen und Kleinunternehmen können darüber hinaus technische Dokumentationen in vereinfachter Form erstellen, die die Europäische Kommission bereitstellen wird. Unterstützung kann zudem im Rahmen des Digital Europe Programme in Anspruch genommen werden, das entsprechende Förder- und Unterstützungsprojekte für betroffene Unternehmen bereithält.

Fazit

Für Softwareunternehmen ist der CRA nicht nur eine Frage der IT-Sicherheit. Er verändert, wie Produkte entwickelt, dokumentiert, bepreist und vertrieben werden und die Herstellung der Konformität kann den Vertrieb im EU-Markt erheblich verzögern, während eine fehlende Konformität ihn verhindern kann. Gleichzeitig schafft der CRA einen harmonisierten Rechtsrahmen, der Vertrauen in sicherheitssensiblen Märkten stärken kann.

Wir sind für Sie da

Dieser GT Alert wurde erstellt von:

Dr. Viola Bensinger | +49 30.700.171.150 | Viola.Bensinger@gtlaw.com

Jana Rudt | +49 30.700.171.336 | Jana.Rudt@gtlaw.com

Abu Dhabi⁺, Albany, Amsterdam, Aspen, Atlanta, Austin, Berlin⁺, Boston, Charlotte, Chicago, Dallas, Delaware, Denver, Dubai⁺, Fort Lauderdale, Houston, Las Vegas, London⁺, Long Island, Los Angeles, Mexico City⁺, Miami, Milan⁺.

Minneapolis. Munich–. New Jersey. New York. Northern Virginia. Orange County. Orlando. Philadelphia. Phoenix. Portland. Riyadh*. Sacramento. Salt Lake City. San Diego. San Francisco. São Paulo». Seoul«. Shanghai. Silicon Valley. Singapore«. Tallahassee. Tampa. Tel Aviv^ . Tokyo«. Warsaw–. Washington, D.C. West Palm Beach. Westchester County.

*Dieser Greenberg Traurig Alert wird ausschließlich zu Informationszwecken herausgegeben und ist weder als allgemeine Rechtsberatung noch als Aufforderung zu irgendeiner Art von Beratung zu verstehen oder zu verwenden. Bitte wenden Sie sich an den/die Autor(en) oder Ihren Ansprechpartner bei Greenberg Traurig, wenn Sie Fragen zur Aktualität dieser Informationen haben. Die Beauftragung eines Anwalts ist eine wichtige Entscheidung. Bevor Sie sich entscheiden, sollten Sie schriftliche Informationen über die rechtlichen Qualifikationen und Erfahrungen des Anwalts einholen. Greenberg Traurig ist eine Dienstleistungsmarke und ein Handelsname von Greenberg Traurig, LLP und Greenberg Traurig, P.A. –Die Büros von Greenberg Traurig in Berlin und München werden von Greenberg Traurig Germany, LLP, einer Tochtergesellschaft von Greenberg Traurig, P.A. und Greenberg Traurig, LLP, betrieben. *Tätigkeit als separate, in Großbritannien registrierte juristische Person. "Greenberg Traurig ist im Königreich Saudi-Arabien über die Greenberg Traurig Khalid Al-Thebity Law Firm tätig, eine professionelle Gesellschaft mit beschränkter Haftung, die vom Justizministerium zur Ausübung der Anwaltstätigkeit zugelassen ist. +Das Büro von Greenberg Traurig in Mexiko-Stadt wird von Greenberg Traurig, S.C. betrieben, einer Tochtergesellschaft von Greenberg Traurig, P.A. und Greenberg Traurig, LLP. "Das Büro von Greenberg Traurig in Mailand wird von Greenberg Traurig Studio Legal Associato betrieben, einer Tochtergesellschaft von Greenberg Traurig, P.A. und Greenberg Traurig, LLP. Das Büro von Greenberg Traurig in São Paulo wird von Greenberg Traurig Brazil Consultores em Direito Estrangeiro - Direito Estadunidense betrieben, die in Brasilien als ausländische Rechtsberatungsgesellschaft gegründet wurde. Die Anwälte des Büros in São Paulo sind nicht im brasilianischen Recht tätig. ∞Betreibt als Greenberg Traurig LLP Büro für ausländische Rechtsberatung. ¯Das Büro von Greenberg Traurig in Singapur wird von Greenberg Traurig Singapore LLP betrieben, die als ausländische Anwaltskanzlei in Singapur zugelassen ist. ^Greenberg Traurigs Büro in Tel Aviv ist eine Niederlassung von Greenberg Traurig, P.A., Florida, USA. ¢Das Büro von Greenberg Traurig in Tokio wird von GT Tokyo Horitsu Jimusho und Greenberg Traurig Gaikokuhojimubengoshi Jimusho, Tochtergesellschaften von Greenberg Traurig, P.A. und Greenberg Traurig, LLP, betrieben. Das Büro von Greenberg Traurig in den Vereinigten Arabischen Emiraten wird von Greenberg Traurig Limited betrieben. ~Das Warschauer Büro von GREENBERG TRAURIG wird von GREENBERG TRAURIG Nowakowska-Zimoch Wysokiński sp.k. betrieben, einer Tochtergesellschaft von Greenberg Traurig, P.A. und Greenberg Traurig, LLP. Einige Partner von GREENBERG TRAURIG Nowakowska-Zimoch Wysokiński sp.k. sind auch Gesellschafter von Greenberg Traurig, P.A. Die Bilder in dieser Anzeige stellen keine Anwälte, Mandanten, Mitarbeiter oder Einrichtungen von Greenberg Traurig dar. Kein Aspekt dieser Werbung wurde vom Supreme Court of New Jersey genehmigt. ©2026 Greenberg Traurig, LLP. Alle Rechte vorbehalten.*