Piltz Legal

Datenschutz, IT-Security und IT-Recht

Beraten.
Begleiten.
Voranbringen.

12/2024

Piltz Legal

Beratung zum Cyber Resilience Act

Was ist Gegenstand des Cyber Resilience Act?

Die europäische Verordnung über horizontale Cybersicherheitsanforderungen für Produkte mit digitalen Elementen (Cyberresilienz-Verordnung), insbesondere bekannt als der Cyber Resilience Act (CRA), zielt darauf ab, einen harmonisierten rechtlichen Standard auf dem Gebiet der Cybersicherheit im europäischen Binnenmarkt vorzuschreiben. Als Verordnung gilt der CRA ab dem Inkrafttreten unmittelbar in jedem Mitgliedstaat, sodass ein einheitliches Cybersicherheitsniveau im europäischen Binnenmarkt gewährleistet werden kann.

Um dem wachsenden Risiko von Cyberangriffen und Sicherheitsvorfällen aufgrund von Schwachstellen in Produkten entgegenzutreten, legt der CRA Mindestanforderungen für die Sicherheit von Produkten mit digitalen Elementen und an die Verfahren zur Behandlung von Schwachstellen fest.

Der CRA zeichnet sich zudem durch eine horizontale Geltung aus, sodass nicht Regelungen für eine bestimmte Sparte von Erzeugnissen festgelegt werden, sondern sämtliche „Produkte mit digitalen Elementen“ von den Cybersicherheitsvorschriften adressiert werden.

Neben Vorgaben zu den Sicherheitsanforderungen an Produkte enthält die Verordnung Verpflichtungen für die entlang einer Lieferkette involvierten Akteure.

Welche Produkte sind vom Cyber Resilience Act umfasst?

Der CRA gilt für Produkte mit digitalen Elementen, die auf dem Unionsmarkt bereitgestellt werden und deren bestimmungsgemäßer Zweck oder vernünftigerweise vorhersehbare Verwendung eine direkt oder indirekt stattfindende logische oder physische Datenverbindung mit einem Gerät oder Netz einschließt.

Zu den Produkten mit digitalen Elementen gehören Softwarelösungen, wie z. B. Computerprogramme oder Apps, und Hardwareprodukte, wie Smartphones, Laptops oder SmartTVs. Sogenannte Datenfernverarbeitungslösungen, wie Smart-Home-Geräte, die mittels einer App bedient werden können, fallen ebenfalls unter den Produktbegriff.

Maßgeblich ist, dass das Produkt mit digitalen Elementen eine Datenverbindung mit einem Gerät oder Netz eingehen kann und dies unter den Verwendungszweck fällt. Zu den Datenverbindungen gehören sogenannte logische Verbindungen, wie Programmierschnittstellen, oder physische Verbindungen, zum Beispiel über USB und Thunderbolt oder Bluetooth und WLAN.

Schließlich muss das zur Datenverbindung bestimmte Produkt mit digitalen Elementen im Rahmen einer Geschäftstätigkeit zum Vertrieb oder zur Verwendung auf den Unionsmarkt abgegeben und damit auf dem Unionsmarkt bereitgestellt werden.

Der CRA ordnet Produkte mit digitalen Elementen abhängig von ihrer Kritikalität in die Kategorien „wichtige“ und „kritische“ Produkte ein, für die ein besonderes Konformitätsverfahren gilt. Dasselbe gilt für Hochrisiko-KI-Systeme, die unter bestimmten Voraussetzungen ebenfalls einem Konformitätsverfahren nach dem CRA unterliegen können.

Wen betrifft der Cyber Resilience Act?

Achtung: Der CRA erfasst sowohl Organisationen (juristische Personen) als auch Einzelpersonen (natürliche Personen). Prinzipiell kommen damit auch öffentliche Stellen, wie z. B. Verwaltungsbehörden, als Adressaten in Betracht. Jedoch muss eine öffentliche Stelle dafür die Anforderungen an eine der unten genannten Rollen erfüllen.

Piltz Legal

Der CRA unterscheidet maßgeblich drei große Gruppen an verpflichteten Stellen:

Hersteller: Organisationen und Einzelpersonen, die Produkte mit digitalen Elementen entwickeln (lassen) und unter eigenem Namen / Marke vermarkten. Beispiele für Hersteller: Smartphone-Hersteller, Smart-Home-Geräte-Hersteller, Softwareentwickler, Hersteller von IoT-Geräten. Wichtig ist, dass man auch Hersteller i. S. d. CRA ist, wenn man im Auftrag herstellen lässt. Damit geraten auch ganze Lieferketten in den Fokus des CRA.

Einführer: In der EU ansässige / niedergelassene Organisationen und Einzelpersonen, die Produkte mit digitalen Elementen unter dem Namen / Marke eines außerhalb der EU ansässigen Organisation oder Einzelperson in den Verkehr bringen. Beispiele für Einführer sind etwa jene, wie im Fall des Herstellers, nur dass dieser Produkte mit digitalen Elementen von außerhalb der EU einführt. So kann z. B. ein Softwarehändler mit Niederlassung in der EU Einführer i. S. d. CRA sein, wenn er eine Software-Applikation auf dem Unionsmarkt anbietet, die von einem Unternehmen von außerhalb der EU entwickelt wurde. Zu denken wäre also bspw. an eine SaaS-Software, die durch ein US-amerikanisches Softwareunternehmen entwickelt und dann durch einen deutschen Softwarehändler in der Europäischen Union angeboten wird. Gleiches gilt für den Fall, dass ein chinesisches Unternehmen bspw. ein Smartphone entwickelt, das durch einen französischen Elektronikhändler auf dem französischen Markt angeboten wird.

Händler: Organisationen und Einzelpersonen, die Produkte mit digitalen Elementen aus einem Drittland in der EU auf den Markt bringen. Beispiele für Händler nach dem CRA können z. B. Elektronik- und Softwarehändler oder aber auch Industrieausrüster sein.

Der CRA erfasst darüber hinaus auch weitere Rollen, so u. a. den **Verwalter quelloffener Software** für kommerzielle Open-Source-Produkte.

Welche Pflichten treffen mich, wenn ich in den Anwendungsbereich des CRA falle?

Die Pflichten der einzelnen Adressaten sind abgestuft, wobei den Hersteller die meisten Pflichten treffen. Diese Pflichten umfassen u. a. Folgendes:

- Implementierung grundsätzlicher Cybersicherheitsanforderungen in das Produkt mit digitalen Elementen (Hersteller; Achtung: Diese Pflicht kann auch Händler und Einführer treffen, sofern sie wesentliche Änderungen an dem Produkt vornehmen)
- Bewertung relevanter Cybersicherheitsrisiken (gilt für Hersteller, ggf. Händler oder Einführer)
- Bereitstellung von Informationen für die Nutzer (gilt für Hersteller, ggf. Händler oder Einführer)
- Aufbewahrung technischer Dokumentation (gilt für Hersteller, ggf. Händler oder Einführer)
- Meldepflichten an Behörden (gilt für Hersteller, ggf. Händler oder Einführer)
- Prüfpflichten für Einführer, ob Hersteller ein Konformitätsbewertungsverfahren durchgeführt und technische Dokumentation bereitgestellt haben.

Ab wann gilt der CRA?

Der CRA trat am 10. Dezember 2024 in Kraft und folgende Umsetzungsfristen beginnen zu laufen:

Geltung ab 11. Juni 2026: Kapitel 4 (Notifizierung von Konformitätsbewertungsstellen) gilt.

Geltung ab 11. September 2026: Art. 14 CRA mit den Meldepflichten für Hersteller bei Schwachstellen gilt.

Geltung ab 11. Dezember 2027: Der CRA gilt vollständig.

Achtung: Für Produkte mit digitalen Elementen, die vor Dezember 2027 in Verkehr gebracht werden, gilt grds. nur Art. 14 CRA (Meldepflichten der Hersteller) und der CRA im Übrigen sonst nur bei wesentlichen Änderungen des Produkts mit digitalen Elementen. Eine wesentliche Änderung in diesem Sinn liegt u. a. dann vor, wenn durch die Änderung des Produkts eine neue oder andere Gefährdung schafft. Bspw. dann, wenn dem Produkt eine KI-Funktion hinzugefügt wird, die ausschließlich über eine Datenverbindung angebunden ist.

Wir sind durch den Cyber Resilience Act verpflichtet. Was sollten wir tun?

Handlungsempfehlungen: Erarbeitung konkreter Maßnahmen zur Anpassung und Verbesserung Ihrer verwendeten Produkte mit digitalen Elementen, um die Anforderungen des CRA und der Aufsichtsbehörden zu erfüllen.

1. Prüfung, ob die Organisation Produkte mit digitalen Elementen einsetzt.
2. Prüfung, welche Rollen (insbesondere Hersteller, Händler oder Einführer?) meine Organisation erfüllt.
3. Prüfung, welche Anforderungen durch die Organisation zu erfüllen sind, also bspw. die Herstellerpflichten. Identifizierung von Pflichten, die bereits aufgrund anderer gesetzlicher Vorgaben, wie z. B. der DSGVO, erfüllt werden.
4. Prüfung der Lieferkette auf Anpassung von Vorgaben hinsichtlich des CRA.
5. Prüfung, inwieweit Meldefristen nach dem CRA in das bestehende Meldepflichtenmanagement eingebunden werden müssen.

Kontaktieren Sie uns über unsere E-Mail info@piltz.legal, um mehr über unsere Dienstleistungen und wie wir Sie unterstützen können, zu erfahren.

Piltz Rechtsanwälte PartGmbB
Südwestkorso 3, 12161 Berlin

Telefon +49 30 814 53 50 00
Fax +49 30 814 53 50 09
E-Mail: info@piltz.legal