orka Newsletter Datenschutz, IT & Outsourcing

Neue Cybersicherheitsanforderungen für Hardware- & Softwareprodukte

Mit einer neuen EU-Verordnung strebt die Europäische Union ein erhöhtes Maß an **Cybersicherheit von sog. Produkten mit digitalen Elementen** sowie einen verbesserten Umgang mit IT-Schwachstellen an, um den gestiegenen Risiken im Kontext der Cybersicherheit zu begegnen. Zudem soll der Informationszugang für die Nutzer verbessert werden, um Cyberrisiken angemessen zu begegnen.

Mit dem **Cyber Resilience Act (CRA)** will die Europäische Union einen EU-weit einheitlichen Rechtsrahmen für Hardware- und Softwareprodukte schaffen, damit Produkte mit weniger IT-Schwachstellen in Verkehr gebracht werden. Die **Hersteller betroffener Produkte** müssen insbesondere für die Sicherheit ihrer Produkte über deren gesamten Lebenszyklus sorgen.

Darüber hinaus nimmt der CRA grundsätzlich **sämtliche beteiligten Wirtschaftsakteure** in die Pflicht. Das bedeutet, neben Herstellern erfasst der CRA insbesondere auch die Einführer und Händler sowie alle anderen Stellen, die Verpflichtungen im Zusammenhang mit der Herstellung oder Bereitstellung von Produkten mit digitalen Elementen unterliegen.

Die Ziele des CRA

Die neue Verordnung ist aus Sicht der EU erforderlich, um den *„legislativen Flickenteppich“* und die daraus resultierende Rechtsunsicherheit zu beseitigen und durch einen **EU-weit einheitlichen Rechtsrahmen** zu ersetzen. Das bestehende EU-Recht enthalte bislang keine unmittelbaren verbindlichen Anforderungen bezüglich der Sicherheit von Produkten mit digitalen Elementen.

Die auf EU-Ebene und in den EU-Mitgliedstaaten existierenden Vorschriften würden sich nur teilweise mit den Problemen und Risiken im Kontext der Cybersicherheit befassen, so die EU-Kommission. Durch den CRA soll nun für mehr Rechtssicherheit gesorgt werden, sowohl für Nutzer als auch alle beteiligten Wirtschaftsakteure.

Die Gesetzesinitiative fügt sich ein in **weitere, aktuelle Gesetzesvorhaben** der EU im Kontext der Produktsicherheit und der Produkthaftung: Zum einen modernisiert die EU die Vorschriften zur **Produkthaftung** (hierzu unser Newsletter). Zum anderen gilt ab Dezember 2024 eine neue **Produktsicherheitsverordnung** (hierzu unser Newsletter).

Anfang Oktober 2024 hat der Rat der EU den Gesetzesentwurf angenommen. Nach der **baldigen Veröffentlichung im Amtsblatt der EU** tritt der CRA 20 Tage später in Kraft und gilt nach einer grundsätzlich 36-monatigen Übergangsphase unmittelbar in allen EU-Mitgliedstaaten.

Produkte mit digitalen Elementen

Produkte mit digitalen Elementen dürfen zukünftig nur dann auf dem Markt bereitgestellt werden, wenn sie **gesetzlich definierten Cybersicherheitsanforderungen** genügen. Die gesetzlichen Anforderungen beziehen sich auf verschiedene technische und organisatorische Maßnahmen im Hinblick auf die Gewährleistung eines angemessenen Cybersicherheitsniveaus.

Die neuen gesetzlichen Anforderungen des CRA beziehen sich allesamt auf sog. Produkte mit digitalen Elementen. Der **Begriff „Produkte mit digitalen Elementen“** erfasst eine große Bandbreite verschiedener vernetzter Hardware- und Softwareprodukte. Die Anforderungen des CRA gelten unabhängig davon, ob die Produkte an Verbraucher (B2C) oder Unternehmen (B2B) bereitgestellt werden.

Entscheidendes Merkmal von Produkten mit digitalen Elementen ist das **Vorhandensein einer sog. Datenfernverarbeitungslösung**, d.h. einer außerhalb des Produkts stattfindenden Datenverarbeitung (z.B. in einer Cloud). Die Datenfernverarbeitung muss dabei für das Produkt mit digitalen Elementen wesentlich sein, sodass das Produkt eine oder mehrere seiner Funktionen ohne die außerhalb des Produkts stattfindende Datenverarbeitung nicht erfüllen könnte. Diese Voraussetzung erfüllen regelmäßig insbesondere **Internet of Things-(IoT-)Produkte**, wie smarte Haushaltsgeräte und Wearables.

Die Anforderungen des CRA beziehen sich sowohl auf Produkte, die physisch über Hardware-Schnittstellen verbunden werden können, als auch auf Produkte, die logisch verbunden werden (z.B. über Anwendungsprogrammierschnittstellen, engl.: Application Programming Interfaces – API). Zudem sollen nach dem Willen des Gesetzgebers auch Produkte erfasst werden, die nur indirekt mit anderen Geräten oder Netzen verbunden sind.

Für spezifische Bereiche sieht der CRA **Bereichsausnahmen** vor. So fallen Produkte mit digitalen Elementen, die beispielsweise den gesetzlichen Vorschriften für Medizinprodukte oder In-Vitro-Diagnostika unterliegen, ausnahmsweise nicht in den Anwendungsbereich des CRA.

Herstellerpflichten

Der CRA verpflichtet die Hersteller von Produkten mit digitalen Elementen, im Rahmen der **Konzeption, der Entwicklung und der Herstellung betroffener Produkte** diverse durch den CRA definierte Cybersicherheitsanforderungen zu berücksichtigen, beispielsweise sichere Standardkonfigurationen („*Security by Default*"), Maßnahmen zum Schutz vor unbefugten Zugriffen oder die Bereitstellung von Sicherheitsupdates.

Die Herstellerpflichten beziehen sich nicht nur auf selbst hergestellte Produkte, sondern grundsätzlich auch auf von Dritten bezogene Komponenten, die herstellerseitig in die Produkte integriert werden.

In diesem Zusammenhang müssen Hersteller zukünftig eine **Bewertung der Cybersicherheitsrisiken** ihrer jeweiligen Produkte durchführen. Das Bewertungsergebnis muss während des gesamten Lebenszyklus' (Planungs-, Konzeptions-, Entwicklungs-, Herstellungs-, Lieferungs- und Wartungsphase) berücksichtigt und grundsätzlich während der gesamten Produktlebensdauer, jedenfalls aber während des jeweiligen Unterstützungszeitraums, aktualisiert werden. Somit soll ein **angemessenes Cybersicherheitsniveau während des gesamten Lebenszyklus'** eines Produkts gewährleistet werden.

Darüber hinaus müssen Hersteller zukünftig **Verfahren im Kontext der Cybersicherheit** ihrer Produkte etablieren, die ebenfalls diversen gesetzlich definierten Anforderungen entsprechen müssen. Insoweit sieht der CRA u.a. vor, dass Hersteller erkannte Sicherheitsschwachstellen ihrer Produkte dokumentieren und unverzüglich beheben sowie Informationen über beseitigte Schwachstellen veröffentlichen.

Im Hinblick auf die **Beseitigung von Sicherheitsschwachstellen** verpflichtet der CRA die Hersteller grundsätzlich zur Bereitstellung von Sicherheitsupdates an die Nutzer. Nach der Bereitstellung müssen Sicherheitsaktualisierungen für einen gewissen Zeitraum für die Nutzer verfügbar bleiben, um den Nutzern auch spätere Updates zu ermöglichen.

Sofern Hersteller Kenntnis davon erlangen, dass Sicherheitsschwachstellen ihrer Produkte mit digitalen Elementen aktiv ausgenutzt wurden, trifft sie grundsätzlich eine **Meldepflicht**, gemäß derer sie einen Vorfall unverzüglich, jedenfalls aber innerhalb von 24 Stunden nach Kenntnis, an die zuständigen Behörden melden müssen.

Zudem trifft Hersteller unter solchen Umständen eine **Informationspflicht gegenüber den Nutzern** der betroffenen Produkte mit digitalen Elementen. Hersteller müssen die Nutzer insbesondere über Maßnahmen informieren, die Nutzer ergreifen können, um die Auswirkungen der jeweiligen Vorfälle zu mindern.

In Bezug auf die Melde- und Informationspflichten sollten Hersteller **Präventionsmaßnahmen** ergreifen und die erforderlichen Prozesse etablieren, um fristgerechte Meldungen sowie Informationen zu gewährleisten.

Einführer & Händler

Neben den Herstellern statuiert der CRA Pflichten für Einführer und Händler von Produkten mit digitalen Elementen.

Bevor sie ein Produkt mit digitalen Elementen in Verkehr bringen, müssen **Einführer** diversen Sorgfalts- und Transparenzpflichten entsprechen. Unter anderem müssen Einführer sicherstellen, dass der Hersteller der jeweiligen Produkte die geeigneten Konformitätsbewertungsverfahren durchgeführt und eine den gesetzlichen Anforderungen entsprechende technische Dokumentation erstellt hat. Einführer betroffener Produkte trifft eine **Rechenschaftspflicht**, wonach sie in der Lage sein müssen, die Einhaltung der gesetzlichen Anforderungen nachweisen zu können.

Auch die **Händler** von Produkten mit digitalen Elementen treffen diverse Sorgfalts- und Transparenzpflichten. Unter anderem werden Händler verpflichtet, zu überprüfen, ob der Hersteller und der Einführer eines Produkts diverse gesetzliche Anforderungen des CRA erfüllt und dem Händler alle erforderlichen Dokumente bereitgestellt haben.

Sofern die Einführer bzw. Händler betroffener Produkte Grund zu der Annahme haben, dass ein Produkt ein **erhebliches Cybersicherheitsrisiko** birgt, dürfen sie das betroffene Produkt nicht in Verkehr bringen bzw. auf dem Markt bereitstellen. Stattdessen müssen Einführer bzw. Händler die Hersteller und die Marktüberwachungsbehörden informieren. Zudem können Einführer bzw. Händler u.U. zur **Ergreifung von Korrekturmaßnahmen** bezüglich der von ihnen in Verkehr gebrachten bzw. auf dem Markt bereitgestellten Produkte verpflichtet sein (z.B. Behebung von Sicherheitsschwachstellen, Produktrückruf).

Unter gewissen Umständen können **Herstellerpflichten auch unmittelbar für die Einführer bzw. Händler eines Produkts mit digitalen Elementen gelten**. Dies gilt insbesondere in Fällen, in denen Einführer bzw. Händler ein betroffenes Produkt unter ihrem eigenen Namen bzw. ihrer eigenen Marke in Verkehr bringen (z.B. White-Label-Produkte) oder wesentliche Änderungen an Produkten vornehmen.

Marktüberwachung

Im Kontext der **Marktüberwachung** sieht der CRA weitreichende behördliche Befugnisse vor. Insoweit nimmt der CRA Bezug auf die EU-Marktüberwachungsverordnung (Verordnung (EU) 2019/1020).

Im Rahmen ihrer behördlichen Befugnisse können die Marktüberwachungsbehörden grundsätzlich einen Anspruch auf **Zugang zu Daten und Dokumenten** haben, die für eine Bewertung der Konzeption, Entwicklung, Herstellung und die Behandlung von Schwachstellen von Produkten mit digitalen Elementen erforderlich sind.

Zudem haben die Marktüberwachungsbehörden grundsätzlich die Befugnis zur **Anordnung von Korrekturmaßnahmen oder Produktrückrufen**, sofern sie hinreichenden Grund zu der Annahme haben, dass ein betroffenes Produkt ein erhebliches Cybersicherheitsrisiko birgt.

Der CRA sieht darüber hinaus auch die Möglichkeit für gleichzeitig stattfindende, **koordinierte Kontrollen mehrerer Marktüberwachungsbehörden (sog. Sweeps)** vor. Sweeps sollen primär von der EU Kommission koordiniert werden und eine EU-weit einheitliche Kontrolle bestimmter Produkte mit digitalen Elementen ermöglichen.

Sanktionen

Im Falle von Verstößen gegen die gesetzlichen Vorgaben statuiert der CRA grundsätzlich **empfindliche Sanktionen**, unter anderem die Möglichkeit zur Verhängung von Geldbußen. Sanktionen müssen wirksam, verhältnismäßig und abschreckend sein.

Vergleichbar zu anderen EU-Verordnungen gibt der CRA einen Rahmen für die Höhe von Geldbußen vor. Insoweit sieht der CRA die Möglichkeit zur **Verhängung von Geldbußen** in Höhe von bis zu 15 Mio. Euro oder – im Falle von Unternehmen – von bis zu 2,5% des gesamten weltweiten Jahresumsatzes vor, je nachdem, welcher Betrag höher ist. Die Einzelheiten bezüglich der Sanktionen müssen von den EU-Mitgliedstaaten im jeweiligen nationalen Recht geregelt werden.

Sofern Verstöße von Unternehmen gegen den CRA die Kollektivinteressen von Verbrauchern beeinträchtigen bzw. zu beeinträchtigen drohen, sieht der CRA zudem die Möglichkeit zur **Verbandsklagen** durch bestimmte Verbände vor.

Zeitliche Anwendbarkeit

Der CRA wird zwanzig Tage nach der baldigen Veröffentlichung im Amtsblatt der EU in Kraft treten. Der CRA sieht einen **Übergangszeitraum** nach Inkrafttreten der neuen Verordnung vor. Das bedeutet, der CRA wird **grundsätzlich 36 Monate nach Inkrafttreten** unmittelbare Geltung in der gesamten EU beanspruchen. Bestimmte gesetzliche Anforderungen, u.a. die Meldepflichten für Herstellung von

Produkten mit digitalen Elementen, gelten allerdings bereits früher, nämlich bereits 21 Monate nach dem Zeitpunkt des Inkrafttretens.

Für betroffene Produkte, die bereits vor dem allgemeinen Anwendbarkeitszeitpunkt des CRA (36 Monate nach Inkrafttreten) in Verkehr gebracht wurden, sieht der CRA eine **Übergangsbestimmung** vor. Danach unterliegen solche Produkte den Anforderungen des CRA nur dann, wenn sie nach dem allgemeinen Anwendbarkeitszeitpunkt wesentlich geändert wurden.

Unsere Empfehlung

Hersteller, Einführer und Händler von Hardware- und Softwareprodukten sollten sich **rechtzeitig mit den Anforderungen des CRA beschäftigen und erforderliche Umsetzungsmaßnahmen ergreifen**.

Insbesondere für Hersteller könnte die Umsetzung des CRA mit einem **größeren Aufwand** einhergehen, sofern die Konzeptions-, Entwicklungs- und Herstellungsprozesse für betroffene Produkte an die neuen Cybersicherheitsanforderungen angepasst werden müssen.

Ihre Ansprechpartner

Dr. Ulla Kelp, LL.M.
Rechtsanwältin, Partnerin

T +49 211 600 35-176
ulla.kelp@orka.law

Dr. Philipp Mels
Rechtsanwalt, Partner

T +49 211 600 35-180
philipp.mels@orka.law

Dr. Michael Grobe-Einsler
Rechtsanwalt, Salary Partner

T +49 211 600 35-450
michael.grobe-einsler@orka.law

Felix Meurer
Rechtsanwalt, Senior Associate

T +49 30 50 93 20-117
felix.meurer@orka.law

Marieke Schwarz
Rechtsanwältin, Salary Partnerin

T +49 211 600 35-422
marieke.schwarz@orka.law

Volker Herrmann
Rechtsanwalt, Partner

T +49 30 50 93 20-136
volker.herrmann@orka.law


One Team.
One Goal.