www.compliance-berater.de

Compliance Berater

1-2 / 2023

Betriebs-Berater Compliance

19.1.2023 | 11.Jg
Seiten 1–48

Fachmedien Recht und Wirtschaft | dfv Mediengruppe | Frankfurt am Main

CB-BEITRAG

Hans-Joachim Hess, RA

Haftungsverschärfung für Produkte in der EU

Neue Haftungsregeln für Digitalprodukte, zur Künstlichen Intelligenz (KI) und Hochrisikotechnologie sowie zum Maschinensicherheitsrecht und eine vollständige Revision der Produkthaftungsrichtlinie: Produkthersteller und Softwareentwickler müssen in den nächsten Monaten erhöhte Wachsamkeit zeigen, denn die novellierten und neuen EU-Vorschriften zum Produkthaftungs- und Produktsicherheitsrecht werden die Rechte der Anwendenden sowie der Verbraucher erheblich erweitern.

I. Einleitung

Die nachfolgende Übersicht will die Entwürfe zur neuen
- KI-Verordnung (im Folgenden KI-E)[1], zur
- Produktsicherheitsverordnung (im Folgenden E-PrS)[2], zur
- Cybersicherheitsverordnung für Produkte mit digitalen Elementen (im Folgenden E-CRA)[3] und zur
- Produkthaftungsrichtlinie (im Folgenden E-PrRL)[4], sowie zur
- Verordnung über Maschinenprodukte (im Folgenden E-MaschV)[5]

vorstellen und aufzeigen, in welchen Bereichen Hersteller, Importeure, Händler sowie die Entwickler von Software besondere Obacht walten lassen müssen.

1. Weißbuch zur Künstlichen Intelligenz (KI)

Mit dem Weißbuch zur Künstlichen Intelligenz (KI)[6] wollte die Europäische Union Regeln verbindlich festlegen, um das unaufhaltsame Vordringen digitaler Technologien nicht sich selber zu überlassen, sondern in mehrfacher Hinsicht einen verlässlichen Rechtsrahmen für die Industrie (B2B), die öffentliche Verwaltung und die Verbraucher zu schaffen. KI ist ein Bestand an Technologien, die Daten, Algorithmen und Rechenleistung kombinieren. Fortschritte in der Informatik und die zunehmende Verfügbarkeit von Daten sind der Schlüsselfaktor für den derzeitigen Aufstieg der KI. Europa muss daher seine technologischen und industriellen Stärken mit einer hochwertigen digitalen Infrastruktur und einem Rechtsrahmen kombinieren, der auf seinen Grundwerten beruht.

Europa ist zwar derzeit in den Bereichen Verbraucheranwendungen und Online-Plattformen nicht so stark aufgestellt, was zu einem Wettbewerbsnachteil hinsichtlich des Zugangs zu Daten führt, aber es stehen bedeutende Veränderungen an hinsichtlich des Werts und der sektorübergreifenden Weiterverwendung von Daten. Die Menge der weltweit produzierten Daten nimmt rasch zu, von 33 Zettabyte im Jahr 2018 auf voraussichtlich 175 Zettabyte im Jahr 2025.[7] Jede neue Datenwelle bringt Europa Möglichkeiten, sich in der datenagilen Wirtschaft zu positionieren und an die Weltspitze zu setzen. Abgesehen davon wird sich die Art und Weise, wie Daten gespeichert und verarbeitet werden, in den kommenden fünf Jahren drastisch verändern. Gegenwärtig erfolgt die Verarbeitung und Analyse von Daten in der Cloud zu 80% in Rechenzentren und zentralen Rechenanlagen und zu 20% in intelligenten vernetzten Objekten wie Autos, Haushaltsgeräten oder Fertigungsrobotern und in Rechnern nahe beim Nutzer („Edge-Computing", d. h. dezentrale Datenverarbeitung am Rand des Netzes). Bis zum Jahr 2025 dürften sich diese Anteile deutlich verschieben[8]:
- Europa ist weltweit führend in der Elektronik mit geringem Stromverbrauch, die für die nächste Generation spezialisierter KI-Prozessoren von zentraler Bedeutung ist.
- Die jüngsten Fortschritte in der Quanteninformatik werden zu exponentiellen Steigerungen der Verarbeitungskapazität führen[9]. Europa kann hier dank seiner akademischen Stärken im Bereich Quanteninformatik und der starken Position der europäischen Industrie im Bereich Quantensimulatoren und Programmierumgebungen für Quantencomputer eine Vorreiterrolle einnehmen.
- Parallel dazu wird Europa auf der Grundlage seiner eigenen wissenschaftlichen Exzellenz weiterhin eine Vorreiterrolle bei den algorithmischen Grundlagen der KI einnehmen. Zwischen Fachdisziplinen, die gegenwärtig separat voneinander arbeiten, wie maschinelles Lernen und „Deep Learning" (dessen Merkmale begrenzte Interpretierbarkeit, Bedarf an großen Datenmengen für das Trainieren von Modellen und Lernen durch Korrelationen sind) und symbolischen Ansätzen (bei denen Regeln durch menschliche Eingriffe geschaffen werden) müssen Brücken geschlagen werden. Die Kombination von symbolischem Schlussfolgern und tiefen neuro-

1 COM (2021) 206 final vom 21.4.2021.
2 COM (2021) 346 final vom 30.6.2021.
3 COM (2022) 454 final vom 15.9.2022.
4 COM (2022) 495 final vom 28.9.2022.
5 COM (2021) 202 final vom 21.4.2021.
6 COM (2020) 65 final vom 19.2.2020.
7 International Data Corporation, IDC, 2019.
8 Gartner Market Reports, 2017, in Weißbuch KI, S. 5.
9 Quantencomputer werden in Bruchteilen von Sekunden sehr viel umfangreichere Datensätze verarbeiten können als heutige Höchstleistungsrechner, was die Entwicklung neuer KI-Anwendungen für alle Sektoren ermöglicht.

nalen Netzen kann u. U. helfen, die Erklärbarkeit von KI-Ergebnissen zu verbessern.

Entwickler und Nutzer von KI unterliegen bereits europäischen Rechtsvorschriften über Grundrechte (z. B. Datenschutz, Schutz der Privatsphäre und Nichtdiskriminierung), Verbraucherschutz sowie Produktsicherheit und -haftung. Die Verbraucher erwarten die gleiche Sicherheit und die gleiche Achtung ihrer Rechte, unabhängig davon, ob ein Produkt oder System KI-gestützt ist oder nicht. Allerdings können bestimmte Besonderheiten der KI (z. B. die Opazität) die Anwendung und Durchsetzung dieser Rechtsvorschriften erschweren.

Die besonderen Merkmale vieler KI-Technologien wie Opazität (mangelnde Transparenz oder „Blackbox-Effekt"), Komplexität, Unvorhersehbarkeit und teilautonomes Verhalten können die Prüfung der Vereinbarkeit und die wirksame Durchsetzung von EU-Rechtsvorschriften zum Schutz der Grundrechte erschweren. Strafverfolgungsbehörden und Betroffene können unter Umständen nicht nachvollziehen, wie eine bestimmte unter Einsatz von KI getroffene Entscheidung gefällt wurde, und somit auch nicht verifizieren, ob die einschlägigen Vorschriften eingehalten wurden. Natürliche wie juristische Personen könnten in Fällen, in denen sich solche Entscheidungen nachteilig auf sie auswirken, beim effektiven Zugang zur Justiz auf Schwierigkeiten stoßen.

Nach der Produkthaftungsrichtlinie haften beispielsweise Hersteller für Schäden, die durch fehlerhafte Produkte verursacht werden. Im Falle KI-gestützter Systeme, wie z. B. bei autonomen Fahrzeugen, kann es jedoch schwierig sein, einen Produktfehler, den entstandenen Schaden und den Kausalzusammenhang zwischen diesen beiden nachzuweisen. Darüber hinaus besteht eine gewisse Unsicherheit darüber, wie und in welchem Umfang die Produkthaftungsrichtlinie auf bestimmte Arten von Mängeln Anwendung findet, z. B. wenn diese auf Schwächen bei der Cybersicherheit des Produkts zurückzuführen sind.

Treten Sicherheitsrisiken tatsächlich auf, ist es aufgrund des Fehlens klarer Anforderungen und der oben genannten Merkmale der KI-Technologien schwierig, potenziell problematische Entscheidungen, die unter Einbeziehung von KI-Systemen getroffen wurden, zurückzuverfolgen. Dadurch kann es für Personen, die einen Schaden erlitten haben, schwer werden, eine Entschädigung nach dem geltenden EU- und nationalen Haftungsrecht zu erhalten.

2. Haftung beim Einsatz Künstlicher Intelligenz

Die Entwicklung der Robotik war unter anderem Anlass, dass eine haftungsrechtliche Diskussion über IT-Systeme in Gang gesetzt wurde. Wie schon zuvor aufgezeigt, bestehen vor allem im Bereich der Autonomie besonders gravierende Haftungslücken, aber auch die stark zunehmende Vernetzung der Systeme hat den EU-Gesetzgeber veranlasst, eine KI-Verordnung vorzuschlagen und dabei einen risikobasierten Ansatz gewählt. Die Risiken sind allerdings je nach angewandter Technologie unterschiedlich, so ist eine klare Rechtsformel, die über Taschenrechner, Excel oder ein Programm ausgeführt wird, nicht zu vergleichen mit einem trainierten System, das eben in seiner Beherrschbarkeit gewisse Unsicherheiten aufweist.[10]

a) Regelungsinhalt

Die Verordnung will festlegen, dass KI-Systeme sicher, transparent, ethisch, unparteiisch und unter menschlicher Kontrolle sind. In Art. 3 Abs. 1 KI-E werden zunächst KI-Systeme festgelegt. Damit soll eine gewisse Rechtssicherheit garantiert werden, aber auch genügend Flexibilität, um künftigen technologischen Entwicklungen nicht im Wege zu stehen.[11]

Dabei werden folgende Systeme in der Verordnung unterschieden:
- Verbotene KI-Systeme (Art. 5 KI-E)
- Hochrisikosysteme (Art. 6–51 KI-E, hier ist das „Herzstück des Entwurfs")
- Systeme mit geringem Risiko (Art. 52 KI-E)
- Systeme mit einem minimalen Risiko (Art. 69 KI-E)

Alles, was als eine eindeutige Bedrohung für EU-Bürger angesehen wird, wird verboten.

b) Verbotene KI

In Titel II KI-E werden die verbotenen Praktiken aufgezählt, die als unannehmbar gelten, weil sie Werte der EU, beispielsweise Grundrechte, verletzen. Dies reicht von der behördlichen Bewertung des sozialen Verhaltens (Social Scoring) bis hin zu Spielzeug mit Sprachassistenten, das Kinder zu riskantem Verhalten verleitet.

c) KI-Systeme mit hohem Risiko

Zusätzliche Prüfungs-, Dokumentations- und Registrierungspflichten müssen alle KI-Systeme mit einem hohen Risiko in einer eigenen EU-Datenbank nachweisen. In Titel III Kapitel 1 KI-E sind die Einstufungsregeln angegeben und zwei Hauptkategorien für Hochrisiko-KI-Systeme festgelegt. Dies sind:
- KI-Systeme, die als Sicherheitskomponenten von Produkten, die einer vorgängigen Konformitätsbewertung durch Dritten unterliegen, verwendet werden sollen;
- sonstige eigenständige KI-Systeme, die ausdrücklich im Anhang III genannt werden und sich vor allem auf Grundrechte auswirken.

Zu den in Anhang III aufgezählten Systemen gehören:
- Kritische Infrastrukturen (z. B. im Verkehr), in denen das Leben und die Gesundheit der Bürger gefährdet werden könnten;
- Schul- oder Berufsausbildung, wenn der Zugang einer Person zur Bildung und zum Berufsleben beeinträchtigt werden könnte (z. B. Bewertung von Prüfungen);
- Sicherheitskomponenten von Produkten (z. B. eine KI-Anwendung für die roboterassistierte Chirurgie);
- Beschäftigung, Personalmanagement und Zugang zu selbstständiger Tätigkeit (z. B. Software zur Auswertung von Lebensläufen für Einstellungsverfahren);
- zentrale private und öffentliche Dienstleistungen (z. B. Bewertung der Kreditwürdigkeit, wodurch Bürgern Darlehen verwehrt werden);
- Strafverfolgung, die in die Grundrechte der Menschen eingreifen könnte (z. B. Überprüfung der Echtheit von Beweismitteln);
- Migration, Asyl und Grenzkontrolle (z. B. Überprüfung der Echtheit von Reisedokumenten).

---

10 *Jörn Erbguth*, NJW aktuell 46/2022, 19.

11 Definition der KI einer hochrangige EU-Expertengruppe: „Künstliche-Intelligenz-(KI)-Systeme sind vom Menschen entwickelte Software- (und möglicherweise auch Hardware-) Systeme, die in Bezug auf ein komplexes Ziel auf physischer oder digitaler Ebene agieren, indem sie ihre Umgebung durch Datenerfassung wahrnehmen, die gesammelten strukturierten oder unstrukturierten Daten interpretieren, Schlussfolgerungen daraus ziehen oder die aus diesen Daten abgeleiteten Informationen verarbeiten und über die geeignete (n) Maßnahme(n) zur Erreichung des vorgegebenen Ziels entscheiden. KI-Systeme können entweder symbolische Regeln verwenden oder ein numerisches Modell erlernen, und sind auch in der Lage, die Auswirkungen ihrer früheren Handlungen auf die Umgebung zu analysieren und ihr Verhalten entsprechend anzupassen." in Weißbuch KI (Fn. 6), S. 19., Fn. 47.

– Rechtspflege und demokratische Prozesse (z. B. Anwendung der Rechtsvorschriften auf konkrete Sachverhalte)

Alle Systeme sind sorgfältig zu prüfen, bevor sie in Verkehr gebracht werden – und auch während ihres gesamten Lebenszyklus. In Kapitel 2 KI-E ist darüber hinaus festgelegt, welche rechtlichen Anforderungen Hochrisiko-KI-Systeme in Bezug auf Daten, Daten-Governance, Dokumentation und das Führen von Aufzeichnungen, Transparenz und Bereitstellung von Informationen für die Nutzer, menschliche Aufsicht, Robustheit, Genauigkeit und Sicherheit erfüllen.

d) Systeme mit begrenztem Risiko

Für KI-Systeme wie „Chatbots" gelten minimale Transparenzverpflichtungen, die es den mit ihnen interagierenden Nutzern ermöglichen sollen, fundierte Entscheidungen zu treffen. Die Nutzer können dann entscheiden, ob sie die Anwendung weiter nutzen oder nicht.

e) Systeme mit minimalem Risiko

Kostenlose Nutzung von Anwendungen wie KI-gestützten Videospielen oder Spamfiltern: Unter diese Kategorie, in der die neuen Vorschriften nicht greifen, fällt die große Mehrzahl der KI-Systeme, weil diese Systeme nur ein minimales oder kein Risiko für die Bürgerrechte oder die Sicherheit darstellen.

f) Verhaltenskodizes

Titel IX KI-E enthält die Grundlagen zur Schaffung von Verhaltenskodizes, die Anbietern von KI-Systemen, die kein hohes Risiko darstellen, Anreize geben sollen, die zwingend vorgeschriebenen Anforderungen an Hochrisiko-KI-Systeme (nach Titel III KI-E) freiwillig anzuwenden. Anbieter von KI-Systemen, die kein hohes Risiko darstellen, können selbst Verhaltenskodizes festlegen und umsetzen. Nach Art. 2 Abs. 1 a KI-E wird überdies ein bereits aus der DSGVO bekannter, extraterritorialer Anwendungsbereich festgelegt an den sich auch KI-Systeme halten müssen, die aus nicht EU-Staaten in der EU KI-Systeme anbieten.

3. Neue Produktsicherheitsverordnung

Die neue Produktsicherheitsverordnung soll die alte Richtlinie 2001/957/EG (Allgemeine Produktsicherheitsrichtlinie) aus dem Jahr 2001 ersetzen.

a) Neuerungen

Um mehr Sicherheit zu gewährleisten, werden Klarstellungen zu Schlüsseldefinitionen wie „Produkt" und „sicheres Produkt" vorgenommen, dies vor allem deswegen, damit die Wirtschaftsakteure[12] und die Behörden mehr Sicherheit erhalten. Die Verordnung soll im Übrigen für eine vereinheitlichte Auslegung der Begriffe in der EU sorgen und differente Gerichtsentscheidungen vermeiden helfen.

Das Kapitel II über die Sicherheitsanforderungen erhält eine neue Struktur, um alle Phasen, die zur Sicherheitsbewertung durch den betreffenden Wirtschaftsakteur und zur Sicherheitsvermutung führen, näher zu erläutern.

Die Anforderungen in Bezug auf die Herstellerpflichten hinsichtlich der technischen Unterlagen und eingegangener Beschwerden (Art. 8 E-PrS) werden geändert, zur Wahrung der Verhältnismäßigkeit beim Umgang mit kleinen Erzeugern und Sektoren mit geringem Risiko.

b) Erfasste Produkte

Der Anwendungsbereich umfasst nach wie vor Non-Food-Verbraucherprodukte (einschließlich relevanter Migrationsprodukte) und neu auch lebensmittelähnliche Produkte.

c) Digitalisierung der Information

Noch nicht entschieden ist, ob die Wirtschaftsakteure die wichtigsten Informationen (z. B. technische Dokumentation, Anleitung und Sicherheitsinformationen) in digitaler Form bereitstellen können.

Das Angebot von Produkten online oder über Fernabsatz soll flächendeckend als „Bereitstellen" behandelt werden, wenn das Angebot an EU-Verbraucher gerichtet ist. Für Letzteres kann die Verwendung einer Sprache oder Währung von EU-Mitgliedstaaten, die Domain-Registrierung in einem Mitgliedstaat oder das Angebot des Versands in einen Mitgliedstaat ausreichend sein (Art. 4 E-PrS).

d) Vermutungswirkung von harmonisierten Normen

Seitens der EU-Kommission soll es Durchführungsakte geben, die für in Einklang mit harmonisierten Normen stehende Produkte (für die weiterhin die Konformitätswirkung gelten soll) „spezifische Sicherheitsanforderungen" festlegen, die nötig sind, damit diese Produkte generelle Sicherheitsanforderungen nach Art. 5 E-PrS einhalten. Für die Bewertung der Einhaltung der Sicherheitsvorgaben außerhalb der Vermutungswirkung auf Basis technischer Normen enthält der Vorschlag einen umfassenden Kriterienkatalog. Außer bekannten Aspekten sind dort Cyber Security und Künstliche Intelligenz aufgeführt. Außerdem können etwa freiwillige Zertifizierungen, Kommissions-Empfehlungen und -Richtlinien, technische Standards und Good-Practice-Faktoren in die Bewertung einfließen.

e) Erweiterte Herstellerpflichten

Unter Bezugnahme auf die Regeln des „New Legislative Framework (NLF)"[13] wurden die Herstellerpflichten neu angepasst und erheblich erweitert. So soll es für Hersteller eine Pflicht zur fortlaufenden Information von Händlern, Importeuren und Online-Marktplätzen über identifizierte Sicherheitsprobleme geben. Gibt es Anhaltspunkte dafür, dass ein Produkt nicht sicher ist, soll neu die Pflicht bestehen, unverzüglich Korrekturmaßnahmen durchzuführen. Die Meldepflicht gegenüber den Marktüberwachungsbehörden wird erweitert um eine entsprechende Pflicht gegenüber den Verbrauchern (über das Safety Business Gateway[14]).

Von größerer Tragweite wird allerdings – sollte sie durch den Ministerrat angenommen werden – die Verpflichtung der Hersteller sein, dass diese innerhalb von zwei Arbeitstagen nach Kenntniserlangung die Marktüberwachungsbehörden über Unfälle informieren müssen, die von einem von ihnen bereitgestellten Produkt verursacht wurden und im Falle des Rückrufs eine kostenfreie Reparatur, Ersatzlieferung oder Rückzahlung des Kaufpreises anzubieten haben (Art. 35 E-PrS).

---

12 Dazu Art. 8 ff. E-PrS, namentlich Hersteller, Bevollmächtigte, Einführer, Händler.

13 Beschluss (EU) Nr. 768/2008/EG.

14 Mithilfe des Schnellwarnsystems werden täglich Warnmeldungen der nationalen Behörden weitergeleitet. Jede Warnmeldung enthält Angaben zu dem als gefährlich eingestuften Produkt, eine Beschreibung der Risiken und die von Wirtschaftsbeteiligten ergriffenen oder von den Behörden angeordneten Maßnahmen. Jede Warnmeldung wird von anderen Behörden weiterverfolgt, die eigene Maßnahmen ergreifen, sollte dasselbe Produkt auch auf ihrem nationalen Markt in Umlauf sein. Andere Länder sind verpflichtet, diesen Informationen Rechnung zu tragen. Sollten sie dasselbe Produkt auf ihren eigenen Märkten auffinden, müssen sie dies ebenfalls über das Schnellwarnsystem melden; vgl. auch E-PrS, Art. 23.

Sind durch die Wirtschaftsakteure sogenannte Korrekturmaßnahmen (wie Rückruf oder Warnungen) durchzuführen, sollen vorhandene persönliche Daten ihrer Kunden genutzt werden. Sie müssen bei vorhandenen Systemen zur Produktregistrierung oder Treueprogrammen den Kunden die Möglichkeit der Hinterlegung persönlicher Daten für Sicherheitsmaßnahmen einräumen (Art. 33 Abs. 2 E-PrS).
Art. 34 E-PrS verlangt bei einem schriftlichen Rückruf eine genaue Umsetzung von zahlreichen Produkt-Informationen an die Verbraucher und die vom Verbraucher zu ergreifenden Maßnahmen, inklusive die Bereitstellung einer kostenfreien Hotline.

f) Pflichten für Online-Handelsplattformen
Sogenannte Online-Marktplätze[15] (wie beispielsweise eBay oder Amazon) müssen auf Anordnung der Marktaufsichtsbehörden etwa die Entfernung gefährlicher Produkte von Online-Schnittstellen verlangen können. Ferner müssen die Online-Marktplätze die technischen Voraussetzungen schaffen, dass Händler rechtlich erforderliche Informationen bereitstellen können. Außerdem müssen sie umfassend mit den Marktüberwachungsbehörden und anderen Wirtschaftsakteuren im Hinblick auf erforderliche Korrekturmaßnahmen zusammenarbeiten.

g) Schlichtungsverfahren zwischen Marktaufsichtsbehörden
Sollten Marktüberwachungsbehörden verschiedener Mitgliedstaaten über Risikobeurteilungen oder Risikograde unterschiedliche Auffassungen haben, kann ein freiwilliges Schlichtungsverfahren bei der EU-Kommission durchgeführt werden.

4. EU-Cybersicherheitsverordnung
Als erster europäischer Rechtsakt (sog. „Cyber Resilience Act", CRA) dieser Art werden durch die geplante Cybersicherheitsverordnung verbindliche Regeln für Produkte mit digitalen Elementen während des gesamten Lebenszyklus vorgelegt. Der Entwurf beruht ebenfalls auf dem New Legislative Framework und folgt dessen grundlegender Regelungsstruktur.

a) Erfasste Geräte
Die Verordnung wird für alle Produkte gelten, die entweder direkt oder indirekt mit einem anderen Gerät oder Netz verbunden sind. Sie erfassen nach Art. 3 Abs. 1 E-CRA Hard- und Software gleichermaßen. Vom Anwendungsbereich ausgenommen sind jedoch Erzeugnisse, bei denen die Anforderungen an die Cybersicherheit bereits in bestehenden EU-Rechtsakten festgelegt sind.[16]

b) Formelle Anforderungen
Zu den formalen Anforderungen gehören etwa die Ausstellung einer EU-Konformitätserklärung nach Art. 20 CRA-E und die Anbringung der CE-Kennzeichnung im Sinne des Art. 22 CRA-E. Wie üblich, hat letzteres vorrangig auf dem Produkt selbst oder nachrangig auf der Verpackung zu erfolgen. Bei Stand-alone-Software kann die CE-Kennzeichnung auch auf der EU-Konformitätserklärung oder einer produktbegleitenden Website angebracht werden.

c) Materielle Anforderungen
Produkte müssen den grundlegenden Cybersicherheitsanforderungen nach Art. 5 E-CRA i. V. m. Anhang I des E-CRA erfüllen. Dabei wird gemäß Art. 18 E-CRA vermutet, dass das Produkt die Anforderungen erfüllt, wenn es harmonisierten Standards entspricht.
Das für die Einhaltung der materiellen Anforderungen maßgebliche Konformitätsbewertungsverfahren führt der Hersteller nach Art. 24 E-CRA in der Regel selbst durch. Bei sog. „kritischen" Produkten mit digitalen Elementen[17] im Sinne des Art. 6 E-CRA ist dies allerdings anders. Ein Erzeugnis unterfällt dieser Kategorie, wenn seine Kernfunktion einer der in Anhang III des E-CRA abschließend aufgeführten Anwendungen entspricht, wobei zwischen Produkten der Klasse I und solchen der Klasse II unterschieden wird. Bei Klasse-I Produkten kann der Hersteller die Konformität durch die vollständige Anwendung harmonisierter Standards im Sinne des Art. 18 E-CRA nachweisen, andernfalls hat er eins der in Art. 24 E-CRA aufgeführten Verfahren unter Einbindung einer notifizierten Stelle durchzuführen. Bei Produkten der Klasse II ist hingegen zwingend ein Konformitätsbewertungsverfahren unter Einbindung einer notifizierten Stelle zu durchlaufen.

d) Pflichten der Wirtschaftsakteure
In den Art. 10 ff. CRA-E werden Pflichten an die Hersteller, Bevollmächtigte, Importeure und Händler festgelegt.

e) Hersteller
Der Herstellerbegriff des Art. 3 Abs. 18 CRA-E entspricht dem üblichen Verständnis und erfasst auch sogenannte Quasi-Hersteller. Nach Art. 16 CRA-E wiederum reicht auch die Vornahme einer wesentlichen Veränderung an einem Produkt mit digitalem Element aus, um als Hersteller angesehen zu werden.
Der Hersteller trägt die primäre Verantwortung für die Produktkonformität. Ausdruck der Produktverantwortung sind die klassischen Vormarkt- und Nachmarktpflichten, die sich jedoch teilweise von den bestehenden Harmonisierungsrechtsvorschriften der Union unterscheiden:
- Informations- und Instruktionspflichten mit dem Mindestinhalt des Anhangs II des CRA-E
- Produktbeobachtungspflichten, insbesondere hinsichtlich der Anfälligkeit für Sicherheitslücken und der davon ausgehenden Risiken
- Prüfpflichten in Bezug auf zugekaufte Komponenten
- proaktive Nachmarktpflichten über die ganze Lebensdauer des Produkts, höchstens aber für fünf Jahre nach der Markteinführung wie etwa Software-Updates bei Sicherheitslücken oder Korrekturmaßnahmen bei fehlender Konformität
- Mitwirkungs- und Meldepflichten gegenüber den Marktüberwachungsbehörden; speziell eine sehr kurz bemessene Meldefrist von höchstens 24 Stunden gegenüber der Agentur der Europäischen Union für Cybersicherheit (ENISA) bei Entdeckung aktiv ausgenutzter Sicherheitslücken

f) Verhältnis zu anderen EU-Produktrechtsvorschriften
Als horizontaler Rechtsakt sieht der Entwurf der EU-Cybersicherheitsverordnung vor, dass diese parallel mit anderen Harmonisierungs-

15 Art. 3 Ziff. 14, Art. 4 E-PrS: „Online-Marktplatz" ist ein Vermittlungsdienst, der unter Einsatz einer Software, einschließlich einer Internetseite, Teilen einer Internetseite oder einer Anwendung, von einem Unternehmer oder in dessen Auftrag betrieben wird und es Verbrauchern ermöglicht, mit anderen Unternehmern oder Verbrauchern Fernabsatzverträge über den Verkauf von Produkten zu schließen, auf die diese Verordnung Anwendung findet.

16 So z. B. für Medizinprodukte (RL 2017/745/EG), für die Luftfahrt (Verordnung 2018/1139) und Fahrzeuge (Verordnung 2019/2144).

17 Beispielsweise: Software für Identitätsmanagementsysteme und Software für die Verwaltung des privilegierten Zugangs, eigenständige und eingebettete Browser; Passwort-Manager; Software für die Suche, Entfernung und Quarantäne von Schadsoftware; Produkte mit digitalen Elementen mit der Funktion eines virtuellen privaten Netzes (VPN); Netzmanagementsysteme.

rechtsvorschriften anzuwenden ist. Zu drei EU-Produktrechtsvorschriften wird das Verhältnis ausdrücklich geregelt:

- nach Art. 7 CRA-E haben Harmonisierungsrechtsvorschriften der Union und die sich noch im Entwurf befindliche EU-Produktsicherheitsverordnung hinsichtlich der Anforderungen an die Produktsicherheit Vorrang vor der E-CRA
- nach Art. 8 CRA-E gelten die Anforderungen an die Cybersicherheit nach Art. 15 KI-Verordnung-E als erfüllt, wenn das Produkt bereits nach der E-CRA konform ist
- mit der Einhaltung der Anforderungen der CRA-E gelten gemäß Art. 9 CRA-E die Anforderungen der Nr. 1.1.9 und 1.2.1 des Anhangs III des EU-Maschinenverordnung-E als erfüllt

5. Das neue Regime der Produkthaftung

Im Jahr 1985 läutete die Europäische Gemeinschaft, wie die heutige Europäische Union damals noch hieß, ein neues Zeitalter der Haftung von Herstellern für ihre Produkte ein. Die EG-Richtlinie 85/374/EG brachte ein modernes Haftungsrecht und einen hohen Gewinn an Rechtsvereinheitlichung mit sich. Allerdings muss einschränkend konstatiert werden, dass den Vorschriften auch ein beträchtliches Harmonisierungsdefizit zu bescheinigen war. Im Verlauf der vergangenen 37 Jahre seit Inkrafttreten der Richtlinie ist sie mit weiteren legislatorischen Maßnahmen – so der EG-Richtlinie über die Produktsicherheit 2001/95/EG – ergänzt worden, die ein umfassendes Sicherheitsnetz für die europäischen Verbraucher geflochten haben. Dabei ging es primär um die Neuverteilung der Haftungsrisiken in einer damals schon hochentwickelten Industriegesellschaft. Die einzelnen Berichte der EG-Kommission über die Anwendung der Richtlinie, die alle fünf Jahre zu erstatten waren (Art. 21 RL), haben die Diskussion um die Produkthaftung nicht zur Ruhe kommen lassen.[18] Alle Berichte geben eine große Akzeptanz der Richtlinie wieder und halten fest, dass die Vollharmonisierung der Produkthaftung ausdrücklich nicht das Ziel der weiteren Bemühungen sein soll.

So ist festzuhalten, dass allein die Rechtsprechung des Europäischen Gerichtshofs (EuGH) über die weitere Entwicklung im Rahmen der Umsetzung der Richtlinie ins nationale Recht und deren Anwendung eine entscheidendere Rolle spielt und bereits maßgeblich die Produkthaftung in Europa geprägt hat. So geht der EuGH davon aus, dass der Aspekt der Rechtsvereinheitlichung primäres Ziel der Richtlinie sei. Gerade weil die Richtlinie auf eine Vereinheitlichung des Produkthaftungsrechts ziele, seien die nationalen Produkthaftungsvorschriften unter Einbeziehung der rechtsvergleichenden Methode so auszulegen, dass im Einzelfall größtmögliche Harmonisierungseffekte erzielt würden.[19]

Durch die neuen Technologien entstehen nun allerdings seit Jahren neue Produktkategorien, die durch die alte Richtlinie nicht mehr abgedeckt werden. Dazu gehören beispielsweise intelligente und auf künstliche Intelligenz (KI) abgestützte Produkte. Zweifelhaft blieb auch zuletzt die Frage, wer für Fehler bei Software-Updates, Algorithmen für maschinelles Lernen oder digitalen, für das Funktionieren eines Produkts unentbehrlichen Dienstleistungen haftbar ist.

a) Erfasste Produkte

Der Entwurf sieht vor, dass die Richtlinie für alle Produkte gilt, von einem einfachen Küchengerät über Maschinen bis hin zu Medikamenten gegen Krebs und auch für landwirtschaftliche Erzeugnisse, neu aber auch für Software-Updates. Die Richtlinie wird zukünftig zulassen, dass geschädigte Personen Entschädigung fordern können, wenn der Schaden durch Software oder KI-Systeme oder etwa Cybersicherheitsvorfälle verursacht wurde.

b) Haftung für Schäden

Neben den Personenschäden und Sachschäden wird neu auch für Datenverlust gehaftet. Der Anspruch besteht auch, wenn der Sachschaden an Gütern entstanden ist, die sowohl beruflich wie auch privat genutzt werden (Firmen-Lastenfahrrad oder Home-Office-Ausrüstung). Schadenersatz kann auch dann verlangt werden, wenn durch eine fehlerhafte Software zum Beispiel Updates, Upgrades und digitale Dienste beeinträchtigt werden.

Die neuen Vorschriften sorgen außerdem für die gleiche Behandlung zwischen den Personen, die auf Entschädigung klagen, und den Herstellern, indem sie die Hersteller zur Offenlegung von Informationen verpflichten und in komplexen Fällen, beispielsweise im Zusammenhang mit pharmazeutischen Produkten oder KI, die Beweislast erleichtern.

Auch Personen, die einen Schaden an einer Immobilie erleiden, werden entschädigt, sofern die Immobilie nicht ausschließlich zu beruflichen Zwecken genutzt wird, dazu zählen auch gemischt genutzte Immobilien.

Keine Entschädigung erhalten Personen für Verletzung von Grundrechten, etwa wenn jemand wegen diskriminierender KI-basierter Rekrutierungssoftware bei einer Bewerbung scheitert. Diese Verstöße sollen durch die KI-Verordnung verhindert werden.

c) Haftung von Importeuren und Händlern

Wer Produkte aus dem Nicht EU-Ausland in die EU einführt, haftet grundsätzlich für die Fehlerfreiheit der Produkte. Allerdings nimmt die neue Richtlinie Rücksicht auf den Umstand, dass Produkte auch auf direktem Weg aus dem Ausland – ohne einen EU-Zwischenhändler – zum Kunden kommen. Unter Berücksichtigung der EU-Marktüberwachungsverordnung[20] und der neuen Produktsicherheitsverordnung muss gewährleistet sein, dass stets eine in der EU ansässige haftbare Person verfügbar ist, von der Schadenersatz verlangt werden kann.

Auch Händler (offline- und Online-Verkäufer, sog. „Erfüllungsdienstleister“) können haftbar gemacht werden, wenn sie der geschädigten Person den Namen der in der EU ansässigen haftbaren Person auf Anforderung nicht mitteilen. Dies gilt auch für online-Marktplätze, aber nur wenn sie dem Verbraucher gegenüber als Händler auftreten.

d) Keine Bagatellschwelle für Schadenshöhe und Haftungshöchstgrenze

Die derzeitige Beschränkung auf Ansprüche mit einem Schwellenwert von weniger als 500 EUR wird wie die Haftungshöchstgrenze von 70 Mio. ECU (85 Mio. Euro) gestrichen.

e) Änderungen der Beweislast

Neu ist, dass Unternehmen Beweismittel offenlegen müssen, die ein Kläger zum Nachweis seines Vorbringens vor Gericht benötigt. Damit diese Beweislastregel allerdings nicht zulasten der Hersteller ausartet, werden dem Kläger, der nach wie vor nachweisen muss, dass das Produkt fehlerhaft war, nur dann Beweiserleichterungen zugestanden, wenn

- das Gericht der Auffassung ist, dass der Beklagte seinen Informationspflichten nicht nachkam,

---

18 Zu den einzelnen Berichten ausführlich *Oechsler*, in: Staudinger Julius, Kommentar zum Bürgerlichen Gesetzbuch, Buch 2, Berlin 2021, N 25 ff. Einl. zum ProdHaftG.

19 EuGH, Urt. v. 25.4.2002 – C-52/00, Slg. 2002, 1–3827.

20 VO (EU) 2019/1020.

- der Ursachenzusammenhang zwischen Fehler und Schaden schwer nachzuweisen ist, aber der Schaden „typischerweise" mit dem betreffenden Fehler zusammenhängt,
- das Gericht der Auffassung ist, dass aufgrund der technischen oder wissenschaftlichen Komplexität die Fehlerhaftigkeit des Produkts oder der Kausalzusammenhang zwischen seiner Fehlerhaftigkeit und dem Schaden nur schwer nachzuweisen ist.[21]

f) Angepasste Verjährungsfristen

Gilt momentan noch eine 10-jährige Verjährung, so wird zukünftig für Personenschäden die Verjährungsfrist auf 15 Jahre verlängert, wenn eine geschädigte Person aufgrund der Latenzzeit eines Personenschadens nicht in der Lage war, innerhalb von 10 Jahren ein Verfahren einzuleiten.

6. Neue Verordnung über Maschinenprodukte

Mit der Veröffentlichung eines ersten Entwurfs zu einer Maschinenverordnung am 21.4.2021 – im Übrigen zeitgleich mit der Veröffentlichung eines Entwurfs zur KI-Verordnung – nimmt sich nun die EU auch einer Totalrevision der noch geltenden Maschinenrichtlinie (2006/42/EG) an, die seit 16 Jahren fast unverändert nun dem New Legislative Framework angepasst werden soll. Die Maschinensicherheit spielt in der Europäischen Union eine wesentliche Bedeutung. Europa ist Zentrum für Innovation und Technologie, was die Konstruktion und den Bau von Maschinen und Anlagen anbelangt. Über 1.000 europäische Normen legen anerkannte Regeln der Technik nur für den Maschinensektor fest.

So stellt die EU-Kommission zu Anfang des Entwurfs[22] sechs Problembereiche dar, warum neue Rechtsvorschriften zur Maschinensicherheit erlassen werden müssen:

Problem 1: In der Maschinenrichtlinie werden neue Risiken, die sich aus aufstrebenden Technologien ergeben, nicht ausreichend abgedeckt.

Gemeint sind zum einen mögliche Risiken, die von einer direkten Mensch-Roboter-Zusammenarbeit ausgehen, da die Zahl der kollaborativen Roboter (Cobots), die für die Zusammenarbeit mit menschlichen Mitarbeitern konzipiert sind, exponentiell zunehmen. Zum anderen gehen mögliche Risiken von Maschinen aus, die mit dem Internet verbunden sind. Ein dritter Problembereich betrifft die Art und Weise, wie Software-Updates das „Verhalten" der Maschine nach dem Inverkehrbringen beeinflussen. Ein viertes Anliegen betrifft die Fähigkeit der Hersteller, eine vollständige Risikobewertung für Anwendungen des maschinellen Lernens durchzuführen, bevor das Produkt in Verkehr gebracht wird. Was schließlich autonome Maschinen und Fernüberwachungsstationen betrifft, so ist in der aktuellen Maschinenrichtlinie ein Fahrer oder Bediener vorgesehen, der für das Verfahren einer Maschine verantwortlich ist. Der Fahrer kann entweder von der Maschine transportiert werden, die Maschine begleiten oder die Maschine per Fernsteuerung führen – die Möglichkeit, dass kein Fahrer vorhanden ist, wird jedoch nicht berücksichtigt, und es werden keine Anforderungen für autonome Maschinen festgelegt.

Problem 2: Rechtsunsicherheit aufgrund mangelnder Klarheit über den Anwendungsbereich und die Begriffsbestimmungen und mögliche Sicherheitslücken bei traditionellen Technologien.

Es wurden einige Überschneidungen oder Unstimmigkeiten mit anderen einschlägigen EU-Rechtsvorschriften festgestellt. In Bezug auf die in der Richtlinie festgelegten Begriffsbestimmungen gab die Definition von „unvollständigen Maschinen" Anlass zu einer Reihe von Bedenken, die sich insbesondere auf die Abgrenzung zur Definition von „Maschinen" beziehen, woraufhin die Definition von „Maschinen" präzisiert wurde.

Problem 3: Unzureichende Bestimmungen für Hochrisiko-Maschinen.

Die derzeitige Liste der Hochrisiko-Maschinen in Anhang I wurde vor 15 Jahren erstellt und seitdem hat sich der Markt stark entwickelt. Es ist notwendig, Maschinen zu streichen, die nicht mehr als risikoreich gelten, und/oder neue aufzunehmen (z. B. Maschinen, in die KI-Systeme integriert sind, die eine Sicherheitsfunktion erfüllen).

Problem 4: Monetäre und ökologische Kosten durch umfangreiche papierbasierte Dokumentation.

In der Maschinenrichtlinie wird von den Herstellern verlangt, dass sie die notwendigen Maschineninformationen, z. B. die Betriebsanleitung, bereitstellen. Um sicherzustellen, dass jeder Verwender der Maschine Zugang zur Betriebsanleitung hat, wurde die Bereitstellung einer gedruckten Version als die praktikabelste Option angesehen. Seitdem hat jedoch die Nutzung des Internets und der Digitaltechnik vor allem im B2B stark zugenommen. Die Anforderung, gedruckte Versionen zur Verfügung zu stellen, erhöht die Kosten und den Verwaltungsaufwand für die Wirtschaftsakteure und hat negative Auswirkungen auf die Umwelt.

Problem 5: Unstimmigkeiten mit anderen Rechtsvorschriften der Union über Produktsicherheit.

Obwohl die Maschinenrichtlinie bereits eine Richtlinie nach dem neuen Konzept darstellt, ist sie noch nicht an den NLF angeglichen. Die fehlende Angleichung der Richtlinie an den NLF führt zu Inkonsistenzen mit anderen EU-Produktvorschriften.

Problem 6: Divergenzen in der Auslegung aufgrund der Umsetzung in einzelstaatliches Recht.

Die Tatsache, dass es sich bei der aktuellen Maschinengesetzgebung um eine Richtlinie handelt, die es den Mitgliedstaaten überlässt, die Mittel zur Erfüllung der gesetzgeberischen Ziele zu wählen, hat zu unterschiedlichen Auslegungen der Bestimmungen der Maschinenrichtlinie geführt und damit zu Rechtsunsicherheit und mangelnder Kohärenz im gesamten Binnenmarkt. Darüber hinaus ist es in einigen Mitgliedstaaten zu Verzögerungen bei der Umsetzung der Richtlinie gekommen.

a) Ziel der Verordnung

Mit der Verordnung verfolgt die EU das Ziel, das ordnungspolitische Umfeld zu vereinfachen und die Notwendigkeit, eine EU-weit einheitliche Durchführung der vorgeschlagenen Rechtsvorschriften sicherzustellen.[23]

b) Ende der Vermutungswirkung

Mit Auslaufen der Gültigkeit der aktuellen Maschinenrichtlinie verlieren alle bisherigen nach der alten Richtlinie harmonisierten Normen ihre Vermutungswirkung. Sie erhalten nicht automatisch die Vermutungswirkung zur neuen Verordnung. Anhang III der neuen Maschinenverordnung (war bisher Anhang I der alten Maschinenrichtlinie) führt mehrere Veränderungen auf. Aus diesem Grund müssen sämtliche Normen auf diese Veränderungen überprüft und gegebenenfalls ange-

21 Zu den Beweisproblemen bei komplexen Sachverhalten, Herbert Zech, Empfehlen sich Regelungen zu Verantwortung und Haftung beim Einsatz Künstlicher Intelligenz? NJW-Beilage 2/2022, S. 33.

22 Die sechs Problemfelder wurde zum besseren Verständnis und Vollständigkeit wörtlich aus dem Verordnungsentwurf COM (2021) 202 final, S. 2–3 übernommen und durch den Verfasser gekürzt.

23 So COM (2021) 202 final, Begründung Ziff. 2.4.

passt werden. Von den momentan für Maschinen gelisteten 1112 geltenden Normen sollen über 350 Normen zurückgezogen und teilweise überabreitet werden.[24] Der Maschinenhersteller hat also zum Stichtag mit dem Inkrafttreten der neuen Maschinenverordnung dafür Sorge zu tragen, dass er Normen anwendet und angibt, die tatsächlich noch die Vermutungswirkung beinhalten. Ansonsten hat er die Sicherheitsziele der Verordnung auf andere Weise zu erfüllen.

c) Anforderungen an Künstliche Intelligenz

Von Maschinenprodukten, die eine WLAN-Funktion oder ein System künstlicher Intelligenz enthalten, können Risiken ausgehen, die von den in der neuen Maschinenverordnung festgelegten grundlegenden Sicherheits- und Gesundheitsschutzanforderungen nicht berücksichtigt werden, da sich diese Verordnung nicht mit den spezifischen Risiken solcher Systeme befasst. Für Systeme künstlicher Intelligenz sollten die spezifischen Rechtsvorschriften der Union über künstliche Intelligenz gelten[25], da sie besondere Sicherheitsanforderungen für Systeme künstlicher Intelligenz mit hohem Risiko enthalten.

Um Inkohärenz in Bezug auf die Art der Konformitätsbewertung sowie die Einführung von Anforderungen zur Durchführung von doppelten Konformitätsbewertungen zu vermeiden, sind diese spezifischen Sicherheitsanforderungen jedoch im Rahmen des in dieser Verordnung festgelegten Verfahrens der Konformitätsbewertung zu überprüfen. Die grundlegenden Sicherheits- und Gesundheitsschutzanforderungen dieser Verordnung sollten in jedem Fall vom Hersteller angewandt werden, um gegebenenfalls die sichere Integration des Systems künstlicher Intelligenz in die Gesamtheit der Maschine zu gewährleisten, damit die Sicherheit des Maschinenprodukts als Ganzes nicht beeinträchtigt wird.

d) Schutz vor Manipulation der sicherheitsrelevanten Steuerung

Industrielle Anlagen werden durch eine sogenannte „Operational Technology" (OT) im Hard- und Softwarebereich gesteuert und überwacht. Daher gelten im OT-Bereich unterschiedliche Anforderungen an die Security als im IT-Umfeld in der Büroebene. Deswegen soll im Anhang III E-MaschV ein neues Kapitel 1.1.9 mit dem Titel „Schutz vor Manipulation" konkrete Schutzmaßnahmen für Maschinen gegen Manipulation der sicherheitsbezogenen Steuerung vorsehen. Nach allem muss ein Remote- ebenso wie ein Vor-Ort-Zugriff auf die Sicherheitseinrichtung beherrschbar sein. Je nach Anwendung werden dies nur technische Lösungen sein. OT-Security (vgl. IEC 62443) erfordert eine umfassende Betrachtung, die je nach den spezifischen Anforderungen einen mehrstufigen Schutz bedingt.

Weitere Risiken im Zusammenhang mit der neuen Digitaltechnik sind solche, die durch böswillige Dritte hervorgerufen werden und sich auf die Sicherheit von Maschinenprodukten auswirken. Diesbezüglich sollten die Hersteller dazu verpflichtet sein, verhältnismäßige Maßnahmen zu ergreifen, die sich auf den Schutz der Sicherheit des Maschinenprodukts beschränken. Dies schließt nicht aus, dass andere Rechtsvorschriften der Union, die sich speziell mit Aspekten der Cybersicherheit[26] befassen, auf Maschinenprodukte angewendet werden.

e) Änderungen bei der Konformitätsbewertung

Die Hersteller sind auch nach der neuen Verordnung für die Bescheinigung der Konformität ihrer Maschinenprodukte mit dieser Verordnung grundsätzlich selber verantwortlich. Für einige Arten von Hochrisiko-Maschinenprodukten (früher Anhang IV der Maschinenrichtlinie, in Zukunft Anhang I der Verordnung) wird jedoch ein strengeres Zertifizierungsverfahren vorgeschrieben, das die Beteiligung einer notifizierten Stelle erfordert, alternativ kann sich der Hersteller sein Qualitätssicherungssystem (QS) von der benannten Stelle zertifizieren lassen, um die Maschine konform in den Verkehr zu bringen.

f) Software als Sicherheitsbauteil

Die Entwicklung im Maschinensektor hat dazu geführt, dass zunehmend digitale Mittel eingesetzt werden und Software eine immer wichtigere Rolle bei der Konstruktion von Maschinen spielt. Folglich wird die Definition von Maschinen angepasst werden. In dieser Hinsicht werden Maschinen, bei denen lediglich das Aufspielen einer für die spezifische Anwendung der Maschine bestimmten Software fehlt, unter die Begriffsbestimmung für Maschinen und nicht unter die Begriffsbestimmung für unvollständige Maschinen fallen. Darüber hinaus wird die Begriffsbestimmung für Sicherheitskomponenten nicht nur physische, sondern ferner auch digitale Komponenten umfassen. Um der zunehmenden Verwendung von Software als Sicherheitskomponente Rechnung zu tragen, wird Software, die eine Sicherheitsfunktion erfüllt und separat in Verkehr gebracht wird, als Sicherheitskomponente betrachtet.

II. Fazit

Die hier vorgestellten fünf Verordnungs- und Richtlinien-Entwürfe werden jeweils mit Übergangsfristen zwischen 24 und 48 Monaten spätestens 2023 durch die EU verabschiedet werden. Es ist das erste Mal, dass die Hersteller auf einmal mit einer solchen Vielzahl von neuen Rechtsnormen konfrontiert werden. Insbesondere sind die Softwareentwickler nun in der Haftung und auch die Sicherheit der gesamten IT-Struktur wird nun als „Chefsache" betrachtet. Hinzu kommt eine Liste von weiteren vor allem Nachmarkt- und Dokumentationspflichten, die durch die Hersteller, Importeure und Händler zu beachten sind, worunter die uneingeschränkte Meldepflicht (nun auch für B2B-Produkte) gegenüber den nationalen Marktaufsichtsbehörden für den Fall, dass „unsichere" Produkte auf den Markt gebracht wurden, die wohl härteste Verpflichtung darstellt. Die Inverkehrbringer von Produkten in der EU sind nun gefordert, denn „unvorbereitet sein, heißt hilflos sein".

AUTOR

Hans-Joachim Hess, *Hess & Partner Rechtsanwälte, Küsnacht/ZH, Schweiz. Er berät Unternehmen in allen Fragen des Produktesicherheits- und Haftpflichtrechts. Ferner berät er deutsche und schweizerische Unternehmen zum europäischen und internationalen Haftpflicht-, Vertrags- und Organisationsrecht.*

24 COMMISSION STAFF WORKING DOCUMENT IMPACT ASSESSMENT (SWD (2021) 82 final v. 21.4.2021) accompanying the Proposal for a Regulation of the European Parliament and of the Council on machinery products {COM (2021) 202 final}).

25 COM (2021) 206 final.

26 Vgl. dazu den Entwurf zur Cybersicherheitsverordnung COM (2022) 454 final vom 15.9.2022.