tifizierten Stelle erfolgt.[65] Dabei kann in Zukunft auch die Konformitätsvermutung nach Art. 8 des Entwurfs zum Cyber Resilience Act[66] Bedeutung erlangen, wonach unter bestimmten Voraussetzungen Hochrisiko-KI-Systeme als konform anzusehen sind, wenn sie die Anforderungen gemäß Art. 15 des Entwurfs zum Cyber Resilience Act erfüllen. Des Weiteren gibt Art. 16 Buchst. d des KI-VO-E vor, die von Hochrisiko-KI-Systemen automatisch erzeugten Protokolle aufzubewahren, soweit diese aufgrund einer vertraglichen Vereinbarung mit dem Nutzer oder aufgrund gesetzlicher Grundlage ihrer Kontrolle unterliegen.[67]

(2) Transparenz- und Bereitstellungspflichten

434 Der KI-VO-E sieht außerdem Transparenz- und Bereitstellungspflichten der Anbieter gegenüber den Nutzern vor. Dazu zählt die Pflicht, den Nutzern diejenigen Informationen bereitzustellen, die es ihnen ermöglichen, die Ergebnisse des KI-Systems angemessen zu interpretieren und zu verwenden.[68] Dafür ist den Nutzern eine Gebrauchsanweisung in einem geeigneten digitalen Format zur Verfügung zu stellen. Diese Gebrauchsanweisung ist in einer barrierefrei zugänglichen und verständlichen Form zu gestalten und muss präzise, vollständige, korrekte und eindeutige Informationen enthalten.[69]

435 Ferner treffen die Anbieter auch Aufzeichnungspflichten, wie beispielsweise die Pflicht zur automatischen Protokollierung von Prozessen und Ereignissen im Hochrisiko-KI-System.[70] Diese Protokollierung muss gewährleisten, dass während des gesamten Lebenszyklus des KI-Systems dessen Funktionieren in einem, angesichts der Zweckbestimmung des Systems angemessenen Maße, rückverfolgbar ist.[71] Bei in Anhang III Abs. 1 Buchst. a zum KI-VO-E genannten Hochrisiko-KI-Systemen, welche es ermöglichen natürliche Personen biometrisch zu identifizieren und zu kategorisieren, sind noch weitergehende Protokollierungsfunktionen vorgesehen.[72] Anbieter dieser KI-Systeme müssen jeden Zeitraum aufzeichnen, in dem das System verwendet wurde und erfassen, anhand welcher Eingabedaten eine Abfrage zu einer Übereinstimmung geführt hat und welche natürlichen Personen an der Überprüfung des Ergebnisses beteiligt waren.[73]

(3) Korrekturmaßnahmen

436 Die Anbieter sind außerdem dazu verpflichtet, Korrekturmaßnahmen vorzunehmen, sofern das Hochrisiko-KI-System nicht den vorgegebenen Sicherheitsanforderungen entspricht und ein Risiko iSd Art. 65 des KI-VO-E birgt.[74] Ein solches Risiko liegt vor, wenn das KI-System die Gesundheit und Sicherheit oder den Schutz von Grundrechten stärker beeinträchtigen kann, als es im Verhältnis

[65] Vgl. Art. 19 Abs. 1 des KI-VO-E, KOM(2021) 206 endg.; BT-Drs. 20/1289, 6.
[66] Hierzu → Rn. 462 f.
[67] Art. 16 Buchst. d iVm Art. 20 Abs. 1 des KI-VO-E, KOM(2021) 206 endg.
[68] Art. 13 Abs. 1 S. 1 des KI-VO-E, KOM(2021) 206 endg.
[69] Art. 13 Abs. 2 und 3 des KI-VO-E, KOM(2021) 206 endg.
[70] Art. 12 Abs. 1 des KI-VO-E, KOM(2021) 206 endg.
[71] Art. 12 Abs. 2 des KI-VO-E, KOM(2021) 206 endg.
[72] Art. 14 Abs. 4 des KI-VO-E, KOM(2021) 206 endg.
[73] Art. 12 Abs. 4 Buchst. a, c und d des KI-VO-E, KOM(2021) 206 endg.
[74] Art. 16 Buchst. g iVm Art. 21 S. 1 des KI-VO-E, KOM(2021) 206 endg.

zu seiner Zweckbestimmung als vernünftig und vertretbar gilt.[75] Neben dem Ergreifen von Korrekturmaßnahmen können Anbieter dabei gegebenenfalls auch zur Rücknahme oder zum Rückruf des Hochrisiko-KI-Systems verpflichtet sein. Über die Nichtkonformität sowie die getroffenen Korrekturmaßnahmen sind die zuständigen Aufsichtsbehörden zu informieren.[76]

(4) Melde- und Registrierungspflichten

437 Um die Transparenz gegenüber der Öffentlichkeit zu erhöhen und die zuständigen Behörden bei der Aufsicht und Ex-post-Überwachung zu stärken, sind die in Art. 16 Buchst. f iVm Art. 51 des KI-VO-E aufgeführten Registrierungspflichten einzuhalten.[77] Für diese Zwecke soll insbesondere eine Registrierung der KI-Systeme in einer öffentlich zugänglichen EU-Datenbank über Hochrisiko-Systeme erfolgen.[78] Zusätzlich zu den Angaben, die eine Identifizierung des jeweiligen KI-Systems ermöglichen sollen, müssen dabei ua auch Angaben zu dessen Zweckbestimmung und eine elektronische Gebrauchsanweisung bereitgestellt werden. Diese Informationen sind nach der Registrierung auf dem neusten Stand zu halten.[79]

(5) Einrichtung eines Qualitätsmanagementsystems

438 Eine weitere Pflicht der Anbieter von Hochrisiko-KI-Systemen besteht gemäß Art. 16 Buchst. b iVm Art. 17 des KI-VO-E darin, ein Qualitätsmanagementsystem einzurichten und aufrechtzuerhalten. Dieses soll sicherstellen, dass über den gesamten Lebenszyklus des KI-Systems die gesetzlichen Anforderungen nach dem KI-VO-E eingehalten werden können.[80] Um die Konformität des KI-Systems zu sichern, müssen die Anbieter bereits in der Konzeptions- und Entwicklungsphase Qualitätssicherungsmaßnahmen ergreifen, beispielsweise Kontrollen, Prüfungen, Untersuchungs-, Test- und Validierungsverfahren.[81] Das KI-System muss außerdem so konzipiert werden, dass für die Dauer der Verwendung eine menschliche und wirksame Aufsicht gewährleistet ist.[82]

439 Nach der Inbetriebnahme des KI-Systems treffen die Anbieter im Rahmen des Qualitätsmanagementsystems weitere Pflichten. So muss durch ein System zur Beobachtung des KI-Systems sichergestellt sein, dass etwaige Korrektur- und Präventivmaßnahmen rechtzeitig ergriffen werden können.[83] Nach Art. 9 des KI-VO-E ist neben diesem System zur Beobachtung auch ein Risikomanagement-

[75] Vgl. auch Roos/Weitz MMR 2021, 844.
[76] Art. 16 Buchst. h iVm Art. 22 des KI-VO-E, KOM(2021) 206 endg.
[77] Vgl. Begründung der EU-Kommission zum KI-VO-E, KOM(2021) 206 endg., S. 16, Nr. 5.2.3.
[78] S. Art. 16 Buchst. f, 51, 60 u. Anhang VIII zum KI-VO-E, KOM(2021) 206 endg.
[79] Anhang VIII zum KI-VO-E, KOM(2021) 206 endg.
[80] ErwG Ziff. 54 des KI-VO-E, KOM(2021) 206 endg.
[81] Vgl. Art. 17 Abs. 1 Buchst. d des KI-VO-E, KOM(2021) 206 endg.
[82] Art. 14 des KI-VO-E, KOM(2021) 206 endg.; ErwG Ziff. 48 des KI-VO-E, KOM(2021) 206 endg.
[83] Art. 9 Abs. 2 Buchst. c iVm Art. 17 Abs. 1 Buchst. h des KI-VO-E iVm Art. 61 desKI-VO-E, KOM(2021) 206 endg.; s. zudem zur Definition der „Beobachtung nach dem Inverkehrbringen" Art. 3 Nr. 25 des KI-VO-E, KOM(2021) 206 endg.; ErwG Ziff. 54 u. 78 des KI-VO-E, KOM(2021) 206 endg.

system einzurichten, das eine angemessene Risikobewertung und -minimierung oder -beseitigung gewährleistet.

Ferner schreibt Art. 15 Abs. 1 des KI-VO-E vor, dass ein Hochrisiko-KI-System **440** ein angemessenes Maß an Robustheit, Cybersicherheit und Genauigkeit einhalten muss. Insbesondere die Cybersicherheit ist wesentlich, damit KI-Systeme gegenüber Versuchen böswilliger Dritte widerstandsfähig sind.[84] Daher sollten Anbieter von Hochrisiko-KI-Systemen geeignete Maßnahmen treffen, um solche Angriffe zu verhindern und zu kontrollieren. Gegebenenfalls ist auch die zugrundeliegende KI-Infrastruktur zu berücksichtigen.[85]

cc) Pflichten für KI-Systeme unabhängig von einem erhöhten Risiko

Des Weiteren werden Anbietern, Nutzern und Verwendern bestimmter KI- **441** Systeme gemäß Art. 52 des KI-VO-E umfassende Transparenzpflichten auferlegt. Diese Pflichten sind nicht an der Einstufung der KI-Systeme in bestimmte Risikoklassen ausgerichtet, sondern gelten insbesondere für alle KI-Systeme, die hinsichtlich der Manipulation von privaten Nutzern besonders riskant sind. Ein solches Risiko kann sich beispielsweise daraus ergeben, dass das System zur Interaktion mit Menschen oder zur Erzeugung von Bild-, Audio- oder Video-Inhalten auf eine Weise verwendet wird, die es erschwert zu erkennen, dass kein authentischer Inhalt vorliegt, sondern ein KI-System verwendet wird.[86] Die Gefahr der Manipulation privater Nutzer ist insbesondere im Metaverse hoch, in dem die Nutzer anhand von Avataren miteinander agieren und nicht ohne weiteres erkennen können, ob diese von Menschen oder von KI-Systemen gesteuert werden. Sofern es sich nicht offensichtlich aus den Umständen und der konkreten Nutzung ergibt, werden Anbieter von KI-Systemen im virtuellen Raum daher idR verpflichtet sein, natürliche Personen darüber zu informieren, dass sie mit einem KI-System interagieren.[87]

Neben den Anbietern werden iRd Transparenzpflichten auch Verwender und **442** gewerbliche Nutzer von KI-Systemen adressiert. Die Verwender müssen natürliche Personen darüber informieren, wenn sie einem Emotionserkennungssystem oder einem System zur biometrischen Kategorisierung ausgesetzt sind.[88] Gewerbliche Nutzer sind verpflichtet offenzulegen, wenn ein KI-System sog. *Deepfake*-Inhalte künstlich erzeugt. Unter einem „*Deepfake*" versteht man, dass ein KI-System Bild-, Ton- oder Videoinhalte erzeugt oder manipuliert, die wirklichen Personen, Gegenständen, Orten oder anderen Einrichtungen oder Ereignissen merklich ähneln und einer Person fälschlicherweise als echt oder real erscheinen würden.[89]

d) Marktüberwachung und Durchführung

Für Situationen, in denen die soeben dargestellten Verpflichtungen von den **443** jeweiligen Normadressaten nicht eingehalten werden, sieht der KI-VO-E Durch-

[84] ErwG Ziff. 51 des KI-VO-E, KOM(2021) 206 endg.
[85] ErwG Ziff. 51 des KI-VO-E, KOM(2021) 206 endg.
[86] Vgl. Begründung der EU-Kommission zum KI-VO-E, S. 17, Nr. 5.2.4.
[87] Art. 52 Abs. 1 des KI-VO-E, KOM(2021) 206 endg.
[88] Art. 52 Abs. 2 des KI-VO-E, KOM(2021) 206 endg.; ErwG Ziff. 70 des KI-VO-E, KOM(2021) 206 endg.
[89] Art. 52 Abs. 3 des KI-VO-E, KOM(2021) 206 endg.

setzungsmechanismen vor, die sowohl die Wahrung der Grundrechte als auch der Sicherheitsanforderungen gewährleisten und wiederherstellen sollen.[90]

(1) Marktüberwachung

444 Für die Aufsicht und die Durchsetzung des KI-VO-E sind die Verwaltungsbehörden der Mitgliedstaaten zuständig.[91] Gemäß Art. 59 Abs. 1 S. 1 des KI-VO-E soll daher jeder Mitgliedstaat verpflichtet werden, entsprechende nationale Behörden einzurichten und die EU-Kommission über diese in Kenntnis zu setzen. Diese Behörden agieren dann sowohl als notifiziernde Behörde als auch als Marktüberwachungsbehörde. Von diesem Grundsatz kann abgewichen werden, wenn ein Mitgliedstaat darlegt, dass er aus organisatorischen und administrativen Gründen mehr als eine Behörde benennen möchte.[92] Es bleibt abzuwarten, welche nationale Behörde in Deutschland zuständig sein wird.

445 Die zuständige nationale Aufsichtsbehörde muss gemäß Art. 65 Abs. 2 UAbs. 2 des KI-VO-E tätig werden, wenn ein KI-System den Anforderungen des KI-VO-E nicht entspricht und daher ein Risiko für die Gesundheit, Sicherheit oder den Schutz von Grundrechten darstellt. Die Behörde muss den jeweiligen Akteur unverzüglich auffordern, alle Korrekturmaßnahmen zu ergreifen, die dazu geeignet sind, die Konformität wiederherzustellen, das KI-System vom Markt zu nehmen oder es innerhalb einer angemessenen Frist zurückzurufen.[93] Gemäß Art. 65 Abs. 4 des KI-VO-E ist der jeweilige Akteur dazu verpflichtet, alle geforderten Korrekturmaßnahmen umzusetzen. Kommt er dieser Verpflichtung nicht innerhalb der von der Behörde zu bestimmenden Frist nach, so hat die Aufsichtsbehörde selbst alle geeigneten Maßnahmen zu treffen, um die Bereitstellung des KI-Systems auf ihrem nationalen Markt zu verbieten oder einzuschränken, das Produkt vom Markt zu nehmen oder zurückzurufen.[94] Wenn sie in dieser Weise tätig wird, muss die Aufsichtsbehörde die EU-Kommission und die anderen Mitgliedstaaten, unter Beigabe einer entsprechenden Dokumentation des Falls, informieren.[95] Die Maßnahme der Aufsichtsbehörde gilt dann als gerechtfertigt, wenn innerhalb von drei Monaten nach Eingang der Unterrichtung weder ein anderer Mitgliedstaat noch die EU-Kommission Einwände gegen die vorläufige Maßnahme geltend macht.[96] Bei Vorliegen einer gerechtfertigten Maßnahme sind sodann alle Mitgliedstaaten verpflichtet, ebenfalls geeignete einschränkende Maßnahmen zu ergreifen.[97]

446 Die effektive Durchsetzung dieser Maßnahmen im Metaverse kann die Mitgliedstaaten allerdings vor einige Herausforderungen stellen. Zunächst stellt sich die Frage danach, wie im Metaverse, das geographische Grenzen überschreitet, die zuständige Behörde zu bestimmen ist. Denn ohne entsprechendes Geoblocking sind auch die Produkte im Metaverse global und im gesamten EU-Binnenmarkt

[90] Vgl. Begründung der EU-Kommission zum KI-VO-E, S. 103, Einzelziel Nr. 3.
[91] Vgl. ErwG Ziff. 88 des KI-VO-E, KOM(2021) 206 endg.
[92] Art. 59 Abs. 2 des KI-VO-E, KOM(2021) 206 endg.
[93] Art. 65 Abs. 2 UAbs. 2 des KI-VO-E, KOM(2021) 206 endg.
[94] Art. 65 Abs. 5 des KI-VO-E, KOM(2021) 206 endg.
[95] Art. 65 Abs. 5 S. 2 des KI-VO-E, KOM(2021) 206 endg.
[96] Art. 65 Abs. 8 S. 1 des KI-VO-E, KOM(2021) 206 endg.
[97] Art. 65 Abs. 9 des KI-VO-E, KOM(2021) 206 endg.

verfügbar, ohne dass sie je tatsächliche Ländergrenzen überschreiten. Zur Bestimmung der zuständigen Behörde könnte dabei zum einen auf das aus dem allgemeinen Produktsicherheitsrecht bekannte Prinzip zurückgegriffen werden, dass jeweils die Aufsichtsbehörde in deren Zuständigkeitsbereich ein Sicherheitsrisiko bei einem Produkt eintritt, zuständig ist. Daneben bietet auch der KI-VO-E selbst einen Ansatz, um die Zuständigkeit bereits in einem frühen Stadium zu klären: wenn eine Marktüberwachungsbehörde zu dem Schluss gelangt, dass die Nichtkonformität nicht auf ihr nationales Hoheitsgebiet beschränkt ist, unterrichtet sie die EU-Kommission und die anderen Mitgliedstaaten über die Ergebnisse der Prüfung, ob ein bestimmtes KI-System den Anforderungen des KI-VO-E genügt, und die Maßnahmen, zu denen sie den betroffenen Akteur aufgefordert hat.[98]

Neben der Bestimmung der Zuständigkeitsfrage dürfte auch die Vornahme **447**
eines Produktrückrufs im Metaverse die Behörden vor Schwierigkeiten stellen. Gegebenenfalls müssen die Befugnisse der Behörden erweitert und bestehende Vorschriften darauf überprüft werden, ob sie den Behörden auch im Metaverse ausreichende Handlungsbefugnisse verschaffen. Möglicherweise werden auch neue Instrumente geschaffen werden müssen, um die Vorschriften des KI-VO-E im Metaverse effizient umzusetzen.[99]

(2) Sanktionen

Die Mitgliedstaaten werden gemäß Art. 71 Abs. 1 des KI-VO-E verpflich- **448**
tet, Sanktionsvorschriften zu erlassen, die bei Verstößen gegen die Verordnung Anwendung finden. Diese Sanktionen müssen wirksam, verhältnismäßig und abschreckend sein. Dabei sind die vom KI-VO-E vorgeschriebenen Sanktionsobergrenzen zu berücksichtigen.[100]

Art. 71 Abs. 3 und 4 des KI-VO-E sehen allerdings erhebliche Geldbußen **449**
vor: bei der Missachtung des Verbots der in Art. 5 des KI-VO-E genannten KI-Praktiken sowie bei der Nichtkonformität des KI-Systems mit den in Art. 10 des KI-VO-E festgelegten Anforderungen bis zu 30 Mio. EUR oder 6% des weltweiten Jahresumsatzes im vorangegangenen Geschäftsjahr, bei Verstößen gegen andere Pflichten bis zu 20 Mio. EUR oder bis zu 4% des weltweiten Jahresumsatzes des vorangegangenen Geschäftsjahrs, wobei jeweils der höhere Betrag maßgeblich ist. Auch bei falschen, irreführenden oder unvollständigen Angaben gegenüber notifizierten Stellen und Marktüberwachungsbehörden können gemäß Art. 53 Abs. 5 des KI-VO-E Geldbußen von bis zu 10 Mio. EUR oder von bis zu 2% des weltweiten Jahresumsatzes des vorangegangenen Geschäftsjahrs verhängt werden, wobei ebenfalls der höhere Betrag maßgeblich ist. Bei der Festsetzung der Geldbußen werden in jedem Einzelfall alle relevanten Umstände und die Art, Dauer und Schwere des Verstoßes sowie dessen Folgen berücksichtigt. Einkalkuliert werden außerdem die Größe und der Markanteil des Akteurs und ob dieser für denselben Verstoß bereits mit Geldbußen sanktioniert wurde.[101]

---

[98] Art. 65 Abs. 3 des KI-VO-E, KOM(2021) 206 endg.
[99] Vgl. Europäisches Parlament, Briefing, Metaverse: Opportunities, risks and policy implications, PE 733.557 von Juni 2022, S. 7.
[100] Art. 71 Abs. 3, Abs. 4, Abs. 5 des KI-VO-E, KOM(2021) 206 endg.; ErwG Ziff. 84 des KI-VO-E, KOM(2021) 206 endg.
[101] Art. 71 Abs. 6 des KI-VO-E, KOM(2021) 206 endg.

450 Damit gibt der KI-VO-E einen empfindlichen Bußgeldrahmen vor, der mit Sanktionsvorschriften in den Bereichen Datenschutz und Kartellrecht vergleichbar ist. Im Metaverse wird insbesondere die Bestimmung der zuständigen Gerichtsbarkeit für die Geltendmachung solcher Geldbußen zu Herausforderungen führen. So könnte für diese Bestimmung beispielsweise der Standort des Anbieters des KI-Systems, der Standort des entsprechenden Servers oder der Standort des Avatars entscheidend herangezogen werden.[102]

e) Fazit

451 Es bleibt abzuwarten, welche Veränderungen und Anpassungen der KI-VO-E im weiteren Gesetzgebungsverfahren erfahren wird. Die Abstimmung im Europäischen Parlament ist für Ende März 2023 geplant und die Verkündung der endgültigen Fassung für Ende 2023. Aktuell drängt insbesondere Deutschland in den Verhandlungen (im Rat) darauf, weitere KI-Systeme und KI–Anwendungen als hochriskant einzustufen. Dies soll beispielsweise biometrische Kategorisierungssysteme, emissionsintensive Industrien, Abwasserentsorgung und Sicherheitskomponenten für kritische digitale Infrastrukturen betreffen.[103] Außerdem könnte die Definition des KI-Systems im Gesetzgebungsverfahren aufgrund der Kritik an ihrer Unbestimmtheit und dem daraus folgenden (zu) weiten Anwendungsbereich noch angepasst werden.[104]

452 Unternehmen könnte die Implementierung eines Product Compliance Systems für KI in den nächsten Jahren insbesondere dadurch vor Herausforderungen stellen, dass sich die Produkteigenschaften einer KI zum Zeitpunkt des Bereitstellens auf dem Markt oft noch nicht abschließend beurteilen lassen. Da es sich um selbstlernende Systeme handelt, wird es erforderlich sein, bei der Produktkategorisierung auch künftige Entwicklungen in den Blick zu nehmen und mögliche spätere Anwendungsfälle möglichst zu antizipieren.[105] Product Compliance im Bereich der KI wird außerdem dadurch erschwert, dass in diesem Bereich noch kaum technische Normungen und Standardisierungen bestehen.[106]

3. Cyber-Resilience-Act-Entwurf

453 Ein weiterer Rechtsakt, den Akteure im Metaverse im Blick behalten sollten, ist der Vorschlag der EU-Kommission für eine Verordnung des Europäischen Parlaments und des Rates über horizontale Cybersicherheitsanforderungen für Produkte mit digitalen Elementen und zur Änderung der Verordnung (EU) 2019/1020 (Entwurf des „Cyber Resilience Act" (nachfolgend „**CRA-E**")).[107] Dieser wurde von der EU-Kommission am 15.9.2022 als Teil ihrer Cybersecurity-Strategie vor-

[102] Vgl. Europäisches Parlament, Briefing, Metaverse: Opportunities, risks and policy implications, PE 733.557 von Juni 2022, S. 5.
[103] Vgl. Luca Bertuzzi Deutschland geht KI-Gesetz nicht weit genug, abrufbar unter: https://www.euractiv.de/section/digitale-agenda/news/deutschland-hegt-weiterhin-vorbehalte-gegen-ki-gesetz-der-eu/, zuletzt abgerufen am 7.2.2023.
[104] Reusch Future Law IV. Produktsicherheitsrechtlicher Rahmen 2. Aufl. 2022, Rn. 225; Roos/Weitz MMR 2021, 844 (845, 850 f.).
[105] Chibanguza/Kuß/Steege Künstliche Intelligenz/Heuer-James § 5 Kap. L Rn. 59.
[106] Chibanguza/Kuß/Steege Künstliche Intelligenz/Heuer-James § 5 Kap. L Rn. 81.
[107] KOM(2022) 454 endg.

gestellt.[108] Als horizontale Regulierung soll er unabhängig von den Funktionen und dem Nutzerkreis auf jegliche Produkte mit digitalen Elementen Anwendung finden.[109] Dieser Regulierungsansatz erklärt sich vor dem Hintergrund der Zielsetzung des CRA-E: Etwaige regulatorische **Lücken in der produktbezogenen Cybersicherheitsarchitektur** der EU, die ua dadurch entstehen, dass es für die Cybersicherheit der meisten Hardware- und Softwareprodukte derzeit keine europäischen Vorschriften gibt, sollen geschlossen werden.[110] Diese Zielsetzung wird im CRA-E in vier spezifische regulatorische Ziele unterteilt[111]: Der CRA-E soll einen kohärenten Cybersicherheitsrahmen zur Verfügung stellen, damit

1. Hersteller die Cybersicherheit von Produkten mit digitalen Elementen von der Entwurfs- und Entwicklungsphase an und während des gesamten Lebenszyklus gewährleisten;
2. Hardware- und Software-Herstellern die Einhaltung der Vorschriften durch die Gewährleistung eines kohärenten Cybersicherheitsrahmens erleichtert wird;
3. die Transparenz in Bezug auf die Sicherheitseigenschaften von Produkten mit digitalen Elementen verbessert werden; und
4. Unternehmen und Verbraucher zur sicheren Nutzung von Produkten mit digitalen Element befähigt werden.

a) Sachlicher Anwendungsbereich

Um diese Ziele zu erreichen, ist der sachliche Anwendungsbereich des CRA-E **454**
sehr weit gestaltet.[112] Erfasst werden jegliche **Produkte mit digitalen Elementen**, deren bestimmungsgemäße oder vernünftigerweise vorhersehbare Verwendung eine direkte oder indirekte logische oder physische Datenverbindung mit einem Gerät oder Netz einschließt. Ein Produkt mit digitalen Elementen wird dabei definiert als ein Software- oder Hardwareprodukt und dessen Datenfernverarbeitungslösungen, einschließlich Software- oder Hardwarekomponenten, die getrennt in Verkehr gebracht werden sollen.[113] Vom Anwendungsbereich erfasst sind daher auch KI-Systeme, die unter den oben dargestellten KI-VO-E fallen.[114] Dies wird auch ausdrücklich in einem Briefing des Europäischen Parlaments zum CRA-E hervorgehoben.[115]

Von diesem sehr weiten Anwendungsbereich werden wiederum bestimmte **455**
Produkte mit digitalen Elementen ausgenommen, die bereits von anderen Rechtsakten der Union erfasst werden (beispielsweise Medizinprodukte, Kraftfahrzeuge, Luftfahrt).[116] Nicht erfasst sind außerdem Produkte mit digitalen Elementen, die ausschließlich für Zwecke der nationalen Sicherheit, für militärische Zwecke oder

[108] Teil dieser sind auch der KI-VO-E sowie die geplante Überarbeitung der EU-Produkthaftungsrichtlinie.
[109] ErwG Ziff. 14 des CRA-E, KOM(2022) 454 endg.; Schweinoch/Meßmer CR 2022, R112–R113.
[110] Vgl. Begründung der EU-Kommission zum CRA-E, S. 1; Kipker MMR-Aktuell 2022, 452009.
[111] Vgl. Begründung der EU-Kommission zum CRA-E, S. 1 f.; Kipker MMR-Aktuell 2022, 452009.
[112] Art. 2 Abs. 1 des CRA-E, KOM(2022) 454 endg.
[113] Art. 3 Nr. 1 des CRA-E, KOM(2022) 454 endg.
[114] Art. 8 des CRA-E, KOM(2022) 454 endg.
[115] Vgl. Europäisches Parlament, Briefing, „EU cyber-resilience act", S. 6.
[116] Art. 2 Abs. 2 des CRA-E, KOM(2022) 454 endg.

speziell für die Verarbeitung von Verschlusssachen entwickelt wurden.[117] Zusätzlich hat die EU-Kommission die Befugnis, delegierte Rechtsakte zu erlassen, um die Anwendung der Verordnung auf Produkte mit digitalen Elementen einzuschränken oder auszuschließen, wenn diese unter andere Rechtsvorschriften der Union fallen und dadurch die Anforderungen des Anhang I des CRA-E bereits abgedeckt werden.[118]

456 Der CRA-E könnte auch für Unternehmen relevant werden, die Produkte mit digitalen Elementen im Anwendungsumfeld des Metaverse in den Verkehr bringen. Zwar regelt der CRA-E, ebenso wie der KI-VO-E, nicht ausdrücklich, dass der Verordnungsentwurf auch für Aktivitäten im Metaverse Geltung entfalten soll. Es spricht aber auch nichts gegen die Anwendbarkeit. Vielmehr wurde der CRA-E ausdrücklich in einem Briefing des Europäischen Parlaments zu den Chancen und Risiken des Metaverse genannt.[119] Als Anwendungsfall ist beispielsweise an VR-Brillen zu denken, die Nutzern den Zugang zu virtuellen Räumen ermöglichen. Oder auch Ganzkörperanzüge, wie die Teslasuits, die durch Muskel- und Nervenstimulation das haptische Erleben im Metaverse verbessern sollen. Dadurch, dass auch KI-Systeme in den Anwendungsbereich des CRA-E fallen,[120] könnte der CRA-E auch für KI-Systeme im Metaverse Bedeutung erlangen, die dort beispielsweise zur Entwicklung neuer Softwaresysteme eingesetzt werden oder zur Bildanalyse, zur Optimierung von Produktentwicklungen oder zur Herstellung, Vermarktung und Verwendung virtueller Produkte.[121]

b) Allgemeine Marktzugangsregelungen

457 Für Produkte mit digitalen Elementen, die gemäß Art. 2 des CRA-E vom Anwendungsbereich erfasst sind, stellt der Entwurf produktrechtliche Anforderungen für den Marktzugang auf. Die Produktanforderungen betreffen sowohl die Gestaltung, Entwicklung und Produktion, als auch die Prozesse für den Umgang mit Schwachstellen während des gesamten Produktlebenszyklus.[122] So darf ein Produkt mit digitalen Elementen nur auf dem Markt bereitgestellt werden, wenn es den Anforderungen in Anhang I Abschnitt 1 zum CRA-E genügt und unter der Bedingung, dass es ordnungsgemäß installiert, gewartet und bestimmungsgemäß oder unter vernünftigerweise vorhersehbaren Umständen verwendet sowie gegebenenfalls aktualisiert wird.[123] Anhang I Abschnitt I zum CRA-E legt beispielsweise fest, dass Produkte mit digitalen Elementen so konzipiert werden müssen, dass sie ein angemessenes Cybersicherheitsniveau gewährleisten.[124] Zusätzlich müssen auch die vom Hersteller festgelegten Verfahren den Anforderungen in Anhang I Abschnitt 2 zum CRA-E entsprechen.[125] Das umfasst beispielsweise

[117] Art. 2 Abs. 5 des CRA-E, KOM(2022) 454 endg.
[118] Art. 2 Abs. 4, Art. 50 des CRA-E.
[119] Vgl. European Parliament Briefing Metaverse Opportunitites, risks and policy implications, S. 9.
[120] Art. 8 des CRA-E, KOM(2022) 454 endg.; Europäisches Parlament, Briefing EU cyber-resilience act, S. 6.
[121] → Rn. 454 ff.
[122] Schweinoch/Meßmer CR 2022, R112–R113.
[123] Art. 5 des CRA-E, KOM(2022) 454 endg.
[124] Anhang I Abschnitt 1 Ziff. 1 zum CRA-E, KOM(2022) 454 endg.
[125] Art. 5 des CRA-E, KOM(2022) 454 endg.