DeutscherAnwaltVerein

Stellungnahme

des Deutschen Anwaltvereins durch den Ausschuss Informationsrecht

zum Vorschlag 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

Stellungnahme Nr.: 73/2022 Berlin, im Dezember 2022

Mitglieder des Ausschusses

Rechtsanwalt Dr. Helmut Redeker, Bonn (Vorsitzender)
Rechtsanwalt Dr. Simon Assion, Frankfurt am Main
Rechtsanwältin Dr. Christiane Bierekoven, Düsseldorf
Rechtsanwältin Isabell Conrad, München
Rechtsanwalt Dr. Malte Grützmacher, LL.M., Hamburg
Rechtsanwalt Prof. Niko Härting, Berlin
Rechtsanwalt Peter Huppertz, LL.M, Düsseldorf
Rechtsanwältin Birgit Roth-Neuschild, Karlsruhe
Rechtsanwalt Dr. Robert Selk, LL.M. (EU), München (Berichterstatter)

Zuständig in der DAV-Geschäftsstelle

- Rechtsanwältin Nicole Narewski, Berlin

Ansprechpartnerin in Brüssel:

- Hannah Adzakpa, LL.M.

Deutscher Anwaltverein
Littenstraße 11, 10179 Berlin
Tel.: +49 30 726152-0
Fax: +49 30 726152-190
E-Mail: dav@anwaltverein.de

Büro Brüssel
Rue Joseph II 40, Boîte 7B
1000 Brüssel, Belgien
Tel.: +32 2 28028-12
Fax: +32 2 28028-13
E-Mail: bruessel@eu.anwaltverein.de
EU-Transparenz-Registernummer:
87980341522-66

www.anwaltverein.de

Verteiler

Europa

Europäische Kommission
- Generaldirektion für Kommunikationsnetze, Inhalte und Technologie

Europäisches Parlament
- Ausschuss für Industrie, Forschung und Energie (ITRE)

Rat der Europäischen Union
Ständige Vertretung der Bundesrepublik Deutschland bei der EU
Justizreferenten der Landesvertretungen
Rat der Europäischen Anwaltschaften (CCBE)
Bundesverband der Freien Berufe
European Digital Rights (EDRi)

Deutschland

Bundesministerium des Innern und für Heimat
Bundesministerium der Justiz
Bundesministerium für Wirtschaft und Klimaschutz

Ausschuss für Recht im Deutschen Bundestag
Ausschuss für Wirtschaft im Deutschen Bundestag
Ausschuss Digitales im Deutschen Bundestag

Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit
Die Datenschutzbeauftragten der Bundesländer

Europäische Kommission - Vertretung in Deutschland
Bundesrechtsanwaltskammer
Bundesnotarkammer
Bundesverband der Freien Berufe
Deutscher Richterbund
Deutscher Notarverein e.V.
Deutscher Steuerberaterverband
Bundesverband der Deutschen Industrie (BDI)
Arbeitsgemeinschaft berufsständischer Versorgungseinrichtungen e. V. – ABV
GRUR
BITKOM
DGRI

DAV-Vorstand und Geschäftsführung
Vorsitzende der DAV-Gesetzgebungsausschüsse
Vorsitzende der DAV-Landesverbände
Vorsitzende des FORUMs Junge Anwaltschaft

Presse

Frankfurter Allgemeine Zeitung

Süddeutsche Zeitung GmbH
Redaktion NJW
Juve-Verlag
Redaktion Legal Tribune Online / LTO
Redaktion Anwaltsblatt
Juris
Redaktion MultiMedia und Recht (MMR)
Redaktion Zeitschrift für Datenschutz ZD
Redaktion heise online

Der Deutsche Anwaltverein (DAV) ist der freiwillige Zusammenschluss der deutschen Rechtsanwältinnen und Rechtsanwälte. Der DAV versammelt mehr als 61.000 Rechtsanwältinnen und Rechtsanwälte sowie Anwaltsnotarinnen und Anwaltsnotare, die in 253 lokalen Anwaltvereinen im In- und Ausland organisiert sind. Er vertritt die Interessen der deutschen Anwaltschaft auf nationaler, europäischer und internationaler Ebene. Der DAV ist im Lobbyregister für die Interessenvertretung gegenüber dem Deutschen Bundestag und der Bundesregierung zur Registernummer R000952 eingetragen.

Kurzzusammenfassung

Die Stellungnahme nimmt die vorgesehene parallele Geltung des CRA neben der Datenschutzgrundverordnung (DSGVO) in den Blick, prüft, ob es im Überschneidungsbereich zu Kollisionen kommt und konzentriert sich auf ausgewählte Punkte, die in diesem Zusammenhang zu berücksichtigen sind.

Der DAV kommt dabei zu dem Ergebnis, dass die hier von der Kommission vorgeschlagene Parallelität ein sinnvoller Weg ist, um auf mehreren Ebenen für einen Schutz zu sorgen, wenngleich aus unterschiedlichen Richtungen. Er regt an

- auch sog. Stand-alone-Produkten in den Anwendungsbereich des CRA mit aufzunehmen,
- die aus der DSGVO greifenden Prinzipien „data protection by design“ und „data protetion by default“ im Katalog der grundlegenden Sicherheitsanforderungen aufzugreifen,
- die zeitliche Begrenzung der Herstellerpflichten auf längstens 5 Jahre zu überdenken,
- bei den strengen Meldepflichten mit einer Fristdauer von nur 24 Stunden nachzubessern, so dass auch kleine Unternehmen nicht gegen Arbeitszeitgesetze verstoßen müssen
- die vorgesehenen Einsichtsrechte der Datenschutzbehörden mit einer entsprechenden Informationspflicht der Controller zu flankieren,
- den Anwender trennschärfer vom Hersteller abzugrenzen,

- auch ASP, SaaS- und Cloud-Anwendungen grundsätzlich unter dem CRA aufzunehmen und
- zu prüfen, inwiefern, Aspekte der Gefährlichkeit berücksichtigt und insb. hobbymäßige Programmierer vom Anwendungsbereich ausgenommen werden können.

Short Summary

The position paper considers the proposed parallel application of the Cyber Resilience Act alongside the General Data Protection Regulation (GDPR) and examines whether there are contradictions in the areas of overlap between the two. Hence, the focus lies on only certain points.

In doing so, the DAV concludes that the parallelism proposed here by the Commission is a sensible way to ensure protection at several levels, albeit from different directions. Hence, the DAV suggests

- to include so-called stand-alone products in the scope of application of the Cyber Resilience Act
- to take up the principles of ‘data protection by design’ and ‘data protection by default’ in the catalogue of basic security requirements
- to reconsider the time limit of the manufacturer's obligations to a maximum of 5 years
- to increase the time limit of only 24 hours in the context of the strict notification obligations, so that small companies do not have to violate working time laws
- to flank the data protection authorities' envisaged rights of inspection with a corresponding controllers’ duty to inform
- to distinguish more clearly between the user and the producer
- to include ASP, SaaS and cloud applications in the scope of application of the Cyber Resilience Act
- to examine to what extent aspects of dangerousness can be considered and, in particular, whether hobbyist programmers can be excluded from the scope of application.

1. Überblick und Einleitung

Die EU-Kommission veröffentlichte am 15.09.2022 ihren Entwurf einer neuen EU-Verordnung „über horizontale Cybersicherheitsanforderungen für Produkte mit digitalen Elementen“, im Deutschen auch „EU-Cybersicherheitsverordnung“ oder im Englischen „Cyber Resilience Act“ genannt, nachstehend kurz „CRA“.

Der Entwurf definiert verbindliche Anforderungen an die Cybersicherheit für Produkte mit digitalen Elementen“ für deren Lebenszyklus. Wichtig für das Verständnis ist, dass die Normadressaten nur die Hersteller solcher Produkte, die Importeure sowie Händler sind, nicht dagegen die Anwender solcher Produkte.

Produkte mit digitalen Elementen sind solche, deren bestimmungsgemäße oder vernünftigerweise vorhersehbare Verwendung eine direkte oder indirekte logische oder physische Datenverbindung mit einem Gerät oder Netz einschließt. Umfasst davon sind Software wie Hardware.

Der Entwurf enthält für die Hersteller, Importeure und Händler umfassende Pflichten, v.a. Dokumentations- und Meldepflichten, sowohl die Herstellung der Produkte betreffend, wie deren Inverkehrbringen und deren Bereitstellung auf dem Markt. Wie erwähnt, die Anwendung solcher Produkte ist nicht geregelt – dafür gelten andere Gesetze, wie etwa für eine etwaige damit verbundene Verarbeitung personenbezogener Daten die DSGVO.
Ein Produkt mit digitalen Elementen muss definierten grundlegenden Cybersicherheitsanforderungen genügen, die in Anhang 1 des Entwurfs festgelegt sind. Ferner besteht die Anforderung zur Ausstellung einer EU-Konformitätserklärung und die Anbringung der CE-Kennzeichnung. Es gibt zudem die Pflicht, begleitend zum Produkt den Nutzern umfangreiche Informationen zur Sicherheit bereitstellen zu müssen, ebenso bei Kenntnis über ausgenutzte Sicherheitsschwachstellen oder Vorfällen die sog. Marktüberwachungsbehörde zu informieren, ebenso wie in solchen Fällen auch die Nutzer zu unterrichten.

Der Marktüberwachungsbehörde stehen umfangreiche Rechte zu, etwa auf Einsicht in Unterlagen und Dokumentationen, sie kann aber in bestimmten Fällen ein Produkt vom Markt nehmen.

Der CRA weist in seinem Aufbau eine Reihe von Parallelen zur DSGVO und den dortigen Regelungsmechanismen auf. Es kann auch inhaltlich Überschneidungen zwischen den beiden Rechtsakten geben, da der CRA keinen Unterschied macht, ob es um Produkte mit digitalen Elementen geht, die personenbezogene Daten oder andere, nicht-personenbezogene Daten verarbeiten.

Dies führt zur Anwendbarkeit beider Rechtsakte. Nachstehend werden ausgewählte Punkte zu dieser Schnittmenge herausgegriffen und dazu Stellung genommen, ebenso ergänzend zu einigen weiteren im Gesetzgebungsverfahren noch zu diskutierenden Themen.

2. Parallelität von CRA und DSGVO

Zunächst stellt sich die Frage, ob es zwischen CRA und DSGVO ein Rangverhältnis in dem Sinne gibt, dass einer der beiden Rechtsakte vorrangig vor dem anderen Akt sein soll.

Zumindest die Rechtsnatur lässt eine solche Abstufung nicht vor, da – wie die DSGVO – auch der CRA als EU-Verordnung geplant ist.

Dies ist in Anbetracht der grenzüberschreitenden Thematik von Produkten mit digitalen Elementen und vor allem dem Umstand, dass ein Sicherheitsvorfall keine Ländergrenzen kennt, nachvollziehbar und sinnvoll. Zudem ist nur eine EU-Verordnung vollharmonisierend und vermeidet durch ansonsten bei einer bloßen Richtlinie nötige Umsetzungsdifferenzen in den Mitgliedsstaaten ein nationales Auseinanderfallen und ein Ungleichgewicht: Gerade zum freien Waren- und Datenverkehr sowie für einen fairen Wettbewerb ist es wichtig und nötig, in allen EU Mitgliedsstaaten identische Regelungen für Cybersicherheit und Sicherheitsvorfälle zu haben. Nur so ist auch eine effiziente Risikoreduzierung möglich.

Eine explizite Norm zum Verhältnis des CRA zur DSGVO findet sich im Entwurf nicht. Aus zwei Umständen ergibt sich allerdings, dass seitens der Kommission bewusst eine Parallelität und ein gleichberechtigtes Nebeneinander gewollt ist: Zum einen handelt es sich beim CRA gemäß seiner offiziellen Bezeichnung (siehe den Titel „Verordnung

…über *horizontale* Cybersicherheitsanforderungen (….)“) um eine „horizontale“ Regelung, also eine solche, die parallel zu anderen EU-Harmonisierungsvorschriften anzuwenden ist.

Als Ausnahme davon ist im CRA für bestimmte Produktrechtsvorschriften (siehe Art. 7, 8 und 9 CRA) geregelt, dass diese vorrangig sind – die DSGVO ist dort aber nicht erwähnt.

Vielmehr findet sich in Erwägungsgrund 17 die Aussage, dass der CRA „unbeschadet“ der DSGVO gelten soll – also beide Rechtsakte parallel.

Damit stellt sich die Frage, ob – dies ist nur relevant, wenn es um personenbezogene Daten geht – es im Überschneidungsbereich zu Kollisionen kommt oder sich beide Rechtsakte ergänzen.

Betrachtet man den CRA, ist erkennbar, dass dieser andere Ziele als die DSGVO verfolgt, nämlich die Schaffung einer hohen „Cybersicherheit“ für Produkte. Im CRA geht es also primär um Produktsicherheit, im Fokus ist das „Produkt“, sofern es digitale Elemente hat. Das Produkt soll sicher hergestellt sein und während seines Lebenszyklus bleiben, ganz unabhängig, ob es um personenbezogene Daten geht oder nicht. Im Blick ist u.a. die Auswirkung eines Cybersicherheitsvorfalls, etwa auf andere Produkte bzw. eine Kette von angebundenen Produkten, auf Märkte, etc. Natürlich soll durch eine hohe Cybersicherheit auch vermieden werden, dass natürliche Personen als „Betroffene“ im Sinne der DSGVO Nachteile erleiden – aber nur als einer von mehreren Aspekten.

Insofern verwendet die Kommission in ihrem Entwurf des CRA auch nicht den im Datenschutzrecht üblichen Begriff der „Datensicherheit“, wie er sich in der DSGVO findet, sondern den Begriff der „Cybersicherheit“, der offenbar deutlich weiter zu verstehen ist.

Dies lässt sich auch aus der primärrechtlichen Kompetenznorm ableiten, nämlich der Norm des Art. 114 AEUV, die die Annahme von Maßnahmen für die Errichtung und das Funktionieren des Binnenmarkts vorsieht.

Zweck des Entwurfs ist – so explizit die Begründung zum CRA unter Ziffer 2 - die Harmonisierung der Cybersicherheitsanforderungen für Produkte mit digitalen Elementen in allen Mitgliedstaaten und die Beseitigung von Hindernissen für den freien Warenverkehr.

Es geht also im CRA primär um „Produktrecht“. Dementsprechend richtet es sich an die Hersteller von Produkten, aber auch – um Lücken zu vermeiden – an die Importeure solcher Produkte sowie die Händler. Der CRA richtet sich aber nicht an die Anwender von Produkten mit digitalen Elementen.

Den Schutz der Betroffenen durch ein solches Produkt durch einen datenschutzrechtlich Verantwortlichen hat dagegen die DSGVO zum Ziele. Deren Regelungskompetenz basiert auf Art. 16 AEUV – dabei geht es um den Schutz der Menschen vor einer übermäßigen Verdatung.

So ist aus rechtsdogmatischen Gründen die hier von der Kommission vorgeschlagene Parallelität in Form eines horizontalen Rechtsaktes nachvollziehbar und ein sinnvoller Weg, auf mehreren Ebenen für einen Schutz zu sorgen, wenngleich aus unterschiedlichen Richtungen.

Dass sich beide Rechtsakte ergänzen, betont die Kommission an mehreren Stellen, zum Teil auch in der Form, dass der CRA den Zielen der DSGVO helfen kann, in dem der CRA zur Herstellung und Inverkehrbringung nur von „sicheren“ Produkten verpflichtet – die damit auch verhindern, dass es zu einer Verletzung des Schutzes personenbezogener Daten überhaupt erst kommen kann.

Die Parallelität ergibt sich auch aus den Normadressaten: Der CRA richtet sich an die Hersteller, Importeure und Händler von Produkten mit digitalen Inhalten, die typischerweise diese Produkte „nur“ herstellen und vertreiben. Sie verarbeiten damit also keine personenbezogenen Daten, sondern verkaufen nur das „Werkzeug“ dazu an die Anwender und Nutzer, die das Produkt dann konkret einsetzen und darüber möglicherweise personenbezogene Daten verarbeiten – also dann datenschutzrechtlich Verantwortlicher bzw. Controller sind.

So gesehen liegt auch ein zeitliches Nacheinander vor: Der CRA regelt die zeitlich zu Beginn stehende Herstellung eines Produkts und dessen sich anschließender Vertrieb, nicht aber den späteren Einsatz des Produkts. Für den Einsatz dagegen – sofern personenbezogene Daten betroffen sind – gilt dann die DSGVO.

Genau genommen liegt damit kein „Nebeneinander“, sondern ein „Nacheinander“ vor. Beide Rechtsakte – die DSGVO und der Entwurf des CRA – ergänzen sich damit und sind tatsächlich „nebeneinander/nacheinander“ und sich ergänzend zu sehen.

3. Einzelanmerkungen

Damit stellt sich umso mehr die Frage, ob es der Parallelität wegen innerhalb des überschneidenden Anwendungsbereiches zu inhaltlichen Kollisionen kommen kann. Nachstehend werden einige relevante Bereiche dargestellt:

a. Stand-Alone-Systeme

Reine Stand-alone-Systeme scheinen vom CRA nicht umfasst, da er nur für solche Produkte gilt, die eine „Datenverbindung“ mit einem Gerät oder Netz aufweisen. In Erwägungsgrund 7 stellt die Kommission auf „verbindungsfähige Produkte mit digitalen Elementen“ ab.

Dies ist eine bemerkenswerte Einschränkung und zeigt den Unterschied zur DSGVO: Liegt etwa eine Software vor, mit der umfangreich personenbezogene Daten verarbeitet werden, ggfls. sogar Daten besonderer Kategorien wie Gesundheitsdaten oder Gendaten und fehlt es etwa komplett an einem Rollen- und Berechtigungskonzept, handelt es sich aber um eine Stand-Alone-Software, greift der CRA nicht.
Dies mag dem Gedanken geschuldet sein, dass mangels Vernetzung ein Cybersicherheitsvorfall sich nicht weiter (digital) ausbreiten kann, übersieht aber den Umstand, dass darin dennoch ein massiver Mangel am Software-Design und grundlegenden Anforderungen an die (Cyber-)Sicherheit liegen kann und liegen wird. Dies gilt umso mehr, als dass in Anhang 1 des CRA, Ziffer 1.3 (c) explizit „geeignete Kontrollmechanismen“ zum „Schutz vor unbefugten Zugriff“ verlangt werden.

Nach der DSGVO läge in dem Fehlen jeglichen Rollen- und Berechtigungskonzept ein Verstoß gegen Art. 32 DSGVO, v.a. in Verbindung mit dem „Stand der Technik“ vor, der über Art. 83 DSGVO auch bußgeldgewehrt wäre.

Die DSGVO möchte insofern die Personen schützen, um deren Daten es geht – und dabei spielt es keine Rolle, ob es sich um ein „vernetztes“ Produkt handelt oder nicht. Aus Produktsicherheitssicht dagegen handelt es sich um ein isoliertes Problem und wird daher seitens der Kommission offenbar als gering(er) eingestuft.

Wir halten daher die Beschränkung auf Produkte mit Datenverbindungen zu anderen Geräten oder einem Netz und damit das Ausnehmen von Stand-alone-Produkten aus dem Anwendungsbereich des CRA nicht für richtig und zu eng:
Ein Cybersicherheitsvorfall kann auch in nicht-vernetzten Geräten und Produkten auftreten und massive Folgen haben, ebenso wie dort Schwachstellen ausgenutzt werden können.
Zudem ist die Grenze zwischen “verbindungsfähig“ oder nicht oft fließend, zum Teil auch einfach durch Software-Einstellungen oder Hinzufügen von Hardware änderbar.
Wo liegen die Grenzen? Wofür gilt der CRA noch oder nicht?
Wo wird hier an „bestimmungsgemäß oder vernünftigerweise vorhersehbare Verwendung“ angeknüpft.
Sollte dagegen die diesbezügliche Formulierung in Art. 2 Abs. 1 CRA-Entwurf so gemeint sein, dass ausreicht, dass eine *Software* nur eine Verbindung mit einer *Hardware* hat (dem „Gerät“), auf der sie läuft, wäre dies wenig glücklich formuliert: Denn dies ist zwingend immer und ausnahmslos der Fall. Eine Software läuft stets nur auf Hardware, also einem „Gerät. Diese Sichtweise hätte also keinen Mehrwert. Gemäß Erwägungsgrund 7 scheint dies aber ohnehin nicht gemeint, sondern die mögliche Verbindung bzw. Verbindungsfähigkeit zu anderen Geräten und Netzwerken.
Angeregt wird, in der Definition des Produkts mit einem digitalen Inhalt zu überprüfen, ob die Beschränkung auf „vernetzte“ Produkte sinnvoll ist.

Auffallend ist ferner, dass in Ziffer 1 des Annex 1 – also den grundlegenden Sicherheitsanforderungen - die Prinzipien des Art. 25 Abs. 1 und 2 DSGVO nicht genannt sind, namentlich „data protection by design“ und „data protetion by default“. Beides sind allerdings – auch über Art. 5 Abs. 1 lit. f) DSGVO – grundlegende

Anforderungen für den Betrieb und damit den Anwender, im Ergebnis aber auch nur leistbar, wenn das entsprechende Produkt mit digitalen Elementen so ausgeliefert bzw. einstellbar ist.

Damit wird die Aufnahme dieser beiden Prinzipien aus Art. 25 Abs. 1 und Abs. 2 DSGVO in den Katalog der Ziffer 1 des Annex 1 angeregt.

b. Begrenzung der Anwendbarkeit auf längstens 5 Jahre

U.a. trifft die Hersteller nach Art. 10 Abs. 6 die Pflicht, wenn sie ein Produkt mit digitalen Elementen in Verkehr bringen und während der erwarteten Produktlebensdauer oder während eines Zeitraums von fünf Jahren ab dem Inverkehrbringen des Produkts - je nachdem, welcher Zeitraum kürzer ist - , dass Schwachstellen dieses Produkts wirksam und im Einklang mit den grundlegenden Anforderungen in Anhang I Abschnitt 2 des CRA behandelt werden.

Diese zeitliche Begrenzung auf längstens 5 Jahre findet sich im CRA verschiedentlich. Eine Erläuterung, warum es genau 5 Jahre sind, findet sich in den Erwägungsbegründung bzw. dem Entwurf nicht.

5 Jahre mag für einige Softwareanwendungen eine typische, oft steuerlich geprägte Nutzungszeit sein. Eine große Anzahl von Softwareprodukten wird aber regelmäßig länger genutzt, v.a. Betriebssystemsoftware. Betrachtet man etwa den Umstand, wie lange Windows 7, das 2009 auf den Markt kam, noch verwendet wurde – derzeit ist es im Jahre 2022 noch auf rund 12,8 % der Windows-Desktop-Systemen im Einsatz. Windows 10, das 2015 veröffentlicht wurde, erfreut sich ebenfalls noch großer Beliebtheit, es wurde von Microsoft 2015 auf den Markt gebracht, also vor rund 7 Jahren, Microsoft wird den Support voraussichtlich 2025 beenden, also nach rund 10 Jahren.

Aber auch Software für große Industrieanlagen wird oft länger als 5 Jahren eingesetzt, oft über 10, 15 oder auch 20 Jahre, selbst Alltagsprogramme wie Office Programme, Grafiksoftware, Tonsoftware, etc. kann nach 5 Jahren noch ausreichend gut funktionieren. Vor allem bei einer Bindung an bestimmte spezielle Hardware und der bei

einem Wechsel entstehenden hohen Kosten wird eine Nutzungsdauer von über 5 Jahren relevant sein.

Zudem zeigt die Praxis, dass gerade ältere Software deutlich fehler- und sicherheitsvorfallanfälliger ist, alleine schon der Entwicklung seit Veröffentlichung, neuer Hacking-Methoden, leistungsfähiger Rechner mit mehr Möglichkeiten etwa für Brute-Force-Attacken oder dem Entschlüsseln von Verschlüsselungsalgorithmen, etc. Wenn es etwa um personenbezogene Daten geht, sind diese in einer Software, die vor mehr als 5 Jahren auf den Markt kam, auch nach dieser Zeit noch genauso „schützenswert“ wie vorher. Warum also soll nach längstens 5 Jahren dafür der Hersteller keine Korrekturen mehr für Schwachstellen bereitstellen?

Man stößt noch auf ein anderes Problem: Wie ist es, wenn ein Nutzer ein Produkt mit digitalen Elementen quasi im letzten Monat erwirbt? Dann käme er in diesem Beispiel noch für 1 Monat in den Genuss von Sicherheitsupdates, würde aber das Produkt uU noch jahrelang nutzen – es wäre dann ein Sicherheitsrisiko.

Zwar sieht der Entwurf in seinem Anhang 2 im Rahmen der Pflichtinformationen für ein solches Produkt vor, dass der Hersteller auch darüber informieren muss, bis wann er Sicherheitsunterstützung anbietet (Nr. 8 des Anhangs 2) – dies ändert an der Risikolage an dem Produkt nichts.

Die DSGVO etwa kennt keine zeitliche Begrenzung, hat aber natürlich auch nicht den Hersteller, sondern den Nutzer einer Datenverarbeitungsanlage als Normadressaten, den sog. „Verantwortlichen“ bzw. „Controller“ der Verarbeitung personenbezogener Daten. Folge ist, dass der Controller in obigem Beispiel nach 1 Monat keinen Support mehr zu Sicherheitsthemen vom Hersteller erhalten müsste, nach der DSGVO aber für die restliche Nutzungsdauer der Software über Art. 32 DSGVO verpflichtet ist, beim Einsatz genau dieser Software eine ausreichende Datensicherheit zu gewährleisten. Wie aber soll dies ohne Support des Herstellers möglich sein?

Insofern besteht zwar gerade keine Kollision beider Rechtsakte, da sie sich ergänzen bzw. nebeneinander gelten – es fehlt aber an der inhaltlichen Abstimmung.

Eine pragmatische Lösung könnte sein, dass der Controller alle 5 Jahren (bzw. bei einer kürzeren erwarteten Nutzungsdauer nach deren Ablauf) die Software immer wieder durch eine neue Software ersetzt, dies ist aber weder nachhaltig noch wirtschaftlich sinnvoll oder technisch nötig, kann vielmehr für hohen Migrations- und Umschulungsaufwand, Risiken dabei, etc. sorgen.
Für Verbraucher kann sich eine bessere Situation aufgrund der Aktualisierungspflicht gemäß § 327f BGB ergeben – allerdings ist dabei zu beachten, dass sich dies auf Verbraucher beschränkt und damit den gesamten Einsatz von Software in Unternehmen ausnimmt und zum anderen, dass selbst für Verbraucher dies nur für „digitale Produkte“ im Sinne von § 327 BGB gilt, die nur eine Teilmenge der vom CRA erfassten „Produkte mit digitalen Elementen“ umfasst.
Die etwas willkürlich scheinende Frist von 5 Jahren sollte nochmals überdacht werden – aus Cybersicherheitsgesichtspunkten dürfte sie in einigen wichtigen Fällen zu kurz sein – zugleich stellt jede Verlängerung eine erhöhte Belastung der Hersteller dar.

c. Melde- und Informationspflichten

In Art. 11 des CRA finden sich eine Reihe von Melde- und Unterrichtungspflichten für den Hersteller, die inhaltlich an die Meldepflichten der DSGVO nach Art. 33 und 34 DSGVO erinnern.

So muss der Hersteller nach Art. 11 Abs. 1 CRA unverzüglich, aber binnen 24 Stunden nach Kenntnis, jede aktiv genutzte Schwachstelle eines Produkts mit digitalen Inhalten sowie jeden Vorfall, der sich auf die Sicherheit eines Produkts mit digitalen Inhalten auswirkt, der ENISA als dafür zuständiger europäischer Behörde melden. Die ENISA leitet diese Meldung dann an andere Anlaufstellen weiter, wie im Detail in Art. 11 CRA geregelt.

Nach Abs. 4 muss der Hersteller unverzüglich auch die Nutzer bei einem solchen Vorfall und über Korrekturmaßnahmen, die der Nutzer ergreifen kann, informieren; eine Maximalfrist findet sich hier nicht.

Letzteres überrascht, da vor allem die Nutzer die Weiterverbreitung eines Risikos durch das Einspielen von Update o.Ä. vermeiden können, was aber nur möglich ist, wenn sie Kenntnis haben und informiert wurden.

Soweit bei der erfolgten Ausnutzung einer Schwachstelle oder einem Vorfall auch personenbezogene Daten betroffen sind, greift für die Anwender der Software, also die datenschutzrechtlich Verantwortlichen, die DSGVO und es kann die Behörden-Meldepflicht nach Art. 33 DSGVO sowie die Unterrichtungspflicht gegenüber den Betroffenen nach Art. 34 DSGVO einschlägig sein. Art. 33 DSGVO schreibt eine Maximalfrist von 72 h vor, also eine dreimal längere Zeit als Art. 11 Abs. 1 CRA. Gegenüber den Betroffenen kennt Art. 34 DSGVO dagegen ebenfalls keine Maximalfrist.

Auch hier ist es aber so, dass der CRA nicht die Controller, also nicht die Personen oder Stellen, die das Produkt mit digitalen Inhalten, adressiert, sondern die Hersteller. Die DSGVO dagegen gilt für die „Nutzer“ des Produkts, also etwa ein Unternehmen, dass eine solche Software einsetzt.

Eine Überschneidung gibt es daher nicht, beide Melde- und Unterrichtungsmechaniken kollidieren nicht.

Es stellt sich allerdings die Frage, wie ein kleinerer Hersteller von Produkten mit digitalen Inhalten – etwa eine Startup-Firma mit einigen wenigen Mitarbeitern - eine Frist von 24 Stunden in der Praxis einhalten soll, etwa bei einem Vorfall zu Beginn des Wochenendes oder Feiertagen und zwar z.B. auch in arbeitsrechtlicher Hinsicht. Denn zumindest nach deutschem Arbeitsrecht ist es aufwendig, für das Wochenende, erst recht für Sonn- und Feiertage, einen Bereitschaftsdienst oder einen regulären Arbeitsdienst vorzusehen, es ist mit Genehmigungen durch die Gewerbeaufsichtsämter etc. verbunden und typischerweise auf Ausnahmen beschränkt.

Große Hersteller haben dafür ihre Abläufe und internen Regelungen, schon deswegen, weil dort auch aus anderen Gründen an Wochenenden und Feiertagen eine „Notbesetzung“ vorhanden sein muss. Für kleine Hersteller dagegen wird diese Pflicht bzw. die dafür nötige betriebsinterne Organisation auf große Schwierigkeiten stoßen.

Insofern fällt zudem auf, dass die Meldepflicht grundsätzlich gilt, also auch eine noch so kleine, aber vorhandene Schwachstelle diese auslöst – selbst wenn es keine spürbaren

Folgen gibt; gleiches gilt bei Art. 11 Abs. 2 für den „Vorfall“: Voraussetzung ist auch hier nur, dass sich dieser auf das Produkt auswirkt – nicht, dass dies spürbar oder nennenswert erfolgt, zumindest dem Wortlaut nach wäre sogar eine positive Auswirkung umfasst – was dem Zweck der Regelung nicht entsprechen dürfte.

Zuletzt ist noch auf Art. 11 Abs. 7 CRA hinweisen: Dort ist eine weitere Meldepflicht des Herstellers konstituiert und zwar gegenüber der Person oder Einrichtung, die eine von einer Schwachstelle oder Vorfall betroffenen Komponente innerhalb des Produkts wartet. Inhaltlich ist dies nachvollziehbar – es fehlen dann aber Regelungen zur Folge, zudem ist die Wartungs-Person nicht Adressat des CRA.

Damit ist hier an drei Stellen nachzubessern:

- Eine Spürbarkeitsgrenze ist einzuführen
- Es muss Ausnahmen für kleine Hersteller geben, zumindest was die Fristdauer von 24 Stunden betrifft.
- Zudem wird angeregt, zu regeln, was die Wartungs-Person in Folge für Pflichten treffen. Denn sich hier nur auf den Umstand eines „Bösgläubigmachen“ und jeweils national vorhandene (oder auch nicht vorhandenen) Regelungen zu verlassen, widersprich einerseits dem klaren Ziel des CRA einer Vollharmonisierung und der daraus resultierenden deutlich erhöhten Rechtssicherheit, andererseits auf einen möglichst effizienten Schutz und Maßnahmen bei Vorfällen.

d. Marktbeobachtungsbehörden

In den Art. 41 ff CRA ist die Marktüberwachung und Rechtsdurchsetzung durch eine Art Aufsichtsbehörde, der „Marktüberwachungsbehörde“, geregelt. Wie schon betont, ist der Fokus des CRA und damit dieser Behörden die „Produkt-Sicht“ und der CRA v.a. „Produkt-Recht“, nicht der Datenschutz – dessen Überwachung verbleibt vielmehr den Datenschutzbehörden.

Auch hier gibt es daher keine Kollision, schon der unterschiedlichen Normadressaten wegen: der CRA richtet sich an Hersteller, Importeure und Händler, die DSGVO an die Betreiber von Software als Controller. Beide Rechtsakte ergänzen sich auch hier.

Dementsprechend ist in Art. 41 Abs. 5 CRA explizit die Zusammenarbeit beider Behörden genannt und in Grundzügen geregelt, v.a. das Recht der Datenschutzbehörden alle im Rahmen des CRA erstellen oder geführten Unterlagen anzufordern und darauf zuzugreifen, soweit zur Aufgabenerfüllung nötig. Dies wird dann der Fall sein, wenn es – auch – um einen möglichen Datenschutzverstoß oder einen Fall des Art. 33 oder Art. 34 DSGVO geht und die Behörde gegen die Betreiber des Produkts ermittelt – der Hersteller ist nicht im Fokus der Datenschutzbehörden, da dieser in der Regel nicht die personenbezogenen Daten der Betroffenen verarbeitet, sondern nur das Produkt dazu hergestellt hat Dies mag im Cloud und SaaS-Bereich anders sein, dort sind Hersteller zugleich auch die Betreiber von einer Cloud-Lösung – also über diese, von seiner Herstellerseite getrennt zu sehenden Rolle direkter Normadressat der Datenschutzgesetze.

Für die Arbeit der Datenschutzbehörden wird diese Zugriffsmöglichkeit auf Unterlagen nach dem CRA hilfreich sein, da ein Unternehmen, das ein Produkt mit digitalen Elementen als reiner „Anwender“ betreibt (etwa Microsoft Office Produkte oder SAP Produkte), eben auch nur die Anwendersicht hat und meist nur sehr begrenzt, wenn überhaupt, Einblick in die Details des Produkts haben wird, also der Datenschutzbehörde dementsprechend nicht oder nur wenige Unterlagen zur Verfügung stellen kann.

Gemäß dem CRA könnte die Datenschutzbehörde insofern dann umfänglich auf die Hersteller zugehen und Einblick in die technische Dokumentation etc. nehmen, um sich einen deutlich detaillierten Blick auf die Software- bzw. Produktarchitektur zu verschaffen.

Damit erlangt sie dann uU aber mehr Information und Einblicke als der eigentliche datenschutzrechtliche Controller, der als Anwender eines Produkts „nur“ die normalen Informationen des Herstellers erhält, die diese gegenüber seinen Kunden – also dem datenschutzrechtlichen Controller – zu erteilen hat. Dies kann zu einer Schieflage in einem datenschutzrechtlich geführten Verfahren führen, dem man zwar in der Praxis durch Akteneinsicht in Grenzen begegnen kann, aber nicht immer wird überhaupt oder ausreichend zügig Akteneinsicht gewährt oder möglich sein.

Zu prüfen ist damit hier, ob in dem Fall, in dem eine Datenschutzbehörde in einem konkreten Verfahren gegen einen Datenschutz-Verantwortlichen von der Befugnis nach Art. 41 Abs. 5 CRA Gebraucht macht und Unterlagen des Herstellers erhält, nicht an dieser Stelle noch eine Pflicht der Datenschutz-Behörde aufgenommen werden muss, diese Informationen zwingend auch dem betroffenen Controller zugänglich machen oder zumindest auf das Vorliegen dieser Informationen hinweisen zu müssen, damit „Waffengleichheit“ herrscht.

Es gibt einen zweiten Punkt, der auffällt:
Nach Art. 42 CRA erhalten die Marktüberwachungsbehörden auf begründeten Antrag Zugang zu den Daten, die für die Bewertung der Konzeption, Entwicklung, Herstellung und die Behandlung von Schwachstellen solcher Produkte erforderlich sind, einschließlich der betreffenden internen Unterlagen des jeweiligen Wirtschaftsakteurs. Dies kann und wird in der Praxis auch personenbezogene Daten umfassen, sei es von den Mitarbeitern des Herstellers, dessen Lieferanten, uU sogar auch Kundendaten o.Ä. Dafür benötigt die Marktüberwachungsbehörde dann gemäß Art. 6 DSGVO eine ausreichende datenschutzrechtliche Erlaubnis und zwar in Form einer gesetzlichen Rechtsgrundlage, da eine Einwilligung aus praktischen Gründen ausscheidet.
Im Ergebnis wird nur Art. 6 Abs. 1 S. 1 lit. e) DSGVO bleiben – wofür die Verarbeitung der personenbezogenen Daten durch die Marktüberwachungsbehörde für die Wahrnehmung einer Aufgabe erforderlich sein muss, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die der Marktüberwachungsbehörde als Verantwortlichem übertragen wurde.

Nach Art. 6 Abs. 3 DSGVO muss insofern entweder das Unionsrecht oder nationales Recht die eigentliche datenschutzrechtliche Rechtsgrundlage festlegen. Daran sind zudem formale Anforderungen in Art. 6 Abs. 3 DSGVO geknüpft.

Die Zugangsnorm des Art. 42 CRA erfüllt diese Anforderungen derzeit nicht – dazu müsste dort gezielt und transparent eine zudem dem Bestimmtheitsgrundsatz genügende Eingriffsnorm vorhanden und sprachlich klar geregelt sein, dass und in welchem Umfang und Zweck die Verarbeitung personenbezogener Daten darüber erlaubt ist – immerhin geht es um einen staatlichen Zugriff auf personenbezogene Daten, die über Art. 8 EU-Grundrechtscharta primärrechtlich geschützt sind.

Insofern bietet sich dann sogleich auch eine Regelung im Sinne von Art. 14 Abs. 5 lit. c) DSGVO an, ansonsten müsste die Marktüberwachungsbehörde nach Art. 14 DSGVO binnen 1 Monats nach Datenerlangung die Betroffenen darüber informieren – was wenig sinnvoll scheint, auch praktisch kaum machbar sein dürfte.

Positiv ist, dass Art. 52 CRA eine Vertraulichkeitspflicht statuiert – die genau genommen aber bei personenbezogenen Daten ohnehin eine gesetzliche Pflicht aus der DSGVO ist, zudem keine Rechtsgrundlage darstellt. An dem Erfordernis einer solchen (siehe vorstehend) verbleibt es also.

Angeregt wird, in Art. 52 CRA zu den schon vorhandenen Beispielen explizit auch noch personenbezogene Daten zu nennen.

e. Wesentliche Änderungen, Hersteller-Begriff und Individual-Software

Nach Art. 16 CRA kann quasi jedermann zum „Hersteller“ im Sinne des CRA werden und zwar dann, wenn er wesentliche Änderungen an dem Produkt mit digitalen Elementen vornimmt.

Art. 16 CRA bestimmt, dass für ihn dann betreffend des Teils des Produkts, das von den wesentlichen Änderungen betroffen ist, weitgehend die Pflichten eines Herstellers gelten. Dies kann sich auf das gesamte Produkt erstrecken, wenn sich die wesentlichen Änderungen auf die Cybersicherheit des gesamten Produkts auswirken.
Was „wesentliche Änderungen“ sind, ist in Art. 3 Nr. 31 CRA definiert: „Wesentliche Änderung“ sind danach eine Änderung des Produkts mit digitalen Elementen nach dessen Inverkehrbringen, die sich auf die Konformität des Produkts mit den grundlegenden Anforderungen in Anhang I Abschnitt 1 auswirkt oder zu einer Änderung der bestimmungsgemäßen Verwendung, für die das Produkt geprüft wurde, führt.

Bespiele:
Hier stellt sich etwa die Frage, ob ein umfassenderes Customizing eines Produkts durch den Kunden, der es erwirbt, zu einer solchen Situation führen kann.
Betrachtet man Anhang I und dort den Abschnitt 1, kann dies sehr häufig der Fall sein, etwa schon, wenn man die „sichere“ Standardkonfiguration anpasst – denn wer kann

beurteilen, ob etwa das Einsetzen anderer Verfahren zu einer Verbesserung oder Verschlechterung führt, oder nur zu einem anderen Ansatz?

Man wird an größeren Software-Installationen zwingend etwa das standardmäßig voreingestellte Rollen- und Berechtigungskonzept ändern und ändern müssen, alleine schon, um es den betrieblichen Gegebenheiten anzupassen, ggfls. auch etwaigen Vereinbarungen in Betriebsvereinbarungen o.Ä.

Es kann also oft der Fall sein, dass durch ein „normales“, betriebliches Customizing oder auch nur intensivere Parametrisierung eine „wesentliche Änderung“ im Sinne des CRA ergibt.

Folge wäre dann, dass ein Unternehmen, dass insofern etwa SAP oder eine andere umfangreichere ERP- oder HR-Software einsetzt und sich auf seine Bedürfnisse anpassen lässt, zum „Hersteller“ im Sinne des CRA wird. Dies zwar nur für die veränderten Teile – was aber sehr umfänglich sein kann, nimmt man eine typische, maßgeschneiderte ERP Anwendung.

Zudem wird ein solches Unternehmen den Pflichten rein faktisch nicht nachkommen können, nimmt es doch „nur“ Customizing oder Parametrisierungen vor, hat aber keinen echten Einblick, in das Produkt selbst, sondern bewegt sich im Rahmen desjenigen, was der eigentliche Hersteller an Anpassbarkeit vorgesehen hat und/ oder lizenzrechtlich (nur) gestattet.

Diesem Unternehmen, etwa einem Krankenhaus, einer Schule, einer Werbeagentur, einem größeren Handwerksbetrieb, etc. dann die Pflichten eines Produkt-Herstellers aufzubürden, geht deutlich zu weit.
Hier ist nötig, eine deutlich trennschärfere Abgrenzung zu treffen und reine Anwender, wenn diese nur dasjenige an Möglichkeiten ausnutzen, was der eigentliche Hersteller technisch oder rechtlich vorsieht, von der Regelung des Art. 16 CRA auszunehmen.

Wenn sich ein Unternehmen Individual-Software programmieren lässt, wird es dagegen nicht zum Hersteller. Denn der Herstellerbegriff knüpft daran an, dass ein hergestelltes Produkt im Anschluss auch vertrieben wird, nicht nur rein intern selbst genutzt.

Dies zeigt einen weiteren Missklang zu den „wesentlichen Änderungen“: Denn für diese und die darüber erfolgende Anwendbarkeit der Herstellervorschriften wird nicht auf den Vertrieb abgestellt, sondern nur die Vornahme der wesentlichen Änderung.

Insofern wäre nötig, in Art. 16 auch noch diesen Teil der Definition aus Art. 3 Nr. 18 und der dortigen Hersteller-Definition zu übernehmen, also auf die Vermarktung abzustellen.

Dann fielen auch oben genannte Unternehmen, die ein Produkt mit digitalen Elementen nur für sich selbst und den eigenen Betrieb des Produkts verändern, aus Art. 16 CRA heraus.

f. Zu enger Nutzer-Begriff

Eine weitere Unschärfe des CRA betrifft den verschiedentlich im CRA verwendeten Nutzer-Begriff.

Er ist nicht legaldefiniert, so dass offen bleibt, wer genau darunter fällt. Dem Sinn und Zweck nach, aber auch dem Wortlaut wird es jedenfalls die Person sein, die ein Produkt mit digitalen Inhalten tatsächlich nutzt, also etwa sich in eine Software einloggt und in diese Daten eingibt oder eine Maschine mit digitalen Elementen bedient.

Im Unternehmensumfeld stellt sich aber die Frage, ob das Unternehmen, das ein Produkt mit digitalen Elementen einsetzt, ebenfalls ein „Nutzer“ ist, selbst wenn das Produkt dann naturgemäß nicht vom Unternehmen, sondern dessen Mitarbeitern genutzt wird. So ist in solchen Fällen auch nur das Unternehmen der Lizenznehmer, nicht die das Produkt eigentlich nutzenden Mitarbeiter.

Würde man Unternehmen, die Produkte mit digitalen Inhalten durch ihre Mitarbeiter nutzen lassen, nicht auch als „Nutzer“ im Sinne des CRA sehen, käme es zu einer großen Lücke: Denn in diesem Kontext trifft die Entscheidung für oder gegen ein Produkt, die nach dem Willen der Kommission über den CRA und dessen Pflichtinformationen der Anlage 2 auch in Hinblick auf die vom Hersteller vorgesehene Cybersicherheit getroffen werden soll, das Unternehmen, nicht die nutzenden Mitarbeiter. Diese werden vielmehr mit der Beschaffung nichts zu tun haben, sie wären dafür auch nicht zuständig oder verantwortlich. Sie werden auch in den wenigsten

Fällen dafür ausgebildet sein, sich ein Bild von der Cybersicherheit eines Tools machen zu können, das sie dienstlich während ihres Arbeitstages für das Unternehmen nutzen müssen.

Insofern wird angeregt, den Begriff des „Nutzers“ einerseits der Rechtsklarheit und Bestimmtheit wegen in den Katalog der Definitionen in Art. 3 CRA aufzunehmen, andererseits auch so zu formulieren, dass nicht nur die „End-Nutzer“ erfasst sind, sondern auch Stellen, die ein Produkt mit digitalen Inhalten durch ihre Mitarbeiter für sich nutzen lassen.

g. Ausnahme für SaaS und Dienstleistungen

Aus dem Erwägungsgrund 9 ergibt sich, dass der CRA „keine Vorschriften für Dienstleistungen, wie Software-as-a-Service (SaaS)“ enthalte, mit Ausnahme von solchen (wohl: SaaS)- Datenfernverarbeitungslösungen, die

- sich auf ein Produkt mit digitalen Elementen beziehen
- und als entfernt stattfindende Datenverarbeitung verstanden werden, für die
    - eine Software vom Hersteller selbst oder unter dessen Verantwortung konzipiert und entwickelt wird
    - und ohne die das Produkt mit digitalen Elementen eine seiner Funktionen nicht erfüllen könnte.

Liest man diese Rückausnahmen, wonach der CRA doch gilt, drängt sich der Eindruck auf, dass damit doch die meisten SaaS-Anwendungen (bzw. deren Herstellung und Vertrieb) in den Anwendungsbereich fallen, etwa klassische Cloud-Softwarelösungen.

Diese umfangreichen Rückausnahmen und damit doch breite Anwendung ist in der Sache richtig, da sich gerade dort Cybersicherheitsrisiken realisieren können und schnell ausbreiten: Denn SaaS-Anwendungen zeichnet aus, dass sie mandantenfähig sind, also aus einer großen Datenbank für alle Kunden des Herstellers bestehen, in der einzelne Kunden nur ihre „Abschnitte“ haben, oft nur logisch voneinander getrennt. Ein Fehler oder Sicherheitsvorfall kann daher alle Kunden und deren Bereiche betreffen bzw. sich darauf auswirken oder ausbreiten.

Die Formulierung „Dienstleistungen“ ist allerdings begrifflich schwierig und sollte zumindest in den Erwägungsgründen noch genauer beschrieben werden, denn der

deutsche BGH etwa ordnete noch unter dem Begriff „ASP – Application Service Providing“ eine solche Bereitstellung als Miete ein, nicht als Dienstvertrag. Zwar muss der Begriff der „Dienstleistung“ im CRA autonom und rein nach EU-Recht ausgelegt werden, das BGH-Beispiel zeigt aber, wie unterschiedlich man dies national verstehen kann.

Insgesamt ist die Ausnahme und Rückausnahme in Erwägungsgrund 9 unklar. Nach der aktuellen Formulierung wird die Rückausnahme in Erwägungsgrund 9 die Regel sein.
Insofern wäre zu prüfen, die Mechanik umzukehren: Auch ASP, SaaS- und Cloud-Anwendungen fallen grundsätzlich unter den CRA, es sei denn, es liegen bestimmte, dann zu definierende Bereiche vor, in denen dies ausnahmsweise nicht der Fall ist.

h. Keine Einbeziehung der Gefährlichkeit von Produkten/ Ausnahmen für KMU

V.a. dem Hersteller werden im CRA eine Vielzahl von zum Teil nur sehr aufwendig zu erfüllenden Pflichten auferlegt.

Diese Pflichten mögen für große Hersteller nur einige von vielen Unternehmenspflichten sein und in Summe nur begrenzt ins Gewicht fallen, für kleine Hersteller, Startup-Unternehmen, Einzelunternehmen, die hoch innovative Produkte schaffen, wird dies in der Praxis nicht stemmbar sein. Es besteht vielmehr das Risiko, das mit der dadurch entstehenden Bürokratie Innovation und Ideen gehemmt werden – etwas, was die EU im Rahmen ihrer Digitalisierungsstrategie andererseits gerade zu vermeiden versucht. Natürlich kann ein Produkt von einem kleinen Hersteller genau gefährlicher oder noch gefährlicher sein als dasjenige von einem großen Hersteller. Rein aus Cybersicherheitsgesichtspunkten wäre es also nicht zu rechtfertigen, kleine Hersteller auszunehmen. Aus wirtschaftlicher und Innovationssicht dagegen wäre es dagegen zu begrüßen, hier über Ausnahmen nachzudenken.

Viele hobbymäßige Programmierer, die etwa Freeware der Allgemeinheit anbieten, fielen darunter – denn es handelt sich bei Software um ein Produkt mit digitalen Elementen, zumindest wenn es eine Datenverbindung beinhaltet, diese Programmierer wären ferner „Hersteller“ im Sinne von Art. 3 Nr. 18 CRA, da dort nicht auf die Entgeltlichkeit abgestellt wird. Selbst wenn es nur um ein einfaches Freeware-

Computerspiel eines Teenagers ginge, das über dessen Homepage zum Download unentgeltlich angeboten wird und mit einer Internetverbindung arbeitet, etwa, um nach Updates zu suchen, wäre der CRA einschlägig und der Teenager ein „Hersteller“ im Sinne des CRA.

Ein Weg dazu kann sein, diese Ausnahmen

- an die „Cybersicherheit-Gefährlichkeit“ von Produkten mit digitalen Elementen zu knüpfen, und/ oder
- auf die Gewerblichkeit des Vertriebs abzustellen (angenähert an die in Erwägungsgrund 10 zu findende Bereichsausnahme für Open Source Software).