Kommentar zum Data Act-Entwurf

Der Data Act Entwurf der Europäischen Kommission vom 23.02.2022 („DA-E“) verfolgt die Ziele, eine ausgewogene Allokation der Wertschöpfung aus Daten im gesamtgesellschaftlichen Interesse durch die Formulierung von Zugangsansprüchen zu erreichen, die Handlungskompetenz der Menschen in Bezug auf ihre Daten zu stärken, sowie Innovation durch Daten zu ermöglichen. Einerseits hat der aktuelle DA-E noch erhebliche Schwächen, Lücken, und Unstimmigkeiten, andererseits verfehlt er seine Ziele in mehrfacher Hinsicht. Die Ziele stehen zudem teilweise im Widerspruch und müssen sorgfältig gegeneinander ausbalanciert werden. Auch die aktuellen, teilweise divergenten, Änderungsvorschläge des Europäischen Parlaments und des Europäischen Rats[1] lösen diese Unzulänglichkeiten allenfalls teilweise auf. Entsprechend gewagt erscheint das Experiment der Europäischen Kommission durch ein komplexes horizontales Regelwerk, ohne Präzedenz in spezifischen Sektoren, Gerätedaten sehr umfassend und pauschal zum Gemeingut der Gesellschaft zu erklären und die europäische Datenwirtschaft grundlegend auf den Kopf zu stellen. Statt lediglich das Risiko von Marktversagen durch regulatorische Leitplanken zu adressieren oder bestehende Ungleichgewichte sowie Hemmnisse für Datennutzung und Datenaustausch zu beseitigen, wird der europäische Markt selbst im internationalen Wettbewerb beispiellos ausgebremst.

Hier soll insbesondere die Problematik in Hinblick auf datengetriebene Innovationen diskutiert werden. Der DA-E sorgt für eine Entflechtung von der Hardware bzw. Infrastruktur zum Generieren der Daten (z.B. Sensoren, IoT) und der Software zum Auswerten generierter Daten. Der DA-E schafft die grundsätzliche Möglichkeit, andere Hersteller als den Hersteller der Hardware bzw. Infrastruktur für die Verarbeitung der Daten zu nutzen. Und genau dieses Konzept ist ein zweischneidiges Schwert: Einerseits können dadurch neue Anbieter Daten aus Sensoren auswerten, zu denen sie bisher keinen Zugang hatten. Andererseits untergräbt die Verpflichtung, generierte Daten mit Nutzern und Dritten zu teilen, den Anreiz selbst durch die Kombination von Hardware und Software neue Innovation anzustoßen sowie zu vermarkten, und somit einen gesellschaftlichen Mehrwehrt sowie einen Beitrag zur Resilienz Europas zu schaffen.

Problem 1: Unverhältnismäßige Überregulierung

Die im DA-E vorgeschlagenen umfassenden Regelungen in Bezug auf Datenzugang sind nicht gerechtfertigt. Schon die Europäische Kommission hatte auf Seite 16 ihrer Datenstrategie vom 19.02.2020 betont, dass „*die Gewährung des Zugangs zu Daten [nur dann] verbindlich vorgeschrieben werden*“ soll, „*wenn besondere Umstände dies erfordern*“. Gemäß zugehöriger Fußnote 39 solle daher ein Recht auf Datenzugang „*stets sektorspezifisch sein und nur dann gewährt werden, wenn in diesem Sektor ein Marktversagen festgestellt wird bzw. vorherzusehen ist und durch das Wettbewerbsrecht allein nicht behoben werden kann*“. Ein europäisches Marktversagen – insbesondere im Bereich der Medizintechnik – wurde jedoch nicht festgestellt oder vorhergesehen. Vielmehr verweist die Begründung des DA-E nur auf etwaige „*Marktungleichgewichte*“ und konstatiert, dass „*die gemeinsame Nutzung von Daten zwischen*

[1] vgl. Vierter Kompromisstext des Rats der Europäischen Union vom 24.01.2023 sowie Kompromissvorschlag vom 30.01.2023 (EPP, S&D, Renew, Greens, ECR).

Unternehmen gängige Praxis ist“.[2] Die Datenzugangsrechte aus Kapitel II des DA-E (faktisch zugunsten anderer Unternehmen) greifen daher unverhältnismäßig in die grundrechtlich geschützte Position von Dateninhabern ein. Der DA-E sollte deshalb grundsätzlich neu durchdacht werden und sein Anwendungsbereich sollte zunächst auf einzelne, spezielle Sektoren begrenzt werden.

Problem 2: Isolierung von Geschäftsmodellen lähmt Markterschließung

Europa, und insbesondere Deutschland, hinkt hinsichtlich Digitalisierung hinterher. Das betrifft insbesondere Infrastruktur wie IoT und intelligente Sensoren allgemein, sowohl im privaten als auch im unternehmerischen Bereich. Unternehmen leisten oft Pionierarbeit mit der Erschließung neuer Märkte durch innovative Geräte. Der Mehrwert der dabei generierten Daten erwächst oft erst mit der Zeit, und der Markt hat noch keinen etablierten Benchmark für die Bemessung des Mehrwertes. So kommt es oft vor, dass Unternehmen neue Produkte zunächst zu schlechten Margen im Markt platzieren müssen, um dann später durch Software-as-a-Service-Angebote oder durch den Erlös aus verknüpften anderen Geräten die initiale Markterschließung quer zu subventionieren. Dieser Ansatz wird ausgebremst, wenn jeder „Second Mover“ sich einfach auf die Auswertung der Daten konzentrieren kann, ohne die Anstrengungen für das Platzieren der Infrastruktur zu haben. Denn „Second Mover“ können dann durch preiswertere Angebote oder durch Fokussierung auf bessere Produkte bereits in Konkurrenz zu einem neuen Produkt treten, bevor es richtig etabliert ist. Da aber gerade ein Mangel an vernetzter Infrastruktur und IoT das Problem ist, wirkt der DA-E kontraproduktiv.

Problem 3: Benachteiligung des deutschen Mittelstandes

Deutschlands Hidden Champions legen als Hersteller von Spezialmessgeräten, Sensoren, und andere komplexen Komponenten den Grundstein für die Sammlung des Datenschatzes. Dominiert wird dieses Segment von viele kleinen und mittelständischen Unternehmen. Diesen Unternehmen wird gemeinhin vorgeworfen, dass sie bei der Digitalisierung hinterherhinken und die Daten mit der eigenen Software nicht ausreichend nutzen. Zu befürchten ist allerdings, dass andere größere, oftmals nicht-europäische Unternehmen (mit deren Niederlassungen in der EU) mit skalierbarem Knowhow und massiveren Softwareressourcen das Feld der Auswertesoftware dieser Daten übernehmen. Das wäre nicht nur in Bezug auf technische Souveränität Europas problematisch, sondern würde viele deutsche Unternehmen für alle Zeiten zu Komponentenlieferanten degradieren. Das Potential der Wertschöpfung würde eben nicht durch diese Unternehmen gehoben, deren Partizipation an der Verwertung der Daten wäre marginal. Entsprechend wird weder die besondere Industriestruktur Deutschlands in dem DA-E berücksichtigt noch das Ziel der fairen Allokation der Wertschöpfung durch Daten erreicht.

[2] vgl. S. 2 und S. 12 des DA-E der Europäischen Kommission vom 23.02.2022.

Forderungen

Über die grundsätzliche Kritik an dem Verordnungskonzept in seiner Gesamtheit hinaus sollen hier Anpassungen spezifischer Teilaspekte dargelegt werden, um wesentliche Punkte zu entschärfen.

Innovation und geistiges Eigentum konsequent schützen

Hersteller sollten als Dateninhaber für diejenigen Daten den Zugang verweigern können, für die sie ein in Europa gültiges Patent halten das die Kombination aus einem Gerät und Verarbeitungsschritten mit den von dem Gerät gewonnenen Daten schützt. So soll eine Patentverletzung ausgeschlossen oder eine Umgehung durch die exakte Kenntnis der Struktur der Daten verhindert werden. Diese Einschränkung wäre nur konsequent zur Stärkung von Innovation und geistigem Eigentum.

Kein Datenzugang für Konkurrenzunternehmen

Der DA-E sieht in Art. 4 Abs. 4 sowie Art. 6 Abs. 2 lit. e ein Verbot für Nutzer und Dritte vor, die Daten für die Entwicklung von Konkurrenzprodukten desjenigen Produktes zu nutzen, von dem die Daten stammen. Es wäre also nur konsequent, Nutzer und Dritte schon dann von einem Datenzugang komplett auszuschließen, wenn sie selbst Produkte herstellen, die hinsichtlich der technologischen Ausgestaltung oder des Verwendungszwecks mit dem Produkt, von dem die Daten stammen, in Konkurrenz stehen. Ohnehin ist der Wert dieser Daten für den Nutzer oder Dritten erheblich eingeschränkt, wenn er damit kein Konkurrenzprodukt entwickeln darf. Weiter ist zu berücksichtigen, dass der stärkste Schutz für Geschäftsgeheimnisse und geistiges Eigentum stets die Nicht-Offenlegung ist.

„Reverse Data Access“ für Hersteller, die nicht Dateninhaber sind

Ist ein Nutzer Dateninhaber, sollte auch ein Recht des Herstellers ausgestaltet werden, Zugang zu den Daten zu erhalten. So ist es beispielsweise denkbar, dass der Autohersteller und nicht der Bremsenhersteller Dateninhaber der Daten eines Sensors von Bremsen ist. Ein Hersteller, der nicht zugleich Dateninhaber ist, sollte berechtigt sein, auf bestimmte Produktdaten zuzugreifen beziehungsweise diese bei einem Servicebesuch auszulesen. Insofern weist der DA-E, ob bewusst oder unabsichtlich, eine Lücke auf.

Produktsicherheit messen und Produktentwicklung begünstigen

Außerdem sollte der DA-E eine Datenverarbeitungsbefugnis des Herstellers zu Zwecken der Produktsicherheit und Produktentwicklung vorsehen, und zwar unabhängig von einer vertraglichen Erlaubnis des Nutzers.[3]

[3] Art. 4 Abs. 6b des Kompromissvorschlags vom 30.01.2023 geht insofern nicht weit genug.

Wertschöpfung aus Daten fördern – Zugang auf Rohdaten beschränken

Der DA-E sieht in seinem Erwägungsgrund 17 bereits vor, abgeleitete Daten von der Zugangsverpflichtung auszunehmen. Das ist auch notwendig, um einen Anreiz für das Strukturieren, Bereinigen, und sonstige Aufbereiten an Daten, welche den Wert der Daten erhöht, zu schaffen. Die Definition, welche Daten hiervon betroffen sind, sollte präzisiert werden, insbesondere in Hinblick auf Metadaten und Zwischenergebnisse. Wenn die Bereitstellung aufbereiteter Daten ein wesentlicher Teil des Produktes ist, und die aufbereiteten Daten dem Nutzer zur Verfügung stehen, dann sollten diejenigen Daten von der Zugangsverpflichtung ausgenommen werden, die Zwischenergebnisse oder Metadaten in Bezug auf diese aufbereiteten Daten sind.[4] Insbesondere Neuronale Netze, wie sie beispielsweise für föderiertes Machine Learning eingesetzt werden, sollten von der Zugangsverpflichtung ausgenommen werden, um Innovation in diesem Bereich nicht zu verhindern.

Definition von „Gatekeepern“ über DMA hinaus erweitern

Ein Datenzugang für „Gatekeeper" ist gemäß Art. 5 Abs. 2 und Art. 6 Abs. 2 DA-E nicht gestattet. Da der DA-E hierzu aber auf die entsprechende Definition aus dem DMA abstellt, erfasst das Verbot aber nur die großen amerikanischen und chinesischen Hyperscaler. Betrachtet man jedoch die einzelnen Sektoren, wie Gesundheit oder Mobilität, muss die Definition „Gatekeeper“ für den DA-E erweitert werden, da andere Kriterien zu betrachten sind: Beispielsweise sollten im Bereich der Gesundheitsdaten nicht Firmen mit ohnehin breitem Zugang zu den Nutzern die Möglichkeit haben, durch Koppelgeschäfte die Datenzugangsberechtigung von diesen Nutzern übertragen zu bekommen. Es sollten also Unternehmen vom Zugang zu solchen Daten ausgenommen sein, die durch Geräte generiert werden, von denen mehr als 50 % der Nutzer auch gleichzeitig Nutzer eigener (anderer) Produkte dieser Unternehmen sind.

Freiräume für Neuproduktentwicklungen durch Umsatzschwellwerte schaffen

Innovation startet oft mit einer Idee, die sich auch innerhalb größerer Unternehmen als kleinere Einheit etablieren muss. Werden also in einem spezifischen Anwendungsbereich innerhalb eines Unternehmens neue Produkte entwickelt, die völlig neue Daten sammeln, dann sollten auch hier ähnliche Mechanismen zum Tragen kommen, wie sie für Kleinunternehmen beispielsweise in Art. 7 Abs. 1 DA-E vorgesehen sind. Der Aufwand der Datenbereitstellung wäre andernfalls unangemessen und damit unwirtschaftlich hoch für diese neu entstehenden Produkte, die eventuell auch langfristig nur eine Marktnische abdecken. Wenn also ein Unternehmen mit einem bestimmten Produkt Daten generiert, dann sollte es insofern bis zur Erreichung eines jährlichen Mindestumsatzes von EUR 300 Millionen als Kleinunternehmen gelten. Dabei wären jeweils diejenigen Produkte zusammenzurechnen, welche sich entweder in Verwendungszweck, technologischer Ausgestaltung und damit verwendeten Sensoren, oder bei den grundsätzlich zugänglich zu machenden Daten um mindestens 50 % überschneiden.

[4] Art. 5 Abs. 1 des Kompromissvorschlags vom 30.01.2023 adressiert beispielsweise den Gedanken, greift jedoch zu kurz.

Ungleichgewichte durch „Buy-Out“ Verträge unterbinden

Es sollten im DA-E Schutzmechanismen vorgesehen werden, die einen Verkauf der Daten seitens des Dateninhabers ebenso unterbinden, wie einen Verkauf des Zugangsrechts sowie sonstige Exklusivverträge in Bezug auf den Datenzugang seitens des Nutzers. So wird der Nutzer vor Klauseln geschützt, die ihn unter Umständen übervorteilen, und eine faire Verteilung entlang der Wertschöpfungskette unterstützt.[5] Hierbei besteht die Gefahr, dass eine Konzentration von Daten bei höchstbietenden Unternehmen entsteht, die dann eine gemeinsame Datennutzung unterbinden könnten.

Gestaltungsmöglichkeiten bei Zugangsmodalitäten klarstellen

Nach einer Ansicht sieht der DA-E lediglich einen „in-situ“ Zugriff auf die Daten vor, nicht aber einen Anspruch auf deren Übermittlung.[6] Diese Ansicht stützt sich auf Erwägungsgrund 21 und sollte in den Artikeln 4 und 5 DA-E klarstellenden Einzug finden. Die Verpflichtung zur Herausgabe von Daten sollte klar ausgeschlossen sein. Auch ist unklar, mit welcher Zugangsart sich der Vorteil eines Zugangs für den Nutzer maximieren lässt, denn der Nutzer ermöglicht nach Art. 5 Abs. 1 DA-E erst die Datenweitergabe an Dritte.[7] Bei dem geschilderten Zugang innerhalb des Produktes wäre vermutlich eine statistische Darstellung der Daten im Interesse des Nutzers. Beispielsweise werden die Rohdaten eines Fitnessarmbandes kaum einem Verbraucher von Nutzen sein, viel eher eine sinnvolle statistische Darstellung. Zu klären wäre, welches Gestaltungsrecht dem Hersteller dabei zukommt.

Zugang von öffentlichen Stellen auf Notsituationen einschränken

Ausschließlich zur Bewältigung bestimmter öffentlicher Notstände (vgl. Art. 15 lit. a DA-E), nicht jedoch zur Verhinderung oder Erholung hiervon oder zur allgemeinen Aufgabenerfüllung (vgl. Art. 15 lit. b und c DA-E) ist ein staatlicher Zugang zu Daten im öffentlichen Interesse angebracht (vgl. Art. 15 lit. a DA-E). Allerdings sollte einerseits ausgeschlossen sein, dass Daten für jedwede Art der Überwachung von Nutzern als auch Herstellern eingesetzt werden können. Andererseits sollte sich der staatliche Zugang im Sinne der Datensparsamkeit auf aggregierte Daten beschränken, soweit nicht nachgewiesen wird, dass der Zweck nur mit Zugriff auf Einzeldaten erreicht werden kann, die dann in Bezug auf den Nutzer als auch den Hersteller anonymisiert werden dürfen.[8]

Zugangsverpflichtung für Medizinprodukte ausschließen

Sensible Gesundheitsdaten stellen einen besonders schützenswerten Sonderfall da. Fast alle Daten von Medizingeräten, die für die Diagnose oder die Therapie eingesetzt werden, haben eine

[5] Art. 4 Abs. 6c des Kompromissvorschlags vom 30.01.2023 verkennt diese Problemstellung grundsätzlich. Auch die Hinzufügungen in Erwägungsgrund 24 „user should be given (...) opportunity to reject this Agreement“ dieses Kompromissvorschlags sind nicht ausreichend.

[6] vgl. Specht-Riemenschneider, MMR 2022, 809, 815f.

[7] vgl. neue Überschrift Kap. 2 des Vierten Kompromisstextes vom 24.01.2023. Der Kompromissvorschlag vom 30.01.2023 verkennt diese Zielrichtung, da er in Art. 4 Abs. 1 auf die Nutzbarkeit durch einen Dritten abstellt.

[8] vgl. Art. 15 des Kompromissvorschlags vom 30.01.2023 „An exceptional need to use non-personal data“, wohingegen nach Art. 17 Abs. 2 lit. d und lit. fa des Vierten Kompromisstextes vom 24.01.2023 auch personenbezogene Daten zur Verfügung gestellt werden sollen.

Beziehung zu Patienten. Um beispielsweise Privatheit zu schützen und eine Zuordnung zu einzelnen Patienten von vornherein auszuschließen, sollte die Zugangsverpflichtung auf aggregierte Daten beschränkt sein. Die MDR schreibt vor, dass nur Daten aus validiertem Ursprung in die Produktentwicklung einfließen dürfen. Da diese Validierung für Dritte ohnehin nicht umsetzbar wäre, ist der Nutzen solcher Daten folglich auf statistische Zwecke und Forschungsvorhaben limitiert. Darüber hinaus wird die EHDS-VO die Nutzung der Gesundheitsdaten spezifischer regeln und ist deshalb eher geeignet, die spezifischen Sicherheitsaspekte zu adressieren.

Verhältnis zur DSGVO klarstellen

Der DA-E ist kein lex specialis zur DSGVO, sondern tritt neben sie, wobei eine Regelung für Konfliktfälle fehlt. [9] Dateninhaber müssen personenbezogene Daten sowie etwaige Rechtsgrundlagen und Hindernisse für deren Zugänglichmachung umständlich identifizieren. Zur Lösung dieses Problems sollten DA-E und DSGVO praktikable Lösungen aufzeigen.[10] Schließlich bergen etwaige Datenschutzverstöße erhebliche Haftungsrisiken für Dateninhaber.

[9] vgl. insofern aber z.B. Art. 1 Abs. 3 des Kompromissvorschlags vom 30.01.2023.
[10] vgl. hierzu S. 5 ff. der Stellungnahme des BDI zum Legislativvorschlag des EU-Data Act, Stand: 13. Mai 2022.