Stellungnahme

zum Legislativvorschlag des EU-Data Act

Please note: An english version of this position paper will be published soon on our website: www.bdi.eu

Bundesverband der Deutschen Industrie e.V.

Stand: 13. Mai 2022

Inhaltsverzeichnis

Vorbemerkung

Der BDI unterstützt die Intention der EU-Kommission, die Nutzung und das faire Teilen von Daten zu fördern. Dass viele Unternehmen noch Nachholbedarf bei der wirtschaftlichen Nutzung von Daten aufweisen, belegt eine vom BDI beauftragte repräsentative Studie „Datenwirtschaft in Deutschland“[1]. Von den etwa 500 befragten Unternehmen konnten nur insgesamt 28 Prozent als „digital“ hinsichtlich des eigenen Datenmanagements eingestuft werden. 23 Prozent der befragten Unternehmen gaben an, im Rahmen eines strategischen Prozesses regelmäßig nach neuen Datenquellen und Einsatzmöglichkeiten zu suchen. 45 Prozent der Unternehmen nutzen gar keine Daten zur Optimierung von Produkten oder Geschäftsmodellen. Spiegelbildlich sind nur zwölf Prozent der befragten Unternehmen bereit, eigene Daten mit Dritten zu teilen.

Der Data Act bietet die Chance, eine von europäischen Werten geleitete Datenwirtschaft zu gestalten. Allerdings ist mit der Ausgestaltung des vorliegenden Entwurfs zu befürchten, dass der Data Act mit erheblichem zusätzlichem Aufwand, Kosten und Rechtsunsicherheiten für viele Unternehmen verbunden sein wird und diese im Ergebnis weniger Anreize haben, in eigene IoT-Produkte und Services zu investieren.

Mit dem vorliegenden Verordungsvorschlag über harmonisierte Vorschriften für einen fairen Datenzugang und eine faire Datennutzung (Data Act) wählt die Europäische Kommission ein überaus komplexes horizontales Regelwerk, das die „Spielregeln“ der europäischen Datenwirtschaft grundlegend verändern würde. Wie bereits in unseren Eingaben im Vorfeld des Legislativvorschlags angemerkt[2], ist für uns die Notwendigkeit eines solchen breit gelagerten Eingriffs in die Grundprinzipien der Datenwirtschaft in noch jungen Märkten nicht hinreichend ersichtlich. Die EU-Kommission weist in ihrem jüngsten Sachstandsbericht mit Blick auf die EU-Datenräume selbst auf eine sehr heterogene Entwicklung in den einzelnen Branchen und Sektoren hin.[3] Insofern erscheint eine stärkere sektor- und anwendungsspezifische Betrachtungsweise deutlich zielführender, um die Datenwirtschaft in Europa voranzubringen.

Mit dem Entwurf wird die Chance verpasst, einige wesentliche Hemmnisse bei der wirtschaftlichen Nutzung von Daten – beispielsweise die Abgrenzung zum Anwendungsbereich der Datenschutzgrundverordnung (DSGVO) –

[1] Datenwirtschaft in Deutschland – Wo stehen die Unternehmen in der Datennutzung und was sind ihre größten Hemmnisse?“, IW-Studie im Auftrag des BDI, Februar 2021, abrufbar unter: https://bdi.eu/media/publikationen/?publicationtype=Studien#/publikation/news/datenwirtschaft-in-deutschland/.

[2] BDI-Stellungnahme vom 03.09.2021 im Rahmen der öfftl. Konsultation.

[3] Commission Staff Working Document on Common European Data Spaces, SWD (2022) 45 final.

Bundesverband der Deutschen Industrie e.V.

Lobbyregisternummer
R000534

Hausanschrift
Breite Straße 29
10178 Berlin

Postanschrift
11053 Berlin

Ansprechpartner
Dr. Michael Dose
T: 030 2028 1560
F: 030 2028 2560
E-Mail: m.dose@bdi.eu

Internet
www.bdi.eu

auszuräumen. Stattdessen werden sämtliche IoT-Anwendungsfelder mit beträchtlichen Zusatzanforderungen, Eingriffen in die Privatautonomie sowie Vorgaben für das Produktdesign belegt, ohne dass ersichtlich wird, ob dies zu dem gewünschten positiven Effekt für die europäische Datenwirtschaft führt oder gar negative Effekte zu befürchten sind, z. B. wenn Unternehmen zukünftig Daten absichtlich nicht erheben.

Die Rolle der EU-Kommission sollte sich auf die Verabschiedung von Maßnahmen beschränken, die den Datenaustausch in industriellen Sektoren fördern und zu einem Datenökosystem führen würden, in dem beispielsweise freiwillige Mustervertragsbedingungen, die von der EU-Kommission empfohlen werden, eine wichtige Rolle spielen. Parallel dazu können auch die vorhandenen Instrumente, insb. das EU-Wettbewerbsrecht dazu genutzt werden, um im Falle eines strukturellen Marktversagens das entstandene Ungleichgewicht in den betroffenen Branchen bzw. Märkten zu beheben. Wichtig ist zudem eine größtmögliche Kohärenz des Data Acts mit anderen europäischen Regulierungsaktivitäten. Dies betrifft beispielsweise den Digital Markets Act, den Digital Services Act, den Data Governance Act sowie den AI Act.

Der Data Act muss von einer allgemeinen und undifferenzierten Verpflichtung zur Bereitstellung von B2B-Maschinendaten von Betreibern oder Ausrüstern von Industrieanlagen absehen. Die gemeinsame Nutzung von Daten im B2B-Kontext sollte in erster Linie auf Vertragsfreiheit und Marktanreizen beruhen.

Im vorgelegten Legislativvorschlag stellen wir an mehreren Stellen fest, dass der Schutz sensibler Informationen, einschließlich Geschäftsgeheimnissen, nicht hinreichend gewährleistet ist. Solche sensiblen Informationen müssen generell von der Verpflichtung zum Datenaustausch ausgenommen und Mechanismen zum Schutz gegen Wettbewerbsnachteile verankert werden, da die Schutzvorkehrungen, die der Data Act vorsieht (Abschluss von NDAs, Verbot der Entwicklung konkurrierender Produkte, Zweckbindung der Datennutzung) nicht ausreichend sind, um dem Schutzbedürfnis der Daten (Rückschlüsse auf Algorithmen, Source Codes, Rezepturen) gerecht zu werden. Zu diesem Zweck ist eine Überarbeitung zentraler Definitionen in Kapitel I im industrietauglichen Sinne unerlässlich.

Nachfolgend nehmen wir zu den einzelnen Aspekten des Legislativvorschlags der EU-Kommission Stellung:

Zu Kapitel I: Allgemeine Bestimmungen

1.1. Verhältnis zur DSGVO

Mit seinem weiten Verständnis von „Daten“ sind von den Vorgaben des Data Acts personenbezogene und nicht-personenbezogene Daten gleichermaßen erfasst. Der Legislativvorschlag versäumt es, notwendige Klarstellungen und Harmonisierungen mit der Datenschutzgrundverordnung EU 2016/679 (DSGVO) vorzunehmen. Hierdurch wird die Chance verpasst, eines der zentralen praktischen Hemmnisse von Unternehmen in der Datenwirtschaft aufzugreifen. In einer vom BDI beauftragten Studie des IW Köln „Datenwirtschaft in Deutschland“ gaben 85 Prozent der Unternehmen „datenschutzrechtliche Grauzonen“ als zentrales Hemmnis für eine stärkere wirtschaftliche Nutzung von Daten an.[4] Es besteht zu befürchten, dass der Data Act in seiner vorliegenden Form diese Hemmnisse noch verstärken wird.

Für eine rechtskonforme und praktikable Datenwirtschaft, die den Vorgaben und Pflichten des Data Act einerseits und denen der DSGVO andererseits genügt, braucht es praktikable Kriterien zur rechtssicheren Abgrenzung von personenbezogenen und nicht personenbezogenen Daten. Denn nach Kapitel II des Data Act können die Zugangspflichten des Dateninhabers auch personenbezogene Daten betreffen und insofern auch solche, die sich nicht auf den Nutzer, sondern Dritte beziehen. Aus Art. 4 und 5 des Data Act wird deutlich, dass die Zugangs- und Weitergabeansprüche von Nutzern auch nutzungsgenerierte Daten mit Bezug zu anderen Personen als dem Nutzer umfassen können. Hierfür setzt der Data Act zwar jeweils eine Rechtfertigung nach der DSGVO voraus, verlangt aber vom Dateninhaber, dies zu prüfen. Kann der Dateninhaber nutzungsgenerierte Daten mit Bezug zu anderen Personen als dem Nutzer nicht datenschutzkonform dem Nutzer zugänglich machen oder auf Wunsch des Nutzers einem Dritten weitergeben, muss der Dateninhaber nach der DSGVO den Zugang bzw. die Weitergabe verweigern. Für Dateninhaber ergibt sich daraus die Notwendigkeit, für jedes Datum zu prüfen und zu bestimmen, ob es sich um ein personenbezogenes oder nicht personenbezogenes Datum handelt. Da in der industriellen Praxis die faktische Abgrenzung zwischen personenbezogenen Daten und nicht personenbezogenen Daten (etwa bei „Mixed Data Sets") mit großer Rechtsunsicherheit verbunden ist, besteht mit Blick auf Kapitel II des Data Act die Gefahr, dass der „Dateninhaber“ einem Dritten unbewusst Zugang zu personenbezogenen Daten, die nicht den Nutzer betreffen, verschafft, ohne dass ein solcher von der DSGVO legitimiert wäre; wenn andererseits Daten

[4] Datenwirtschaft in Deutschland – Wo stehen die Unternehmen in der Datennutzung und was sind ihre größten Hemmnisse?“, IW-Studie im Auftrag des BDI, Februar 2021, abrufbar unter: https://bdi.eu/media/publikationen/?publicationtype=Studien#/publikation/news/datenwirtschaft-in-deutschland/.

fälschlicherweise als personenbezogene Daten eingestuft werden und der Dateninhaber daraufhin der Zugang aus Gründen des Datenschutzes verweigert wird, droht ein Verstoß gegen die Pflichten des Data Act zur Zugangsgewährung. Bei Verstößen können sowohl nach dem Data Act als auch der DSGVO jeweils empfindliche Sanktionen gegen den Dateninhaber bzw. Verantwortlichen verhängt werden. Dieses Spannungsverhältnis führt bei „Dateninhabern", die zugleich Verantwortliche nach der DSGVO sind, dazu, dass für jedes einzelne Datum verbindlich bestimmt werden müsste, ob ein Personenbezug vorliegt, um die Verpflichtungen aus dem Data Act und der DSGVO erfüllen zu können. Eine solche definitive Bestimmung eines jeden Datums ist angesichts der bestehenden Rechtsunsicherheit, wann bei einem Datum (noch) ein Personenbezug vorliegt, praktisch nicht möglich. Dies gilt insbesondere auch vor dem Hintergrund der bestehenden Unsicherheiten, wie personenbezogene Daten anonymisiert und nicht nur pseudonymisiert werden können; auch pseudonymisierte Daten unterfallen der DSGVO als personenbezogene Daten, wohingegen anonymisierte Daten von der DSGVO ausgenommen sind. Im Übrigen würde eine definitive Klassifizierung von Daten als nicht-personenbezogene oder personenbezogene Daten, selbst wenn sie möglich wäre, einen immensen Personal- und Zeitaufwand erfordern, der insbesondere für KMU praktisch nicht leistbar ist. Des Weiteren würden sich im Hinblick auf die Überprüfbarkeit einer solchen Klassifizierung im Sinne der Überprüfbarkeit der Wahrung von Anforderungen aus dem Data Act einerseits und der DSGVO andererseits eine Vielzahl von ungeklärten, aber für die Praxis unerlässlichen Fragen ergeben, z. B.:

- Gäbe es nutzerseitig Ansprüche auf ein stufenweises Vorgehen, wonach zunächst die Klassifizierung und anschließende Offenlegung verlangt werden kann, um dann ggf. weitere Ansprüche aus dem Data Act ableiten zu können?

- Wird für „Dateninhaber" bzw. Verantwortliche nach der DSGVO eine Erweiterung von Aufklärungs- und Einwilligungsbögen notwendig?

- Wie soll über die Einhaltung von Anforderungen der DSGVO und des Data Act informiert werden (beispielsweise bei der Patientenaufklärung)?

Ohne praktikable Kriterien zur eindeutigen und rechtssicheren Einstufung von Daten als personenbezogen oder nicht personenbezogen sollte im Data Act klargestellt werden, dass der Datenzugangsanspruch des „Nutzers" aus Kapitel II keinen Rechtsanspruch zur Anforderung von personenbezogenen Daten anderer Betroffener begründet. Denn der derzeitige Wortlaut von Art. 4 Abs. 5 bzw. Art. 5 Abs. 6 des Data Act sieht vor, dass es dem für die Datenverarbeitung Verantwortlichen (Dateninhaber) obliegt, nach der DSGVO zu beurteilen, dem Nutzer Zugang zu den personenbezogenen Daten

anderer betroffener Personen zu gewähren. In derartigen Fällen ist der genaue Mechanismus zwischen den Portabilitätsrechten nach Art. 20 DSGVO einerseits und den Portabilitätsrechten nach Art. 4 und 5 des Data Acts noch nicht ausreichend geklärt. Dies gilt auch für Auskunftsrechte in Situationen, in denen die Rechte Dritter als Betroffene berührt werden.

Daneben benötigen Unternehmen verlässliche und zugleich praktikable Orientierungshilfen bei der Anwendung und Auslegung der DSGVO. Dies gilt exemplarisch für Orientierungshilfen hinsichtlich der Anforderungen für eine datenschutzkonforme Anonymisierung personenbezogener Daten. Für die deutsche Industrie steht außer Frage, dass die in der DSGVO normierten Regelungen und die grundrechtlich geschützten Freiheiten, insbesondere das Recht auf informationelle Selbstbestimmung des Einzelnen, wichtige Grundpfeiler für das hohe Datenschutzniveau ausmachen, das Europa im internationalen Vergleich vorweisen kann. Deshalb haben viele Industrieunternehmen ein großes Interesse daran, in deutlich größerem Maße mit anonymisierten Daten zu arbeiten. Mit Blick auf die legislativen Vorgaben ist zu konstatieren, dass die DSGVO keine konkreten Vorgaben zur Anonymisierung personenbezogener Daten enthält und der Data Act die bereits bestehenden Unsicherheiten in der Praxis weiter verschärfen wird. Aufgrund der hieraus resultierenden Rechtsunsicherheit und in Ermangelung einheitlicher Standards nehmen Unternehmen derzeit häufig von diesem Vorhaben Abstand. In der Studie des IW Köln „Datenwirtschaft in Deutschland“ gaben 73 Prozent der Unternehmen „fehlende Standards bei der Anonymisierung personenbezogener Daten“ als Hemmnis für eine stärkere wirtschaftliche Nutzung von Daten an.[5] Um das wirtschaftliche Potenzial anonymisierter Daten nutzen zu können und gleichzeitig das hohe europäische Datenschutzniveau aufrechtzuerhalten, sind aus Sicht des BDI rechtssichere und zugleich praktikable Vorgaben, etwa über die Möglichkeit von Verhaltensregeln („Code-of-Conduct“) gem. Art. 40 DSGVO, für eine datenschutzkonforme Anonymisierung personenbezogener Daten von zentraler Bedeutung. Entsprechende Vorgaben sollten in enger Abstimmung und Zusammenarbeit mit der Industrie entwickelt werden und auf bewährte Verfahren aufbauen.[6]

1.2. Definitionen

Ein grundsätzliches Problem des Kommissionsvorschlags besteht darin, dass zentrale Begrifflichkeiten entweder gar nicht, oder nur wenig trennscharf definiert werden. Der Data Act-E lässt insofern erheblichen

[5] Datenwirtschaft in Deutschland – Wo stehen die Unternehmen in der Datennutzung und was sind ihre größten Hemmnisse?“, IW-Studie im Auftrag des BDI, Februar 2021, abrufbar unter: https://bdi.eu/media/publikationen/?publicationtype=Studien#/publikation/news/datenwirtschaft-in-deutschland/.

[6] Vgl. hierzu BDI-Leitfaden „Anonymisierung personenbezogener Daten“, 2020, abrufbar unter: https://bdi.eu/publikation/news/anonymisierung-personenbezogener-daten/.

Interpretationsspielraum über den Anwendungsbereich und die praktische Reichweite vieler Regelungen, was zu großer Unsicherheit in der Anwendungspraxis führt. Die Definitionen in Art. 2 DA-E bergen aus industrieller Perspektive die Gefahr, zu mehr Rechtsunsicherheit und somit zu weniger Wertschöpfung zu führen. Dafür sollten die zentralen Definitionen nicht nur beiläufig in den Erwägungsgründen erwähnt, sondern direkt in Art. 2 DA-E präzisiert werden.

Art. 2 Nr. 1 DA-E „Daten“: Die Definition von „Daten“ ist denkbar weit und mit Blick auf die zahlreichen Vorgaben – insbesondere bei der Datenbereitstellungspflicht in Kapitel II – sehr unpräzise. Schließlich sind die in Maschinen gewonnenen Daten und dann erzeugten Dateien keinesfalls homogen. Daten, die von Industriemaschinen stammen, können sich in Bezug auf die Verarbeitung (Rohdaten vs. analysierte oder verarbeitete Daten), die Preisgabe von Geschäftsgeheimnissen und Know-how sowie die kommerzielle und technische Durchführbarkeit ihrer Bereitstellung unterscheiden. Unklar ist auch, wann die Schwelle zu den „aus diesen Daten abgeleitete[n] oder gefolgerte[n] Informationen“ (Erwägungsgrund 14) vorliegen, die dem Data-Act nicht unterliegen.

Die vorliegende Definition wird zu großer Unsicherheit in der Anwendungspraxis führen, welche (nicht-)personenbezogenen Daten etwa von den Datenzugangsansprüchen des Kapitel II erfasst sind. Damit die von der EU-Kommission intendierte positive Wirkung für eine faire Datenallokation überhaupt eintreten kann, darf eine solche Differenzierung nicht den Unternehmen selbst überlassen werden. Um Praktikabilität und Rechtssicherheit aller Akteure zu gewährleisten, muss der Data Act eine differenzierte Behandlung von „Daten“ vorsehen, wobei die Art der Daten sowie die Durchführbarkeit und die Nebeneffekte ihrer Bereitstellung (z. B. in Dateien oder Datenbanken) zu berücksichtigen sind.

Es muss klar bestimmt sein, ob lediglich Rohdaten erfasst sind, und lediglich vom „Dateninhaber“ tatsächlich für seine eigenen Geschäftsvorfälle verwendete Daten betroffen und keine flüchtigen Daten von der Definition umfasst sind. Zudem muss sichergestellt werden, dass sich keinerlei (Gewährleistungs- und/oder Haftungs-) Ansprüche aufgrund ihrer Beschaffenheit ergeben (data „as it is“).

Art. 2 Nr. 2 und 3 DA-E „Produkt“ und „verbundener Dienst“: Es bleibt unklar, welche Komponenten (bspw. Sensoren) und Funktionen eines physischen Assets unter die Definition eines Produktes fallen, insbesondere unter Berücksichtigung der begleitenden Erwägungsgründe 14 und 15. Bei industriellen Anwendungen können einzelne Komponenten nicht spontan Daten sammeln, sondern nur aufgrund ihrer speziellen und individuell auf den Anwendungsfall zugeschnittenen Konfiguration durch den jeweiligen Nutzer bzw. den von ihm beauftragten Engineering-Anbieter. Aus Erwägungsgrund 15 folgt jedoch gerade, dass Produkte, die relevante Daten

nur auf der Grundlage menschlicher Eingaben („human input“) erfassen, nicht in den Anwendungsbereich des Data Act fallen. Vor diesem Hintergrund wäre daher wünschenswert, dass (1) das zusätzliche Erfordernis der „menschlichen Eingabe" in die Produktdefinition und (2) industrielle Anwendungen (etwa industrielle Steuerungen sowie industrielle PCs) in die Beispiele des Erwägungsgrunds 15 klarstellungshalber aufgenommen werden. Gerade industrielle Komponenten können ihre Funktionen nur auf der Grundlage bestimmter menschlich eingegebener Konfigurationen des Nutzers erfüllen. Darüber hinaus wäre eine Klarstellung dahingehend wünschenswert, ob die einzelne Komponente aufgrund ihrer Konstruktion bereits in der Lage sein muss, die technischen Anforderungen eigenständig zu erfüllen, oder ob es ausreicht, dass die technischen Anforderungen im Zusammenspiel mit weiteren selbstständigen Modulen erfüllt werden. Beispielsweise stellt ein Industrieregler nicht standardmäßig eine eigene Netzwerkverbindung her, sondern kann das nur, wenn der Nutzer ein zusätzliches Netzwerkmodul anschließt. Ferner ist unklar, wessen Perspektive bei der Beurteilung bei den einzelnen Voraussetzungen des Art. 2 Nr. 2 DA-E maßgeblich sein soll. Hier ist eine Klarstellung notwendig, weil dies unmittelbar Auswirkungen auf Kapitel II und eine etwaige Datenbereitstellungspflicht hätte. Des Weiteren ist die Definition von „Verbundener Dienst“ in Art. 2 Nr. 3 dringend zu präzisieren. Angesichts der Tatsache, dass der Schwerpunkt des Artikels auf den Produktherstellern sowie ihren mit den Produkten angebotenen Dienstleistungen liegt, sollten auch lediglich die physischen Produkte sowie ihre Kernfunktionen von ihm erfasst werden. Andernfalls würde praktisch jede Art von „verbundenen Diensten“ (Dienstleistung) von jedem Marktteilnehmer unter den Anwendungsbereich fallen. Datendienste, die zwar Daten eines Produkts nutzen, aber nicht direkt mit dem Produkt verknüpft oder verkauft werden, sollten demnach aus dem Anwendungsbereich herausgenommen werden.

Dem Legislativvorschlag fehlt die Definition für das „konkurrierende Produkt“. Dies wird etwa in Erwägungsgrund 35 genannt und ist für die Wirtschaft/den fairen Wettbewerb von großer Bedeutung, da etwa Art. 6 Abs. 2 e) DA-E diesbezügliche Vorgaben enthält. In Ermangelung einer Definition bleibt unklar, ob mit dem „konkurrierenden Produkt“ lediglich Produkte im Sinne des Art. 2 Abs. 2 DA-E, folglich nur körperliche und bewegliche Gegenstände gemeint sind oder das Begriffsverständnis über Art. 2 Abs. 2 DA-E hinaus auch „verbundene Dienste“, d. h. Software und datengetriebene Services erfasst. Das Verbot, die vom Dateninhaber erhaltenen Daten für die Entwicklung eines konkurrierenden Produkts zu verwenden, sollte nicht nur für Produkte, sondern auch für damit verbundene Dienste und virtuelle Assistenten gelten. Es gibt keinen offensichtlichen Grund, den Geltungsbereich eines solchen Verbots in Art. 6 Abs. 2e DA-E auf Produkte zu beschränken, während die Daten auch von verbundenen Diensten und virtuellen Assistenten bezogen werden können. Ein an Art. 2 Abs. 2 DA-E angelehntes Verständnis birgt die Gefahr, dass Konkurrenten mittelbar davon profitieren könnten, indem sie aufgrund der ausgeleiteten Daten

(softwaregetriebene) Produkte/Services entwickeln, die dann wiederum in direkter Konkurrenz zum ursprünglichen Produkt/Service treten.

Art. 2 Nr. 5 und 6 DA-E „Nutzer“ und „Dateninhaber“: Der Legislativvorschlag vermittelt den Eindruck eines sehr vereinfachten, dichotomen und nicht praxisnahen Verständnisses der Beziehungen von Herstellern und Kunden in vielen Bereichen der Industrie. Der Entwurf lässt unberücksichtigt, dass in multilateralen und -direktionalen Wertschöpfungsnetzwerken auch – und in vielen Branchen sogar in aller Regel – der „Nutzer“ eines physischen Assets der „Dateninhaber“ ist. Soweit der DA-E einleitend also feststellt, dass „the manufacturer or designer of a product or related service typically has exclusive control over the use of data generated by the use of a product or related service” (vgl. S. 13 des DA-E), kann dies für den industriellen Bereich nicht in allen Fällen Geltung beanspruchen. Die Gleichung „Hersteller („manufacturer“) = Dateninhaber („data holder“)“ wird der industriellen Realität in vielen Fällen nicht immer gerecht. Vor diesem Hintergrund muss eine Präzisierung der Begriffe Nutzer („user“) und Dateninhaber („data holder“) entsprechend der industriellen Praxis erfolgen. Präzisierungsbedarf besteht darüber hinaus dahingehend, dass der „Nutzer“ in Anlehnung an Erwägungsgrund 18 über ein entsprechendes Vertragsverhältnis definiert wird. Dies kommt in der Formulierung gem. Art. 2 Nr. 5 DA-E durch die Formulierung „oder eine Dienstleistung in Anspruch nimmt“ nicht deutlich genug zum Ausdruck, sondern sollte eher durch „oder eine *vertragliche* Dienstleistung in Anspruch nimmt“ ersetzt werden. Um Rechtssicherheit zu gewährleisten, sollte zudem klargestellt werden, dass es mehrere „Nutzer“ geben kann.

Auch mit Blick auf die Definition des „Dateninhabers“ sind Präzisierungen erforderlich. Dabei erscheint die Definition des Dateninhabers zumindest teilweise zirkulär, da der DA-E den zu definierenden Begriff des Dateninhabers mit „the right or obligation, in accordance with this Regulation (…) to make available certain data“ (vgl. Art. 2 Nr. 6 DA-E) selbst definiert. So bleibt derzeit unklar, ob der „Dateninhaber“ derjenige ist, der das Produkt herstellt (was in vielen Fällen an der industriellen Praxis vorbeigeht) oder vielmehr derjenige, der die Kontrolle über die Daten – und somit die tatsächlichen Einwirkungsmöglichkeiten – hält. Wir sprechen uns daher für eine Präzisierung des Dateninhabers als desjenigen aus, der faktisch über die Daten verfügt und weisen darauf hin, dass diese Rolle in vielen industriellen Anwendungsfällen gleichzeitig von dem Nutzer der fraglichen Komponente ausgefüllt wird. Mit Blick auf den Fahrzeugmarkt stellt sich bspw. die Frage, wer bei sog. „Third Party Apps“, die im Produkt „Fahrzeug“ angeboten werden und Daten erzeugen, als „Dateninhaber“ anzusehen ist.

Art. 2 Nr. 13 DA-E: Der Begriff „Dienstart“ nimmt für die Abgrenzung des Anwendungsbereichs der in Kapitel VI vorgesehenen Regelungen eine zentrale Bedeutung ein. Allerdings lässt die Definition zu großen Interpretationsspielraum, da der ihr zugrundeliegende Begriff

„Dienstmodell“ nicht genauer spezifiziert wird und auch im IT-Bereich keine einheitliche Definition für „Dienstmodell“ existiert.

Der DA-E verzichtet auf eigene Definitionen der Begriffe „Hersteller“ („manufacturer“) bzw. „Diensteanbieter“ („service provider“), obgleich Hersteller und Diensteanbieter gleichermaßen von dem Anwendungsbereich des Data Act erfasst sein sollen, vgl. Art. 1 Nr. 2 a) DA-E.

Zu Kapitel II: Datenweitergabe von Unternehmen an Verbraucher und zwischen Unternehmen

Wie die EU-Kommission selbst in Erwägungsgrund 28 richtigerweise betont, ist bei gesetzlichen Datenzugangsregelungen das Spannungsverhältnis zwischen den berechtigten Interessen des „Dateninhabers“ und des „Nutzers“ bzw. „Datenempfängers“ gleichermaßen zu berücksichtigen. Bei jedem legislativen Eingriff muss berücksichtigt werden, dass nicht-personenbezogene Industriedaten auf vorherigen Investitionen in die Erhebung, Speicherung, Strukturierung und (Vor-)verarbeitung der Daten beruhen und einen wirtschaftlichen Wert besitzen. Die Entwicklung und Implementierung von vernetzten Industrieanlagen erfordert hohe Investitionen und ist Know-how-intensiv. Eine Industrie 4.0-Lösung setzt sich aus Sensoren, Aktoren, Konnektivität, Datenkonzepten und oft kundenspezifischen Serviceangeboten zusammen. Daten sind kein freies Gut und Märkte müssen ausreichende Anreize für Investitionen in vernetzte Maschinen und datenbasierte Dienste bieten. Der rechtliche Rahmen muss diese Investitionen schützen. In vielen industriellen B2B-Anwendungsfällen ist der „Dateninhaber“ als KMU zu klassifizieren. Die technische und rechtliche Verpflichtung, Daten zur Verfügung zu stellen, wird eine erhebliche Belastung für solche Unternehmen darstellen – insbesondere für diejenigen, die in kleinen Mengen produzieren und nicht von Größenvorteilen profitieren können. Es ist deshalb zu begrüßen, dass Kleinst- und Kleinunternehmen von den Verpflichtungen des Kapitels II ausgenommen werden sollen.

Der Legislativvorschlag wählt einen breiten, horizontalen Ansatz, ohne die unterschiedlichen Anforderungen und Bedarfe unterschiedlicher Sektoren im B2B- und B2C-Verhältnis hinreichend zu berücksichtigen. Der im Data Act vorgeschlagenen „one-size fits all“-Ansatz wird diesen heterogenen Marktverhältnissen nicht gerecht. So werden etwa (vor-) vertragliche Informations- und Transparenzpflichten auch auf den B2B-Kontext erstreckt, ohne dass hierbei ein besonderes Regelungsbedürfnis ersichtlich wird. Gleichzeitig enthält der Data Act viele Überlegungen zur Übertragung von Daten an, ohne dass hinreichend sichergestellt werden kann, dass die Daten an den berechtigten Nutzer/die berechtigte Nutzerin weitergegeben werden. Die Weitergabe bedarf weiterer technischer Spezifikationen, die nicht ungeregelt bleiben sollten, um die Qualität der Daten und die Sicherheit der

Daten sicherzustellen. Gleichzeitig sollte der Data Act die Besonderheiten bestimmter Bereiche berücksichtigen und bspw. für Medizinprodukte bestimmte Abgrenzungen beachten, die sich aus dem Medizinprodukterecht (MDR) ergeben.

Mit Blick auf die Produktdesignanforderungen und die Datenzugangs- und Übertragungsregeln ist unklar, inwiefern sich diese Anforderungen auf bereits auf dem Markt befindliche Produkte erstrecken. Aufgrund der enormen Kosten einer etwaigen nachträglichen Veränderung der Produkte muss klargestellt werden, dass Kapitel II nur auf Neuprodukte Anwendung findet.

2.1. Access-by-design

Damit der Data Act zu mehr datengetriebener Wertschöpfung führt, müssen Rechtsunsicherheiten, die sich aus zusätzlichen Produktanforderungen nach dem „access-by-design"-Prinzip gem. Art. 3 DA-E ergeben, verhindert werden. Gem. Art. 3 Abs. 1 DA-E müssen Hersteller ihre Produkte so gestalten, dass der Zugang zu den durch Nutzung des Produkts generierten Daten standardmäßig ermöglicht werden kann. Insbesondere für KMU ergeben sich hieraus erhebliche Anforderungen an den Hersteller, die nicht nur das Produkt, sondern auch Transparenz- und Informationspflichten etwa über die Art und den Umfang der Datenerhebung betreffen. Diese erheblichen Eingriffe ins Produktdesign dürfen nur für neue Produkte gelten und müssen über entsprechende Vorlaufzeiten für die Produktion und Entwicklung der entsprechenden Produkte berücksichtigt werden, zumal derartige Eingriffe ggf. eine erneute Produkt-Zertifizierung mit einem Prozesszeitraum von mindestens einem Jahr erforderlich macht.

Derartige Eingriffe in die Produktbauart könnten im Übrigen die Funktionalitäten der Produkte ganz erheblich gefährden. Würde z. B. eine industrielle Steuerung nun so gestaltet werden müssen, dass sie aus sich heraus den Datenzugang gewähren muss – und nicht über zusätzliche Module – könnten besondere Eigenschaften einer Steuerung (Deterministik, Äquidistanz) leiden. Gerade weil sich industrielle Steuerungen auf der I/O-Ebene ganz auf ihre Funktion fokussieren müssen, werden sie bewusst ausschließlich mit Minimalfunktionen, die zu einer Inbetriebnahme der Steuerung erforderlich sind, ausgestattet. Deshalb sollte der Zugang nur auf diejenigen Daten beschränkt werden, die überhaupt ausgeleitet werden: So existieren bisweilen Daten, die zwar bei der Nutzung anfallen, aber – zumindest bislang – im Produkt verbleiben und auch nicht verwertet werden, weil sich hierfür zum jetzigen Zeitpunkt noch kein sinnvolles Anwendungsszenario ergibt. Wenn undifferenziert sämtliche durch die Nutzung des Assets anfallenden Daten vom Data Act betroffen wären, würde das den nicht intendierten Anreiz setzen, Assets so wenig Daten wie möglich generieren zu lassen. Wären auch diese Daten von der zwingenden Zugriffsmöglichkeit umfasst, wären Hersteller ggf. gezwungen,

entsprechende Schnittstellen, etc. einzuarbeiten (Investitionen) oder das Produkt technisch derart zu verändern, dass eine Datennutzung niemals in Betracht kommen wird, selbst wenn sich in Zukunft ein Anwendungsszenario ergeben hätte. Das gilt insbesondere für batteriebetriebene low-power IoT-Produkte, deren sehr limitiertes Energiebudget für mehrere Jahre (typischer Weise fünf bis zehn Jahre) ausreichen muss. Datenübertragungen außerhalb des spezifizierten Anwendungsfalls können die Lebenszeit dieser Produkte drastisch verkürzen. Zudem würden datenbasierte innovative Zusatzangebote, die zuvor Investitionen für die Datengenerierung erfordern, verhindert werden. Das liefe dem Ziel des Data Acts, datenbasierte Wertschöpfung zu fördern, diametral entgegen.

Präzisierungsbedarf besteht weiterhin dahingehend, dass die bei ihrer Nutzung erzeugten Daten standardmäßig für den Nutzer einfach, sicher und direkt zugänglich sind („data access by design“ bzw. „by default“) und somit in Einklang sowohl mit den Datensicherheitsvorgaben aus den Art. 25 und 32 DSGVO als auch mit den von der EU-Kommission forcierten Produktregulierungen wie der Funkanlagenrichtlinie (RED) und der technischen Standardisierung zu mehr Daten- und Cybersicherheit gebracht werden sollen.

2.2. Das „Dreiecksverhältnis“ aus Dateninhaber, Nutzer und Drittem

Die EU-Kommission wählt hinsichtlich der Datenzugangs- und Datenportabilitätsrechte von IoT-Produktdaten in Kapitel II des Data Acts mit dem „Dateninhaber“, dem „Nutzer“ und dem „Dritten“ ein Modell, das komplexe industrielle Wertschöpfungsketten nicht hinreichend abbildet. Die hier gewählte stark vereinfachte Annahme der EU-Kommission über Wertschöpfungsketten hindert den Data Act sein volles Potenzial datengetriebener Wertschöpfung freizusetzen. In der Industrie 4.0 arbeiten eine Vielzahl an Akteuren (Maschinenhersteller, Software- und Komponentenanbieter sowie Kunden) zusammen und teilen Daten untereinander zu gegenseitigem Vorteil.

Insbesondere im Zusammenspiel mit den sehr unscharfen Definitionen in Kapitel I lässt der Data Act viele Fragen offen, wie der hier gewählte Ansatz in diesem industriellen Kontext funktionieren soll. So fokussiert sich der Ansatz einseitig auf die Rolle des Asset Users bzw. Betreibers und lässt dabei die Rolle des Komponentenproviders unberücksichtigt bzw. scheint diese unter den Asset Provider bzw. Ausrüster zu subsumieren, der ebenfalls ein Interesse an den Nutzungsdaten seiner Komponente besitzt, über die er jedoch in der industriellen Praxis i.d.R. nicht verfügt. Hier zeigt sich exemplarisch die fehlgeleitete Grundannahme des Data Act, dass im industriellen Bereich der Hersteller eines Produkts als Dateninhaber zu qualifizieren ist. Im Gegenteil ist der (Komponenten-)Hersteller in der Regel von einer Nutzung der durch seine Komponenten generierten Daten technisch

und aufgrund vertraglicher Bestimmungen abgeschnitten. Kapitel II suggeriert (auch unter Berücksichtigung des einleitenden Explanatory Memorandum), dass der IoT-Asset-Provider faktisch als „Dateninhaber“ anzusehen ist. Dieses Verständnis geht jedoch in vielen Fällen an der industriellen Praxis vorbei, weil hier i.d.R. der „Nutzer“, also der Kunde, der das Produkt nutzt, auch über die Nutzungsdaten verfügt.

Unklar bleibt auch, wie weitreichend die in Art. 4 Abs. 1 DA-E genannte Pflicht, „die bei der Nutzung eines Produktes oder verbundenen Dienstes erzeugten Daten“ bereitzustellen, zu verstehen ist. Müssen bspw. in Fällen, in denen mit den Daten des Nutzers KI-Algorithmen trainiert werden, auch die Ergebnisse an den Nutzer herausgegeben werden? Das würde die Leistung des Algorithmen-Entwicklers urheber- oder ggf. patentrechtlich entwerten. Unklar ist weiterhin, ob die Pflicht zur Bereitstellung der Daten zu einer Pflicht führt, entsprechende Daten zu erheben, auch wenn diese in der Standardkonfiguration nicht erhoben werden.

2.3. Geschäftsgeheimnisschutz

Vertrauen zwischen unterschiedlichen Akteuren ist die Basis, damit eine datenbasierte Wertschöpfung erreicht werden kann. Industrielle Datenteilung im B2B-Kontext ist hinsichtlich des Schutzes von Geschäftsgeheimnissen sowie der betriebswirtschaftlichen Aspekte sehr sensibel, weshalb ein spezifischer Ansatz angestrebt werden sollte, um Rechtsunsicherheiten zu vermeiden. Ein für den „Dateninhaber“ zentrales Interesse liegt in dem Schutz seiner Geschäftsgeheimnisse. Anders als im Verhältnis zur DSGVO greift Kapitel II jedoch das Verhältnis zum geltenden Geschäftsgeheimnisschutz auf, indem derartige Daten über die Datenzugangsansprüche dem Einflussbereich des Dateninhabers entzogen werden. Um die hierdurch zu befürchtenden negativen Folgen für die Innovations- und Investitionsbereitschaft zur Generierung und Aufbereitung von Daten entgegenzuwirken, fordert der BDI, dass der Schutz sensibler Informationen, einschließlich Geschäftsgeheimnissen, generell von der Verpflichtung zum Datenaustausch ausgenommen werden oder zumindest mit dem auf Geschäftsgeheimnisse beschränkten Recht der offenlegenden Seite einhergehen, deutlich weitergehende Sicherungsmaßnahmen (etwa technischer Art) fordern zu dürfen, die aber ggf. einer freien Nutzung der Daten durch den Nutzer entgegenstehen. Eine solche Ausnahme würde auch die drohenden Inkonsistenzen mit Blick auf Kapitel III (Art. 8 Abs. 6 DA-E) beseitigen. Während Art. 8 Abs. 6 DA-E die Offenlegung von Geschäftsgeheimnissen vom Grundsatz des Datenzugangsanspruchs grundsätzlich ausnimmt, weicht Kapitel II hiervon ab. Insbesondere mit Blick auf etwaige weitere sektorale Datenzugangsregulierungen bedarf es hier einer einheitlichen Festlegung auf den Grundsatz des Geschäftsgeheimnisschutzes und dessen konkreten Umfang.

Nach der Konzeption des Art. 4 Abs. 3 bzw. Art. 5 Abs. 8 DA-E werden „Dateninhaber“ zukünftig verpflichtet, auch solche Daten grundsätzlich an den „Nutzer“ oder auch von ihm beauftragte Dritte weiterzugeben. Das Geschäftsgeheimnis verlässt insofern den Einflussbereich des Dateninhabers und dieser muss selbst mit dem „Nutzer“ oder „Dritten“ angemessene Schutzmaßnahmen vereinbaren. Um Missbrauch zu verhindern, sieht der Entwurf des Data Act zwar zahlreiche Nutzungsbeschränkungen für Weiterverwender vor, etwa das Verbot, die Daten für andere Zwecke oder für die Entwicklung von Konkurrenzprodukten zu nutzen. Wie deren Einhaltung kontrolliert, nachgewiesen und durchgesetzt werden soll, bleibt aber völlig offen, da es den Herstellern an hinreichenden Kontrollmöglichkeiten fehlt. Auch bleibt die Beweislastverteilung unklar. Es ist dabei völlig fernliegend, dass bspw. KMU etwaig vereinbarte Audit-Rechte im Rahmen der Kundenbeziehung auch nur im Ansatz wahrnehmen könnten. Dies gilt insbesondere dann, wenn die Daten in internationale Wertschöpfungsketten gelangen. Es bleibt auch ungeklärt, inwiefern derartige Schutzvorkehrungen einseitig auferlegt werden können. So bleibt offen, welche Folgen es hat, wenn „Nutzer“ bzw. „Drittempfänger“ der Daten der von dem „Dateninhaber“ vorgelegten Vertraulichkeitsverpflichtungs- oder Datennutzungsvereinbarung nicht bzw. nur mit (nicht-akzeptablen) Änderungen zustimmen.

Da der Grundsatz der Datenbereitstellung sogar gegenüber Wettbewerbern unter Berücksichtigung der kartellrechtlichen Regelungen gem. Art. 101, 102 AEUV gilt, sind klare Regularien zum Schutz der Dateninhaber notwendig, um hemmende Effekte bei Innovations- und Investitionsbereitschaft zu vermeiden. Hierzu zählt, dass der Dateninhaber vom Nutzer oder Dritten Schadenersatz verlangen kann, wenn die bereitgestellten Daten missbraucht wurden – z. B. für die Entwicklung eines konkurrierenden Produkts. Das Recht auf eine bloße Löschung der Daten ist hierbei nicht ausreichend. Ansonsten besteht die Gefahr, dass der Data Act sein Ziel, Investitionen in datengenerierende Produkte zu fördern, untergräbt. Ebenso ist unklar, wie Auftragsforschung im Kontext des Data-Acts zu bewerten ist. Für die deutsche Industrie stellt die Auftragsforschung einen wichtigen Baustein dar und sollte daher wie Forschung im eigenen Unternehmen behandelt werden, um einen wirksamen Schutz von Geschäftsgeheimnissen sicherzustellen.

2.4. Vertragliche Nutzung von nicht personenbezogenen Daten gem. Art. 4 Abs. 6 DA-E

Mit Blick auf die Rahmenbedingungen der vertraglichen Ausgestaltung nach Art. 4 Abs. 6 DA-E für nicht-personenbezogene Daten ist unklar, welche Auswirkungen etwa eine Beendigung eines solchen Vertrages zwischen „Dateninhaber“ und „Nutzer“ nach sich zieht. Wenn das IoT-Produkt beispielsweise vom Nutzer an einen Dritten weiterverkauft wird, bedarf es einer neuerlichen vertraglichen Einigung gem. Art. 4 Abs. 6 DA-E. Gerade

in industriellen B2B-Verhältnissen kann der „Nutzer“ dabei eine starke Verhandlungsposition haben und andere Nutzungsbedingungen gegenüber dem „Dateninhaber“ einfordern. Deshalb bedarf es einer Klarstellung, dass die dem Dateninhaber einmal überlassenen Daten bei diesem verbleiben können.

Zusätzlich ist es bei IoT-Produkten und verbundenen Diensten mit einer angenommenen Lebensdauer von fünfzehn Jahren unmöglich, schon beim Kauf die im Produktlebenszyklus zu erwartende Datennutzung zum Zeitpunkt des Vertragsschlusses vorauszusehen bzw. unveränderlich zu lassen. Nachträgliche Anpassungen der Datennutzungsvereinbarung müssen demzufolge möglich sein. Zudem müssen die Datennutzungsvereinbarungen hinreichend abstrakt sein dürfen, um Softwareupdates „over-the-air“, die neue Datenpunkte erzeugen aber den vereinbarten Zwecken dienen, ohne vertragliche Anpassungen durchführen zu können. Andernfalls würden Grundsätze der modernen, innovativen, inkrementellen Produktentwicklung durch administrative Aufwände verhindert werden.

Zu Kapitel III: Pflichten der Dateninhaber, die rechtlich verpflichtet sind, Daten bereitzustellen

Horizontale Modalitäten, unter welchen Bedingungen gesetzlich zur Datenbereitstellung verpflichtete Unternehmen eine solche vorzunehmen haben, erscheinen sinnvoll, um einen kohärenten Rahmen bei etwaigen sektorspezifischen Datenzugangsansprüchen zu gewährleisten.

Die Beschränkung des Anspruchs auf angemessenen Kostenersatz gegenüber KMU auf die direkten Kosten bedeutet eine massive Benachteiligung von Großunternehmen, die sich im Zweifel einer großen Anzahl von Herausgabeansprüchen ausgesetzt sehen, ohne dafür ausreichenden Kostenersatz zu erhalten. Problematisch erscheint insbesondere, dass eine solche Beschränkung auch in Konstellationen auftritt, in denen KMU selbst als „Dateninhaber“ auftreten. Es ist dabei nicht ersichtlich, warum in einer vertraglichen Datenzugangsregelung zwischen KMU kein Gewinn erzielt werden kann. Eine solche Bestimmung ginge über den Telos von Art. 9 Abs. 2 DA-E hinaus.

Wünschenswert wäre zudem eine ausdrückliche Klarstellung, wie sich Kapitel III zum bereits existierenden (z.T. sektorspezifischem) Gemeinschaftsrecht verhält, das Regelungen für die Vergütung des Datenzugangs trifft (wie z.B. die PSI-Richtlinie oder die FahrgastrechteVO). Art. 40 Abs. 1 DA-E ist insoweit nicht hinreichend deutlich.

Zu Kapitel IV: Missbräuchliche Klauseln in Bezug auf den Datenzugang und die Datennutzung zwischen Unternehmen

Um das große Innovationspotenzial der europäischen Datenwirtschaft zu heben, müssen Daten freiwillig geteilt werden können. Nach dem Grundsatz der Vertragsfreiheit müssen Unternehmen im Rahmen der gesetzlichen Bestimmungen frei entscheiden können, mit wem und unter welchen Bedingungen sie selbst erhobene nicht-personenbezogene Daten teilen, sei es durch vertragliche Vereinbarungen, durch privatwirtschaftliche Datenpartnerschaften oder durch einen freiwilligen Open-Data-Ansatz. Über die gesamte Industrie hinweg gibt es zahlreiche gute Beispiele für datengetriebene Geschäftsmodelle, die auf Basis von unternehmerischer Initiative und Vertragsfreiheit zum gemeinsamen Vorteil sämtlicher Beteiligter entstanden sind.

Mit dem Data Act greift die EU-Kommission erheblich in die Vertragsfreiheit und die unternehmerische Freiheit ein. Dies ist aus Sicht des BDI vor allem deshalb abzulehnen, weil selbst in mittelständisch geprägten Industriesektoren bislang keine generellen strukturellen Ungleichgewichte identifiziert werden konnten, die den Austausch von Industriedaten zwischen einem Hersteller und seinem Kunden behindern. Die Ausgestaltung datenrechtlicher Nutzungsbestimmungen im industriellen B2B-Bereich lässt sich grundsätzlich am besten durch maßgeschneiderte vertragliche Regelungen zwischen den beteiligten Parteien erreichen. Insofern können Unternehmen privatautonom entscheiden, in welchem Umfang und unter welchen Bedingungen sie ihre Daten untereinander teilen.

Mit der Einführung eines Sonderzivilrechts für Datenverträge ist zu befürchten, dass Datenbeziehungen zwischen Industriepartnern, die in der Praxis bereits gut funktionieren, gefährdet werden und der Data Act insofern zu Rechtsunsicherheiten und Irritationen zwischen den Geschäftspartnern führt. Unklar ist hierbei, ob sich die vertragsrechtlichen Vorgaben auch auf bereits bestehende Verträge auswirken.

Im Data Act sollte daher von Eingriffen in die – meist gut funktionierenden – Geschäftsbeziehungen in komplexen industriellen Datenwertschöpfungsketten abgesehen und genügend Raum für maßgeschneiderte Lösungen gelassen werden. Falls es Ungleichgewichte oder Lücken gibt, sollten diese durch das EU-Wettbewerbsrecht oder sektorspezifische Rechtsvorschriften behoben werden.

<u>Zu den einzelnen Klauseln:</u>

Die Generalklausel des Art. 13 Nr. 2 DA-E führt zu erheblichen Rechtsunsicherheiten. Es bleibt unklar, welche Kriterien zur Feststellung der bewährten Geschäftspraxis beim Datenzugang und bei der Datennutzung („good commercial practice“) bzw. zur Feststellung einer erheblichen

Abweichung („grossly deviates“) heranzuziehen sind und wer diese Kriterien festlegt.

Art. 13 Nr. 3 a) DA-E bestimmt die Missbräuchlichkeit einer Klausel, die die Haftung auf Vorsatz und grobe Fahrlässigkeit beschränkt bzw. die Haftung gänzlich ausschließt. Gleichzeitig bestimmt die Klausel nicht, was Bezugspunkt der Haftung ist.

Zu Kapitel V: Bereitstellung von Daten für öffentliche Stellen und Organe, Einrichtungen und sonstige Stellen der Union wegen außergewöhnlicher Notwendigkeit

Im Bereich B2G-Data Sharing ist für den BDI nicht hinreichend belegt, inwiefern die bisherigen freiwilligen Kooperationen die nunmehr vorgesehenen Zugangsverpflichtungen für Daten „im öffentlichen Interesse“ notwendig machen. Ein strukturelles (Markt-)Versagen, das legislatives Einschreiten in Form einer Zugangsverpflichtung rechtfertigen würde, ist hier weiterhin nicht erkennbar.[7] Nicht zuletzt die COVID-19-Pandemie hat verdeutlicht, dass bereits heute eine Vielzahl von Unternehmen aus den unterschiedlichsten Branchen sehr uneigennützig und erfolgreich mit öffentlichen Stellen kooperieren.

Dem Legislativvorschlag fehlt es in Art. 15 DA-E darüber hinaus an einem expliziten und präzisen Anwendungsbereich, in denen ein obligatorischer B2G-Datenaustausch aufgrund einer „außergewöhnlichen Notwendigkeit“ erforderlich wäre. Die Definitionen eines „öffentlichen Notstands“ und der in Art. 15 a) und b) DA-E und insbesondere eine „bestimmte, gesetzlich ausdrücklich vorgesehene Aufgabe im öffentlichen Interesse“ in Art. 15 c) DA-E sind sehr weit gefasst und bieten Unternehmen keine notwendige Rechtssicherheit, in welchen Konstellationen eine Datenbereitstellungspflicht vorgesehen ist. Selbiges gilt für den Schutz von Geschäftsgeheimnissen gem. Art. 17 Abs. 2 c) DA-E, insbesondere vor dem Hintergrund einer möglichen Weitergabe der Daten an öffentliche Forschungsorganisationen gem. Art. 21 DA-E. Hier bedarf es dringend einer Präzisierung, um ein unionsweit einheitliches Verständnis für die Vielzahl an anspruchsberechtigten öffentlichen Stellen zu gewährleisten. Zudem muss sichergestellt werden, dass von den Unternehmen bereitgestellte Daten nach Ende eines „öffentlichen Notstands“ wieder zu löschen sind.

Mit Blick auf Art. 15 c) DA-E erscheint zudem unklar, welche konkreten Anforderungen an die öffentlichen Stellen im Vorfeld an eine gesetzliche

[7] Dies wurde bspw. auch durch die Europäische Kommission selbst in ihrer Mitteilung aus 2018 (SWD (2018) 125), die entsprechende Guidance im B2B, B2G Bereich ausgibt, bestätigt: „A broad stakeholder dialogue was conducted on the basis of that Communication. It concluded that the issue at stake did not justify horizontal legislative intervention at this stage and that guidance would be more appropriate.“

Inanspruchnahme der Unternehmen gestellt werden. Gerade im Falle unternehmensspezifischer Daten sind die Kriterien, unter denen auf „dem Markt zu Marktpreisen“ ein vergeblicher Datenbereitstellungsersuchen erfolgen soll, nicht hinreichend kalkulierbar.

Neben dem Anwendungsbereich ist es für die Unternehmen zwingend erforderlich, auch die datenschutzrechtlichen und (nicht-)technischen Anforderungen an Sicherheitsvorkehrungen für die Informationssicherheit im Zuge der Datenbereitstellung mit der öffentlichen Stelle zu präzisieren. Um den Schutz der informationellen Selbstbestimmung und der Datensicherheit unternehmensseitig gewährleisten zu können, müssen zudem angemessene Datenbereitstellungsfristen gem. Art. 17 Abs. 1 e) DA-E sichergestellt werden. Schließlich führt bereits eine datenschutzadäquate Pseudonymisierung und Anonymisierung personenbezogener Daten zu einem erheblichen Zeit- und Arbeitsaufwand, der nicht nur in den zeitlichen Fristen zu berücksichtigen, sondern auch über eine angemessene Entschädigung ausgeglichen werden muss.

Schließlich müssten B2G-Datenteilungspflichten zugleich rechtssicher und praktikabel ausgestaltet werden. Dies gilt zunächst mit Blick auf personenbezogene Daten in Form von rechtssicheren und zugleich praktikablen Orientierungshilfen zur hinreichenden Anonymisierung und Pseudonymisierung personenbezogener Daten. Analog zu den Diskussionen im laufenden Verfahren zum Data Governance Act ist in der Anwendungspraxis völlig unklar, welche technischen Maßnahmen zu einer hinreichenden Anonymisierung personenbezogener Daten erforderlich sind. Darüber hinaus sollten entsprechende Verpflichtungen ausschließlich an Dateninhaber („data holder“) gerichtet werden, damit nicht etwaige Datenverarbeiter („data processor“) entgegen ihren vertraglichen Verpflichtungen gezwungen werden, Kundendaten an öffentliche Stellen weiterzugeben.

Zu Kapitel VI: Wechsel zwischen Datenverarbeitungsdiensten

Neben einem hohen Maß an Flexibilität und Skalierbarkeit bieten Cloud-Dienste ihren Kunden eine hohe Benutzerfreundlichkeit. Die einfache Handhabung kann jedoch damit einhergehen, dass die Anwendungen der Kunden tief in das anbieterspezifische (proprietäre) Ökosystem des jeweiligen Cloud Service Providers integriert sind. Dies kann in bestimmten Fällen dazu führen, dass Anbieterwechsel mit signifikanten Hürden verbunden sind.

Der BDI begrüßt mit Blick auf solche Konstellationen das Ziel der EU-Kommission, Anwendern einen Anbieterwechsel zu erleichtern und auf diese Weise die Offenheit des Cloud-Marktes zu erhöhen

Die Maßnahmen, die auf Seiten der Anbieter entsprechender Dienste zur Erreichung dieses Ziels umgesetzt werden sollen, weisen in ihrer Gesamtheit jedoch eine hohe Eingriffstiefe auf, die zudem der technischen Komplexität von Cloud-Lösungen in der Praxis sowie der Heterogenität der am Markt angebotenen Dienste nicht ausreichend Rechnung tragen. Beispielsweise werden Datenverarbeitungsdienste – auch wenn sie die gleiche Funktion erfüllen – in der Regel auf unterschiedliche Weise realisiert, etwa im Hinblick auf Datenformate, Datensemantiken oder Hardwarearchitekturen. Auch berücksichtigt der Kommissions-Entwurf nicht ausreichend den Umstand, dass – je nach Anwendungskontext – die Menge der erzeugten Daten viel zu groß sein kann, um von einem Dienstanbieter mit vertretbarem Aufwand kontinuierlich gespeichert und für einen möglichen späteren Portierungsvorgang bereitgehalten werden zu können. Ein weiteres Beispiel stellt die Ausgestaltung von Kündigungsfristen dar, bei der es einer Differenzierung zwischen hochgradig standardisierten Cloud-Dienstleistungen (mit AGB als Vertragsgrundlage) und komplexen kundenindividuellen Lösungen, denen ein individueller Projektvertrag zugrunde liegt, bedarf. Insgesamt sollten die Anforderungen des Kapitel VI so ausgestaltet werden, dass sie realistischerweise und mit einem vertretbaren wirtschaftlichen Aufwand von Marktteilnehmern aller Unternehmensgrößen umgesetzt werden können.

Der BDI spricht sich vor diesem Hintergrund für ausgewogenere Regelungen unter Berücksichtigung bereits existierender Vorgehensweisen aus, die von Marktteilnehmern im Rahmen der Selbstregulierung entwickelt wurden. Mit der Verabschiedung impraktikabler Anforderungen wäre hingegen das Risiko verbunden, dass bestimmte Cloud-Dienste aufgrund betriebswirtschaftlich nicht vertretbarer Aufwände nicht länger in Europa angeboten werden und Innovationen in diesem Bereich gehemmt werden.

Wichtig ist zudem eine größtmögliche Kohärenz des Data Acts mit anderen europäischen Regulierungsaktivitäten. Dies betrifft beispielsweise den Digital Markets Act, der ebenfalls Anforderungen in Bezug auf den Wechsel zwischen digitalen Diensten und die Portabilität von Daten enthält. Aus diesen überlappenden Vorgaben resultieren offene Fragen, die im weiteren Rechtsetzungsprozess geklärt werden müssen.

Zu Kapitel VII: Schutzvorkehrungen für nicht personenbezogene Daten im internationalen Umfeld

Der Data Act Entwurf sieht in Kapitel VII „Schutzvorkehrungen für nicht-personenbezogene Daten im internationalen Umfeld“ vor, welche die Ansprüche der DSGVO zu spiegeln versuchen. Damit wird dem Schutz von industriellen Daten ein Schutzniveau auferlegt, das normalerweise nur zum Schutz personenbezogener Daten und somit von Grundrechten erforderlich ist.

Internationale Datenströme sind für die Industrie von entscheidender Bedeutung. Der Ansatz der Europäischen Kommission in Kapitel VII des Data Acts stellt einen gezielten Ansatz dar, der auf einen speziellen Fall von grenzüberschreitenden Datenübertragungen abzielt, die sich aus einem Zugangs-Ersuchen einer Nicht-EU-Behörde auf nicht-personenbezogene Daten ergibt. Es bleibt allerdings unklar, wie oft nicht-personenbezogene Daten tatsächlich das Ziel von Anfragen sind, insbesondere wenn man davon ausgeht, dass in den meisten Fällen auch personenbezogene Daten betroffen sind.

Da die Anbieter von Cloud-Diensten verpflichtet sind, potenzielle Anfragen zu überprüfen, muss es klare Leitlinien geben, anhand welcher eine solche Bewertung vorgenommen werden muss. Nur so kann sichergestellt werden, dass kein Nachteil für internationale Datenströme und kein unverhältnismäßiger bürokratischer Aufwand für die Unternehmen entsteht. Zudem würde vermieden, das ungeklärte Fragen des Drittstaatentransfers von personenbezogenen Daten, die sich aus dem Schrems II Urteil ergeben, auch auf den Bereich der nicht-personenbezogenen Daten übertragen werden. Wir begrüßen deshalb, dass die EU-Kommission Bestimmungen in Art. 27 DA-E aufgenommen hat, um zusätzliche Leitlinien für den Überprüfungsprozess bereitzustellen. Damit diese wirksam sind sollten sie auf der Grundlage von Konsultationen mit der Industrie entwickelt und zur Verfügung gestellt werden, bevor der Data Act rechtlich anwendbar wird.

Mehr Klarheit ist auch in Bezug auf die Anforderung erforderlich, „alle angemessenen technischen, rechtlichen und organisatorischen Maßnahmen“ zu ergreifen, um einen unrechtmäßigen Zugang oder eine unrechtmäßige Übertragung von Daten außerhalb der EU zu verhindern. In Erwägungsgrund 78 wird eine Reihe von Maßnahmen genannt, darunter die Verschlüsselung von Daten. Die genaue Art der Schutzmaßnahmen, die umgesetzt werden müssen, sollte jedoch genauer definiert werden und bestehende Standards und Rahmenwerke berücksichtigen, die von Industrie-Initiativen wie Gaia-X entwickelt werden.

Zu Kapitel VIII: Interoperabilität

Die vorstehenden Regelungen zur Verbesserung der Interoperabilität müssen bestehende Standards sowie laufende Industrie-Initiativen hinreichend berücksichtigen. Im Rahmen von Industrie 4.0-Anwendungen sind bereits eine Reihe von Interoperabilitätsstandards entwickelt worden oder befinden sich in der Entwicklung. Exemplarisch zu nennen ist die im Bereich des Maschinen- und Anlagebaus entwickelte Weltsprache der Produktion auf Basis der OPC-UA-Technologie. Derartige Standardisierungsprozesse müssen auch in Zukunft industriegetrieben, bottom-up und pragmatisch verbleiben. Der Data Act sollte zwingend auf diesen Entwicklungen aufbauen und bestehende, bewährte und industriegetriebene Standards für die Betriebsfähigkeit verwenden.

Smart Contracts erfordern eine enge Verzahnung zwischen den beteiligten Unternehmen, so dass automatisch Vertrauen und der Willen zur Zusammenarbeit bestehen. Regulative Vorgaben für allgemeine IT-Sicherheitsstandards und andere etablierte technische Standards für die Entwicklung sowie der Einsatz von Software/Anwendungen sind bereits heute umfassend geregelt. Insofern ist die in Art. 30 DA-E vorgesehene „EU-Konformitätserklärung“ und eine Überprüfung von intelligenten Verträgen nicht nur überflüssig, sondern verursacht zusätzlich hohe administrative Hürden. Darüber hinaus werden insbesondere im Bereich von Blockchain, Distributed-Ledger-Technologien und andere mit digitalen Verträgen verbundene Innovationen gehemmt.

Zu Kapitel IX: Anwendung und Durchsetzung

Die in Art. 31 ff. DA-E vorgesehene dezentrale Durchsetzung durch mitgliedstaatliche Behörden birgt die Gefahr einer fragmentierten Anwendung der Verordnung in den EU-Mitgliedstaaten sowie unterschiedlicher lokaler bzw. regionaler Standards beim Zugang zu Daten. Es besteht die Gefahr, dass hier weitere Bürokratie aufgebaut wird, deren Durchschlagskraft völlig unklar ist.

Zu Kapitel X: sui-generis-Recht im Rahmen der Richtlinie 1996/9/EG

Die in Art. 35 DA-E vorgesehene Einschränkung des sui-generis-Datenbankschutzrechts nach Art. 7 RL 1996/9/EG geht mit erheblichen Beeinträchtigungen der Investitionsanreize einher, da die gesamte Datenbank – unabhängig davon, wie viele Daten unter den Datenzugangsanspruch gem. Art. 4 oder 5 DA-E fallen – künftig ungeschützt bleibt. Eine solch weitreichende Einschränkung erscheint weder notwendig noch angemessen, um das erklärte Ziel der Wahrung der Rechte nach Art. 4 und Art. 5 DA-E

sicherzustellen. Stattdessen sollte das sui-generis-Datenbankschutzrecht lediglich auf die entsprechend bereitzustellen Daten nach dem Data Act beschränkt werden.

Zu Kapitel XI: Schlussbestimmungen

In Anbetracht des Umfangs und der Tiefe der neuen Verpflichtungen, die den Dateninhabern und insbesondere den Herstellern auferlegt werden, sollte die Übergangsfrist vor Beginn der Anwendung dieser Verordnung deutlich länger sein als die in Art. 42 DA-E vorgeschlagenen zwölf Monate. Eine Übergangsfrist von 36 Monaten erscheint hier sachgerecht.

Überdies sollte der Zeitraum für die vorgesehene Evaluation des Data Acts von bis zu fünf Jahren für die Analyse der KMU-spezifischen Wirkungen verkürzt werden.

Über den BDI

Der BDI transportiert die Interessen der deutschen Industrie an die politisch Verantwortlichen. Damit unterstützt er die Unternehmen im globalen Wettbewerb. Er verfügt über ein weit verzweigtes Netzwerk in Deutschland und Europa, auf allen wichtigen Märkten und in internationalen Organisationen. Der BDI sorgt für die politische Flankierung internationaler Markterschließung. Und er bietet Informationen und wirtschaftspolitische Beratung für alle industrierelevanten Themen. Der BDI ist die Spitzenorganisation der deutschen Industrie und der industrienahen Dienstleister. Er spricht für 40 Branchenverbände und mehr als 100.000 Unternehmen mit rund acht Mio. Beschäftigten. Die Mitgliedschaft ist freiwillig. 15 Landesvertretungen vertreten die Interessen der Wirtschaft auf regionaler Ebene.

Impressum

Bundesverband der Deutschen Industrie e. V. (BDI)
Breite Straße 29, 10178 Berlin
www.bdi.eu
T: +49 30 2028-0

Lobbyregisternummer: R000534
EU-Transparenzregisternummer: 1771817758-48

Ansprechpartner

Dr. Michael Dose
Senior Manager
Abteilung Digitalisierung und Innovation
T: +49 30 2028 1560
m.dose@bdi.eu

BDI Dokumentennummer: D 1540