MMR

Zeitschrift für IT-Recht und Recht der Digitalisierung

TK · IT-Security · Medien · Robotik · KI · Datenschutz · Games

In Kooperation mit: Bitkom – Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. · davit im DAV – Arbeitsgemeinschaft IT-Recht im Deutschen Anwaltverein · eco – Verband der Internetwirtschaft e.V. · game – Verband der deutschen Games-Branche e.V. · Legal Tech Verband Deutschland e.V. · VAUNET – Verband Privater Medien

Beilage zu MMR 9/2022

LOUISA SPECHT-RIEMENSCHNEIDER

Der Entwurf des Data Act

Eine Analyse der vorgesehenen Datenzugangsansprüche im Verhältnis B2B, B2C und B2G

Der Data Act wird den Umgang mit Daten auf Jahrzehnte beeinflussen und dies nicht nur im Bereich der After-Market-Services, sondern ganz generell. Er setzt sich dabei hehre Ziele, die gerade auch im gesamtgesellschaftlichen Interesse liegen, die er jedoch mit den von ihm vorgesehenen Maßnahmen nicht erreichen wird. Denn zwar verfolgt der Data Act Entwurf (DA-E) mit der Normierung von Datenzugangsansprüchen grundsätzlich eine jedenfalls wissenschaftlich konsentierte Linie: In der Debatte um die Datenpolitik der vergangenen Jahre war man sich im Wesentlichen einig darüber, dass ein Dateneigentum nicht das richtige Instrument ist, um den Herausforderungen im Umgang mit Daten zu begegnen, sondern dass es vielmehr Datenzugangsrechten bedarf.

Der DA-E zeigt nun: Nicht jedes Datenzugangsrecht ist geeignet, die Probleme im Umgang mit Daten zu lösen, es kommt auf seine konkrete Ausgestaltung an. Entgegen dem ersten Eindruck, den die Normierung von Datenzugangsansprüchen im DA-E erweckt, legitimieren und schützen sie in der gewählten Ausgestaltung und in ihrem Zusammenspiel mit den übrigen Regelungen des DA-E vor allem die technisch-faktische Herrschaft des Dateninhabers. Denn die Daten werden weiterhin in der technisch-faktischen Herrschaftssphäre des Dateninhabers gespeichert und das Datenzugangsrecht des Nutzers ist als bloßes „in situ right" ausgestaltet und damit nicht geeignet, diese technisch-faktische Herrschaft anzutasten.

Art. 4 Abs. 6 DA-E enthält zwar die Vorgabe, dass der Dateninhaber die Daten nur auf Grundlage einer vertraglichen Vereinbarung mit dem Nutzer nutzen darf, diese vertragliche Vereinbarung ist aber in Anbetracht fehlender Schutzvorgaben für den Nutzer eine allzu leicht zu überwindende Hürde. Der Dateninhaber ist hier nach dem derzeitigen Entwurfstext frei, im Verhältnis zum Nutzer einseitig umfassende „Buy-out-Verträge" vorzugeben.

Die Handlungskompetenz der Menschen in Bezug auf ihre Daten wird der DA-E daher entgegen seiner Intention nicht stärken. Aber auch zur Gewährleistung von Innovation, die sich der DA-E zum Ziel gesetzt hat, fehlen geeignete Regelungen. Dies lässt sich jedoch, ebenso wie die Fehlallokation der Wertschöpfung aus Daten, zu der der DA-E in seinem derzeitigen Entwurf führt, durchaus noch beheben – der Gesetzgeber hat die Mittel dazu. Erforderlich hierfür sind jedoch mehr als vorsichtige Korrekturen.

I. Einleitung

Am 23.2.2022 hat die EU-Kommission ihren Entwurf eines Datengesetzes (COM (2022) 68 final – DA-E) vorgelegt, mit dem auf Grundlage von Art. 114 AEUV eine gerechte Verteilung der Wertschöpfung aus Daten auf die Akteure der Datenwirtschaft gewährleistet werden sowie der Datenzugang und die Datennutzung gefördert werden sollen.[1] Übergeordnetes politisches Ziel ist es, die „Innovations- und Wettbewerbsfähigkeit von EU-Unternehmen sämtlicher Branchen sicherzustellen, die Handlungskompetenz der Menschen in Bezug auf ihre Daten wirksam zu stärken und Unternehmen und öffentliche Stellen besser mit einem angemessenen und vorhersehbaren Mechanismus für die Bewältigung wichtiger politischer und gesellschaftlicher Herausforderungen, einschließlich öffentlicher Notstände und anderer Ausnahmesituationen, auszustatten."[2] Die Erkenntnis, dass Daten deutlich weniger genutzt werden als dies im gesellschaftlichen und wirtschaftlichen Interesse wünschenswert wäre, ist dabei nicht neu. Bereits in der Europäischen Datenstrategie aus dem Jahr 2020 hatte die Kommission einer verbesserten Datennutzung im Interesse von Politik, Wirtschaft und Gesellschaft Priorität beigemessen und angekündigt, in den kommenden fünf Jahren durch politische Maßnahmen die Voraussetzungen für den Aufbau einer Datenwirtschaft zu schaffen.[3] Der DA-E ist die zweite dieser politischen Maßnahmen. Bereits am 16.5.2022 wurde der Data Governance Act (DGA) verabschiedet. Sowohl beim DA-E als auch beim DGA handelt es sich um horizontale, vollharmonisierende Verordnungen, die durch sektorspezifische Regelungen ergänzt werden können.[4]

Während der DGA im Wesentlichen die Voraussetzungen für den Betrieb von Datennutzungsinfrastrukturen normiert, enthält der DA-E Vorschriften über den Zugang zu Daten, die beim Betrieb vernetzter Produkte und verbundener Dienste anfallen, zu Gunsten von Verbrauchern, gewerblichen Nutzern und staatlichen Stellen, Vorgaben zur Ausgestaltung von Verträgen, die geschlossen werden müssen, wenn ein Dateninhaber Daten zur Erfüllung von Datenzugangsansprüchen an Dritte weiterreicht, Schutzvorkehrungen für nicht-personenbezogene Daten im internationalen Umfeld sowie Interoperabilitätsvorgaben. Er ergänzt damit den DGA.[5]

Der DA-E adressiert sowohl das Verhältnis B2C als auch die Verhältnisse B2B und B2G. Welche Anwendungsfälle der DA-E dabei vor allem im Verhältnis B2C und B2B konkret vor Augen hatte, wird zwar nicht explizit ausgesprochen, um eine reine After-Market-Regulierung kann es ihm jedoch nicht gehen, denn dafür wäre, erstens, ein horizontaler Ansatz nicht erforderlich und zweitens erschlössen sich die umfassenden Regelungen zu den Rechten und Pflichten von Nutzern und Dateninhabern nicht. After-Market-Regulierung ist gewiss ein Teil des DA-E, seine Auswirkungen gehen aber weit darüber hinaus: Mit dem DA-E wird eine umfassende Daten-Governance sektorübergreifend festgeschrieben. Ob diese im DA-E konkret vorgesehene Daten-Governance gesellschaftlich und politisch tatsächlich gewollt ist, lässt sich durchaus hinterfragen. Denn zwar verfolgt der DA-E mit der Normierung von Datenzugangsansprüchen grundsätzlich eine jedenfalls wissenschaftlich konsentierte Linie: In der Debatte um die Datenpolitik der vergangenen Jahre war man sich im Wesentlichen einig darüber, dass ein Dateneigentum nicht das richtige Instrument ist, um den Herausforderungen im Umgang mit Daten zu begegnen, sondern dass es vielmehr Datenzugangsrechten bedarf.[6] Der DA-E zeigt nun: Nicht jedes Datenzugangsrecht ist geeignet, die Probleme im Umgang mit Daten zu lösen, es kommt auf seine konkrete Ausgestaltung an. Denn entgegen dem ersten Eindruck, den die Normierung von Datenzugangsansprüchen im DA-E erweckt, legitimieren und schützen sie in der gewählten Ausgestaltung und in ihrem Zusammenspiel mit den übrigen Regelungen des DA-E vor allem die technisch-faktische Herrschaft des Dateninhabers.[7] Die Ziele, denen der DA-E verpflichtet ist,[8] wird er auf diese Weise nicht erreichen.[9] Aufzuzeigen, welche Änderungen hierfür erforderlich sind, ist Ziel dieses Beitrags.

II. Gang der Untersuchung

Dieser Beitrag wird, erstens, das Verhältnis des DA-E zu anderen Rechtsakten, insbesondere zur DS-GVO, aufzeigen (III.). Er wird, zweitens, einen Überblick über die Regelungen des DA-E geben (IV.). Die Datenzugangsmechanismen, die im Mittelpunkt dieses Beitrags stehen sollen, werden, drittens, eingehend analysiert (V.). Dies erfolgt für die durch den DA-E differenzierten Verhältnisse Nutzer – Dateninhaber (V.1.), Dateninhaber – Datenempfänger (V.2.) und Dateninhaber – Staat (V.3.). Jedes Personenverhältnis wird dabei in seiner Ausgestaltung einer kritischen Würdigung in Bezug auf die Ziele des DA-E unterzogen, um letztlich Abhilfemöglichkeiten für die identifizierten Defizite aufzuzeigen. Der Beitrag schließt mit einer Zusammenfassung der Ergebnisse (VI.).

III. Verhältnis zu anderen Rechtsakten

1. Verhältnis zur DS-GVO

Aus dem DA-E soll zunächst keine Einschränkung des Schutzniveaus der DS-GVO ab- oder hergeleitet werden können.[10] Vielmehr stellt er lediglich eine Ergänzung der DS-GVO in Bezug auf solche Daten dar, die durch ein Produkt oder einen verbundenen Dienst eines Nutzers erzeugt werden. Das Verhältnis von DA-E zur DS-GVO ist damit klar: Die DS-GVO wird durch den DA-E nicht abgeändert. Der DA-E ist nicht lex specialis zur DS-GVO. Das führt dazu, dass dort, wo der DA-E auch für personenbezogene Daten gilt, die Regelungen sowohl des DA-E als auch der DS-GVO zu beachten sind. Sollte es zu widersprüchlichen Regelungen kommen, empfiehlt sich eine Klarstellung, welches Gesetz im Konfliktfall vorgeht, zB als neuer Art. 1 Abs. 3 DA-E.[11] Die Datenzugangsansprüche des DA-E begründen solche Konfliktfälle gerade nicht. Zu unterscheiden sind drei Fälle:

- Erstens, der Nutzer verlangt Datenzugang an sich selbst oder einen Dritten und ist die betroffene Person,
- zweitens, der Nutzer verlangt Datenzugang an sich selbst und ist selbst nicht die betroffene Person, und
- drittens, der Nutzer verlangt Datenzugang an einen Dritten und ist selbst nicht die betroffene Person.

Im ersten Fall (Nutzer verlangt Datenzugang an sich selbst oder einen Dritten und ist die betroffene Person) erfolgt der Datenzugang auf Grundlage einer Einwilligung, die konkludent im Datenzugangsverlangen zum Ausdruck kommt. Im zweiten Fall (Nutzer ist nicht die betroffene Person und verlangt Datenzugang an sich selbst, nicht an einen Dritten) sind die Datenzu-

1 DA-E, S. 3.
2 DA-E, S. 3.
3 COM (2020) 66 final v. 19.2.2020, Mitteilung der Europäischen Kommission an das Europäische Parlament, den Rat den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen, Eine Europäische Datenstrategie, S. 1, 2.
4 DA-E, S. 8; Erwägungsgrund 3 DGA-E.
5 DA-E, S. 7.
6 Stellvertretend für die Diskussion: Drexl, Designing Competitive Markets for Industrial Data – Between Propertisation and Access (2016) 16-13 Max Planck Institute for Innovation and Competition Research Paper, abrufbar unter: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2862975.
7 Ähnlich Hennemann/Steinrötter NJW 2022, 1481 Rn. 4: „de facto-Zuordnung".
8 DA-E, S. 5.
9 So bereits: Kerber, Governance of IoT Data, abrufbar unter: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4080436.
10 S. insb. Erwägungsgrund 7 DA-E.
11 EDPB/EDPS, Joint Opinion 2/2022 on the Proposal of the European Parliament and of the Council on harmonised rules on fair access to and use of data (DA-E), 4.5.2022, Rn. 26.

gangsansprüche rechtliche Verpflichtungen iSd Art. 6 Abs. 1 lit. c DS-GVO, denen der Verantwortliche unterliegt. Die Datenverarbeitungsbefugnis öffentlicher Stellen, denen Daten auf Grundlage der Verpflichtungen des DA-E iVm Art. 6 Abs. 1 lit. c DS-GVO übermittelt wurden, erfolgt auf Grundlage von Art. 6 Abs. 1 lit. e DS-GVO.[12] Die Datenzugangsverpflichtungen des DA-E füllen außerdem jedenfalls zT die Öffnungsklauseln der Art. 9 Abs. 2 lit. g–j DS-GVO. Vertreten ließe sich, die Gewährleistung von Datenzugang an den Nutzer liege in Anbetracht der vom DA-E verfolgten gesamtgesellschaftlichen Ziele im erheblichen öffentlichen Interesse iSd Art. 9 Abs. 1 lit. g DS-GVO, sodass die Datenzugangsverpflichtungen an den Nutzer dann, wenn dieser nicht selbst die betroffene Peron ist, sämtliche datenschutzrechtliche Erlaubnistatbestände ausfüllen, sofern sie die Anforderungen der Art. 6 Abs. 1 lit. c DS-GVO bzw. Art. 9 Abs. 1 lit. g DS-GVO erfüllen. Für die Erfüllung dieser teils hohen Anforderungen, hat der Gesetzgeber zu sorgen. Werden die Anforderungen der Art. 6 Abs. 1 lit. c DS-GVO und Art. 9 Abs. 1 lit. g DS-GVO nicht erfüllt, wird die entsprechende Datenzugangsverpflichtung des DA-E durch die Vorgaben der DS-GVO beschränkt, dh sie muss den Anforderungen anderer Erlaubnistatbestände der DS-GVO genügen, so zB Art. 6 Abs. 1 lit. f DS-GVO, wobei durch die Normierung der Datenzugangsverpflichtung zum Ausdruck gebracht wird, dass der Gesetzgeber im Regelfall bei der Erfüllung des Datenzugangsanspruchs zumindest von einer Gleichrangigkeit der Datenverarbeitungsinteressen ausgegangen ist. Dem steht Erwägungsgrund 24 DA-E nicht entgegen, nach dem der DA-E keine Rechtsgrundlage gemäß der DS-GVO schafft, die es dem Dateninhaber ermöglicht, Dritten auf Verlangen eines Nutzers, der keine betroffene Person ist, Zugang zu personenbezogenen Daten zu gewähren oder diese bereitzustellen. Denn ausweislich seines Wortlauts ist Erwägungsgrund 24 lediglich für den letztgenannten Fall relevant (Nutzer ist nicht selbst betroffene Person und verlangt Datenzugang an einen Dritten). Für diesen Fall bedarf es einer Einwilligung der betroffenen Person oder des Eingreifens eines anderen Erlaubnistatbestands. Als neue Rechtsgrundlage iSd Art. 6 Abs. 1 lit. c DS-GVO oder Art. 9 Abs. 1 lit. g DS-GVO können die Datenzugangsverpflichtungen des DA-E in diesem Fall nach dem klaren Wortlaut von Erwägungsgrund 24 gerade nicht gelesen werden. Auch hier ließe sich aber argumentieren, jedenfalls für nicht-sensible Daten gilt eine Vermutung einer Rechtmäßigkeit der Datenübermittlung nach Art. 6 Abs. 1 lit. f DS-GVO, weil der Gesetzgeber durch die Normierung eines Datenzugangsrechtes zum Ausdruck bringt, dass das Datenverarbeitungsinteresse in der Regel dem Betroffeneninteresse mindestens gleichrangig sein wird und die Voraussetzungen des Art. 6 Abs. 1 lit. f DS-GVO damit in der Regel erfüllt sein werden. Hierdurch würde gerade keine neue Rechtsgrundlage iSv Erwägungsgrund 24 geschaffen, sondern lediglich eine bereits bestehende Rechtsgrundlage iSd Ziele des DA-E ausgelegt.

2. Verhältnis zu anderen Rechtsakten

Auch die Verordnung über den freien Verkehr nicht-personenbezogener Daten wird durch den DA-E ergänzt. Darüber hinaus soll der DA-E das Unionsrecht zur Förderung der Interessen der Verbraucher und zur Gewährleistung eines hohen Verbraucherschutzniveaus, zum Schutz ihrer Gesundheit und wirtschaftlichen Interessen ergänzen.[13] Er verdrängt insbesondere nicht die RL 2005/29/EG des Europäischen Parlamentes und des Rates[14], die RL 2011/83/EU des Europäischen Parlaments und des Rates[15] und die RL 93/13/EWG des Europäischen Parlaments und des Rates[16], sondern lässt sie unberührt. Dies gilt ebenso für das Unionsrecht zur Festlegung von Barrierefreiheitsanforderungen für bestimmte Produkte und Dienstleistungen, insbesondere die RL (EU) 2019/882[17]. Die Anwendung des Wettbewerbsrechts (insbesondere Art. 101, 102 AEUV) soll durch den DA-E ebenso nicht berührt werden; vielmehr sollen die Maßnahmen, die im DA-E vorgesehen sind, nicht dazu verwendet werden, den Wettbewerb entgegen einer den AEUV verstoßenden Weise einzuschränken.[18]

Die Vorschriften zum Schutz des geistigen Eigentums werden durch den DA-E nicht berührt, mit Ausnahme des in Art. 7 Datenbank-RL festgelegten Schutzrechts sui generis, das nach Art. 35 DA-E keine Anwendung auf Datenbanken findet, die Daten enthalten, die bei der Nutzung eines Produkts oder verbundenen Dienstes erlangt oder erzeugt wurden. Der Digital Markets Act (DMA) wird ebenso ergänzt wie der DGA.[19] Der DA-E berührt auch nicht die Instrumente für die Datenweitergabe, den Datenzugang und die Datenverwendung in den Bereichen Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten und Ordnungswidrigkeiten, der Vollstreckung strafrechtlicher und verwaltungsrechtlicher Sanktion oder Datenerhebungen für Steuer- oder Zollzwecke.[20] Außerdem berührt der DA-E nicht die Zuständigkeitsverteilungen der Mitgliedstaaten in Bezug auf Tätigkeiten in den Bereichen öffentliche Sicherheit, Verteidigung und nationale Sicherheit im Einklang mit dem Unionsrecht sowie Tätigkeiten des Zolls.[21]

Der DA-E soll auch bestehende sektorspezifische Vorschriften nicht berühren. Einzig künftige Vorschriften, die sich auf Datennutzungs- und -zugangsrechte auswirken, sollen an die Vorgaben des DA-E angeglichen werden.[22] Der am 3.5.2022 vorgelegte Entwurf des European Health Data Space Acts ist die erste dieser sektorspezifisch ergänzenden Vorschriften. Er sieht Datenzugangsgewährleistungen in seinen Artikeln 33 und 34 vor. An der Neufassung der Type Approval Regulation als zweiter ergänzender Regulierung für den Mobilitätssektor wird derzeit gearbeitet. DA-E und DGA bilden zusammen mit den sektorspezifischen Regelungen über Daten sowie flankierender Gesetzgebung wie zB dem sui generis-Datenbankrecht und dem Geschäftsgeheimnisschutz und Teilen von DMA und Digital Service Act (DSA) das europäische Datenwirtschaftsrecht, das seinerseits wiederum durch die Regelungen des europäischen und nationalen Datenschutzrechts ergänzt wird sowie durch die im Koalitionsvertrag angekündigten Regelungen des nationalen Datenwirtschaftsrechts, wie dem Datentreuhandgesetz und dem Datengesetz, dem Forschungsdatengesetz und den bereits existierenden Datenzugangsansprüchen des Datennutzungsgesetzes und den Informationsfreiheitsgesetzen. Spielraum für nationale Gesetzgebung lassen sowohl DA-E als auch DGA wie schon

12 Zum Verhältnis zwischen Art. 6 Abs. 1 lit. c und lit. e vgl. Kühling/Buchner/Buchner/Petri, Art. 6 Rn. 78.
13 Erwägungsgrund 9 DA-E.
14 RL 2005/29/EG des Europäischen Parlaments und des Rates v. 11.5.2005 über unlautere Geschäftspraktiken von Unternehmen gegenüber Verbrauchern im Binnenmarkt und zur Änderung der RL 84/450/EWG des Rates, der RL 97/7/EG, 98/27/EG und 2002/65/EG des Europäischen Parlaments und des Rates sowie der VO (EG) Nr. 2006/2004 des Europäischen Parlaments und des Rates (Richtlinie über unlautere Geschäftspraktiken), ABl. L 149 v. 11.6.2005, 22.
15 RL 2011/83/EU des Europäischen Parlaments und des Rates v. 25.10.2011 über die Rechte der Verbraucher, zur Abänderung der RL 93/13/EWG des Rates und der RL 1999/44/EG des Europäischen Parlaments und des Rates sowie zur Aufhebung der RL 85/577/EWG des Rates und der RL 97/7/EG des Europäischen Parlaments und des Rates.
16 RL 93/13/EWG des Rates v. 5.4.1993 über missbräuchliche Klauseln in Verbraucherverträgen. RL (EU) 2019/2161 des Europäischen Parlaments und des Rates v. 27.11.2019 zur Änderung der RL 93/13/EWG des Rates und der RL 98/6/EG, 2005/29/EG und 2011/83/EU des Europäischen Parlaments und des Rates zur besseren Durchsetzung und Modernisierung der Verbraucherschutzvorschriften der Union.
17 RL (EU) 2019/882 des Europäischen Parlaments und des Rates v. 17.4.2019 über die Barrierefreiheitsanforderungen für Produkte und Dienstleistungen (ABl. L 151 v. 7.6.2019).
18 S. insb. Erwägungsgrund 88 DA-E.
19 DA-E, S. 4 f.
20 S. insb. Erwägungsgrund 60 DA-E.
21 Erwägungsgrund 13 DA-E.
22 DA-E, S. 5.

die DS-GVO allein dort, wo sie Öffnungsklauseln enthalten, sowie außerhalb ihres Anwendungsbereichs. Die Möglichkeiten des nationalen Gesetzgebers sind damit begrenzt, nicht aber ausgeschlossen.

IV. Struktur und Inhalt

Die insgesamt 42 Artikel des DA-E teilen sich in elf Kapitel, deren Inhalt im Folgenden überblicksartig skizziert sein soll. Im ersten Kapitel sind Gegenstand und Anwendungsbereich der Verordnung festgelegt. Nach Art. 1 Abs. 1 enthält der DA-E Vorschriften für drei Fallgruppen: Erstens regelt er die Bereitstellung von Daten, die bei der Nutzung eines Produkts oder verbundenen Dienstes erzeugt werden, für den Nutzer dieses Produkts oder Dienstes. Er enthält, zweitens, Vorschriften über die Bereitstellung dieser Daten durch Dateninhaber für Datenempfänger und er regelt, drittens, die Bereitstellung dieser Daten durch Dateninhaber für öffentliche Stellen oder Organe, Einrichtungen und sonstige Stellen der Union, soweit diese Daten wegen außergewöhnlicher Notwendigkeit zur Wahrnehmung einer Aufgabe von öffentlichem Interesse benötigt werden, Art. 1 Abs. 1 DA-E. Art. 2 DA-E legaldefiniert sodann die zentralen Rechtsbegriffe der Verordnung. Der Regelungsansatz des DA-E folgt – ebenso wie DGA und die DS-GVO – dem Marktortprinzip, Art. 1 Abs. 2 DA-E,[23] richtet sich aber allein an folgende Personen und Stellen:

- Hersteller von Produkten und Erbringer verbundener Dienste, die in der Union in Verkehr gebracht werden, und die Nutzer solcher Produkte oder Dienste;
- Dateninhaber, die Datenempfängern in der Union Daten bereitstellen;
- Datenempfänger in der Union, denen Daten bereitgestellt werden;
- öffentliche Stellen und Organe, Einrichtungen und sonstige Stellen der Union, die von Dateninhabern verlangen, Daten bereitzustellen, sofern diese Daten wegen außergewöhnlicher Notwendigkeit zur Wahrnehmung einer Aufgabe von öffentlichem Interesse benötigt werden, sowie die Dateninhaber, die solche Daten auf ein solches Verlangen hin bereitstellen;
- Anbieter von Datenverarbeitungsdiensten, die Kunden in der Union solche Dienste anbieten.

Kapitel zwei enthält Vorgaben für den Datenaustausch im Verhältnis B2C und B2B und definiert dabei sowohl die Rechte und Pflichten der Nutzer als auch des Dateninhabers und Dritter. Hierzu gehören im Wesentlichen die Gewährleistung von Accessibility by Default in Art. 3 Abs. 1 DA-E, wonach Produkte so konzipiert und hergestellt und verbundene Dienste so erbracht werden müssen, dass die bei ihrer Nutzung erzeugten Daten standardmäßig für den Nutzer einfach, sicher und – soweit relevant und angemessen – direkt zugänglich sind, vorvertragliche Informationspflichten nach Art. 3 Abs. 2 DA-E, einen Datenzugangsanspruch des Nutzers nach Art. 4 Abs. 1 DA-E, der auch die Möglichkeit beinhaltet, die Weitergabe der Daten unmittelbar an einen Dritten (mit Ausnahme von zentralen Plattformdiensten iSd DMA, Art. 5 Abs. 2 DA-E) zu verlangen, Art. 5 Abs. 1 DA-E, ein Datenverarbeitungsverbot des Nutzers zu Zwecken der Entwicklung eines Produkts, das mit dem Produkt, von dem die Daten stammen, im Wettbewerb steht, ein Verbot der Verarbeitung von Nutzerdaten für den Dateninhaber mit vertraglichem Einwilligungsvorbehalt, Art. 4 Abs. 6 DA-E, Datenverarbeitungsverbote für Dritte, Art. 6 DA-E und eine De-minimis-Klausel für Kleinst- und Kleinunternehmen, Art. 7 DA-E.

Das dritte Kapitel unter der Überschrift „Verpflichtungen für Dateninhaber, die rechtlich verpflichtet sind, Daten zur Nutzung bereitzustellen", legt in Art. 8–12 DA-E Bedingungen fest, unter denen Dateninhaber Datenempfängern Daten zur Verfügung stellen (Art. 8 DA-E), insbesondere wird festgeschrieben, dass der Dateninhaber angemessen zu vergüten ist, Art. 9 Abs. 1 DA-E. Art. 10 DA-E gibt vor, dass Streitbeilegungsstellen für Dateninhaber und Datenempfänger zugänglich sein müssen und stellt Anforderungen an diese Streitbeilegungsstellen. Der Dateninhaber kann nach Art. 11 DA-E eine unbefugte Nutzung oder Offenlegung von Daten durch Technische Schutzmaßnahmen unterbinden. Die Vorgaben des dritten Kapitels sind nach Art. 12 Abs. 2 DA-E zwingend.

Das vierte Kapitel regelt in einem einzigen Artikel (Art. 13 DA-E) den Umgang mit missbräuchlichen Klauseln, die einem Kleinstunternehmen, einem kleinen oder mittelständischen Unternehmen einseitig auferlegt werden. Missbräuchliche Klauseln sind danach nicht bindend. Missbräuchlich ist eine Klausel nach Absatz 2, wenn ihre Verwendung gröblich von der guten Geschäftspraxis bei Datenzugang und Datennutzung abweicht und gegen das Gebot von Treu und Glauben und des redlichen Geschäftsverkehrs verstößt. Absatz 3 enthält einen Katalog stets missbräuchlicher Klauseln, Absatz 4 eine Vermutungsregelung.

Im fünften Kapitel wird die Bereitstellung von Daten an öffentliche Stellen sowie Organe und Einrichtungen der Union auf Grund einer außergewöhnlichen Notwendigkeit geregelt, Art. 14 DA-E. Wann eine außergewöhnliche Notwendigkeit besteht, regelt Art. 15 DA-E. Es handelt sich um Fälle, in denen die Daten erforderlich sind zur Bewältigung, zur Verhinderung oder zur Unterstützung bei der Erholung von einem öffentlichen Notstand sowie dann, wenn die öffentliche Stelle bzw. das Organ, die Einrichtung oder sonstige Stelle der Union auf Grund des Fehlens verfügbarer Daten daran gehindert ist, eine bestimmte, gesetzlich ausdrücklich vorgesehene Aufgabe im öffentlichen Interesse zu erfüllen. Art. 19 DA-E enthält Verarbeitungsverbote für öffentliche Stellen, Organe, Einrichtungen und sonstige Stellen der Union in Bezug auf die nach Art. 14 und 15 DA-E erlangten Daten. Die erlangten Daten dürfen nach Art. 21 DA-E unter bestimmten Voraussetzungen auch an gemeinnützige und solche Forschungseinrichtungen zur Verfügung gestellt werden, die iRe anerkannten Aufgabe von öffentlichem Interesse handeln.

Das sechste Kapitel behandelt den Wechsel zwischen Datenverarbeitungsdiensten. Für einen möglichst einfachen und effektiven Wechsel sollen Hindernisse zwischen Anbietern von Datenverarbeitungsdiensten beseitigt werden. Das Recht des Kunden, den Anbieter von Datenverarbeitungsdiensten wechseln zu können, ist gem. Art. 24 Abs. 1 DA-E vertraglich eindeutig festzulegen. Gebühren für den Wechsel sollen nach Art. 25 DA-E schrittweise entfallen.

Das siebte Kapitel schreibt Schutzvorkehrungen für nicht-personenbezogene Daten im internationalen Umfeld fest. Danach sind Anbieter von Datenverarbeitungsdiensten insbesondere verpflichtet, alle angemessenen technischen, rechtlichen und organisatorischen Maßnahmen, einschließlich vertraglicher Vereinbarungen, zu ergreifen, um eine internationale Übermittlung oder einen internationalen staatlichen Zugriff zu in der Union gespeicherten nicht-personenbezogenen Daten zu verhindern, wenn dies im Widerspruch zum Unionsrecht oder zum nationalen Recht des betreffenden Mitgliedstaats stünde, Art. 27 Abs. 1 DA-E.

Das achte Kapitel normiert Interoperabilitätsanforderungen für Daten (Art. 28 DA-E) und Datenverarbeitungsdienste (Art. 29 DA-E). Die Konkretisierung technischer Normen und Standards erfolgt hingegen nicht durch den DA-E selbst, sondern wird de-

23 Vgl. zum Marktortprinzip im Datenwirtschaftsrecht Hennemann/von Ditfurth NJW 2022, 1905 Rn. 12.

legierten Rechtsakten und europäischen Normungsorganisation überlassen, vgl. Art. 28 Abs. 2, Abs. 4–6, Art. 29 Abs. 4, Abs. 5, Art. 30 Abs. 5, Abs. 6 DA-E. Ziel ist insbesondere die Schaffung offener Standards und Schnittstellen. Art. 30 DA-E enthält „wesentliche Anforderungen an intelligente Verträge für die gemeinsame Datennutzung".

Im neunten Kapitel werden zu Zwecken der Umsetzung des DA-E Verfahrensvorgaben festgeschrieben. Mitgliedstaaten sollen eine oder mehrere zuständige Behörden für die Umsetzung des DA-E bestimmen, deren Aufgaben und Zuständigkeit sich insbesondere im Verhältnis zu anderen Behörden aus Art. 31 Abs. 2, 3 DA-E ergibt. Zur Arbeit der zuständigen Behörden soll u.a. die Befassung mit Beschwerden gem. Art. 32 DA-E gehören. Sanktionen müssen allerdings erst durch die Mitgliedstaaten festgelegt werden und sind nicht bereits im DA-E enthalten. Schließlich dürfen auch Datenschutzaufsichtsbehörden bei Verstößen gegen Vorschriften der Kapitel 2, 3 und 5 tätig werden und Sanktionen erlassen, Art. 33 Abs. 3 DA-E. Nach Art. 34 DA-E erstellt und empfiehlt die Kommission unverbindliche Mustervertragsbedingungen für den Datenzugang und die Datennutzung, um die Parteien bei der Ausarbeitung und Aushandlung von Verträgen mit ausgewogenen vertraglichen Rechten und Pflichten zu unterstützen.

In Art. 35 DA-E des zehnten Kapitels wird normiert, dass das in Art. 7 RL 96/9/EG festgelegte spezifische Schutzrecht sui generis (umgesetzt in § 87a UrhG) keine Anwendung auf Datenbanken findet, die Daten enthalten, die bei der Nutzung eines Produkts oder verbundenen Dienstes erlangt oder erzeugt wurden. Die Vorschrift soll vermeiden, dass die Rechte der Nutzer auf Zugang oder Nutzung ihrer Daten sowie das Recht, Daten mit Dritten zu teilen, unterlaufen werden. In Kapitel 11 finden sich die Schlussbestimmungen, die insbesondere das Inkrafttreten des DA-E sowie notwendige Änderungen an anderen EU-Rechtsakten, das Recht, delegierte Rechtsakte zu erlassen sowie die vorgesehene Evaluierung des DA-E zwei Jahre nach dessen Geltungsbeginn betreffen.

V. Datenzugangsregime

1. Verhältnis Nutzer – Dateninhaber

Das Verhältnis zwischen dem Nutzer und dem Dateninhaber wird wesentlich durch Vertrag bestimmt, Art. 4 Abs. 6 DA-E.[24] Danach darf der Dateninhaber nicht-personenbezogene Daten, die bei der Nutzung eines Produkts oder verbundenen Dienstes erzeugt werden, nur auf der Grundlage einer vertraglichen Vereinbarung mit dem Nutzer nutzen. Er darf solche Daten, die bei der Nutzung des Produkts oder verbundenen Dienstes erzeugt werden, nicht verwenden, um daraus Einblicke in die wirtschaftliche Lage, Vermögenswerte und Produktionsmethoden des Nutzers oder in die Nutzung durch den Nutzer zu erlangen, wenn dies die gewerbliche Position des Nutzers auf den Märkten, auf denen dieser tätig ist, untergraben könnte. Produkte werden so konzipiert und hergestellt und verbundene Dienste so erbracht, dass die bei ihrer Nutzung erzeugten Daten standardmäßig für den Nutzer einfach, sicher und – soweit relevant und angemessen – direkt zugänglich sind, Art. 3 Abs. 1 DA-E. Dem Nutzer steht ein Datenzugangsanspruch nach Art. 4 DA-E zu. Wie diese Vorgaben zu verstehen sind, woraus sie sich ableiten und welche Probleme sie aufwerfen, soll im Folgenden erläutert sein.

a) Dateninhaber

„Dateninhaber" ist nach Art. 2 Nr. 6 DA-E eine juristische oder natürliche Person, die nach dieser Verordnung, nach anwendbarem Unionsrecht oder nach den anwendbaren nationalen Rechtsvorschriften zur Umsetzung des Unionsrechts berechtigt oder verpflichtet ist und durch die Kontrolle über die technische Konzeption des Produkts und damit verbundener Dienste in der Lage ist, bestimmte Daten bereitzustellen. Kontrolle über die technische Konzeption eines Produkts hat in der Regel der Hersteller des Produkts, den der DA-E insofern als einzigen Dateninhaber adressiert. Nicht sämtliche Dateninhaber werden also zum Datenzugang verpflichtet, sondern mit den Produktherstellern regelmäßig solche Dateninhaber, zu denen der Nutzer nicht zwingend in einer vertraglichen Beziehung steht. Es kommt auf die faktische Kontrolle über die technische Konzeption eines Produkts sowie auf die technisch-faktische Kontrolle über die Daten an, um die Eigenschaft als Dateninhaber zu begründen. Weder der Hersteller, der nicht in der Lage ist, Daten bereitzustellen, weil er die Daten nicht technisch-faktisch innehat, noch der Dateninhaber, der keine Kontrolle über die technische Konzeption des Produkts hat, werden adressiert. Der Adressatenkreis des DA-E ist damit jedenfalls im Hinblick auf die Datenzugangsansprüche begrenzt. Hersteller und Dateninhaber werden nicht gleichgesetzt, sondern es werden von vornherein lediglich diejenigen Fälle vom DA-E in Bezug auf den Datenzugang adressiert, in denen der Produkthersteller der Dateninhaber ist. Eine Person ist Dateninhaber, wenn und soweit sie die Daten in der eigenen technisch-faktischen Herrschaftssphäre speichert oder die Datenspeicherung kontrolliert. Dies ergibt sich aus Erwägungsgrund 24 der davon spricht, dass ein Dateninhaber auch Verantwortlicher iSd Datenschutzrechts sein sollte, sofern personenbezogene Daten verarbeitet werden. Es wird also vorausgesetzt, dass der Dateninhaber entweder allein oder aber gemeinsam mit anderen über die Zwecke und Mittel der Datenverarbeitung entscheidet. Dies ist aber auch dann der Fall, wenn nicht er selbst die Daten in der eigenen technisch-faktischen Herrschaftssphäre speichert, sondern wenn sich der Speicherort bei einer anderen Person befindet, die die Daten nach den Vorgaben des Dateninhabers verarbeitet und sie ihm oder einem Nutzer bzw. einem Dritten daher auf Verlangen des Dateninhabers bereitstellen muss. Sensordaten sowie Daten aus Third-Party-Apps im vernetzten Fahrzeug können von dem gegen den Automobilhersteller gerichteten Datenzugangsanspruch damit nur erfasst sein, wenn sie entweder in der eigenen technisch-faktischen Herrschaftssphäre des Automobilherstellers gespeichert werden oder in der technisch-faktischen Herrschaftssphäre eines Dritten, der die Daten nach den Vorgaben des Automobilherstellers verarbeitet und sie diesem daher auf Verlangen bereitstellen muss.[25]

b) Nutzer

Ein „Nutzer" wird in Art. 2 Nr. 5 DA-E definiert als eine natürliche oder juristische Person, die ein Produkt besitzt, mietet oder least oder eine Dienstleistung in Anspruch nimmt. Nicht nur der Verbraucher, der das Produkt zu privaten Zwecken nutzt oder den Dienst zu privaten Zwecken bezieht, kann also Nutzer sein, sondern auch ein Unternehmer, zB ein Landwirt, der einen Traktor least, der über eingebaute Sensoren Daten über die Bodenbeschaffenheit sammelt. Selbst eine juristische Person, die ein Produkt „besitzt, mietet oder least"[26], unterfällt dem Begriff des Nutzers.

Rechtmäßiger Besitz als Grundlage der Nutzerrechte

Anders als der Wortlaut des Art. 2 Nr. 5 DA-E suggeriert, muss es sich bei den Voraussetzungen „Besitz" auf der einen und „Miete oder Leasing" auf der anderen Seite nicht um Alternati-

24 Der Vertrag wird insgesamt im DA-E in den Vordergrund gestellt. Hennemann/Steinrötter sprechen daher davon, dass das Vertragsrecht die Führung im Datenwirtschaftsrecht übernehme, vgl. Hennemann/Steinrötter NJW 2022, 1481 Rn. 3.

25 Diese Frage wirft die Stellungnahme des BDI zum Legislativvorschlag des DA-E auf, S. 10.

26 Zu diesen Vorrausetzungen vgl. sogleich.

ven handeln. Ebenso könnte es dem Gesetzgeber für die Nutzereigenschaft in erster Linie darum gehen, dass der Nutzer rechtmäßig auf vertraglicher Grundlage besitzt (besitzrechtliche Theorie). Für diese Auslegung spricht insbesondere Erwägungsgrund 18, der, anders als der Verordnungstext, denjenigen als Nutzer erachtet, der das Produkt gekauft, gemietet oder geleast hat. Dem Gläubiger der genannten Verträge wird auf ihrer Grundlage regelmäßig zumindest mittelbarer rechtmäßiger Besitz verschafft. Der Europäische Gesetzgeber legt das deutsche Trennungs- und Abstraktionsprinzip seinen Gesetzgebungsakten freilich nicht zu Grunde, aber auch in den übrigen mitgliedstaatlichen Rechtsordnungen, die das Trennungs- und Abstraktionsprinzip nicht kennen, dürfte mit den genannten Verträgen eine Besitzüberlassung einhergehen. Gemeinsam ist den in den Erwägungsgründen und dem Verordnungstext genannten Eigenschaften als Käufer, Mieter oder Leasingnehmer damit die Eigenschaft als jedenfalls mittelbarer rechtmäßiger Besitzer. Weshalb im Verordnungstext Besitz, Miete und Leasing, in den Erwägungsgründen aber auch der Kauf als nutzereigenschaftsbegründend genannt sind, könnte sich also daraus erklären, dass es dem Gesetzgeber schlicht nicht darauf ankommt, auf welcher vertraglichen Grundlage der Nutzer rechtmäßig besitzt, sondern allein darauf, dass er auf vertraglicher Grundlage rechtmäßig besitzt. Wenn dies aber richtig ist, kann der unrechtmäßige Besitz nicht ausreichend sein, um die Eigenschaft als Nutzer zu begründen. Der Drittnutzer, der das Produkt stiehlt, erhält durch den DA-E also keinen Datenzugangsanspruch.

Konsequenz dieser „besitzrechtlichen Theorie" auf vertraglicher Grundlage ist erstens, dass unwirksame Verträge nicht geeignet sind, die Nutzerposition nach Art. 2 Nr. 5 DA-E zu begründen und, dass es, zweitens, für die Begründung der Nutzerrechte gerade nicht auf die reale Beteiligung am Wertschöpfungsprozess durch tatsächliche Nutzung des Produkts bzw. verbundenen Dienstes ankommt, ausreichend ist bereits der rechtmäßige Besitz des Gegenstands mit dessen Hilfe die Daten aufgezeichnet werden, auf vertraglicher Grundlage. Neben der besitzrechtlichen Grundlage der Nutzerrechte, die der europäische Gesetzgeber nach der hier vertretenen Ansicht wählt, lässt sich aber freilich auch darauf abstellen, dass der Datenzugangsanspruch in Verträgen zwischen Dateninhabern und Nutzern als vertragliche Nebenpflicht geschuldet ist (vertragliche Theorie).

Vertragsparteien

Zwischen wem der Vertrag zur Nutzung von Produkt oder Dienst geschlossen werden muss, spezifiziert der DA-E nicht. Argumentieren lässt sich aber in systematischer Hinsicht mit der Stellung der Dateninhaber iSd Art. 2 Nr. 6 DA-E als Hersteller von Produkten, die vielfach gerade keine vertragliche Verbindung zum Nutzer haben. Würde ein Vertrag zwischen Dateninhaber und Nutzer vorausgesetzt, würde der Anwendungsbereich des DA-E erheblich eingeschränkt, was den Zielen des DA-E nicht gerecht würde. Auch teleologisch ist es einerlei, mit wem der Nutzer in vertraglichen Beziehungen steht. Denn stellt man, wie geschehen, darauf ab, dass es dem DA-E allein darauf ankommt, dass der Nutzer auf vertraglicher Grundlage rechtmäßig besitzt, ist es irrelevant, mit wem er in einer vertraglichen Beziehung steht; Voraussetzung der Nutzerstellung ist damit, dass der Nutzer Vertragspartei ist, nicht aber auch, dass der Dateninhaber Vertragspartei ist.

c) Produkt und verbundener Dienst

„Produkt" iSd Art. 2 Nr. 2 DA-E meint ausschließlich einen körperlichen beweglichen Gegenstand, der auch in einem unbeweglichen Gegenstand enthalten sein kann, der Daten über seine Nutzung oder Umgebung erlangt, erzeugt oder sammelt und Daten über einen öffentlich zugänglichen elektronischen Kommunikationsdienst übermitteln kann und dessen Hauptfunktion nicht die Speicherung und Verarbeitung von Daten ist. Derartige Produkte können Fahrzeuge, Haushaltsgeräte und Konsumgüter, Medizin- und Gesundheitsprodukte oder landwirtschaftliche und industrielle Maschinen sein, vgl. Erwägungsgrund 14 DA-E.

„Verbundener Dienst" ist nach Art. 2 Nr. 3 DA-E ein digitaler Dienst, einschließlich Software, der so in ein Produkt integriert oder so mit ihm verbunden ist, dass das Produkt ohne ihn eine seiner Funktionen nicht ausführen könnte.

Reine Speichermedien sind daher von vornherein ebenso wenig vom Anwendungsbereich des DA-E erfasst wie reine Online-Dienste. Auch bestimmte Produkte, die in erster Linie dazu bestimmt sind, Inhalte anzuzeigen oder abzuspielen oder diese – u.a. für die Nutzung durch einen Online-Dienst – aufzuzeichnen und zu übertragen, wie Personalcomputer, Server, Tablets und Smartphones, Kameras, Webcams, Tonaufnahmesysteme und Textscanner sollen nicht vom DA-E erfasst werden, vgl. Erwägungsgrund 15 DA-E. Als Begründung des Ausschlusses dieser Produkte nennt Erwägungsgrund 15 DA-E den Umstand, dass sie einen menschlichen Beitrag erfordern, um verschiedene Arten von Inhalten wie Textdokumente, Tondateien, Videodateien, Spiele und digitale Karten zu erstellen und die Daten damit nicht nur aufzeichnen. Daraus sollte indes nicht geschlussfolgert werden, dass jeder menschliche Beitrag ausreicht, um den Anwendungsbereich des DA-E auszuschließen. Schließlich ist zB eine bloße Konfiguration von IoT-Produkten nicht mit der Erstellung von Textdokumenten vergleichbar.

Ohne Relevanz ist, ob das Produkt nach Art. 2 Abs. 2 DA-E, das mittels Sensoren und Software Daten über seine Nutzung oder Umgebung erlangt, dies tut, ohne dass dies erforderlich ist, um seine Funktionen auszuführen oder ob seine Funktionsfähigkeit von dieser Erlangung, Erzeugung oder Sammlung von Daten abhängt. Die schwierige Abgrenzung, die nach Maßgabe der Digitale-Inhalte-Richtlinie und der Warenkaufrichtlinie in dieser Hinsicht zu tätigen ist, entfällt damit. Lediglich der verbundene Dienst nach Art. 2 Abs. 3 DA-E stellt auf diese Differenzierung ab. Eine Beschränkung des Datenzugangsanspruchs auf Daten über vernetzungsabhängige Funktionen der Produkte nimmt der DA-E nicht vor.[27] Sämtliche Daten, die im Produkt bzw. über den verbundenen Dienst erzeugt werden, sind erfasst. Durch die Begrenzung auf Daten aus Produkten und verbundenen Diensten, ist der Anwendungsbereich des DA-E enger als er sein könnte. Ebenso wäre es möglich gewesen, ein generelles Datenzugangsrecht der Nutzer für sämtliche Fälle zu statuieren, in denen eine Person Daten erzeugt, diese aber in der technisch-faktischen Herrschaftssphäre eines anderen gespeichert werden.[28] Dass dies nicht geschehen ist, stützt die Argumentation unter V.1.b) (Rechtmäßiger Besitz als Grundlage der Nutzerrechte und Vertragsparteien), dass es dem Gesetzgeber letztlich darauf angekommen sein dürfte, auf Grundlage von vertraglich vermitteltem rechtmäßigem Besitz Datenzugangs- und Datennutzungsbefugnisse zu begründen.

Auch Daten aus virtuellen Assistenten iSd Art. 2 Nr. 4 DA-E fallen in den Anwendungsbereich des DA-E, allerdings nur die Daten, die aus der Interaktion zwischen dem Nutzer und dem Produkt über den virtuellen Assistenten stammen. Vom virtuellen Assistenten erstellte Daten, die nicht mit der Verwendung eines Produkts zusammenhängen, sind nicht Gegenstand des DA-E, vgl. Erwägungsgrund 22 DA-E.

27 Diese Frage aufwerfend Gerpott CR 2022, 271 (275).

28 Ein solches allgemeines Datenzugangsrecht unter spezifischen Voraussetzungen befürwortend: von Grafenstein, Discussion Paper Reconciling Conflicting Interests in Data through Data Governance, An Analytical Framework, abrufbar unter: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4104502.

d) Rechte und Pflichten der Nutzer

Data Accessibility by Default

Nach Art. 3 Abs. 1 DA-E müssen Produkte so konzipiert und hergestellt und verbundene Dienste so erbracht werden, dass die bei ihrer Nutzung erzeugten Daten standardmäßig für den Nutzer einfach, sicher und – soweit relevant und angemessen – direkt zugänglich sind. Möglich ist dies zB über Benutzeroberflächen. Ob der Datenzugang tatsächlich realisiert wird, liegt in der Entscheidung des Nutzers, den insoweit die Aktionslast trifft. Es wird sich gerade nicht dafür entschieden, dass der Nutzer die Daten standardmäßig erhält, sondern dass er sie erhalten kann, wenn er entsprechende Maßnahmen trifft. Anders wäre dies nur, wenn die Daten neben der Speicherung in der technisch-faktischen Herrschaftssphäre des Herstellers standardmäßig und automatisiert zumindest auch in Speichermedien abgelegt würden, die in der technisch-faktischen Herrschaftssphäre des Nutzers liegen, zB an einem nutzerkontrollierten Cloud-Speicherort. Insofern normiert der DA-E zwar eine „Data Accessibility by Default", faktisch bedeutet dies aber gerade keine technisch-faktische Zuordnung der Daten zum Nutzer, sondern zum Hersteller. Die technisch-faktische Herrschaft des Herstellers ist der Grundsatz, sie wird nur dort durchbrochen, wo der Nutzer von seinen Zugangsmöglichkeiten Gebrauch macht.

Der Datenzugang kann etwa dadurch befriedigt werden, dass die Daten direkt von einem Datenspeicher auf dem Gerät oder von einem entfernten Server, an den die Daten übermittelt werden, bereitgestellt werden. Ob der Zugang zu Datenspeichern auf dem Gerät über kabelgebundene oder drahtlose lokale Funknetze ermöglicht wird, die mit einem öffentlich zugänglichen elektronischen Kommunikationsdienst oder einem Mobilfunknetz verbunden sind, ist irrelevant. Bei dem Server kann es sich um die eigenen lokalen Serverkapazitäten des Herstellers oder um die eines Dritten oder eines Cloud-Diensteanbieters handeln, vgl. Erwägungsgrund 21 DA-E. Der Datenzugang erfordert daher gerade nicht zwingend eine Datenübermittlung, sondern kann ohne besondere Voraussetzungen als bloßer In-situ-Zugang gewährleistet werden.

Datenzugangsanspruch, Art. 4 DA-E

Soweit der Nutzer nicht direkt vom Produkt aus auf die Daten zugreifen kann, stellt der Dateninhaber dem Nutzer nach Art. 4 Abs. 1 DA-E die bei der Nutzung eines Produkts oder verbundenen Dienstes erzeugten Daten unverzüglich, kostenlos und ggf. kontinuierlich und in Echtzeit zur Verfügung, und zwar auf einfaches Verlangen auf elektronischem Wege, soweit dies technisch machbar ist. Erfasst sind sowohl vom Nutzer absichtlich aufgezeichnete Daten, als auch Daten, die als Nebenprodukt von Nutzeraktionen erzeugt werden, wie zB Diagnosedaten, als auch Daten, die ohne jegliche Nutzeraktion anfallen, zB wenn sich das Produkt im Bereitschaftszustand befindet, sowie Daten, die aufgezeichnet werden, während das Produkt ausgeschaltet ist, vgl. Erwägungsgrund 17 DA-E. Es kommt allein darauf an, dass die Daten im rechtmäßigen Besitz des Nutzers erzeugt werden, ohne dass es auf die konkrete Nutzung ankommt und ohne dass es darauf ankommt, dass der Nutzer tatsächlich einen Beitrag zur Datengenerierung leistet, der über den rechtmäßigen Besitz des Produkts hinausgeht.[29] Auch die beim Betrieb eines vernetzten Fahrzeugs aufgezeichnete Wetterdaten sind daher zB vom Datenzugangsanspruch umfasst.

Der Datenzugangsanspruch bezieht sich allerdings nur auf die konkret erzeugten Daten, nicht auch auf abgeleitete Daten, sofern diese „rechtmäßig erlangt wurden", vgl. Erwägungsgrund 17 DA-E. Unrechtmäßig erlangte abgeleitete Daten sind im Umkehrschluss aber sehr wohl erfasst. Wann abgeleitete Daten rechtmäßig oder unrechtmäßig erlangt wurden, stellt der DA-E nicht klar. Es dürfte sich aber insbesondere dann um unrechtmäßig erlangte abgeleitete Daten handeln, wenn die zu Grunde liegenden Daten unrechtmäßig verarbeitet und als Ergebnis dieser Verarbeitung Daten abgeleitet werden. Es wird daher insbesondere auf die Einhaltung der Vorgaben von DS-GVO, dem Geschäftsgeheimnisschutz aber auch vertraglicher Vereinbarungen ankommen. Weshalb abgeleitete Daten jedenfalls dann, wenn sie rechtmäßig erlangt wurden, nicht vom Datenzugangsanspruch umfasst sind, erklärt der DA-E nicht. Auch sie tragen einen Nutzerbezug in sich, weshalb sich gerade in Anbetracht des Ziels des DA-E, eine gerechte Verteilung der Wertschöpfung aus Daten zu gewährleisten, ein sich auch auf sie beziehender Datenzugangsanspruch rechtfertigen ließe.[30] Da hier aber ein „Mehr" an Wertschöpfung des Dateninhabers vorliegt, wäre eine Nutzungsbeschränkung für abgeleitete Daten iSe gerechten Verteilung der Wertschöpfung denkbar.[31]

■ Voraussetzung des Datenzugangsanspruchs, Verhältnis zu Art. 3 DA-E

Voraussetzung des Datenzugangsanspruchs ist das einfache Nutzerverlangen, an das keine weiteren Anforderungen gestellt werden. Insbesondere sind weder spezifische Form- oder Fristvorgaben einzuhalten. Der Datenzugangsanspruch setzt darüber hinaus voraus, dass der Nutzer nicht direkt vom Produkt aus auf die Daten zugreifen kann. Das wirft die Frage nach dem Verhältnis des Datenzugangsanspruchs nach Art. 4 DA-E zur Data Accessibility by Design nach Art. 3 DA-E auf. Denn wenn ein Produkt bereits so konzipiert werden muss, dass die bei seiner Nutzung erzeugten Daten standardmäßig für den Nutzer zugänglich sind, ist ein Datenzugangsanspruch nicht mehr erforderlich. Die Daten wären ohnehin durch den Nutzer selbständig abrufbar, ohne dass es einer Mitwirkung des Dateninhabers bedürfte. Art. 3 DA-E sieht aber allein vor, dass dem Nutzer die bei der Nutzung erzeugten Daten standardmäßig einfach und sicher zur Verfügung gestellt werden. Nur wo dies relevant und angemessen ist, müssen die Daten auch standardmäßig direkt zugänglich sein. Wann eine solche Relevanz und Angemessenheit eines standardmäßig direkten Datenzugangs vorliegen soll, dazu schweigen sowohl der Verordnungstext als auch die Erwägungsgründe. Stellt sich ein standardmäßig direkter Datenzugang nicht als relevant und angemessen dar, ist der Nutzer auf den Datenzugangsanspruch verwiesen. Dasselbe dürfte für den Fall gelten, dass der Dateninhaber seiner Verpflichtung aus Art. 3 DA-E nicht nachkommt.[32] Der Datenzugangsanspruch verpflichtet den Dateninhaber iÜ nicht dazu, die betreffenden Daten zu speichern. Löscht er sie, ist er schon kein Dateninhaber iSd Art. 2 Nr. 6 DA-E mehr und damit auch nicht zum Datenzugang verpflichtet.[33] Im Interesse einer gerechten Verteilung der Wertschöpfung aus Daten auf die Akteure der Datenwirtschaft, wie sie der DA-E intendiert, sollte dem Nutzer aber jedenfalls vor einer Löschung die Gelegenheit zum Datenzugang gegeben werden müssen.

---

29 Zweifelnd: Bomhard/Merkle RDi 2022, 168 Rn. 11.

30 Krit. ebenfalls: Leistner/Antoine, IPR and the use of open data and data sharing initiatives by public and private actors, S. 16, abrufbar unter: https://www.europarl.europa.eu/RegData/etudes/STUD/2022/732266/IPOL_STU(2022)732266_EN.pdf.

31 Dafür: Drexl/Banda/Gonzalez Otero/Hoffmann/Kim/Kulhari/Moscon/Richter/Wiedemann, Position Statement of the Max Planck Institute for Innovation and Competition of 25 May 2022 on the Commission's Proposal of 23 February 2022 for a Regulation on harmonised rules on fair access to and use of data (Data Act), Rn. 25 ff., abrufbar unter: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4136484.

32 Drexl/Banda/Gonzalez Otero/Hoffmann/Kim/Kulhari/Moscon/Richter/Wiedemann, Position Statement of the Max Planck Institute for Innovation and Competition of 25 May 2022 on the Commission's Proposal of 23 February 2022 for a Regulation on harmonised rules on fair access to and use of data (Data Act), Rn. 79, abrufbar unter: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4136484.

33 Bomhard/Merkle RDi 2022, 168 Rn. 41 f.

Ausgestaltung des Datenzugangs

Für Nutzer und Dateninhaber von erheblicher Bedeutung dürfte die Frage sein, ob es sich beim Datenzugangsanspruch des Nutzers um einen Anspruch auf Datenportabilität handelt, dem Nutzer die Daten also tatsächlich zu übermitteln sind und der Dateninhaber die Daten bei Ausübung des Datenzugangsanspruchs ggf. sogar zu löschen hat, oder ob das Zugangsrecht auch als bloßes in-situ-Recht ausgestaltet werden kann, es sich also darauf beschränken kann, dass der Nutzer die Daten beim Dateninhaber ansehen und allenfalls auf den Servern des Dateninhabers verarbeiten kann.[34] Erwägungsgrund 21 DA-E spricht deutlich für ein solches in-situ-Recht: „Er [der Datenzugang] kann so ausgestaltet sein, dass ein Dritter die Daten auf dem Produkt oder auf einer Rechnerinstanz des Herstellers verarbeiten kann." Eine bloße In-situ-Bereitstellung ohne besondere Voraussetzungen steht einer gerechten Verteilung der Wertschöpfung deutlich entgegen. Sie sollte daher allenfalls als Ausnahme möglich, der Grundsatz sollte eine Datenübermittlung sein.

Datenzugang zu Gunsten Dritter

Auf Verlangen des Nutzers oder einer im Namen des Nutzers handelnden Partei stellt der Dateninhaber nach Art. 5 Abs. 1 DA-E die bei der Nutzung eines Produkts oder verbundenen Dienstes erzeugten Daten einem Dritten unverzüglich, für den Nutzer kostenlos, in derselben Qualität, die dem Dateninhaber zur Verfügung steht, ggf. kontinuierlich und in Echtzeit zur Verfügung. Eine Aufbereitung der Daten ist nicht geschuldet.[35] Ein eigener Datenzugangsanspruch des Dritten wird nicht normiert. Dritter ist nach Art. 2 Nr. 7 DA-E ein Datenempfänger, dem der Dateninhaber auf Verlangen des Nutzers oder im Einklang mit einer Rechtspflicht aus anderen Rechtsvorschriften der Union oder aus nationalen Rechtsvorschriften zur Umsetzung des Unionsrechts Daten bereitstellt. Die von dem Anspruch auf Drittbereitstellung erfassten Daten unterscheiden sich ebenso wenig von denjenigen, die dem Nutzer selbst nach Art. 4 Abs. 1 DA-E zur Verfügung zu stellen sind, wie sich auch die Bereitstellungsmodi nicht unterscheiden. Auch hier ist also eine In-situ-Erfüllung ohne besondere Anforderungen möglich.

Es sind keine Anhaltspunkte dafür ersichtlich, dass der Anspruch auf Drittbereitstellung nach Art. 5 Abs. 1 DA-E in einem Alternativverhältnis zum Anspruch auf Datenbereitstellung zu Gunsten des Nutzers nach Art. 4 Abs. 1 DA-E stehen soll. Beide Ansprüche können kumulativ geltend gemacht werden. Dies sollte gesetzlich klargestellt werden. Nicht als Dritte agieren können allerdings Unternehmen, die zentrale Plattformdienste erbringen und für mindestens einen dieser Dienste als Gatekeeper iSd DMA benannt wurde, Art. 5 Abs. 2 DA-E. An sie ist eine Datenweitergabe seitens der Dateninhaber auch auf Nutzerverlangen hin unzulässig.

Schranken des Datenzugangsanspruchs

Der Datenzugangsanspruch des Nutzers unterliegt den Schranken der DS-GVO, dh jeder Datenzugang muss mit den Vorgaben der DS-GVO vereinbar sein. Der DA-E enthält insofern ein klares Vorrangverhältnis der DS-GVO, das aber wenig problematisch ist, weil die Datenzugangsverpflichtungen die Erlaubnistatbestände der DS-GVO konkretisieren und ausfüllen, wo diese Konkretisierungsmöglichkeiten und Öffnungsklauseln enthalten.[36] Problematischer scheint jedenfalls auf den ersten Blick das Verhältnis zum Geschäftsgeheimnisschutz. Im Verhältnis zum Nutzer gilt nach Art. 4 Abs. 3 DA-E, dass Geschäftsgeheimnisse nur offengelegt werden, „wenn alle besonderen Maßnahmen getroffen worden sind, um die Vertraulichkeit der Geschäftsgeheimnisse, insbesondere gegenüber Dritten, zu wahren." Dazu dürften vor allem Geheimhaltungsvereinbarungen zählen.[37] Der DA-E normiert damit einen Vorrang des Datenzugangsanspruchs gegenüber dem Geschäftsgeheimnisschutz jedenfalls im Verhältnis Nutzer – Dateninhaber. Dies wird den grundrechtlich geschützten Rechten und Interessen der Dateninhaber nicht gerecht.[38]

Datenverarbeitungsverbote des Nutzers

Nach Art. 4 Abs. 4 DA-E darf der Nutzer die erlangten Daten nicht zur Entwicklung eines Produkts nutzen, das mit dem Produkt, von dem die Daten stammen, im Wettbewerb steht. Wann dies der Fall ist, wird weder durch den Verordnungstext noch durch die Erwägungsgründe vorgegeben und sollte ergänzt werden.[39] Darüber hinaus darf der Nutzer die Daten zwar frei nutzen,[40] ist das Datenzugangsrecht des Nutzers aber als reines in-situ-Recht ausgestaltet, kann er sie technisch-faktisch nur sehr beschränkt nutzen, weil er sie etwa nicht an Dritte übermitteln kann. Die rechtliche Freiheit von Beschränkungen ist insofern jedenfalls so lange ein nur scheinbarer Gewinn für den Nutzer, wie dem Nutzer nicht auch die technisch-faktische Möglichkeit der Nutzung gewährt wird. Das Recht des Nutzers ist kein absolutes Recht. Ansprüche gegen die unberechtigte Nutzung von Daten entgegen Art. 4 Abs. 6 DA-E begründen damit allein Schadensersatz- und Unterlassungsansprüche gegen den Vertragspartner, nicht aber gegen Dritte.

e) Rechte und Pflichten der Dateninhaber

Recht zur Nutzung der Daten auf vertraglicher Grundlage, Art. 4 Abs. 6 DA-E

Der Dateninhaber darf nicht-personenbezogene Daten, die bei der Nutzung eines Produkts oder verbundenen Dienstes erzeugt werden, allein auf Grundlage einer vertraglichen Vereinbarung mit dem Nutzer nutzen. Dies mag zunächst als hohe Hürde erscheinen und insbesondere im Vergleich mit den Vorgaben des Datenschutzrechts fällt auf, dass die Verarbeitung personenbezogener Daten nach Art. 6 und 9 DS-GVO niedrigeren Vorgaben unterliegt, weil die Einwilligung nur eine von mehreren Rechtsgrundlagen ist, personenbezogene Daten zu verarbeiten.[41] (Ein Vergleich mit der datenschutzrechtlichen Verarbeitungsbefugnis nach Art. 6 Abs. 1 lit. b DS-GVO würde iÜ hinken, weil Art. 6 Abs. 1 lit. b DS-GVO eine Verarbeitung, die für die Erfüllung eines Vertrags erforderlich ist, gestattet, was aber etwas völlig anderes ist als die Verarbeitung auf Grundlage einer vertraglichen Vereinbarung, mit der der Nutzer der Verarbeitung zustimmt. Vergleichsmaßstab muss daher Art. 6 Abs. 1 lit. a DS-GVO sein.)

Ebenso wie die datenschutzrechtliche Einwilligung ist aber auch die in Art. 4 Abs. 6 DA-E geforderte vertragliche Vereinbarung eine allzu leicht zu überwindende Hürde und sichert lediglich formale Selbstbestimmung. Denn der Vertrag zwischen Nutzer und Dateninhaber ist zumindest dann, wenn es sich beim Nutzer um eine natürliche Person handelt, keinen adäquaten Verbraucherschutzvorgaben unterworfen. Zwar wird es sich, wenn der Dateninhaber nicht allein der Hersteller des Produkts ist, sondern sich auch vertraglich gegenüber dem Nutzer zur Bereitstellung des digitalen Produkts verpflichtet und der Nutzer Verbraucher iSd § 13 BGB ist, bei diesem Vertrag nicht selten um einen Vertrag über Sachen mit digitalen Elementen iSd § 327 Abs. 2 BGB handeln. Aus den §§ 327 ff. BGB ergeben sich aber keine Schutzmechanismen, die dem Nutzer die erforderliche materia-

34 Grundlegend: Kerber, Governance of IoT-Data, S. 5, abrufbar unter: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4080436.
35 Gerpott CR 2022, 271 (275).
36 S. dazu bereits oben unter 3.
37 Hennemann/Steinrötter NJW 2022, 1481 Rn. 18.
38 BDI-Stellungnahme zum Legislativvorschlag eines DA-E, S. 15, abrufbar unter: https://bdi.eu/publikation/news/legislativvorschlag-des-eu-data-act-datennutzung-datenwirtschaft/.
39 BDI-Stellungnahme zum DA-E, S. 9.
40 Hennemann/Steinrötter NJW 2022, 1481 Rn. 19.
41 Hennemann/Steinrötter NJW 2022, 1481 Rn. 15; Bomhard/Merkle RDi 2022, 168 Rn. 50.

le Selbstbestimmung bei Abgabe seiner Erklärung nach Art. 4 Abs. 6 DA-E zusichern würden. Nach Vorstellung des Gesetzgebers soll die Klauselrichtlinie (RL 93/13/EWG) auf diesen Vertrag Anwendung finden, vgl. Erwägungsgrund 26 DA-E. Da es sich aber bei der Erlaubnis der Datennutzung häufig um die Hauptleistungspflicht des Nutzers handeln dürfte und die AGB-Kontrolle für Hauptleistungspflichten nicht gilt, Art. 4 Abs. 2 RL 13/93/EWG, ist auch dies kein adäquates Schutzinstrument. Auf Grundlage vermeintlicher (weil in Ermangelung der erforderlichen Verbraucherschutzinstrumente nur formaler, nicht aber materialer) Selbstbestimmung kann sich der Dateninhaber die Nutzungsmöglichkeit der Daten in jeder Hinsicht sichern, die er zur vertraglichen Vereinbarung vorgibt, mit Ausnahme des in Art. 4 Abs. 2 DA-E normierten Verbotes, Daten zu verwenden, um daraus Einblicke in die wirtschaftliche Lage, Vermögenswerte und Produktionsmethoden des Nutzers oder in die Nutzung durch den Nutzer zu erlangen, wenn dies gewerbliche Positionen des Nutzers auf den Märkten, auf denen er tätig ist, untergraben könnte. Der Dateninhaber ist daher frei, umfassende Buy-out-Verträge einseitig vorzugeben, die ihn dazu berechtigen, die Daten ungehindert an Dritte gegen Entgelt weiterzureichen, zu sämtlichen Zwecken, auch an zentrale Plattformdienste iSd DMA, was dem Nutzer noch verboten ist. Es mag sein, dass der DA-E mit Art. 4 Abs. 6 eine de facto Zuordnung der Daten an den Nutzer intendierte[42] und auch dies wäre freilich die falsche Lösung, denn Daten sollten gerade keiner ausschließlichkeitsrechtlichen Zuordnung unterliegen, gelungen ist dem Data Act eine nutzerfreundliche Regulierung aber ohnehin nicht. Ganz im Gegenteil sichert Art. 4 Abs. 6 DA-E rechtlich die technisch-faktische Möglichkeit der Datennutzung durch den Dateninhaber vollständig ab.[43] Hätte der europäische Gesetzgeber eine gerechte Verteilung der Wertschöpfung aus Daten erreichen wollen, hätte er entweder eine standardmäßige Speicherung auch in der Herrschaftssphäre des Nutzers vorgesehen[44] oder jedenfalls das Zugangsrecht des Nutzers nicht als bloßes in-situ-Recht ausgestattet und im Verhältnis Nutzer – Hersteller die erforderlichen Schutzvorgaben normiert.

Die Einwilligung allein granularer auszugestalten und entsprechende Informationspflichten zu verankern, würde dieses Problem iÜ nicht beheben, da aus der Konsumentenverhaltensforschung zur Genüge bekannt ist, dass Informationen nicht zwingend zu einer besseren Entscheidungsfähigkeit des Verbrauchers beitragen, sondern – ganz im Gegenteil – ab einer individuell zu bestimmenden Informationsmenge die Informationsaufnahme nachlässt oder sogar gänzlich abbricht.[45] Aus dem Bereich allgemeiner Geschäftsbedingungen und Datenschutzerklärungen ist dies auch als „clicking without reading"-Phänomen bekannt,[46] das auf verschiedene Marktversagen zurückzuführen ist.[47]

Erforderlich ist vielmehr die zwingende Ausgestaltung von Art. 3–5 DA-E, der Vertrag zwischen Dateninhaber und Nutzer nach Art. 4 Abs. 6 DA-E sollte einem Verbot der Koppelung von Nutzung des Produkts/verbundenen Dienstes und einem „Total-Buy-out" unterworfen werden. Kündigungsmöglichkeiten und zeitliche Begrenzungen sollten vorgesehen werden. Beachtlich ist, dass dann, wenn der Nutzer eine juristische Person ist, zumindest die Missbrauchskontrolle des Art. 13 DA-E Anwendung findet. Dies legen der Tatbestand des Art. 13 Abs. 4 lit. c DA-E nahe, der anderenfalls keinen Anwendungsbereich hätte, aber auch die Stellung des Art. 13 in einem eigenen Kapitel „Missbräuchliche Klauseln in Bezug auf den Datenzugang und die Datennutzung zwischen Unternehmen". Das wiederum bedeutet, dass der Datennutzer in Gestalt juristischer Personen (zB der Landwirt) nach dem Verordnungsentwurf besser geschützt ist als der Verbraucher.

Neben den erforderlichen Schutzvorgaben zu Gunsten des Verbrauchers ist die Frage zu klären, nach welchem Recht sich der nach Art. 4 Abs. 6 DA-E abzuschließende Vertrag beurteilt, zB was seine Rechtsnatur und seine Kündigungsmöglichkeit betrifft.[48]

Datenverarbeitungsverbot, Art. 4 Abs. 2 DA-E

Der Dateninhaber unterliegt im Verhältnis zum Nutzer lediglich dem bereits genannten Datenverarbeitungsverbot aus Art. 4 Abs. 2 DA-E. Die Datenverarbeitungsverbote aus Art. 5 Abs. 2 lit. c und Art. 5 Abs. 3 DA-E gelten im Verhältnis des Dateninhabers zum Dritten. Es ist allerdings nicht verständlich, weshalb den Dateninhaber zwar eine Pflicht nach Art. 5 Abs. 3 S. 2 DA-E trifft, keine Informationen über den Zugang des Dritten zu den verlangten Daten aufzubewahren, die über das hinausgehen, was für die ordnungsgemäße Ausführung des Zugangsverlangens des Dritten und für die Sicherheit und Pflege der Dateninfrastruktur erforderlich ist, dies aber gegenüber dem Verbraucher nicht gelten soll. Art. 5 Abs. 3 S. 2 DA-E ist hier um das Verhältnis Verbraucher – Dateninhaber zu ergänzen.

Vorvertragliche Informationspflichten, Art. 3 Abs. 2 DA-E

Art. 3 Abs. 2 DA-E begründet vorvertragliche Informationspflichten. Nach Art. 3 Abs. 2 DA-E richtet sich diese Verpflichtung aber gerade nicht an alle Vertragspartner der Nutzer, sondern nur an den Dateninhaber, der zugleich Hersteller des Produkts oder des verbundenen Dienstes ist. Die entsprechenden Informationen werden daher herstellerseitig als „Beipackinformationen" in der Lieferkette zur Verfügung gestellt werden. Dem Nutzer werden danach in einem klaren und verständlichen Format bereitgestellt:

„a) Art und Umfang der Daten, die voraussichtlich bei der Nutzung des Produkts oder verbundenen Dienstes erzeugt werden;

b) ob die Daten voraussichtlich kontinuierlich und in Echtzeit erzeugt werden;

c) wie der Nutzer auf diese Daten zugreifen kann;

d) ob der Hersteller, der das Produkt liefert, oder der Dienstleister, der den verbundenen Dienst erbringt, beabsichtigt, die Daten selbst zu nutzen oder einem Dritten die Nutzung der Daten zu gestatten, und falls ja, für welche Zwecke diese Daten genutzt werden sollen;

e) ob der Verkäufer, Mieter oder Leasinggeber der Dateninhaber ist und, falls nicht, die Identität des Dateninhabers, zB sein Handelsname und die Anschrift des Ortes, an dem er niedergelassen ist;

f) die Kommunikationsmittel, mit denen der Nutzer den Dateninhaber schnell kontaktieren und effizient mit diesem kommunizieren kann;

g) wie der Nutzer veranlassen kann, dass die Daten an einen Dritten weitergegeben werden;

---

42 Davon gehen Hennemann/Steinrötter aus, NJW 2022, 1418 Rn. 15.

43 So bereits Kerber, Governance of IoT-Data, S. 6, abrufbar unter: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4080436.

44 Vgl. dazu bereits unter V.1.

45 Alemanno/Sibony, Nudge and the Law, 2015; Hacker, Verhaltensökonomik und Normativität, 2017; Schmölke, Grenzen der Selbstbindung im Vertragsrecht, 2014; Sibony/Micklitz/Esposito, Research Methodes in Consumer Law, 2018; Zamir/Teichmann, Behavioural Law and Economics, 2018.

46 Khong, The Clicking Without Reading Problem, abrufbar unter: https://papers.sioe.org/paper/551.html; Hennemann/Steinrötter NJW 2022, 1481 Rn. 14: „click and forget".

47 Für den Bereich personenbezogener Daten vgl. hierzu Specht FS Tinnefeld – im Erscheinen.

48 Es bietet sich eine Bestimmung nach der Rom-I-VO an, vgl. Hennemann/Steinrötter NJW 2022, 1481 Rn. 16.

h) das Recht des Nutzers, bei der in Art. 31 DA-E genannten zuständigen Behörde Beschwerde wegen eines Verstoßes gegen die Bestimmungen dieses Kapitels einzulegen."

f) Kritik und Abhilfemöglichkeiten

Kritik an den Regelungen des DA-E ist eine Frage der Perspektive. Der DA-E verfolgt mehrere Ziele, deren Verwirklichung teils unterschiedliche Maßnahmen erfordern. Eine gerechte Verteilung der Wertschöpfung auf die Akteure der Datenwirtschaft ist jedenfalls zT durch andere Maßnahmen zu erreichen als die wirksame Stärkung der Handlungskompetenz der Menschen in Bezug auf ihre Daten oder die Förderung von Innovation. Die Zielsetzungen lassen sich – mit Ausnahme des Ziels, öffentliche Stellen besser mit einem angemessenen und vorhersehbaren Mechanismus für die Bewältigung wichtiger politischer und gesellschaftlicher Herausforderungen auszustatten – auch nicht auf einzelne Kapitel beschränken, sondern sollen kumulativ in den Kapitel I–IV verfolgt werden. Die Einzelkritik soll daher aus den verschiedenen Zielperspektiven vorgetragen werden. Es ist aber auch ein systemischer Kritikpunkt zu äußern, der die vom Data Act gewählte Daten-Governance insgesamt betrifft. Denn diese Daten-Governance unterminiert sämtliche vom Data Act gesetzten Ziele und dient ausschließlich dem Investitionsschutz des technisch-faktischen Datenhalters. Diese systemische Kritik ist der Einzelkritik in den nachfolgenden Ausführungen zum Verhältnis Nutzer – Dateninhaber vorangestellt.

Systemische Kritik

Systemisch ist zu sehen, dass der DA-E entgegen dem ersten Eindruck, den die Normierung von Datenzugangsansprüchen erweckt, eine Daten-Governance vorsieht, mit der in erster Linie die technisch-faktische Herrschaft des Dateninhabers legitimiert wird. Dies wird durch folgende drei Instrumente des DA-E deutlich: Erstens, der Dateninhaber behält die technisch-faktische Kontrolle über die Daten und jeder Datenzugang ist als Ausnahme rechtfertigungsbedürftig. Rechtfertigungsbedürftig sein muss aber im Grunde bereits die rechtliche Absicherung der technisch-faktischen Herrschaft des Dateninhabers, die der DA-E nicht erklärt, sondern schlicht voraussetzt. Die vom DA-E adressierten Daten liegen in der Public Domain,[49] das bedeutet aber nicht, dass diese Daten nach Belieben technisch monopolisiert werden dürfen. Weshalb der technisch-faktische Dateninhaber in allen Sektoren derjenige sein sollte, der auch rechtlich mit den Daten nach Belieben verfahren darf, ist zumindest nicht selbstverständlich. Ja, die Datenerzeugung beruht auf Investitionen der Produkt- und Sensorenhersteller,[50] IoT ist nicht umsonst zu haben. Ohne den Nutzer können die Daten aber eben auch nicht entstehen. Darüber hinaus war man sich bislang jedenfalls für den Bereich des Urheberrechts sehr einig, dass diese Investition in die Generierung von Daten gerade nicht schutzrechtsbegründend sein soll.[51] Zu Recht wurde auch von der Etablierung eines Dateneigentums abgesehen, das eben diese Investitionsleistung geschützt hätte, wenn es dem Hersteller oder Erwerber der Datenerhebungsgerätschaften/Software zugeordnet worden wäre. Ein solches Dateneigentum hätte der Rechtfertigung bedurft und diese Rechtfertigung konnte nicht gefunden werden.[52] Dasselbe gilt aber auch für eine starke technisch-faktische Position des Dateninhabers, die rechtlich mit spezifischen Nutzungs- und Abwehrbefugnissen unterlegt wird. Insoweit ist es durchaus gerechtfertigt, die Frage zu stellen, wer im Ausgangspunkt derjenige sein sollte, der die Daten hält und wessen Datenzugang sodann gesetzlich normiert werden muss. Auch dem Nutzer könnten die erzeugten Daten standardmäßig und automatisiert zB in einer Cloud zur Verfügung gestellt werden (es sei denn, der Nutzer optiert aus oder es stehen schützenswerte Interessen des Dateninhabers entgegen; Data Access statt Data Accessibility by Design and Default). Der Aufschrei wäre sicherlich ungleich größer. Denn Design und Default der Datenhaltung bestimmen über die Aktionslast zur Datenerlangung, die mit erheblichem Aufwand und – sofern über den Datenzugang Streit besteht – auch mit erheblichen Kosten verbunden sein kann. Es ist also von nicht zu unterschätzendem Vorteil, derjenige zu sein, der den Datenzugang gewährt, anstatt derjenige, der um ihn ersucht.

Zweitens zeigt Erwägungsgrund 21 DA-E deutlich, dass das Datenzugangsrecht des Nutzers als bloßes in-situ-Recht ausgestaltet werden kann[53] und damit nicht geeignet ist, die technisch-faktische Herrschaft der Dateninhaber anzutasten. Und drittens: Art. 4 Abs. 6 DA-E enthält zwar die Vorgabe, dass der Dateninhaber die Daten nur auf Grundlage einer vertraglichen Vereinbarung mit dem Nutzer nutzen darf, diese vertragliche Vereinbarung ist aber in Anbetracht fehlender Schutzvorgaben für den Nutzer eine allzu leicht zu überwindende Hürde. Bereits aus dem Datenschutzrecht wissen wir, wie wenig tauglich das Instrument der Einwilligung ist, um tatsächliche (materiale) Selbstbestimmung zu gewährleisten, solange nicht Informationsasymmetrien beseitigt, Transaktionskosten gesenkt und Rationalitätsproblemen begegnet wird.[54] Dies gilt nicht minder für die in Art. 4 Abs. 6 DA-E vorgesehene vertragliche Vereinbarung. Der Dateninhaber ist hier nach dem derzeitigen Entwurfstext frei, im Verhältnis zum Nutzer einseitig umfassende „Buy-out-Verträge" vorzugeben.[55] Die politischen Ziele, denen der DA-E verpflichtet ist, werden mit dieser Daten-Governance nicht erreicht.[56] Hierfür erforderlich ist vielmehr eine Daten-Governance, die die Wertschöpfungsanteile von Dateninhabern und Nutzern gleichermaßen berücksichtigt. Den Data-Act zu Gunsten sektorspezifischer Regulierung zurückzuziehen oder jedenfalls sektorspezifische Vorrangregeln vorzusehen, scheint noch immer eine reale Option.[57] Auch wenn die Entscheidung zu Gunsten einer horizontalen Regulierung aber aufrecht erhalten bleibt und die Entscheidung über den Default der Datenhaltung weiterhin zu Gunsten der Dateninhaber ausfällt, lässt sich eine angemessene Berücksichtigung der Nutzerposition durchaus auch innerhalb der jetzt vorgeschlagenen Regelungen noch nacharbeiten. Ansatzpunkte sind hier die Stärkung des Datenzugangsrechts des Nutzers (in-situ-Recht als Ausnahme, Datenübermittlung als Regel) sowie eine adäquate Ausgestaltung der Vertragsbeziehung nach Art. 4 Abs. 6 DA-E mit einem Verbot der Koppelung von Nutzung des Produkts/verbundenen Dienstes und einem Total-

49 Drexl/Banda/Gonzalez Otero/Hoffmann/Kim/Kulhari/Moscon/Richter/Wiedemann, Position Statement of the Max Planck Institute for Innovation and Competition of 25 May 2022 on the Commission's Proposal of 23 February 2022 for a Regulation on harmonised rules on fair access to and use of data (Data Act), Rn. 49, abrufbar unter: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4136484.

50 BDI-Stellungnahme zum Legislativvorschlag des DA-E, S. 11; dafür auch Bomhard/Merkle RDi 2022, 168 (170), die allerdings dafür den Hersteller von seiner Adressatenstellung befreien und allein den Sensorhersteller adressieren wollen.

51 So für § 87a UrhG, vgl. EuGH MMR 2005, 29 mAnm Hoeren – BHB-Pferdewetten; EuGH Urt. v. 9.11.2004 – C-338/02 – Fixtures-Fußballspielpläne I; EuGH Urt. v. 9.11.2004 – C-444/02 – Fixtures-Fußballspielpläne II; EuGH Urt. v. 9.11.2004 – C-46/02 – Fixtures-Fußballspielpläne III; Wiebe CR 2014, 1 (4).

52 Vgl. dazu auch bereits: Specht-Riemenschneider ZRP 2022 – im Erscheinen.

53 Kerber, Governance of IoT Data, S. 1, abrufbar unter: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4080436.

54 Specht FS Tinnefeld – im Erscheinen.

55 So auch Bomhard/Merkle RDi 2022, 168 (174).

56 So zutreffend: Kerber, Governance of IoT Data, S. 1, abrufbar unter: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4080436.

57 Dafür: Leistner/Antoine, IPR and the use of open data and data sharing initiatives by public and private actors, S. 16, abrufbar unter: https://www.europarl.europa.eu/RegData/etudes/STUD/2022/732266/IPOL_STU(2022)732266_EN.pdf.

Buy-Out sowie zwingenden Regelungen zu Gunsten des Verbrauchers. Alternativ ließe sich eine eigenständige Verwertungsmöglichkeit der Daten sowohl für Nutzer als auch für Dateninhaber unter Verzicht auf Art. 4 Abs. 6 DA-E vorsehen.

■ Schranken des Datenzugangsanspruchs angemessen mitdenken

Ausweitung der Schrankenregelung: Systemisch mitzudenken sind aber auch die Schranken des Datenzugangsanspruchs, die derzeit ebenfalls defizitär sind. Gegenüber dem Geschäftsgeheimnisschutz ist ein klares Vorrangverhältnis des Datenzugangs im Verhältnis Nutzer – Dateninhaber normiert. Dies könnte Dateninhaber selbst dann unzulässig in ihren Grundrechten und Grundfreiheiten beeinträchtigen, wenn alle Maßnahmen zwischen den Parteien getroffen wurden, um die Vertraulichkeit der Geschäftsgeheimnisse zu wahren, weil Wahrung von Vertraulichkeit voraussetzt, dass die Geschäftsgeheimnisse jedenfalls den Nutzern offengelegt werden, diese dann aber im Außenverhältnis zur Geheimhaltung verpflichtet sind. Pauschale Verweigerungsmöglichkeiten auf Grund vermeintlicher Geschäftsgeheimnisse sind indes ebenso wenig zweckdienlich. In Betracht sollte vielmehr eine Kombination einer Schrankenregelung nach dem Vorbild des Art. 15 Abs. 4 DS-GVO bzw. Art. 20 Abs. 4 DS-GVO und einer Datentreuhandlösung gezogen werden. Ebenso wie Art. 15 Abs. 4 und Art. 20 Abs. 4 DS-GVO vorsehen, dass das Recht auf Erhalt einer Kopie bzw. die Datenübertragung die Rechte und Freiheiten anderer Personen nicht beeinträchtigen darf, muss der Datenzugangsanspruch der Nutzer die Rechte und Freiheiten anderer Personen einschließlich des Dateninhabers nicht beeinträchtigen dürfen. Dies erfordert stets eine Einzelfallabwägung. Die dieser Einzelfallabwägung immanente Rechtsunsicherheit ist in Anbetracht der hier erforderlichen und durch eine Einzelfallabwägung herzustellenden größtmöglichen Einzelfallgerechtigkeit hinzunehmen. Wegen Unmöglichkeit ist eine Einrede oder Einwendung gegen den Datenzugang hingegen nicht erforderlich, denn diejenigen, die Daten nicht zugänglich machen können, sind schon nicht Dateninhaber und damit schon nicht zum Datenzugang verpflichtet. Die fehlende Unmöglichkeit ist damit bereits anspruchsbegründend.

Datentreuhandlösung: Kumulativ zu einer solchen offenen Schrankenbestimmung ist eine Datentreuhandlösung zur Gewährleistung der einem Datenzugangsanspruch entgegenstehenden Rechte und Freiheiten erforderlich. Eine „Datenzugangstreuhand" könnte als staatlich eingerichtete Stelle ähnlich wie der Koordinator für Digitale Dienste nach Art. 31 DSA zunächst und ggf. als reines In-situ-right-Zugang zu denjenigen Daten erhalten, die nach Auffassung des Dateninhabers entgegenstehende Rechte und Freiheiten beeinträchtigen. Sie könnte die Daten dann entsprechend prüfen, ggf. schwärzen oder andere Maßnahmen ergreifen, um die dem Datenzugang entgegenstehenden Rechte und Freiheiten zu wahren und den Datenzugang letztlich in einer Form anordnen oder auch selbst gewährleisten (zB umfassend, geschwärzt, nur teilweise oder in Ausnahmefällen als bloßer Lesezugriff), die einen angemessenen Ausgleich zur Wahrung des Datenzugangsanspruchs auf der einen und der entgegenstehenden Rechte und Interessen auf der anderen Seite gewährleistet. Im Extremfall könnte der Datenzugang auch gänzlich versagt werden. Diese Datentreuhandlösung hätte den Vorteil, dass Streitigkeiten über den Datenzugang nicht zunächst vom Dateninhaber zu entscheiden und vom Datennutzer anschließend gerichtlich anzugreifen sind, sondern Datentreuhandlösungen würden eine ex-ante Kontrollfunktion übernehmen, damit es erst gar nicht zur Beeinträchtigung von Rechten und Interessen von Dateninhabern und Nutzern kommt.

■ Ermöglichung abweichender Daten-Governance

Ob die vom DA-E gewählte Daten-Governance tatsächlich für sämtliche Sektoren richtig und gewünscht ist, darf aber ganz generell hinterfragt werden. Der DA-E täte gut daran, eine sektorspezifische Hintertür offen zu lassen, die eine alternative Daten-Governance dort ermöglicht, wo die technische Entwicklung dies zukünftig zulässt und wo dies gesellschaftlich und politisch erwünscht ist. Eine solche Daten-Governance könnte zB bedeuten, Daten nicht beim heutigen Dateninhaber speichern zu müssen, sondern in der eigenen technisch-faktischen Herrschaftssphäre der Nutzer oder eines Dritten speichern zu können. Dies könnte einerseits durch sektorspezifische Öffnungsklauseln realisiert werden, und andererseits mit entsprechend starken Nutzerrechten. Denn schon nach dem bisherigen Entwurfstext kann der Nutzer verlangen, die Daten bei einem Dritten und damit auch in einer Datentreuhand oder bei einer daten-altruistischen Person iSd OGA zu speichern. Das Verhältnis zwischen Nutzer und Drittem ist dabei nur rudimentär durch den DA-E ausgestaltet und stünde insofern jedenfalls in Bezug auf die an spezifische Dritte zu stellenden Anforderungen einer mitgliedstaatlichen Ausgestaltung zB in dem im Koalitionsvertrag vorgesehenen Datentreuhandgesetz offen. Aus der Datentreuhand heraus könnten die Daten dann entsprechend der Nutzervorgabe zB auch zu Forschungs- und Innovationszwecken anderen Stellen zugänglich gemacht werden. Sowohl die Möglichkeit alternativer Daten-Governance-Modelle durch sektorspezifische Öffnungsklauseln als auch durch starke Nutzerrechte sind zu empfehlen, um angemessen auf technische Entwicklungen reagieren zu können.

Detailkritik

Ist systemisch über Daten-Governance, den horizontalen Charakter des DA-E, seine Schranken und sektorspezifische Abweichungsmöglichkeiten entschieden, sollten die folgenden Korrekturen auf der Detailebene vorgenommen werden.

1. Maßnahmen zur angemessenen Verteilung der Wertschöpfung auf Akteure der Datenwirtschaft

a) In-situ-Zugang als Ausnahme

Der In-situ-Zugang der Datennutzer ist als Ausnahme vorzusehen, in der Regel sollte eine Datenübermittlung geschuldet sein. Mit einem bloßen In-situ-Zugang ist eine gerechte Verteilung der Wertschöpfung auf die Akteure der Datenwirtschaft nicht möglich. Ein solcher Zugang kann allenfalls als Ausnahme geschuldet sein, anderenfalls wird die Wertschöpfung aus Daten allein den technisch-faktischen Dateninhabern zugewiesen. Sowohl in den Erwägungsgründen, insbesondere in Erwägungsgrund 21 sowie in Art. 3 und 4 des Verordnungstextes sind hierfür Anpassungen erforderlich.

b) Abgeleitete Daten

Abgeleitete Daten sollten ebenfalls vom Datenzugangsanspruch umfasst sein, denn sie könnten ebenfalls nicht entstehen ohne die Mitwirkung des Verbrauchers. Abgeleitete Daten tragen allerdings ein „Mehr" an Wertschöpfung des technisch-faktischen Dateninhabers in sich und könnten daher in der Nutzung durch den Nutzer Restriktionen unterworfen werden.[58] Insbesondere Art. 4 und Erwägungsgrund 14 sind entsprechend anzupassen.

58 Drexl/Banda/Gonzalez Otero/Hoffmann/Kim/Kulhari/Moscon/Richter/Wiedemann, Position Statement of the Max Planck Institute for Innovation and Competition of 25 May 2022 on the Commission's Proposal of 23 February 2022 for a Regulation on harmonised rules on fair access to and use of data (Data Act), Rn. 25 ff., abrufbar unter: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4136484.

d) Zwingende Ausgestaltung von Art. 3 und 4 DA-E
Art. 3 und 4 DA-E sind im Hinblick auf die Nutzerbefugnisse zwingend auszugestalten. Zwar enthält Art. 8 Abs. 2 DA-E die Vorgabe, dass die Nutzerbefugnisse in dem zwischen Dateninhaber und Datenempfänger abgeschlossenen Vertrag nicht abbedungen werden können, es fehlt aber an einer solchen Regelung im Verhältnis Datennutzer – Dateninhaber. Der zwingende Rechtscharakter sollte auch für dieses Verhältnis im Verordnungstext vorgesehen werden.

e) Buy-out-Verträge vermeiden
Der Vertrag zwischen Dateninhaber und Nutzer nach Art. 4 Abs. 6 DA-E sollte Maßnahmen zur Vermeidung von Total-Buy-out-Verträgen unterworfen werden, zB einem Verbot der Koppelung von Nutzung des Produkts/verbundenen Dienstes und vertraglicher Zustimmung zur Datennutzung. Gesetzgeberisch vorgesehene Standardformulare für granulare Vereinbarungen empfehlen sich. Der Zweckübertragungsgedanke aus dem Urheberrrecht ließe sich fruchtbar machen. Kündigungsmöglichkeiten und zeitliche Begrenzungen sollten vorgesehen werden. Rationalitätsproblemen insbesondere durch Dark Patterns ist durch entsprechende gesetzliche Regelungen insbesondere zu den formalen Gestaltungsanforderungen an die Vereinbarung vorzubeugen. Es empfiehlt sich ein eigener Art. 4a, der diese Anforderungen an den Vertrag zwischen Nutzer und Dateninhaber normiert und in dem Art. 4 Abs. 6 DA-E aufgeht. Insgesamt kann hier zwischen gewerblichen Nutzern und Verbrauchern differenziert werden, sofern sich ein unterschiedlicher Schutzbedarf ergibt. Alternativ ist Art. 4 Abs. 6 DA-E zu streichen und zu ersetzen durch Regelungen, die die Nutzungsbefugnisse an den Daten gleichermaßen für Nutzer und Dateninhaber vorsehen und einschränken. Die Datenerhebung ist bislang über die E-Privacy-RL an den Nutzerwillen gebunden. Um die Regelungen zu Erhebung und Nutzung einheitlichen Regelungen zu unterwerfen, ließe sich auch die Erhebung in Art. 4 Abs. 6 bzw. einem neuen Art. 4a DA-E integrieren. Insbesondere bei Streichung der Vorgaben zur Datennutzung nach dem Nutzerwillen sollte die Datenerhebung weiterhin an den Nutzerwillen gebunden sein.

Der Dateninhaber wird durch den DA-E nicht zu einer Datenspeicherung verpflichtet, sondern der Datenzugang des Nutzers setzt eine tatsächlich fortdauernde Speicherung von Daten voraus. Der Dateninhaber kann sich insofern durch Löschung der Daten dem Datenzugangsanspruch entziehen, weil er nach der Löschung nicht mehr Dateninhaber iSd Art. 2 N. 6 DA-E ist. Um eine gerechte Verteilung der Wertschöpfung aus Daten zu gewährleisten, sollte dem Nutzer vor einer Löschung die Gelegenheit zum Datenzugang gegeben werden müssen.

Erweiterung des Art. 5 DA-E
Art. 5 Abs. 1 DA-E sollte klarstellen, dass das Recht der Datenübermittlung an den Dritten neben die Rechte des Nutzers nach Art. 3 und 4 DA-E tritt. Art. 5 Abs. 3 DA-E sollte auf das Verhältnis Nutzer – Datenhalter erstreckt werden.

Reverse Data Access
Der DA-E erfasst möglicherweise nicht alle relevanten Fälle des bei IoT-Produkten erforderlichen Datenzugangs. So scheint es jedenfalls denkbar, dass nicht der Dateninhaber die Daten in seiner technisch-faktischen Herrschaftssphäre hält, sondern, dass dies ausnahmsweise der Nutzer tut. Ebenso wie der Nutzer in Fällen der Co-Generierung von Daten, wie sie bei IoT-Produkten regelmäßig vorliegt, ein schützenswertes Interesse daran hat, die von ihm mitproduzierten Daten zu erhalten, hat der Dateninhaber ein solches schützenswertes Interesse, wenn der Nutzer ausnahmsweise der Dateninhaber ist. Sollte es derartige Fälle geben, empfiehlt sich iSe gerechten Verteilung der Wertschöpfung aus Daten auch ein Reverse Data Access, also ein Datenzugangsanspruch des Herstellers gegen den datenhaltenden Nutzer, der freilich aber identisch mit dem Datenzugangsanspruch des Nutzers gegen den Dateninhaber sein muss.

2. Maßnahmen zur Innovationsförderung
Ein Großteil der Maßnahmen zur Gewährleistung einer gerechten Verteilung der Wertschöpfung aus Daten im Verhältnis Nutzer – Dateninhaber fördert auch Innovation, sofern es dabei bleibt, dass der Datenzugang primär über den Nutzer gewährleistet wird. Auch dann braucht es zwingend starker Nutzerrechte, die entsprechende Datenübermittlungen an Dritte zu Innovationszwecken bewirken können. Darüber hinaus sollte das Datenverarbeitungsverbot des Nutzers in Art. 4 Abs. 4 DA-E konkretisiert werden. Innovation auf Grund der erlangten Daten sollte ermöglicht, nicht verhindert werden. Datennutzungsmöglichkeiten zu Innovationszwecken im Gemeinwohlinteresse in Abweichung von den Vorgaben der DS-GVO empfehlen sich zB in Artikel 6 ebenso wie Einschränkungen der nach der DS-GVO zulässigen Nutzung für besonders gefährliche Datenverarbeitungen, wie etwa Persönlichkeitsprofilbildungen.

3. Maßnahmen zur Stärkung der Handlungsbefugnisse der Nutzer
Von weitergehenden Informationspflichten „zu Gunsten" des Nutzers ist abzusehen, da sie Nutzern nicht helfen, sondern ihnen auf Grund der Informationsüberlastungsproblematik ab einer bestimmten Informationsmenge sogar eher schaden. Im kollektiven Nutzerinteresse an einer Stärkung der Handlungsbefugnisse liegt außerdem eine Datenverarbeitungsbefugnis des Herstellers zu Zwecken von Produktsicherheit und Produktentwicklung, und zwar unabhängig von einer vertraglichen Erlaubnis des Nutzers. Art. 4 Abs. 6 bzw. ein neuer Art. 4a DA-E könnte diese Handlungsbefugnisse des Dateninhabers beinhalten.

2. Verhältnis Dateninhaber – Datenempfänger
Das Verhältnis zwischen Dateninhaber und Datenempfänger ist in Kapitel 3 und 4 ausgestaltet. Nach Art. 8 Abs. 2 DA-E vereinbart der Dateninhaber mit dem Datenempfänger die Bedingungen für die Bereitstellung der Daten. Dieser Kontrahierungszwang gilt allerdings nur, wenn ein Dateninhaber auf Grundlage eines Nutzerverlangens nach Art. 5 DA-E oder auf Grundlage anderer Rechtsvorschriften der Union oder nationalen Rechtsvorschriften zur Umsetzung des Unionsrechts verpflichtet ist, einem Datenempfänger Daten bereitzustellen. In Fällen des freiwilligen Datenteilens gelten die Vorschriften des Kapitels III des DA-E nicht.

Werden Daten auf Grundlage eines Nutzerverlangens oder eines außerhalb des DA-E normierten Datenzugangsanspruchs bereitgestellt, hat dies zu fairen, angemessenen und nicht-diskriminierenden Bedingungen und in transparenter Weise im Einklang mit den Bestimmungen der Kapitel III und IV zu geschehen. Art. 9 DA-E verlangt, wenn eine Gegenleistung für die Bereitstellung von Daten vereinbart wird, dass diese ebenfalls „fair" ist. IÜ gelten die auf vertraglicher Grundlage zwischen dem Dateninhaber und dem Datenempfänger vereinbarten Bedingungen, die im Hinblick auf die Regelungen des Datenzugangs, der Datennutzung, der Haftung und der Rechtsbehelfe bei Verletzung datenbezogener Pflichten der Inhaltskontrolle nach Art. 13 DA-E unterliegen, vgl. Art. 8 Abs. 2 DA-E. Eine Vertragsklausel in Bezug auf den Datenzugang und die Datennutzung oder die Haftung und Rechtsbehelfe bei Verletzung oder Beendigung datenbezogener Pflichten ist nicht bindend, wenn sie die Bedingungen des Art. 13 DA-E erfüllt oder wenn sie die Ausübung der Rechte des Nutzers nach Ka-

pitel II ausschließt, davon abweicht oder deren Wirkung abändert, Art. 8 Abs. 2 DA-E. Eine Kontrolle der Hauptleistungspflicht zur Datenüberlassung findet nicht statt.

Der Dateninhaber darf nach Art. 11 DA-E technische Schutzmaßnahmen anwenden, um einen unbefugten Zugang zu den Daten zu verhindern und die Einhaltung der Art. 5, 6, 9 und 10 DA-E sowie der für die Datenbereitstellung vereinbarten Vertragsbedingungen sicherzustellen. Die Vorgaben der Art. 8–11 DA-E sind gem. Art. 12 Abs. 2 DA-E zwingend. Art. 8–11 DA-E gelten gem. Art. 12 Abs. 3 DA-E nur in Bezug auf Datenbereitstellungspflichten nach Unionsrecht oder nationalen Rechtsvorschriften zur Umsetzung des Unionsrechts, die nach dem Datum des Geltungsbeginns der Verordnung in Kraft treten.

a) Datenempfänger, Dritter

Datenempfänger ist gem. Art. 2 Nr. 7 DA-E eine juristische oder natürliche Person, die zu Zwecken innerhalb ihrer gewerblichen, geschäftlichen, handwerklichen oder beruflichen Tätigkeit handelt, ohne Nutzer eines Produkts oder verbundenen Dienstes zu sein, und der vom Dateninhaber Daten bereitgestellt werden, einschließlich eines Dritten, dem der Dateninhaber auf Verlangen des Nutzers oder im Einklang mit einer Rechtspflicht aus anderen Rechtsvorschriften der Union oder aus nationalen Rechtsvorschriften zur Umsetzung des Unionsrechts Daten bereitstellt. Der Dritte ist damit ein spezifischer Datenempfänger. Die Definition des Datenempfängers ist allerdings zirkelschlüssig,[59] ist doch Voraussetzung und Rechtsfolge zugleich, dass ihm Daten vom Dateninhaber zur Verfügung gestellt werden. Der Halbsatz „und der vom Dateninhaber Daten bereitgestellt werden" sollte daher aus der Definition des Art. 2 Nr. 7 DA-E gestrichen werden.

b) Rechte und Pflichten des Datenempfängers

Kein Datenzugangsanspruch

Art. 8 ff. DA-E gewähren keinen originären Datenzugangsanspruch des Datenempfängers, sondern setzen diesen voraus, vgl. Art. 5 Abs. 1 DA-E. Wo durch sektorspezifische Regulierung ein Datenzugangsanspruch vorgesehen wird oder wo der Nutzer die Datenübermittlung an den Dritten verlangt, gelten die Art. 8 ff. DA-E.

Schranken vorausgesetzter Datenzugangsansprüche

Beschränkt wird auch der Datenzugang im Verhältnis Dateninhaber und Datenempfänger durch den Geschäftsgeheimnisschutz, Art. 8 Abs. 6 DA-E. Anders als Art. 5 Abs. 8 DA-E handelt es sich aber um eine Vorrangregelung des Geschäftsgeheimnisschutzes, dh grundsätzlich sind Daten nicht bereitzustellen, wenn es sich um Geschäftsgeheimnisse handelt. Etwas anderes gilt nur dann, wenn die Daten nach der DS-GVO bereitzustellen wären. Der datenschutzrechtliche Anspruch auf Datenportabilität gem. Art. 20 DS-GVO ist allerdings gem. Art. 20 Abs. 4 DS-GVO – ebenso wie der Auskunftsanspruch nach Art. 15 Abs. 4 DS-GVO – insofern beschränkt, als die Rechte und Freiheiten anderer Personen durch den Datenzugang nicht beeinträchtigt werden dürfen. Für personenbezogene Daten gilt daher die Beschränkung des Datenzugangsanspruchs aus Art. 8 Abs. 6 DA-E nicht absolut. Sofern Geschäftsgeheimnisse vorliegen, ist eine Abwägung zwischen den Rechten aus Art. 7 und 8 GRCh einerseits und Art. 17 GRCh andererseits vorzunehmen. Überwiegt der über Art. 17 GRCh geschützte Geschäftsgeheimnisschutz, müssen die Daten nicht zugänglich gemacht werden. Diese einzelfallbezogene Interessenabwägung gewährleistet größtmögliche Einzelfallgerechtigkeit. Insbesondere kann auch das Schwärzen und Pseudonymisieren von Daten eine Option sein, dem Geschäftsgeheimnisschutz zu genügen und Daten dennoch zugänglich machen zu können.[60] Weshalb der Gesetzgeber in Art. 8 Abs. 6 DA-E stattdessen für nicht-personenbezogene Daten einen Pauschalvorrang des Geschäftsgeheimnisschutzes normiert, ist ebenso wenig nachvollziehbar wie der Pauschalvorrang des Datenzugangsanspruchs in Art. 5 Abs. 8 DA-E. Beide pauschalierte Vorrangregelungen sollten zu Gunsten einer einzelfallabhängigen Abwägungsentscheidung nach dem Vorbild des Art. 15 Abs. 4 bzw. Art. 20 Abs. 4 DS-GVO abgeändert werden. Hilfreich wäre auch hier die Ergänzung einer Datenzugangstreuhand.

Datenvernichtung, Art. 11 Abs. 2 DA-E

Ein Datenempfänger, der dem Dateninhaber zwecks Erlangung der Daten ungenaue oder falsche Informationen gegeben, Täuschungen und Zwangsmittels eingesetzt oder offensichtliche Lücken in der dem Schutz der Daten dienenden technischen Infrastruktur des Dateninhabers missbraucht, die bereitgestellten Daten für nicht genehmigte Zwecke genutzt oder ohne Zustimmung des Dateninhabers an eine andere Partei weitergegeben hat, muss – sofern der Dateninhaber oder der Nutzer nichts anderes anweist – nach Art. 11 Abs. 2 DA-E unverzüglich die vom Dateninhaber bereitgestellten Daten und alle etwaigen Kopien davon vernichten. Waren, abgeleitete Daten oder Dienstleistungen, die auf den mit den Daten erlangten Kenntnissen beruhen, dürfen nicht mehr hergestellt, angeboten, in Verkehr gebracht oder verwendet werden. Rechtsverletzende Waren sind zu vernichten und dürfen nicht mehr eingeführt, ausgeführt oder gelagert werden. Einen Rückruf umfasst der Anspruch nach Art. 11 Abs. 2 DA-E aber nicht. Auch eine Regelung dazu, was mit den Daten zu geschehen hat, die sich bereits außerhalb der Zugriffssphäre des Datenempfängers befinden, existiert nicht, und zwar weder iSe Informationspflicht des Datenempfängers gegenüber denjenigen, an die er die Daten übermittelt hat, noch im Sinne einer unmittelbaren Löschanordnung gegenüber diesen Personen. Dies steht dem Dateninhaber ohne Zutun des Gesetzgebers in Ermangelung des ausschließlichkeitsrechtlichen Charakters der dem Dateninhaber durch den DA-E zugewiesenen Rechtsposition gerade nicht zu und dies sollte auch so bleiben.

Kein „right to hack"

Nach Art. 5 Abs. 4 DA-E darf ein Dritter keine Zwangsmittel einsetzen oder offensichtliche Lücken in der technischen Infrastruktur des Dateninhabers, mit der die Daten geschützt werden sollen, ausnutzen, um Zugang zu Daten zu erlangen. Es besteht daher zu Gunsten des Dritten kein „right to hack". Da es eine entsprechende Regelung, die den Nutzer ebenfalls hierauf verpflichtet, nicht gibt, ließe sich im Umkehrschluss erwägen, dass dem Nutzer ein solches „right to hack" zusteht. Ob der europäische Gesetzgeber aber tatsächlich so weit gehen wollte, darf bezweifelt werden.

c) Rechte und Pflichten des Dateninhabers

Datenbereitstellung zu fairen, angemessenen, nicht-diskriminierenden Bedingungen

Wann Daten zu fairen, angemessenen und nichtdiskriminierenden Bedingungen zur Verfügung gestellt sind, geben Verordnungstext und Erwägungsgründe nicht explizit vor. Ausweislich Erwägungsgrund 5 DA-E soll mit diesen Vorgaben aber die Ausnutzung vertraglicher Ungleichgewichte verhindert werden. Die Fairness einer Klausel ist nach Erwägungsgrund 40 DA-E nach der Klauselrichtlinie zu beurteilen. Nach Erwägungsgrund 41 DA-E ist es Sache des Dateninhabers, nachzuweisen, dass eine Vertragsbedingung nicht-diskriminierend ist. Erwägungsgrund 41 DA-E enthält dabei nur in negativer Hinsicht Anhaltspunkte zur Bestimmung der Diskriminierung. Danach ist es keine rechtswidrige Diskriminierung, wenn der Dateninhaber für die Bereitstellung von Daten unterschiedliche Vertragsbedingungen oder

59 Bomhard/Merkle RDi 2022, 168 (169).
60 Kühling/Buchner/Bäcker, Art. 15 Rn. 42b.

andere Gegenleistungen vorsieht, wenn diese Unterschiede aus objektiven Gründen gerechtfertigt sind.

Verbot von Exklusivvereinbarungen, Art. 8 Abs. 4 DA-E

Ein Dateninhaber darf einem Datenempfänger Daten nur dann exklusiv zur Verfügung stellen, wenn der Nutzer dies gemäß Kapitel II verlangt hat. Anderenfalls sind Exklusivvereinbarungen unzulässig.

Angemessene Gegenleistung

Gem. Art. 9 DA-E kann der Dateninhaber eine angemessene Gegenleistung verlangen, wenn er rechtlich verpflichtet ist, dem Datenempfänger Daten bereitzustellen. Diese Bestimmung sollte nicht als Bezahlung für die Daten selbst verstanden werden, sondern im Falle von Kleinstunternehmen, kleinen und mittleren Unternehmen als Ausgleich für die Kosten und Investitionen, die für die Bereitstellung der Daten erforderlich sind, Erwägungsgrund 42 DA-E. Ist ein Kleinst- oder Kleinunternehmen Datenempfänger, so gilt daher nach Art. 9 Abs. 2 DA-E, dass die vereinbarte Gegenleistung nicht höher sein darf als die Kosten, die mit der Bereitstellung der Daten für den Datenempfänger unmittelbar zusammenhängen und dem Verlangen zuzurechnen sind. Ein nur mittelbarer Zusammenhang ist nicht ausreichend. Mitgliedstaatliche Kausalitäts- und Zurechnungstheorien sind hier nicht maßgeblich. Die Höhe der Kosten muss sich auf denjenigen Betrag beschränken, in dem sich das Datenzugangsverlangen niederschlägt. Es sollte daher besser von „Kompensation des Datenzugangs" statt von einer Gegenleistung gesprochen werden. Der nationale Gesetzgeber kann nach Art. 9 Abs. 3 DA-E Vorschriften vorsehen, nach denen eine Gegenleistung ausgeschlossen ist oder geringer ausfällt. Nach Art. 9 Abs. 4 DA-E hat der Dateninhaber den Datenempfängern Informationen zur Verfügung zu stellen, aus denen die Grundlage für die Berechnung der Gegenleistung so detailliert zu entnehmen ist, dass der Datenempfänger überprüfen kann, ob die Anforderungen des Art. 9 Abs. 1 und 2 DA-E erfüllt sind. Der Verpflichtung zur Gegenleistung könnte der Datenempfänger nach dem bisherigen Verordnungstext dadurch entgehen, dass zunächst der Nutzer Zugang zu den Daten beantragt und diese dann an den Datenempfänger weiterreicht, die Übermittlung also nicht direkt an den Datenempfänger erfolgt, sondern „über Eck".[61]

Klauselkontrolle

Für Klauseln, die ein Unternehmen gegenüber einem Kleinstunternehmen oder einem kleinen oder mittleren Unternehmen iSd Art. 2 DA-E des Anhangs der Empfehlung 2003/361/EG einseitig auferlegt hat, ist für letzteres Unternehmen nicht bindend, wenn sie missbräuchlich ist, Art. 13 Abs. 1 DA-E. Nach Art. 13 Abs. 5 DA-E wird widerleglich vermutet („gilt als"), dass eine Vertragsklausel einseitig auferlegt wurde, wenn sie von einer Vertragspartei eingebracht wird und die andere Vertragspartei ihren Inhalt trotz des Versuchs, hierüber zu verhandeln, nicht beeinflussen kann. Die Vertragspartei, die eine Vertragsklausel eingebracht hat, trägt die Beweislast dafür, dass diese Klausel nicht einseitig auferlegt wurde. Unternimmt die Vertragsgegenseite den Versuch, über die Klausel zu verhandeln und scheitert dieser, reicht dies aus, um von einem einseitigen Auferlegen auszugehen, Erwägungsgrund 52 DA-E. Nur dann also, wenn der Inhalt einer Klausel tatsächlich zwischen den Parteien in Verhandlungen abgeändert wird, ist die entsprechende Klausel nach den Vorgaben des Art. 13 DA-E nicht einseitig gestellt. Die Klauselkontrolle gilt nicht für Hauptleistungspflichten, Art. 13 Abs. 7 DA-E. Art. 13 Abs. 3 DA-E enthält eine Aufzählung absolut unzulässiger Vertragsklauseln (schwarze Liste[62]), nämlich

- den Ausschluss oder die Beschränkung der Haftung der Partei, die die Klausel einseitig auferlegt hat, für vorsätzliche oder grob fahrlässige Handlungen;
- den Ausschluss der Rechtsbehelfe, die der Partei, der die Klausel einseitig auferlegt wurde, bei Nichterfüllung von Vertragspflichten zur Verfügung stehen, oder den Ausschluss der Haftung der Partei, die die Klausel einseitig auferlegt hat, bei einer Verletzung solcher Pflichten;
- das ausschließliche Recht der Partei, die die Klausel einseitig auferlegt hat, zu bestimmen, ob die gelieferten Daten vertragsgemäß sind, oder eine Vertragsklausel auszulegen.

Art. 13 Abs. 4 DA-E enthält sodann einen Katalog mit Tatbeständen, bei deren Vorliegen die Missbräuchlichkeit der Klausel widerleglich vermutet wird, zB wenn vom Klauselverwender die Haftung für eine Verletzung von Vertragspflichten unangemessen eingeschränkt wird.

Technische Schutzmaßnahmen

Art. 11 DA-E erlaubt es dem Dateninhaber, geeignete technische Schutzmaßnahmen, anzuwenden, um einen unbefugten Zugang zu den Daten zu verhindern und die Einhaltung der Art. 5, 6, 9 und 10 DA-E sowie der für die Datenbereitstellung vereinbarten Vertragsbedingungen sicherzustellen. Was technische Schutzmaßnahmen iSd Art. 11 DA-E sind, definiert der Verordnungstext nicht abschließend. Aus Art. 11 Abs. 1 S. 1 DA-E ergibt sich aber, dass auch intelligente Verträge unter den Begriff der technischen Schutzmaßnahmen fallen. Ein intelligenter Vertrag ist nach Art. 2 Nr. 16 DA-E ein in einem elektronischen Vorgangsregistersystem gespeichertes Computerprogramm, bei dem das Ergebnis der Programmausführung in dem elektronischen Vorgangsregister aufgezeichnet wird. In der Regel geht es bei derart „intelligenten Verträgen" darum, dass vereinbarte Vertragsinhalte bei Eintritt der vertraglich vereinbarten Voraussetzungen automatisiert durchgeführt werden, dass also zB im Falle einer unberechtigten Weitergabe von Daten eine automatisierte Löschung der Daten beim Dateninhaber erfolgt. Es böte sich hier allerdings eher an, sinngemäß auf die ebenfalls unionsrechtlich harmonisierte Begriffsbestimmung der technischen Maßnahmen in Art. 6 Abs. 3 Infosoc-RL zurückzugreifen. Danach sind technische Maßnahmen „alle Technologien, Vorrichtungen oder Bestandteile, die im normalen Betrieb dazu bestimmt sind, Werke oder sonstige Schutzgegenstände betreffende Handlungen zu verhindern oder einzuschränken, die nicht von der Person genehmigt worden sind, die Inhaber der Urheberrechte oder der dem Urheberrecht verwandten gesetzlich geschützten Schutzrechte oder des in Kapitel III der Richtlinie 96/9/EG verankerten Sui-generis-Rechts ist."

Bezogen auf Daten könnten technische Schutzmaßnahmen iSd DA-E also verstanden werden als „alle Technologien, Vorrichtungen oder Bestandteile, die im normalen Betrieb dazu bestimmt sind, Handlungen in Bezug auf Daten zu verhindern oder einzuschränken, die nicht durch Art. 5, 6, 9 und 10 für zulässig erklärt werden oder vom Dateninhaber durch zulässige Vertragsbedingung gestattet worden sind."

Der Zusatz „durch zulässige Vertragsbedingungen" ist wichtig, um es dem Dateninhaber nicht zu ermöglichen, auf technischem Wege rechtlich unzulässige Vertragsbedingungen durchzusetzen. Die Erfahrungen aus dem Urheberrecht, wo ein entsprechendes Problem existiert, sollten hier nutzbar gemacht werden.[63]

Technische Schutzmaßnahmen dürfen nicht als Mittel eingesetzt werden, um zu verhindern, dass ein Nutzer sein Recht, Dritten nach Art. 5 DA-E wirksam Daten bereitzustellen, ausübt oder dass ein Dritter ein Recht nach den Rechtsvorschriften der

61 Bomhard/Merkle RdI 2022, 168 Rn. 15 f.; unentschieden, ob dies möglich sein soll: Hennemann/Steinrötter NJW 2022, 1481 Rn. 19.
62 Gerpott CR 2022, 271 (278).
63 Specht, Diktat der Technik, 2019, S. 454.

Union oder nationalen Rechtsvorschriften zur Umsetzung des Unionsrechts gem. Art. 8 Abs. 1 DA-E in Anspruch nimmt, Art. 11 Abs. 1 S. 2 DA-E. Diese Einschränkung des Rechts, technische Schutzmaßnahmen zu ergreifen, ist der eigentliche Regelungsgehalt des Art. 11 DA-E. Denn um technische Schutzmaßnahmen einzusetzen, bedarf es keiner rechtlichen Erlaubnis, der Dateninhaber ist grds. frei, dies zu tun. Diese Freiheit zu beschränken, dient Art. 11 Abs. 1 S. 2 DA-E. Technische Schutzmaßnahmen etwa, die Datenzugang lediglich unter diskriminierenden Bedingungen und damit unter Verstoß gegen Art. 8 Abs. 1 DA-E zulassen, sind ein Verstoß gegen Art. 11 Abs. 1 S. 2 DA-E. Gegen diese unzulässigen technischen Mittel müssen sich Verbraucher und Datenempfänger allerdings zumindest dann rechtlich zur Wehr setzen, wenn man zugrunde legt, dass sie gem. Art. 5 Abs. 4 DA-E kein „right to hack" haben. Diese Aktionslast ist bereits besonders nachteilhaft, weshalb der zu gewährende Rechtsschutz schnell und kostenlos erfolgen muss. Die Streitbeilegungsstellen sollten daher generell auch im Anwendungsbereich von Art. 11 DA-E tätig werden dürfen und – anders als es Art. 10 Abs. 8 DA-E für Streitigkeiten nach Art. 8 und 9 DA-E vorgibt – für Streitigkeiten über Art. 11 DA-E stets bindend sein. Um den Aktionslastnachteil,[64] der mit technischen Schutzmaßnahmen für den Nutzer verbunden ist, auszugleichen, bedarf es Sanktionsmechanismen für den unrechtmäßigen Einsatz von technischen Schutzmaßnahmen, die bislang nicht vorgesehen sind.

d) Kritik und Abhilfemöglichkeiten

Auch im Verhältnis Dateninhaber – Datenempfänger lässt sich systemische sowie Einzelkritik üben.

Systemische Kritik

Unklar ist systemisch zunächst, welches Problem der DA-E im Verhältnis Dateninhaber – Datenempfänger lösen möchte. Sollen auch diese Regelungen primär Teil der umfassenden Daten-Governance sein, die der DA-E sektorübergreifend festzuschreiben intendiert oder geht es hier primär um generelle Vorgaben für Aftermarket-Datenzugangsregelungen, die sich sektorspezifisch noch im Entstehen befinden? Für eine Aftermarket-Regulierung untypisch ist die Vergütungspflicht für die Datenbereitstellung. Sie würde eher für eine generelle Daten-Governance-Lösung sprechen, die ihren Fokus auch und gerade darin hat, Anreize für die Datengenerierung aufrecht zu erhalten und damit eine Stärkung der Rechtsstellung des Dateninhabers fokussiert. Aftermarket-Regulierung bedarf vor diesem Hintergrund einer von der im DA-E gewählten Daten-Governance abweichenden Lösung. Möglicherweise gerade weil der DA-E eben nicht nur aber zumindest auch Aftermarket-Regulierung ist, sieht Art. 9 Abs. 3 DA-E vor, dass sowohl unionsrechtlich als auch durch mitgliedstaatliche Rechtsvorschriften zur Umsetzung von Unionsrecht vorgesehen werden kann, dass eine Gegenleistung für die Bereitstellung der Daten ausgeschlossen werden kann. Wichtig ist, dass dies auch für rein mitgliedstaatliche Regelungen gilt, die die Aftermarket-Problematik zu lösen versuchen. Entsprechend zu ändern ist die Formulierung des Art. 9 Abs. 3 DA-E.

Detailkritik

1. Maßnahmen zur Innovationsförderung

a) Ergänzung von Regelungen im Verhältnis zwischen Nutzer und Datenempfänger

Auch dann aber, wenn der DA-E als generelle Daten-Governance-Regelung erachtet wird, macht der Vergütungsanspruch im Verhältnis Dateninhaber – Datenempfänger wenig Sinn. Denn dem Datenempfänger werden die Daten auf Verlangen des Nutzers bereitgestellt. Im Verhältnis Dateninhaber – Nutzer besteht also mit Art. 5 Abs. 1 DA-E eine drittbegünstigende Regelung. Nicht selten wird der Datenempfänger dem Nutzer für die Ausübung des Art. 5 DA-E eine Vergütung schulden, die durch den DA-E nicht begrenzt und schon gar nicht ausgeschlossen wird, weil das Verhältnis zwischen Nutzer und Datenempfänger im DA-E nur rudimentär geregelt wird. Damit droht dem Datenempfänger eine Doppelvergütungspflicht, die sich aber auf zwei Wegen vermeiden ließe: Entweder könnte die Vergütungspflicht gegenüber dem Dateninhaber dem Nutzer auferlegt werden, der sie dann im Verhältnis zum Dritten ersetzt verlangen kann, sofern der Dritte der Datenbereitstellung an ihn zustimmt bzw. nicht widerspricht. Oder eine Vergütung im Verhältnis Datenempfänger – Nutzer könnte jedenfalls für personenbezogene Daten ausgeschlossen werden, um Anreize für eine Monetarisierung von Daten zu vermeiden. Der DA-E müsste in diesem Fall um weitere Regelungen des Verhältnisses zwischen Nutzer und Datenempfänger ergänzt werden. Dies wäre schon deshalb sinnvoll, weil in diesem Verhältnis wichtige Regelungen dazu fehlen, was dem Datenempfänger insbesondere erlaubt, aber auch, was ihm untersagt sein sollte. Es scheint hier sinnvoll, die erwünschten Datenverarbeitungen durch die Datenempfänger, zB die Datenverarbeitung zu Zwecken der Forschung und Innovation im Gemeinwohlinteresse aber auch zum Zwecke der Erbringung vom Nutzer gewünschter added value services[65] von denjenigen Datenverarbeitungen zu trennen, die man sich im gesamtgesellschaftlichen Interesse von einem Datenempfänger nicht wünscht, so zB die Zusammenstellung der Daten zu Persönlichkeitsprofilen zum Zwecke des Verkaufs dieser Persönlichkeitsprofile an Dritte. Die DS-GVO stellt für die Zusammenstellung und Weiterreichung von Persönlichkeitsprofilen keine absoluten Hürden auf und dass, obwohl ein derartiger Umgang mit personenbezogenen Daten insbesondere auf Grund erheblicher negativer Informationsasymmetrien mit dem Mittel der Einwilligung nicht eingefangen werden kann[66] und auf Grund der Eigenschaft von Datenschutz als öffentlichem Gut[67] gesamtgesellschaftlich erheblich schadet.[68] Dieser Fehler der DS-GVO ließe sich über den Data Act korrigieren, wofür allerdings in diesem Fall ein Anwendungsvorrang für das DA-E formuliert werden müsste. Sollte dies in Betracht kommen, empfiehlt sich aber keine reine Verbotsnorm, sondern eine Differenzierung zwischen im Grundsatz zulässigen Datenverarbeitungen zu Zwecken von Forschung und Innovation (die hierdurch rechtssicher ermöglicht würden) und im Grundsatz unzulässigen Weiterreichungen von Persönlichkeitsprofilen.

b) Streichung der Verpflichtung zum Vertragsschluss zwischen Dateninhaber und Datenempfänger

Der Grund für das Erfordernis eines Vertragsschlusses zwischen Dateninhaber und Datenempfänger ist die Zahlung

64 Zum Nachteil der Aktionslast gegen technische Schutzmaßnahmen im Urheberrecht vgl. Specht, Diktat der Technik, 2019.

65 Eine Beschränkung der Nutzung auf added value services in Bezug auf Nutzer vorschlagend: Drexl/Banda/Gonzalez Otero/Hoffmann/Kim/Kulhari/Moscon/Richter/Wiedemann, Position Statement of the Max Planck Institute for Innovation and Competition of 25 May 2022 on the Commission's Proposal of 23 February 2022 for a Regulation on harmonised rules on fair access to and use of data (Data Act), Rn. 25 ff., abrufbar unter: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4136484.

66 Eine gute Übersicht für das Versagen auf dem Datenprimärmarkt (Daten als Gegenleistung) bieten Hacker, Datenprivatrecht, 2020, § 3; Schweitzer AcP 2020, 544 (570 ff.).

67 Acemoglu et al., Too much Data – Prices and Inefficiencies in Data Markets, NBER Working Paper 26296, September 2019, S. 1 f., abrufbar unter: https://www.nber.org/system/files/working_papers/w26296/w26296.pdf. Dies erklärt womöglich das sog. „privacy paradoxon", vgl. Martens et al., Business-to-Business data sharing: An economic and legal analysis, Digital Economy Working Paper 2020-05, JRC Technical Reports, 2020, S. 17 f., abrufbar unter: https://ec.europa.eu/jrc/sites/default/files/jrc121336.pdf.

68 Specht FS Tinnefeld – im Erscheinen.

der angemessenen Vergütung, zu der der Datenempfänger verpflichtet wird.[69] Da dies – wie schon erläutert – wenig Sinn macht und zudem Innovationszwecken abträglich ist, sollte die Regelung gänzlich gestrichen werden. Sofern am Vertragserfordernis zwischen Dateninhaber und Datenempfänger festgehalten wird, sollte zumindest Art. 9 Abs. 3 DA-E durch eine rein mitgliedstaatliche Abweichungsmöglichkeit von der Vergütungspflicht ergänzt werden.

2. Maßnahmen zwecks gerechter Verteilung der Wertschöpfung aus Daten auf die Akteure der Datenwirtschaft

a) Anpassung der Beschränkungen des Datenzugangs
Art. 8 Abs. 6 DA-E sollte durch eine offene Schrankenbestimmung nach dem Vorbild der Art. 15 Abs. 4 DS-GVO und 20 Abs. 4 DS-GVO in Kombination mit einer Datenzugangsdatentreuhand ersetzt werden.

b) Technische Schutzmaßnahmen
Für Art. 11 DA-E ist in Art. 2 DA-E eine Definition der Technischen Schutzmaßnahmen vorzunehmen als „alle Technologien, Vorrichtungen oder Bestandteile, die im normalen Betrieb dazu bestimmt sind, Handlungen in Bezug auf Daten zu verhindern oder einzuschränken, die nicht durch Art. 5, 6, 9 und 10 DA-E für zulässig erklärt werden oder vom Dateninhaber durch zulässige Vertragsbedingung gestattet worden sind." Es sollten Sanktionen für den unrechtmäßigen Einsatz von technischen Schutzmechanismen sowie für die Umgehung zulässiger Schutzmechanismen vorgesehen werden. Zwar fehlt in Art. 11 Abs. 2 DA-E eine Regelung dazu, was mit den Daten zu geschehen hat, die sich bereits außerhalb der Zugriffssphäre des Datenempfängers befinden, eine solche Regelung empfiehlt sich aber in Anbetracht des fehlenden ausschließlichkeitsrechtlichen Charakters der Rechtsposition des technisch-faktischen Dateninhabers auch nicht.

c) Erweiterung der Streitschlichtung
In Art. 12 DA-E sollten Streitigkeiten im Anwendungsbereich des Art. 11 DA-E aufgenommen sowie Bindungswirkung der Entscheidungen und Kostenneutralität des Verfahrens in Fällen einer Streitigkeit nach Art. 11 DA-E für natürliche Personen, Kleinst- und Kleinunternehmen festgeschrieben werden.

3. Verhältnis B2G

Das Verhältnis B2G letztlich wird in Kapitel V in den Art. 14 ff. DA-E geregelt. Danach stellt der Dateninhaber einer öffentlichen Stelle oder einem Organ, einer Einrichtung oder einer sonstigen Stelle der Union, die eine außergewöhnliche Notwendigkeit der Nutzung der verlangten Daten nachweist, auf Verlangen Daten bereit. Von dieser Verpflichtung sind nach Art. 14 Abs. 2 DA-E kleine Unternehmen und Kleinstunternehmen iSd Art. 2 des Anhangs der Empfehlung 2003/361/EG der Kommission befreit.[70] Ob das Datenverlangen im Wege eines Verwaltungsaktes oder auf privatrechtlichem Wege geltend gemacht wird, wird durch den DA-E nicht vorgegeben und sollte durch den nationalen Gesetzgeber in Umsetzung des DA-E spezifiziert werden. Forschungseinrichtungen erhalten keinen unmittelbaren Datenzugangsanspruch, öffentliche Stellen, Organe, Einrichtungen und andere Stellen der Union dürfen die nach Art. 14 ff. DA-E erlangten Daten aber nach Art. 21 DA-E an Personen oder Organisationen zur Durchführung wissenschaftlicher Forschungstätigkeiten oder Analysen, die mit dem Zweck, für den die Daten verlangt wurden, vereinbar sind, oder an nationale statistische Ämter und an Eurostat zur Erstellung amtlicher Statistiken weitergeben.

a) Öffentliche Stellen

Öffentliche Stellen sind gem. Art. 2 Nr. 9 DA-E die nationalen, regionalen und lokalen Behörden, Körperschaften und Einrichtungen des öffentlichen Rechts der Mitgliedstaaten oder Verbände, die aus einer oder mehreren dieser Behörden, Körperschaften oder Einrichtungen bestehen.

b) Rechte und Pflichten öffentlicher Stellen

Datenzugangsrecht in Fällen außergewöhnlicher Notwendigkeit

■ Außergewöhnliche Notwendigkeit

Eine außergewöhnliche Notwendigkeit liegt nach Art. 15 DA-E in drei Fällen vor: Erstens, wenn die verlangten Daten zur Bewältigung eines öffentlichen Notstands erforderlich sind (lit. a), wobei ein öffentlicher Notstand nach Art. 2 Nr. 10 DA-E eine außergewöhnliche Situation ist, die sich negativ auf die Bevölkerung der Union, eines Mitgliedstaats oder eines Teils davon auswirkt und das Risiko schwerwiegender und dauerhafter Folgen für die Lebensbedingungen oder die wirtschaftliche Stabilität oder die Gefahr einer erheblichen Beeinträchtigung wirtschaftlicher Vermögenswerte in der Union oder in dem bzw. den betroffenen Mitgliedstaaten birgt. Zweitens, das Datenverlangen ist zeitlich befristet, im Umfang begrenzt und erforderlich, um einen öffentlichen Notstand zu verhindern oder die Erholung von einem öffentlichen Notstand zu unterstützen (lit. b), oder, drittens (lit. c), auf Grund des Fehlens verfügbarer Daten ist die öffentliche Stelle oder das Organ, die Einrichtung oder die sonstige Stelle der Union daran gehindert, eine bestimmte, gesetzlich ausdrücklich vorgesehene Aufgabe im öffentlichen Interesse zu erfüllen, und

1. die öffentliche Stelle oder das Organ, die Einrichtung oder die sonstige Stelle der Union kann diese Daten nicht auf andere Weise erlangen, auch nicht durch Datenerwerb auf dem Markt zu Marktpreisen oder auf Grund bestehender Datenbereitstellungspflichten, und durch den Erlass neuer Rechtsvorschriften kann die rechtzeitige Verfügbarkeit der Daten nicht gewährleistet werden, oder

2. die Erlangung der Daten nach dem in diesem Kapitel festgelegten Verfahren würde den Verwaltungsaufwand der Dateninhaber oder anderer Unternehmen erheblich verringern.

Das Datenbereitstellungsverlangen der öffentlichen Stellen muss die Voraussetzungen des Art. 17 DA-E erfüllen und dabei insbesondere die außergewöhnliche Notwendigkeit nachweisen. Die hohen Voraussetzungen der Art. 15 und 17 DA-E dürften den Datenzugang des Staates zur absoluten Ausnahme machen und sollten insbesondere Situationen wie die Hochwasserkatastrophen der letzten Jahre oder auch die Pandemiebekämpfung vor Augen haben. Auch hier wird der umfassende Schutzcharakter des DA-E zu Gunsten der Dateninhaber deutlich, die einem Datenzugang des Staates in der Regel nicht ausgesetzt sein dürften.

■ Schranken des Datenzugangsanspruchs

Eine Offenlegung von Geschäftsgeheimnissen oder mutmaßlichen Geschäftsgeheimnissen gegenüber einer öffentlichen Stelle oder einem Organ, einer Einrichtung oder einer sonstigen Stelle der Union ist nur insoweit erforderlich, wie dies für den Zweck des Verlangens unerlässlich ist. In diesem Falle trifft die

69 Drexl/Banda/Gonzalez Otero/Hoffmann/Kim/Kulhari/Moscon/Richter/Wiedemann, Position Statement of the Max Planck Institute for Innovation and Competition of 25 May 2022 on the Commission's Proposal of 23 February 2022 for a Regulation on harmonised rules on fair access to and use of data (Data Act), Rn. 98 ff., abrufbar unter: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4136484.

70 Specht-Riemenschneider, Studie zur Regulierung eines privilegierten Zugangs zu Daten für Wissenschaft und Forschung durch die regulatorische Verankerung von Forschungsklauseln in den Sektoren Gesundheit, Online-Wirtschaft, Energie und Mobilität, S. 159, abrufbar unter: https://www.jura.uni-bonn.de/fileadmin/Fachbereich_Rechtswissenschaft/Einrichtungen/Lehrstuehle/Specht/Dateien/2021-08-25-LSR.pdf.

öffentliche Stelle oder das Organ, die Einrichtung oder die sonstige Stelle der Union geeignete Maßnahmen, um die Vertraulichkeit dieser Geschäftsgeheimnisse zu wahren. Auch im Verhältnis B2G ist damit – ebenso wie im Verhältnis Nutzer – Dateninhaber – ein Vorrang des Datenzugangsanspruchs normiert. Auch hier wäre es denkbar und möglich, eine offenere Schrankenbestimmung zu normieren und Sicherungsmaßnahmen zB durch die Einbindung von „Datenzugangstreuhändern" (s.o.) vorzusehen, um den Schutz von Geschäftsgeheimnissen bestmöglich mit dem Interesse am Datenzugang in Ausgleich zu bringen.

■ Ausgleichsmöglichkeit

Grundsätzlich ist der in den Art. 14 ff. DA-E normierte Datenzugangsanspruch kostenlos zu gewährleisten, Art. 20 Abs. 1 DA-E. Der Dateninhaber kann aber einen Ausgleich für die Bereitstellung der Daten verlangen, der nach Art. 20 Abs. 2 DA-E die technischen und organisatorischen Kosten, die durch die Erfüllung des Verlangens entstehen, erforderlichenfalls einschließlich der Kosten einer Anonymisierung und technischen Anpassung, zuzüglich einer angemessenen Marge, nicht übersteigen. Auf Anfrage der öffentlichen Stelle oder des Organs, der Einrichtung oder der sonstigen Stelle der Union, die bzw. das die Daten verlangt hat, übermittelt der Dateninhaber Informationen über die Grundlage für die Berechnung der Kosten und der angemessenen Marge.

■ Datenverarbeitungsverbot

Öffentliche Stellen sowie Organe, Einrichtungen und sonstige Stelle der Union dürfen die Rechte aus diesem Kapitel nach Art. 16 Abs. 2 DA-E nicht ausüben, um Tätigkeiten der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder Ordnungswidrigkeiten oder der Strafvollstreckung oder der Zoll- oder Steuerverwaltung durchzuführen. Nach Art. 17 Abs. 3 DA-E dürfen öffentliche Stellen oder Organe, Einrichtungen oder sonstige Stellen der Union nach Kapitel V erlangte Daten nicht zur Weiterverwendung iSd RL (EU) 2019/1024 (OD-PSI-RL) zur Verfügung stellen. Dies soll öffentliche Stellen allerdings nicht daran hindern, die Daten zur Wahrnehmung der in Art. 15 DA-E genannten Aufgaben auszutauschen oder die Daten einem Dritten bereitzustellen, den sie iRe öffentlich zugänglichen Vereinbarung mit technischen Inspektionen oder anderen Aufgaben betraut hat, Art. 17 Abs. 4 DA-E. Außerdem darf die öffentliche Stelle, das Organ, die Einrichtung oder sonstige Stelle der Union die Daten nicht in einer Weise nutzen, die mit dem Zweck, zu dem sie verlangt wurden, unvereinbar ist, Art. 19 Abs. 1 lit a DA-E.

Technische Pflichten, Datenvernichtung und Mitteilungsobliegenheit

Die öffentliche Stelle, das Organ, die Einrichtung oder sonstige Stelle der Union trifft – soweit die Verarbeitung personenbezogener Daten erforderlich ist – technische und organisatorische Maßnahmen zum Schutz der Rechte und Freiheiten der betroffenen Personen. Hier wird man sich zwar nicht 1:1, dennoch aber im Grundsatz an den Vorgaben des Art. 25 DS-GVO orientieren können, für nicht-personenbezogene Daten freilich nur entsprechend. Es besteht außerdem eine Verpflichtung zur Datenvernichtung, sobald die Daten für den im Datenzugangsverlangen angegebenen Zweck nicht mehr erforderlich sind. Die Vernichtung ist dem Dateninhaber mitzuteilen, Art. 19 Abs. 1 lit. c DA-E. Bei Verletzung dieser Vorgabe kann ein erneutes Datenverarbeitungsverlangen abgelehnt werden, Art. 18 Abs. 3 DA-E, weshalb es sich bei dieser Vorgabe um eine Obliegenheit, nicht um eine Verpflichtung handelt. Ihre Verletzung führt allein zur Verkürzung eigener Ansprüche, nicht aber werden Schadensersatzpflichten ausgelöst.

Berechtigung der Weitergabe zu Forschungszwecken

Art. 21 DA-E berechtigt die öffentliche Stelle, das Organ, die Einrichtung oder sonstige Stelle der Union, erhaltene Daten an Personen oder Organisationen zur Durchführung wissenschaftlicher Forschungstätigkeiten oder Analysen, die mit dem Zweck, für den die Daten verlangt wurden, vereinbar sind, oder an nationale statistische Ämter und an Eurostaat zur Erstellung amtlicher Statistiken weiterzugeben. Die Personen oder Organisationen, die Daten erhalten, müssen allerdings gemeinnützig oder iRe im Unionsrecht oder im Recht der Mitgliedstaaten anerkannten Aufgabe von öffentlichem Interesse handeln. Dies umfasst keine Organisationen, die dem bestimmenden Einfluss gewerblicher Unternehmen unterliegen. Außerdem müssen Personen oder Organisationen, die Daten nach Absatz 1 erhalten, die Bestimmungen des Art. 17 Abs. 3 und des Art. 19 DA-E einhalten, Art. 21 Abs. 3 DA-E. Damit dürfen sie Daten insbesondere nicht für andere Zwecke als die iRd Anfrage genannten Zwecke verarbeiten, müssen technische und organisatorische Sicherheitsmaßnahmen ergreifen und Daten löschen, sofern sie für den genannten Zweck nicht mehr erforderlich sind. Außerdem dürfen die Daten nicht für eine Weiterverwendung iSd OD-PSI-RL bereitgestellt werden. Die Weitergabe nach Art. 21 Abs. 1–3 DA-E ist dem Dateninhaber nach Art. 21 Abs. 4 DA-E mitzuteilen.

■ Keine Privilegierung nicht-gemeinnütziger privater Forschung

Einzelpersonen und Organisationen, denen die Daten bereitgestellt werden, müssen entweder gemeinnützig sein oder im Rahmen einer im Unionsrecht oder im Recht der Mitgliedstaaten anerkannten Aufgabe von öffentlichem Interesse handeln. Damit wird nicht gemeinnützige private Forschung von der Privilegierung im Datenzugang ausgeschlossen. Dies ist natürlich nicht zwingend. Gerade in Anbetracht der Erfolge privater Forschung in der Pandemiebekämpfung böte es sich an, statt in Bezug auf die Forschungseinrichtung entlang dem Forschungszweck zu differenzieren: Sofern Forschung im Gemeinwohlinteresse betrieben wird, ließen sich Datenzugangsgewährleistungen zum Wohle der Gesellschaft sowohl zu Gunsten öffentlicher als auch zu Gunsten privater Forschung begründen. Die legitimen Interessen der Dateninhaber ließen sich durch Datenverwertungsverbote, Vergütungspflichten, Schutzkonzepte und zwischengeschaltete Datentreuhänder gewährleisten.[71]

■ Zweckvereinbarkeit

Art. 21 DA-E definiert mit der Weitergabe zu Forschungszwecken im Verhältnis zu der nach Art. 14 DA-E zu gewährleistenden Datennutzung eine Sekundärnutzung der Daten, für die, wie bereits im Datenschutzrecht der Fall, eine Vereinbarkeit von Primär- und Sekundärzweck erforderlich ist. Wonach sich diese Zweckvereinbarkeit richtet, geben weder der Verordnungstext noch die Erwägungsgründe vor. Ob zur Bestimmung der Zweckvereinbarkeit auf Art. 6 Abs. 4 DS-GVO abgestellt wird oder jedenfalls für nicht-personenbezogene Daten andere Grundsätze gelten sollen, sollte der DA-E zumindest klarstellen.

■ Erforderliche Ergänzung eines Datenzugangsanspruchs für Forschung und Wissenschaft

Die Nichtberücksichtigung von Forschung und Wissenschaft bei der Ausgestaltung materiellrechtlicher Datenzugangsansprüche ist nicht gerechtfertigt. Datenzugang für die Wissenschaft ist dringend erforderlich und wird durch die bloße Möglichkeit staatlicher Stellen, die selbst nur in äußerst eng umgrenzten Fäl-

71 Specht-Riemenschneider, Studie zur Regulierung eines privilegierten Zugangs zu Daten für Wissenschaft und Forschung durch die regulatorische Verankerung von Forschungsklauseln in den Sektoren Gesundheit, Online-Wirtschaft, Energie und Mobilität, 2021, S. 119 ff., abrufbar unter: https://www.jura.uni-bonn.de/fileadmin/Fachbereich_Rechtswissenschaft/Einrichtungen/Lehrstuehle/Specht/Dateien/2021-08-25-LSR.pdf.

len Datenzugang erhalten, diese Daten an Forschungseinrichtungen weiterzureichen, nicht ausreichend gewährleistet. Datenzugang für die Wissenschaft ist notwendiges Vehikel, um eine ausreichende Wissensbasis auch und gerade für den Gesetzgeber zu schaffen, damit dieser sinnvoll regulieren kann. Es ist dem DA-E daher dringend ein Kapitel beizufügen, dass eigene Datenzugangsansprüche für die Wissenschaft vorsieht.

c) Rechte und Pflichten des Dateninhabers

Auf zulässiges Datenverarbeitungsverlangen einer öffentlichen Stelle sind die betroffenen Daten grundsätzlich unverzüglich bereitzustellen. Auch hier sollte eine Datenübermittelungspflicht erforderlich sein und ein bloßes in-situ-Recht nicht ausreichen. Sind die Daten nicht verfügbar oder erfüllt das Verlangen nicht die Voraussetzungen des Art. 17 DA-E, so kann das Datenzugangsverlangen innerhalb von 15 Arbeitstagen nach Eingang abgelehnt oder seine Änderung beantragt werden, Art. 18 Abs. 2 DA-E. Außerdem besteht nach Art. 18 Abs. 3 DA-E die Möglichkeit, das Verlangen abzulehnen oder dessen Änderung zu beantragen, wenn der Dateninhaber die verlangten Daten bereits auf ein vorheriges Verlangen einer anderen öffentlichen Stelle oder eines Organs, einer Einrichtung oder einer sonstigen Stelle der Union zu demselben Zweck übermittelt hat und ihm nicht gem. Art. 19 Abs. 1 lit. c DA-E die Vernichtung der Daten mitgeteilt wurde. Die öffentliche Stelle bzw. das Organ, die Einrichtung oder sonstige Stelle ist dann darauf verwiesen, die Daten von derjenigen Stelle bereitgestellt zu bekommen, die die Daten bereits vom Dateninhaber erhalten hat. Gegen eine Ablehnung oder eine beantragte Änderung des Datenzugangsverlangens besteht seitens der öffentlichen Stelle, des Organs, der Einrichtung oder sonstigen Stelle der Union die Möglichkeit, die in Art. 31 DA-E benannte Behörde, die vom Mitgliedstaat zu benennen sind/ist mit der Angelegenheit zu befassen, Art. 18 Abs. 6 DA-E.

d) Kritik und Abhilfemöglichkeiten

Auch im Bereich B2G ist Kritik sowohl systemisch als auch auf Detailebene zu äußern. Systemisch sind insbesondere zwei Aspekte maßgeblich: Erstens stellt sich ganz grundlegend die Frage, ob die Datenzugangsansprüche zu Gunsten des Staates ausreichend sind, oder ob weitgehenderer und schützenswerter Bedarf besteht. Hier ist wohl jedenfalls fraglich, wann ein Datenzugangsanspruch überhaupt bestehen sollte und wann Marktlösungen ausreichend sind. Der Gesetzgeber antwortet darauf bislang mit dem Erfordernis einer außergewöhnlichen Notwendigkeit, das den Datenzugang begründen kann. Ob dies ausreichend und sinnvoll ist, wird sich erst in der Praxis zeigen. Insofern ist es zu begrüßen ist, dass der DA-E mit kurzer Frist (zwei Jahre nach Geltungsbeginn, Art. 41 DA-E) evaluiert wird. Zweitens fehlt es am so wichtigen Datenzugangsanspruch für die Wissenschaft, der sich entsprechend Art. 31 DSA für sämtliche Dateninhaber mit Ausnahme von Klein- und Kleinstunternehmen ausgestalten ließe. Privilegiert werden sollte sowohl die private als auch die öffentliche Forschung. Legitime Interessen der Dateninhaber lassen sich insbesondere berücksichtigen durch Einbindung einer Datenzugangstreuhand wie dem Koordinator für Digitale Dienste, entsprechenden Schrankenbestimmungen und Schutzkonzeptverpflichtungen der Berechtigten. Auf Detailebene bedarf es auch im jetzigen Verordnungsentwurf in Art. 21 DA-E der weitgehenderen Berücksichtigung privater Forschung, einer Modifikation des bloßen in-situ-Zugangsrechts hin zu einer grundsätzlichen Datenübermittlungspflicht[72] sowie einer Bestimmung von Kriterien zur Bemessung der Zweckvereinbarkeit.

VI. Zusammenfassung

Der DA-E ist keine reine Aftermarkt-Regulierung, sondern regelt erstmalig und umfassend die Daten-Governance bei der Nutzung von Produkten und verbundenen Diensten. Sein Verhältnis zur DS-GVO ist dabei klar: Er tritt neben die DS-GVO und ergänzt sie, nicht aber normiert er neue Erlaubnistatbestände. Zu einem Konflikt mit der DS-GVO kommt es jedenfalls hinsichtlich der Datenzugangsverpflichtungen des DA-E nicht: Verlangt der Nutzer, der selbst betroffene Person ist, Datenzugang an sich selbst oder einen Dritten, kann sich der Dateninhaber bei der Erfüllung dieses Datenzugangsanspruchs auf die Einwilligung des Nutzers stützen. Verlangt der Nutzer, der nicht selbst die betroffene Person ist, Datenzugang an sich selbst, füllen die Datenzugangsverpflichtungen des DA-E die Erlaubnistatbestände der Art. 6 Abs. 1 lit. c sowie Art. 9 Abs. 1 lit. g DS-GVO aus. Und verlangt der Nutzer, der nicht selbst betroffene Person ist, Datenzugang an einen Dritten, so muss die betroffene Person einwilligen oder die Datenübermittlung muss sich auf einen anderen Erlaubnistatbestand, zB Art. 6 Abs. 1 lit. f DS-GVO stützen lassen. Eine Vorrangsregelung für ggf. außerhalb der Datenzugangsverpflichtungen auftretende Konflikte empfiehlt sich gleichwohl.

Der DA-E folgt einer besitzrechtlichen Logik: Diejenigen, die auf einer vertraglichen Grundlage berechtigt besitzen, sollen Zugang zu den aus vernetzten Produkten oder verbundenen Diensten anfallenden Daten erhalten. Aus dieser Besitzlogik heraus ist zu erklären, weshalb der europäische Gesetzgeber kein allgemeines Zugangsrecht für die bei der Nutzung von Software generell anfallenden Daten mit dem DA-E einzuführen beabsichtigt.

Die gewählte Daten-Governance stellt den Dateninhaber in den Mittelpunkt. Seine technisch-faktische Herrschaft über die erhobenen Daten erkennt der Gesetzgeber rechtlich an und er ist es, der sich umfassende Rechte an den Daten einräumen lassen kann, ohne dass der Nutzer mit hinreichenden Schutzvorschriften bedacht wird. Ihm will er einen Anreiz zu Investitionen in die Wertschöpfung aus Daten geben.[73] Daran ändert auch ein Zugangsrecht des Nutzers nichts, solange dies als bloßes in-situ-Recht ausgestaltet ist. Wer hieraus eine Grundsatzentscheidung des europäischen Gesetzgebers zu Gunsten einer nutzerfreundlichen IoT-Daten-Governance ableiten will, irrt.

Die Wahl einer Daten-Governance, die den Dateninhaber in den Mittelpunkt stellt, überrascht in Anbetracht der Ziele, denen der DA-E verpflichtet ist. Es bleibt aber festzuhalten, dass der Gesetzgeber die Mittel dazu hat, diese Ziele durch ein umfassendes Maßnahmenbündel noch zu erreichen. Erforderlich hierfür sind jedoch mehr als vorsichtige Korrekturen. Der DA-E wird den Umgang mit Daten auf Jahrzehnte beeinflussen. Bleibt er, wie er ist, wird er Innovation, eine gerechte Verteilung der Wertschöpfung aus Daten sowie die Stärkung der Handlungskompetenzen der Menschen in Bezug auf ihre Daten für diese Zeit in weite Ferne rücken lassen.

Professorin Dr. Louisa Specht-Riemenschneider ist Inhaberin des Lehrstuhls für Bürgerliches Recht, Informations- und Datenrecht an der Rheinischen Friedrich-Wilhelms-Universität Bonn, Direktorin des Instituts für Handels- und Wirtschaftsrecht und Leiterin der Forschungsstelle für Rechtsfragen neuer Technologien sowie Datenrecht (ForTech) und ferner Mitherausgeberin der MMR.

72 Vgl. dazu bereits oben.
73 DA-E, S. 5.