

## Aufsatz

# Freie Fahrt im Datenverkehr? – Der Data Act und der Data Governance Act

---

Hendrik Eppelmann



**Open Peer Review**

Dieser Beitrag wurde lektoriert von: Hanna Brinkmann und Daniel Dischinger

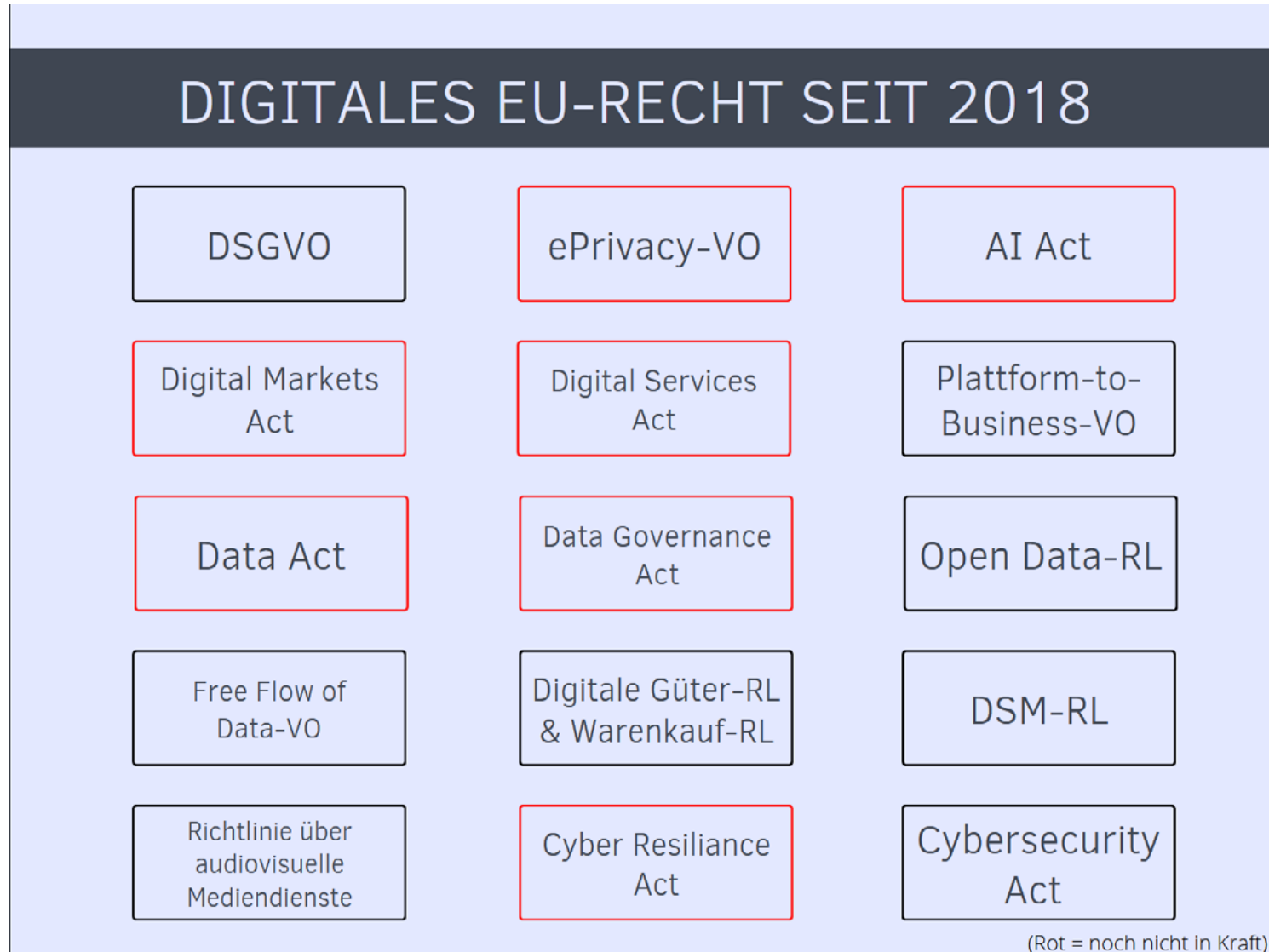


---

Hendrik promoviert an der Universität zu Köln zur kartellrechtlichen Beurteilung des Datenaustauschs über digitale B2B-Plattformen. Zudem ist er wissenschaftlicher Mitarbeiter in den Bereichen Kartell- und Datenschutzrecht bei Loschelder Rechtsanwälte.

**A**m 19.02.2020 veröffentlichte die EU-Kommission ihre „europäische Datenstrategie“ und steckte damit den datenpolitischen Pfad der nächsten Jahre ab. Ambitioniertes Ziel der Kommission ist dabei nichts geringeres als die „Schaffung eines einheitlichen europäischen Datenraums, eines echten Binnenmarkts für Daten [...] in dem sowohl personenbezogene als auch nicht-personenbezogene Daten [...] sicher sind und in dem Unternehmen auch leicht Zugang zu einer nahezu unbegrenzten Menge hochwertiger industrieller Daten erhalten.“<sup>1</sup> Bereits in den Jahren zuvor hat die EU einen legislativen Schwerpunkt auf die Digitalisierung und Datenwirtschaft gelegt. Zur Ausgestaltung der Datenstrategie sollen in den kommenden Jahren diverse weitere Rechtsakte folgen.

<sup>1</sup> Kommission, COM(2020) 66 final, 5, [hier](#) abrufbar (Stand: 31.05.2022).



### Ausgewählte Rechtsakte der EU zu Digital-Themen seit 2018

Auf den Umgang mit und den Fluss von Daten konzentrieren sich auch zwei aktuelle Verordnungsentwürfe: der Entwurf für den Data Governance Act<sup>2</sup> (DGA-E) und der Entwurf für den Data Act<sup>3</sup> (Data Act-E). Während der Data Act-E zurzeit noch rege diskutiert wird und vermutlich nicht vor Ende 2024 in Kraft tritt,<sup>4</sup> wurde der DGA-E bereits vom europäischen Parlament angenommen.<sup>5</sup>

<sup>2</sup> Der offizielle deutsche Kurzname des Verordnungsentwurfs lautet "Daten-Governance-Gesetz". Bislang ist aber auch im deutschsprachigen Raum die Bezeichnung „Data Governance Act“ gebräuchlicher; der letzte Entwurf ist [hier](#) abrufbar (Stand: 31.05.2022).

<sup>3</sup> Der offizielle deutsche Kurzname des Verordnungsentwurfs lautet „Datengesetz“. Bislang ist aber auch im deutschsprachigen Raum die Bezeichnung „Data Act“ gebräuchlicher; der erste Entwurf ist [hier](#) abrufbar (Stand: 31.05.2022).

<sup>4</sup> Gerpott, CR 2022, 271 (280), Rn. 48.

<sup>5</sup> Europäisches Parlament, Presseerklärung vom 06.04.2022, [hier](#) abrufbar (Stand: 31.05.2022).

Doch wird die EU ihr ehrgeiziges Ziel eines Daten-Binnenmarktes mithilfe dieser Verordnungen erreichen? Geben diese Vorhaben tatsächlich grünes Licht für eine freie Fahrt im Datenverkehr oder schickt die EU die Datenwirtschaft auf eine Route voller Kurven und Baustellen? Der folgende Beitrag möchte sich diesen Fragen kritisch nähern, indem er die wesentlichen Normen der Verordnungsentwürfe zum Austausch von Daten erklärt und beleuchtet.

## A. Daten im Internet of Things

Zunächst trifft der Data Act-E wesentliche Regelungen zu Daten, die im Internet of Things (,IoT‘) – also dem System über das Internet vernetzter Gegenstände<sup>6</sup> – anfallen.

### I. Zugang zu IoT Daten

Herzstück des Data Act-E ist der Zugang zu Daten aus dem IoT. Zukünftig sollen die Nutzer<sup>7</sup> von Produkten und verbundenen Diensten (digitale Dienste, die funktionsnotwendig in das Produkt integriert sind, Art. 2 Nr. 3 Data Act-E) einen Zugangsanspruch zu den bei der Nutzung entstandenen Daten haben. Art. 20 DSGVO sieht einen ähnlichen Anspruch bereits für personenbezogene Daten vor. Anders als dieser soll der Data Act-E aber für alle Arten von Daten, unabhängig von einem etwaigen Personenbezug, gelten. Entscheidend ist nur, dass die jeweiligen Daten durch die Nutzung eines Produktes oder eines verbundenen Dienstes erzeugt wurden. Ein solches ‚Produkt‘ im Sinne des Data Act-E ist ein körperlicher beweglicher Gegenstand, der Daten über seine Nutzung oder Umgebung erlangt, erzeugt oder sammelt und Daten elektronisch übermitteln kann und dessen Hauptfunktion nicht die Speicherung und Verarbeitung von Daten ist.<sup>8</sup> Gemeint sind letztlich alle Produkte,

<sup>6</sup> Zum Begriff des „IoT“ ausführlich: Ye, CTRL 1/21, 11.

<sup>7</sup> Zum Zwecke der besseren Lesbarkeit wird bei personenbezogenen Hauptwörtern nur die männliche Form verwendet. Diese Begriffe sollen für alle Geschlechter gelten.

<sup>8</sup> Art. 2 Nr. 2 Data Act-E.



die Teil des IoT sind, etwa Fahrzeuge, Haushaltsgeräte oder industrielle Maschinen.<sup>9</sup> Nicht erfasst sein sollen solche Geräte, die in erster Linie dazu dienen, Inhalte anzuzeigen, abzuspielen, aufzuzeichnen oder zu übertragen; etwa PCs, Server, Tablets, Smartphones, Kameras und Scanner. Solche Geräte erzeugen nicht nur Daten über das Nutzerverhalten, sondern erfordern einen menschlichen Beitrag zur Erstellung von Inhalten.<sup>10</sup> Der Data Act zielt also nur auf maschinengenerierte Daten ab, die durch die Nutzung von vernetzten Gegenständen anfallen. Interessanterweise (und schwer nachvollziehbar)<sup>11</sup> ausgenommen sind rein digitale Produkte wie Software.

Art. 3 I Data Act-E verpflichtet die Anbieter von IoT-Produkten dazu, die Produkte von vornherein so zu konzipieren, dass die Nutzer standardmäßig einfach, sicher und – soweit relevant und angemessen – direkt auf die bei der Nutzung erzeugten Daten zugreifen können. Man spricht hier auch von der Pflicht zum access by design.<sup>12</sup> Der Data Act-E verpflichtet Hersteller also zukünftig dazu, sämtliche ihrer Produkte nur noch mit entsprechenden Zugangs-Features ausgestattet zu vertreiben.

Auch, wenn der Nutzer nicht direkt mittels access by design auf die erzeugten Daten zugreifen kann, hat er einen Anspruch auf Zurverfügungstellung der Daten an sich oder Dritte. Dies muss unverzüglich, kostenlos und gegebenenfalls kontinuierlich und in Echtzeit erfolgen, soweit dies technisch machbar ist (vgl. Art. 4, 5 Data Act-E). Sind Geschäftsgeheimnisse enthalten, müssen alle erforderlichen Schutzmaßnahmen eingehalten werden (Art. 4 III Data Act-E). Erlangte Daten dürfen nicht dazu genutzt werden, Konkurrenzprodukte zu entwickeln (Art. 4 IV Data-Act).

Das Vorhaben, Datenbestände aus dem IoT für die Nutzer zu öffnen, ist zu begrüßen. Hiermit wird das Ziel einer breiten Datenverfügbarkeit aktiv gefördert. Praktisch und wirtschaftlich relevant wird dies vermutlich weniger für den einzelnen Endverbraucher, als insbesondere für Unternehmen, die bisher nicht auf alle Daten zugreifen konnten, die etwa ihre Produktionsmaschinen generiert haben.

<sup>9</sup> Erwägungsgrund 14 Data Act-E.

<sup>10</sup> Erwägungsgrund 15 Data Act-E.

<sup>11</sup> Gerpott, CR 2022, 271 (274), Rn. 12; Hilgendorf/Vogel, JZ 8/2022, 380 (388).

<sup>12</sup> Bspw.: Klink-Straub/Straub, ZD-Aktuell 2022, 01076; Bomhard/Merkle, RD 2022, 168 (173), Rn. 39.



Herzstück des Data Act-E ist der Zugang zu Daten aus dem IoT

## II. Datenlizenz

Hoch brisant und trotzdem geradezu versteckt ist Art. 4 VI Data Act-E: Hiernach darf ein Dateninhaber nicht-personenbezogene Daten, die bei der Nutzung eines IoT-Produktes oder verbundenen Dienstes erzeugt werden, nur dann nutzen, wenn er mit dem Nutzer eine entsprechende vertragliche Vereinbarung über die Nutzung geschlossen hat. Was im Datenschutzrecht als selbstverständlich erscheint, war bisher für nicht-personenbezogene Daten nicht geregelt. Zumindest in der Theorie werden damit dem Produkthersteller Steine in den Weg gelegt, wenn er die bei der Produktnutzung erzeugten Daten verarbeiten möchte. Rein praktisch gesehen dürfte sich (zumindest bei der Produktnutzung durch Endkunden) aber nicht allzu viel ändern, da diese erfahrungsgemäß bereit sind, allen möglichen Pop-up Fenstern oder ähnliches zuzustimmen, die sie von der Nutzung des Produkts abhalten.<sup>13</sup>

<sup>13</sup> Vgl. Kerber, Governance of IoT Data: Why the EU Data Act will not fulfill its objectives, 21, hier abrufbar (Stand: 31.05.2022).

Führt man sich vor Augen, dass es eigentlich das Ziel des Data Act-E ist, die breite Nutzung von Daten zu fördern, stellt sich die Frage, ob es wirklich förderlich ist, die Nutzung nicht-personenbezogener Daten, die im IoT erzeugt werden, von einer vertraglichen Vereinbarung abhängig zu machen. Hier geht es gerade nicht um personenbezogene Daten, die grundrechtlichen Schutz genießen, sondern um nicht-personenbezogene Daten, die für die Verbesserung von Produkten und für neue Innovation genutzt werden sollen, wie etwa die Daten über Leistungsfähigkeit und Produktivität von Maschinen. Den freien Fluss solcher Daten soll der Data Act eigentlich vereinfachen.

### **B. Datenaustausch zwischen Unternehmen und Behörden**

Im Data Act-E und DGA-E regelt die EU auch neue Fälle für den Austausch von Daten zwischen Unternehmen und öffentlichen Stellen.

### **I. Bereitstellung an öffentliche Stellen bei außergewöhnlicher Notwendigkeit**

Zunächst definiert der Data Act-E neue Situationen, in denen Unternehmen staatlichen Behörden Daten übermitteln müssen. Man spricht dann von business to government („B2G“).

Konkret geht es darum, dass eine öffentliche Stelle aufgrund einer „außergewöhnlichen Notwendigkeit“ die Bereitstellung von Daten verlangen kann (Art. 14 I Data Act-E). Die Notwendigkeit der Datennutzung muss die öffentliche Stelle selbst nachweisen. Auch Forschungseinrichtungen wie Universitäten können solche öffentlichen Stellen sein.<sup>14</sup> Art. 15 Data Act-E zählt abschließend Fälle einer außergewöhnlichen Notwendigkeit auf.

Hauptfall einer solchen Notwendigkeit ist die Verhinderung und Bewältigung eines öffentlichen Notstand oder Erholung von einem solchen. Dieser ist in Art. 2 Nr. 10 Data Act-E definiert als eine außergewöhnliche Situation, die das Risiko schwerwiegender und dauerhafter Folgen für die Lebensbedingungen, die wirtschaftliche Stabilität oder wirtschaftliche Vermögenswerte in der Union birgt und sich negativ auf die Bevölkerung auswirkt. Beispiele hierfür sind Pandemien,<sup>15</sup> Naturkatastrophen und Umweltschäden oder große Cyberangriffe.<sup>16</sup> Erwägungsgrund 57 des Data Act-E legt nahe, dass es letztlich auf eine Interessenabwägung ankommen soll; auch wenn der Verordnungstext selbst dies nicht ausdrücklich hergibt.

Eine „außergewöhnliche Notwendigkeit“ kann aber auch darin liegen, dass eine öffentliche Stelle aufgrund des Fehlens verfügbarer Daten eine bestimmte, gesetzlich ausdrücklich vorgesehene Aufgabe im öffentlichen Interesse nicht erfüllen kann und sich die öffentliche Stelle die Daten nicht anderweitig zeitnah besorgen oder kaufen kann bzw. dass der Verwaltungsaufwand der Dateninhaber oder anderer Unternehmen erheblich verringert werden würde.

Die öffentliche Stelle ist dann sogar dazu ermächtigt, die erlangten Daten mit anderen öffentlichen Stellen oder mit öffentlichen Aufgaben betrauten Dritten zu teilen (Art. 17 IV Data Act-E). Sie muss dies lediglich dem ursprünglichen Dateninhaber mitteilen. Freilich dürfen alle Beteiligten die erlangten Daten aber nur für die Zwecke der „außergewöhnlichen Notwendigkeit“ verwenden und müssen sie vernichten, sobald sie nicht mehr für diesen Zweck erforderlich sind (Art. 19 I Data Act-E).

Wenn dies für den Zweck des Verlangens unerlässlich ist, darf die öffentliche Stelle sogar die Offenlegung von Geschäftsgeheimnissen fordern. Die Behörde muss dann aber geeignete Maßnahmen treffen, um die Vertraulichkeit dieser Informationen zu wahren (Art. 19 II Data Act-E). In diesem Bereich wird deutlich, was für ein Streitpotential den B2G-Pflichten des Data Act-E innewohnt.

<sup>15</sup> Beispielhaft über die Nutzung von Daten zur Bewältigung der Corona-Pandemie: *Handelsblatt*, Wie Regierungen versuchen, das Virus mit Big Data zu bändigen, [hier](#) abrufbar (Stand: 31.05.2022).

<sup>16</sup> Erwägungsgrund 57 Data Act-E.

<sup>14</sup> Erwägungsgrund 56 Data Act-E.



ZITAT: Wenn dies für den Zweck des Verlangens unerlässlich ist, darf die öffentliche Stelle sogar die Offenlegung von Geschäftsgeheimnissen fordern

An diesen Regeln ist unter anderem durch den Europäischen Datenschutzausschuss (EDPB) und den Europäischen Datenschutzbeauftragten (EDPS) kritisiert worden, dass weder die Situationen einer „außergewöhnlichen Notwendigkeit“ ausreichend präzise definiert ist, noch die genauen Kategorien von Daten spezifiziert worden sind.<sup>17</sup> Hier hat die Kommission noch Nachbesserungsbedarf, um dem Datenschutzbedürfnis der Bürger gerecht zu werden.

## II. Weiterverwendung von Daten im Besitz öffentlicher Stellen

Der DGA-E wiederum kümmert sich um den Datenfluss in die andere Richtung, also von der Behörde zum Unternehmen („G2B“). Der Staat verfügt über eine Vielzahl hochwertiger Daten, die für Unternehmen von Interesse sein könnten. Beispiele hierfür sind Daten zum Straßenverkehr, Bevölkerungsstatistiken, Katasterdaten oder Daten über die Landwirtschaft.<sup>18</sup> Der DGA-E regelt die Weiterverwendung von Daten im Besitz öffentlicher Stellen durch Dritte.

Bereits 2019 hat die EU eine Richtlinie über die Weiterverwendung von Daten des öffentlichen Sektors erlassen („Open Data RL“, RL 2019/1024). Auch diese regelt Modalitäten zur Erleichterung der Weiterverwendung. Jedoch enthält sie keine Regelungen zu dem geistigen Eigentum Dritter, statistischen Geheimnissen oder Geschäftsgeheimnissen (vgl. Art. 1 II RL 2019/1024). Die zu solchen Daten offengebliebenen Fragen möchte der DGA-E beantworten.<sup>19</sup>

<sup>17</sup> 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 (Data Act), Rn. 78 ff., hier abrufbar (Stand: 31.05.2022).

<sup>18</sup> Czychowski, FS Taeger, 2020, 129 (130).

<sup>19</sup> Vgl. Art. 3 Abs. 1 a.E. DGA-E; Erwägungsgrund 10 DGA-E; Spindler, CR 2021, 98 (100), Rn. 6; Richter, ZD 2022, 3 (4).

Der DGA-E hat das Ziel, zu ermöglichen, dass öffentliche Stellen entsprechend geschützte Daten zur Weiterverwendung durch Unternehmen bereitstellen können. Ausgenommen sind wiederum Daten öffentlicher Unternehmen, Daten von öffentlich-rechtlichen Rundfunkanstalten, die sich auf deren Sendeauftrag beziehen, Daten von Kultur- und Bildungseinrichtungen sowie Daten, die aus Gründen der nationalen Sicherheit geschützt sind (Art. 3 II DGA-E).

Es ist jedoch wichtig, sich stets vor Augen zu führen, was genau der DGA-E hier erreichen möchte: Es geht nicht darum, dass ein Anspruch auf Bereitstellung von Daten zur Weiterverwendung geschaffen wird.<sup>20</sup> Vielmehr geht es um die Schaffung von Rahmenbedingungen, unter denen auch ansonsten geschützte Daten zur Weiterverwendung bereitgestellt werden können.

Doch was heißt ‚Weiterverwendung‘ überhaupt? Nach Art. 2 Nr. 2 DGA-E ist hiermit jede Nutzung von Daten, die im Besitz öffentlicher Stellen sind, durch Dritte gemeint, soweit damit kommerzielle oder nichtkommerzielle Zwecke verfolgt werden, die sich vom ursprünglichen Zweck des öffentlichen Auftrags bei der Erstellung der Daten unterscheiden. Es geht also darum, dass Daten, die mittels öffentlicher Gelder erhoben wurden, in einem breiten Rahmen der Gesellschaft zugutekommen sollen.<sup>21</sup>

Aus Gründen der Chancengleichheit ist es den Behörden grundsätzlich verboten, die Daten nur einzelnen Unternehmen zur ausschließlichen Verwendung zur Verfügung zu stellen (Art. 4 I DGA-E). Die öffentliche Stelle kann festlegen, dass sie nur Daten herausgibt, die sie zuvor anonymisiert hat bzw. solche, bei denen Geschäftsgeheimnisse unkenntlich gemacht wurden (Art. 5 III lit. a) DGA-E). Alternativ kann sie auch dafür sorgen, dass der Datenzugang nur in kontrollierten sicheren Ver-

<sup>20</sup> Erwägungsgrund 11 DGA-E.

<sup>21</sup> Erwägungsgrund 6 DGA-E.

„Wenn dies für den Zweck des Verlangens unerlässlich ist, darf die öffentliche Stelle sogar die Offenlegung von Geschäftsgeheimnissen fordern.“

arbeitungsumgebungen stattfindet; entweder per Fernzugriff oder sogar nur innerhalb der physischen Räumlichkeiten (Art. 5 III lit. b), c) DGA-E). Darüber hinaus muss die öffentliche Stelle die Möglichkeit haben, die Verfahren, Mittel und Ergebnisse der Datenverarbeitung zu überprüfen, um die Verwendung dieser untersagen zu können, falls Rechte und Interessen Dritter gefährdet wären (Art. 5 IV DGA-E).

Die Erlaubnis zur Weiterverwendung der Daten müssen die Behörden aber auch nicht kostenlos gewähren. Vielmehr dürfen sie transparente, nichtdiskriminierende, verhältnismäßige und objektiv gerechtfertigte Gebühren erheben, deren Höhe sich aus den Kosten für die Bereitstellung ableiten (Art. 6 I, II, V DGA-E). Gleichzeitig sollen die Behörden hierbei aber kleinen und mittleren Unternehmen entgegenkommen, um Anreize für eine nichtkommerzielle Nutzung durch diese zu fördern (Art. 6 IV DGA-E).

Dass die neuen Regeln zur Weiterverarbeitung großen praktischen Wert haben werden, darf bezweifelt werden. Letztlich legt man den Behörden Pflichten auf (wie etwa die Löschung von Geschäftsgeheimnissen oder die Anonymisierung personenbezogener Daten) ohne sie gleichzeitig dazu zu verpflichten, auch tatsächlich aktiv zu werden und eine Weiterverwendung zu ermöglichen. Ob damit die Ziele der Verordnung erreicht werden, erscheint fraglich.<sup>22</sup>

### C. Dienste für gemeinsame Datennutzung

Damit es zu einem regen Datenverkehr kommen kann, muss es auch eine funktionierende Infrastruktur dafür geben. Diese könnte unter anderem auf Diensten für gemeinsame Datennutzung im Sinne des Art. 10 DGA-E basieren. Darunter versteht der DGA-E vor allem Dienste, die einen Datenfluss zwischen Dateninhabern und möglichen Datennutzern vermitteln und technisch ermöglichen. Diese Angebote sollen sich an eine unbestimmte Anzahl von Nutzern richten.<sup>23</sup> Hoch spezialisierte

Dienste, die nur auf einzelne konkrete Unternehmen ausgerichtet sind, sind daher nicht vom DGA-E erfasst. Ausgenommen sind auch bloße Vermittler von Inhalten, wie etwa Streaming Plattformen.<sup>24</sup> Vom DGA-E sollen nur solche Dienste erfasst sein, bei denen es wirklich darum geht, Daten zu übertragen und nicht nur Inhalte anzuzeigen. Ein breites Angebot solcher Dienste könnte den europäischen Datenaustausch sicherlich stärken, wenn die potenziellen Nutzer ein ausreichendes Vertrauen in diese haben.

Um ein solches Vertrauen zu erzeugen und aufrecht zu erhalten, sieht der DGA-E ein Anmeldeverfahren für die Diensteanbieter vor. (Wohl) nur wer seinen Dienst angemeldet hat, darf diesen auch betreiben (vgl. Art. 11 IV DGA-E).<sup>25</sup> Ziel ist es, dass die Diensteanbieter stets nur als neutrale Mittler auftreten.<sup>26</sup> Zudem unterliegen diese Dienste einer Liste an Bedingungen aus Art. 12 DGA-E. So darf der Diensteanbieter etwa die Daten nicht zu anderen Zwecken als zur Vermittlung nutzen. Die Dienste für die gemeinsame Datennutzung müssen bei einer gesonderten Rechtsperson angesiedelt sein. Das Angebot und die Preise müssen stets fair, transparent und nichtdiskriminierend sein. Zudem muss der Anbieter unter anderem über Verfahren verfügen und Maßnahmen ergreifen, die betrügerische und missbräuchliche Praktiken der Nutzer verhindern, einen garantierten Datenzugang im Insolvenzfall gewährleisten und Datentransfers verhindern, die nach anderen Gesetzen rechtswidrig wären.

Der Anbieter wird hier also in die Pflicht genommen, seinen Dienst von vornherein so zu gestalten, dass es erst gar nicht zu unerwünschten Datentransfers kommen kann. Das dürfte im Einzelfall komplexe Rechtsfragen aufwerfen. Beispielsweise soll der Anbieter gewährleisten, dass auf seiner Plattform das Wettbewerbsrecht eingehalten wird.<sup>27</sup> Wo die Grenze zwischen einem kartellrechtswidrigen Informationsaustausch und dem politisch erwünschten data sharing verläuft, ist eine im Detail sehr komplexe und alles andere als triviale Frage. Insofern wird dem Anbieter

<sup>22</sup> Kritisch auch *Spindler*, CR 2021, 98 (102), Rn. 18.

<sup>23</sup> Erwägungsgrund 28 DGA-E.

<sup>24</sup> Vgl. Erwägungsgrund 29 DGA-E.

<sup>25</sup> Vgl. *Spindler*, CR 2021, 98 (103), Rn. 23; *Richter*, ZEuP 2021, 634 (647 f.).

<sup>26</sup> Erwägungsgrund 33 DGA-E.

<sup>27</sup> Vgl. Erwägungsgrund 60 DGA-E.



eines Vermittlungsdienstes hier in Ermangelung eines abschließend klaren Rechtsrahmens eine große Verantwortung auferlegt, die mit dem hohen Bußgeldrisiko des Kartellrechts verbunden ist.<sup>28</sup>

Insofern birgt der Katalog der Bedingungen in Art. 12 DGA-E die Gefahr, innovative Anbieter von Diensten für die gemeinsame Datennutzung abzuschrecken. Hier sollte die Kommission mehr Klarheit schaffen oder Risiken entschärfen, um Innovationspotenzial nicht von vornherein abzuwürgen.

### D. Wechsel von Cloud-Diensten & Interoperabilität

Der Data Act-E trifft Regelungen, die es ermöglichen sollen, einfach zwischen digitalen Diensten zu wechseln oder diese parallel zu nutzen.

#### I. Wechsel von Cloud-Diensten

Um den europäischen Datenverkehr zu fördern und die Konzentration von Datenbeständen zu verhindern, versucht der Data Act-E, den Wechsel zwischen Datenverarbeitungsdiensten (gemeint sind vor allem Cloud-Dienste) zu erleichtern. Besonders bemerkenswert ist hierbei, dass es zukünftig eine Kündigungsfrist von höchstens 30 Tagen für Datenverarbeitungsdienste geben darf (Art. 23 I lit. a) Data Act-E). Bisher sind deutlich längere Kündigungsfristen in der Praxis die Regel. Dadurch dürfte eine ganz neue Dynamik auf dem Markt für Cloud-Dienste entstehen. Inwieweit die Anbieter solcher Dienste eine derartige Schnelllebigkeit verkraften und ihre Geschäftsmodelle anpassen können, bleibt abzuwarten. Zu befürchten ist, dass Cloud-Anbieter diese Unwägbarkeiten künftig einpreisen werden.<sup>29</sup>

<sup>28</sup> Gellert/Graef, The European Commission's proposed Data Governance Act: some initial reflections on the increasingly complex EU regulatory puzzle of stimulating data sharing (2021), 14, hier abrufbar (Stand: 31.05.2022); Spindler, CR 2021, 98 (108), Rn. 46; Falkhofen, EuZW 2021, 787 (790).

<sup>29</sup> Bomhard/Merkle, RD 2022, 168 (175), Rn. 56.



Es dürfte eine ganz neue Dynamik auf dem Markt für Cloud-Dienste entstehen.

Der Dienstleister muss zudem den Wechsel seines bisherigen Kunden zu einem anderen Dienstleister aktiv unterstützen, die Daten übertragen und einen nahtlosen kontinuierlichen Übergang gewährleisten (Art. 24 I Data Act-E). Über die ersten drei Jahre nach Inkrafttreten des Data Act sollen die Entgelte für einen solchen Wechsellvorgang schrittweise abgeschafft werden und dann für den Nutzer vollständig kostenlos werden (Art. 25 I, II Data Act-E).

#### II. Interoperabilität

Als wichtiger Faktor für eine offene und faire Datenwirtschaft gilt die sogenannte „Interoperabilität“. Darunter versteht der EU-Gesetzgeber die Fähigkeit von zwei oder mehr Datenräumen, Kommunikationsnetzen, Systemen, Produkten, Anwen-

dungen oder Komponenten, Daten auszutauschen und zu verwenden, um ihre Funktion auszuführen (Art. 1 Nr. 19 Data Act-E). Es geht also letztlich darum, dass Systeme miteinander kommunizieren können, da sie einheitliche Formate, Verfahren und Schnittstellen benutzen. Wenn etwa Cloud-Dienste interoperabel sind, so ist der eben beschriebene Wechsel zwischen Cloud-Diensten deutlich besser zu realisieren.

Art. 28 Data Act-E legt den Betreibern von Datenräumen dafür diverse Dokumentationspflichten auf, um Informationen zu beschreiben, die für die Interoperabilität von Diensten wesentlich sind. Art. 29 Data Act-E sieht europäische Normen vor, die die Interoperabilität von Datenverarbeitungsdiensten vorantreiben sollen.

Wer für die Bereitstellung von Daten smart contracts<sup>30</sup> verwendet, muss gewährleisten, dass diese robust sind, sicher beendet oder unterbrochen werden können, nach Beendigung archiviert werden und über eine strenge Zugriffskontrolle verfügen (Art. 30 Data Act-E). Ob die Praxis diesen Anforderungen ausreichend nachkommen kann, wird sich zeigen.

## E. Datenaltruismus

Um das volle Potenzial von Daten in der Union auszuschöpfen, setzt die Kommission zu guter Letzt auf Freiwilligkeit in Form des sogenannten ‚Datenaltruismus‘. Hierunter versteht der EU-Gesetzgeber die freiwillige Bereitstellung personenbezogener oder nicht-personenbezogener Daten zur Nutzung für Ziele von allgemeinem Interesse (Art. 2 Nr. 16 DGA-E). Gemeint sind etwa die Gesundheitsversorgung, die Bekämpfung des Klimawandels, die Verbesserung der Mobilität oder die bessere Erbringung öffentlicher Dienstleistungen.<sup>31</sup> Ein aktuelles Beispiel für so ein Vorgehen ist die Corona-Datenspende-App des Robert Koch-Instituts.<sup>32</sup>

Der Datenaltruismus soll dazu beitragen, Datenbestände zu schaffen, die umfangreiche Datenanalysen und maschinelles Lernen<sup>33</sup> ermöglichen.<sup>34</sup> Ob in der Praxis die Freiwilligkeit der Bürger ausreicht, um einen dafür ausreichend großen Datenbestand zu schaffen, darf jedoch infrage gestellt werden. Jedenfalls ist zweifelhaft, wie repräsentativ die Erkenntnisse sind, wenn dort nur die Daten derer zu finden sind, die sich dazu berufen gefühlt haben, ihre Daten freiwillig zu spenden.

Art. 17 DGA-E sieht vor, dass sich „datenaltruistische Organisationen“ als solche in ein Register eintragen lassen können. Nach der Eintragung kann sie sich als „in der Union anerkannte datenaltruistische Organisation“ bezeichnen und das entsprechende Logo verwenden. Die Registrierung setzt voraus, dass die Organisation Ziele von allgemeinem Interesse verfolgt, ohne Erwerbszweck tätig ist und diese Tätigkeit über eine Struktur ausübt, die von ihren anderen Tätigkeiten funktionell getrennt ist (Art. 18 i.V.m. Art. 2 Nr. 16 DGA-E). Erlaubt die Organisation die Verarbeitung des Datenbestands durch Dritte, so muss sie dies transparent dokumentieren (Art. 20 DGA-E). Zudem muss die Organisation die Datenspenden über die Ziele der Verarbeitung und etwaige Verarbeitungen in Drittstaaten informieren (Art. 21 I DGA-E). Da das Erfassen von Datenspenden bei personenbezogenen Daten datenschutzrechtlich auf die Einwilligung nach der DSGVO gestützt wird,<sup>35</sup> stellt Art. 25 I DGA-E ein einheitliches europäisches Einwilligungsformular für den Datenaltruismus in Aussicht.

Unter dem Strich scheint die Idee des ‚Datenaltruismus‘ eine gute Sache zu sein. Wieso es hierzu aber neuer Regelungen neben der DSGVO bedurfte und was passieren soll, wenn eine Organisation sich nicht in das Register einträgt, bleibt unklar.<sup>36</sup> Erwägungsgrund 46 stellt sogar klar, dass die Eintragung keine Voraussetzung für die Ausübung datenaltruistischer Tätigkeiten ist. Es scheint sich hier vielmehr um ein reines Gütesiegel zu handeln, als dass eine Zertifizierung als „datenaltruistische Organisation“ tatsächlich rechtliche Auswirkungen hätte. Ob man aber durch (rein

<sup>30</sup> Zum Begriff des Smart Contracts siehe *Dischinger*, CTRL 1/21, 18 (19f.).

<sup>31</sup> Art. 2 Nr. 16 DGA-E a.E.; Erwägungsgrund 45 DGA-E.

<sup>32</sup> Infos zu der App finden sich [hier](#) (Stand: 31.05.2022).

<sup>33</sup> Zum Begriff des maschinellen Lernens siehe *Kupfermann*, CTRL 1/21, 7.

<sup>34</sup> Erwägungsgrund 45 DGA-E.

<sup>35</sup> Erwägungsgrund 50 DGA-E; *Schildbach*, ZD 2022, 148 (151); *von Hagen/Völzmann*, MMR 2022, 176.

<sup>36</sup> Vgl. *Spindler*, CR 2021, 98 (106), Rn. 41; *Schildbach*, ZD 2022, 148 (151f.).



symbolische) neue Bürokratie den Willen zur Datenspenden anregt, darf wiederum bezweifelt werden.<sup>37</sup>

### F. Fazit

Insgesamt hinterlassen DGA-E und Data Act-E ein gemischtes Bild: Die Idee eines Binnenmarktes für Daten, in dem durch den freien Fluss großer Datenmengen Innovation erzeugt wird, scheint eine vielversprechende und zukunftssträchtige Strategie zu sein. Hier sollte die EU weiterhin Energie investieren und einen klaren Weg verfolgen.

Gleichwohl lassen diese beiden Verordnungs-Entwürfe auch ernüchert zurück: Anstatt umfassender und präziser Regeln findet man gewissermaßen ein Sammelsurium an unterschiedlichsten Vorschriften. Diese sind für sich genommen (mehr oder weniger) nachvollziehbar; einen roten Faden, der die Vorschriften verbindet, sucht man jedoch vergebens. Gerade unter einer Verordnung mit dem Namen „Data Act“ hätte man eine umfassende Regulierung der Datenwirtschaft erwartet. Stattdessen werden hier nur einzelne Teilgebiete in Details geregelt. Wieso man statt einer einheitlichen Verordnung zwei verschiedene (DGA und Data Act) kreiert hat, erschließt sich ebenfalls nicht ohne Weiteres. So wird die Rechtslage ohne Not verkompliziert, was letztlich der Akzeptanz und Bereitschaft der Unternehmen und Bürger zur aktiven Teilnahme am unionsweiten Datenverkehr schaden könnte. Es bleibt zu hoffen, dass die EU sich damit nicht selbst ausbremst.

Nach einem gründlichen Blick auf die Verordnungsentwürfe muss man daher feststellen, dass sich die Datenautobahn im Binnenmarkt doch noch in einem frühen Baustadium befindet. Bevor wirklich freie Fahrt im Datenverkehr herrscht, ist noch viel Arbeit zu tun – doch es wird sich sicher lohnen, den Weg weiterzugehen.

<sup>37</sup> Veil, Datenaltruismus: Wie die EU-Kommission eine gute Idee versemelt, [hier](#) abrufbar (Stand: 31.05.2022); Steinrötter, ZD 2021, 61 (62).

Zurück zum  
Inhaltsverzeichnis

# CTRL

2/22

2. Jahrgang, 1. Ausgabe  
[www.legaltechcologne.de/ctrl](http://www.legaltechcologne.de/ctrl)

Cologne Technology  
Review & Law



[Hier geht es zur ganzen Ausgabe!](#)

Reise in 15 Beiträgen durch die Legal-Tech-Welt:

[Von Kolumbien bis nach Finnland](#)  
[und von Compliance bis eSport.](#)



LEGAL TECH LAB  
COLOGNE