C. Kommentare zum Data Act mit Blick auf die Marktöffnung

Der Data Act-E beinhaltet, wie soeben aufgezeigt, viele wegweisende Ansätze. Im Folgenden sollen einige Aspekte des Entwurfs thematisiert werden, die für den Zugang zum Sekundärmarkt, also eine Marktöffnung für Dritte, noch nicht ausgereift sind. Die hier eingenommene Perspektive ist dezidiert darauf ausgerichtet, die Vorschriften auf ihre zugangseröffnende Wirkung für Dritte zu prüfen. Dahinter steht der Gedanke, dass alle Marktakteure faire Chancen in der vernetzten Wirtschaft haben müssen. Kunden sollen die Auswahlentscheidungen treffen können, wer welche Leistung erbringt, ohne in erheblichem Maße prädeterminiert zu sein. Das setzt voraus, dass die Regelungen einfach umzusetzen sind und Bedingungen für den Datenzugang nicht prohibitiv wirken.

I. Eröffnung des Zugangs zu Sekundärmärkten

Die zentrale Überlegung für die Öffnung der Sekundärmärkte ist, dass der Zugang zu diesen Märkten durch den Datenzugangsanspruch, wie er derzeit ausgestaltet ist, nicht gewährleistet wird. Dritte, z.B. Reparaturbetriebe, benötigen für ihr Tätigwerden nicht Zugang zu Rohdaten. Vielmehr müssen sie Zugang zu denjenigen Daten und digitalen Hilfsmitteln erhalten, die erforderlich sind, um auf dem Sekundärmarkt in sinnvoller Weise tätig werden zu können. Dieser Gedanke ist im Data Act nicht verwirklicht. Im Digital Markets Act hingegen hat der europäische Gesetzgeber einen solchen zweckorientierten Zugangsanspruch verwirklicht. Im Folgenden wird zunächst dargestellt, dass alle Marktteilnehmer die Legitimation haben, an den Marktchancen des IoT zu partizipieren (dazu 1.). Sodann wird der zweckbezogene Zugangsanspruch erläutert (dazu 2.). Schließlich wird dargestellt, welche Daten, Softwaredienste und Tools von einem solchen Anspruch umfasst sein müssen (dazu 3.).

1. Legitimation einer zweckgebundenen Zugangseröffnung

Der Data Act-E sieht richtigerweise einen Zugangsanspruch des Nutzers und von ihm benannter Dritter zu Daten vor. Das ist aus Gründen der volkswirtschaftlichen Dynamik (Erwägungsgrund 1) geboten, aber auch ein Gebot der Fairness, „da die von solchen Produkten oder verbundenen Diensten erfassten Daten ein wichtiges Gut für Anschluss-, Neben-, und sonstige Dienste sind" (Erwägungsgrund 6). Der Telos des Data Acts ist darauf gerichtet, den Marktzugang zu sichern.

a) Keine rechtliche Privilegierung des Dateninhabers

Festzuhalten ist, dass der Dateninhaber kein Bestimmungsrecht hat, was mit den Daten passieren soll. Wenn überhaupt ist dieses Recht dem Nutzer zugewiesen.

Der Dateninhaber hat zwar faktisch in der Regel die alleinige Zugriffsmöglichkeit, da er über das Produktdesign bestimmen kann, welche Daten erhoben werden und wo diese in welcher Form gespeichert werden. Der Hersteller hat es damit zu allererst in der Hand, den Zugang zu diesem Datenschatz zu kontrollieren. Diese monopolartige Stellung ist die Folge einer rein faktischen Beherrschung des Produktdesigns. Es gibt für eine Alleinzuweisung der dann entstehenden Daten aber keinerlei rechtliche Grundlage.[57] Das hält auch der Data Act-E unmissverständlich in Erwägungsgrund 19 fest:

> „In vielen Sektoren können die Hersteller oftmals durch ihre Kontrolle über die technische Konzeption des Produkts oder verbundener Dienste bestimmen, welche Daten erzeugt werden und wie darauf zugegriffen werden kann, auch wenn sie keinen Rechtsanspruch auf die Daten haben."

Überdies wird dem Gedanken eine Absage erteilt, es gäbe ein eigenes Schutzrecht an Daten:

> „ein allgemeiner Ansatz für die Zuweisung von Zugangs- und Nutzungsrechten für Daten [ist] der Gewährung ausschließlicher Zugangs- und Nutzungsrechte vorzuziehen."[58]

---

57 Erwägungsgrund 5, 19 Data Act-E.
58 Erwägungsgrund 6 Data Act-E.

Diesem Ausgangsbefund ist uneingeschränkt zuzustimmen. Die Aussagen im Data Act sind das Ergebnis einer seit Langem geführten rechtspolitischen und ökonomischen Diskussion über ein eigenes Schutzrecht an Daten. Auch aus wissenschaftlicher Sicht sprechen die besseren Argumente dafür, kein solches Schutzrecht zu schaffen.[59]

Fragt man sich, wer mit welcher Legitimation auf die Daten zugreifen kann, dann lässt sich rechtlich vor allem zugunsten des Nutzers argumentieren: Der Nutzer erhält das Produkt durch Kauf, Miete o.ä. und entrichtet dafür ein Entgelt. Die Nutzungshandlungen lösen den Datenaufzeichnungsvorgang aus und beziehen sich auch auf das Verhalten des Nutzers.

Die rechtliche Wertung gegen ein Schutzrecht an Daten (und damit letztlich an Informationen)[60] bedeutet aber, dass nicht einmal der Nutzer eine rechtlich abgesicherte Stellung erhält, um die Daten für sich zu vereinnahmen. Das ist rechtlich richtig, weil es eine Grundwertung zugunsten freier Information gibt, die bei der Monopolisierung von Daten gefährdet wäre; es ist volkswirtschaftlich ebenfalls richtig, weil nur so datengetriebene Innovationen ermöglicht werden. Dass es einen freien Zugriff zu Daten geben sollte, leuchtet rasch ein, wenn man sich vor Augen führt, dass das gesamte autonome Fahren zum Erliegen käme, würden Einzelne Verkehrsdaten für sich monopolisieren können.

Dem Data Act liegt die (politische) Wertung zugrunde, dass die Entscheidung über den Datenzugang dem Nutzer des Produkts oder Dienstes zustehen soll, der durch seine Nutzung diese Daten erst erzeugt hat. Dies manifestiert sich insbesondere in dem Umstand, dass selbst der Hersteller eines Produkts zur Verwendung der Daten die Einwilligung des Nutzers benötigt, Art. 4 Abs. 6 S. 1 Data Act-E.

Zwar wäre es auch denkbar und möglicherweise sogar ökonomisch sinnvoll, den Nutzervorbehalt zu streichen und eine Art Allgemeinverfügbarkeit der so generierten Daten zu postulieren.[61] Dieses Modell hat der europäische Gesetzgeber aber nicht gewählt. Eine Abkehr davon würde den Charakter des Data Act grundlegend ändern. Es müsste dann eine

59 Vgl. *Zech*, CR 2015, 137; *Drexl et al.*, Data Ownership and Access to Data, Max Planck Institute for Innovation & Competition Research Paper No. 16–10; *Kornmeier/Baranowski*, BB 2019, 1219; *Amstutz*, AcP 218 (2018), 438; European Commission Expert Group for the Observatory on the Online Platform Economy, Progress Report Work Stream on Differentiated Treatment, o.J. (2020), S. 21

60 Vgl. European Commission Expert Group for the Observatory on the Online Platform Economy, Progress Report Work Stream on Data, O.J. (2020), S. 7 f.; *Zech*, Informationen als Schutzgegenstand, 2012, S. 32.

61 Vgl. *Specht-Riemenschneider*, MMR 2022, 809, 817.

verpflichtende offene Schnittstelle für jedermann zur Verfügung gestellt werden. Die Vermittlung über den Nutzer löst gleichzeitig datenschutzrechtliche Probleme, die sich sonst möglicherweise stellen würden, aber auch nicht unlösbar wären.

Aus der Entscheidung gegen ein Schutzrecht und explizit gegen die Privilegierung des Dateninhabers folgt, dass alle Marktteilnehmer in nichtdiskriminierender Form partizipieren können sollen. Räumt ein Nutzer die entsprechenden Rechte ein, ist Datenzugang zu gewähren. Nur so kann auch das Postulat erfüllt werden, dass eine faire Chancenverteilung und ein offener Wettbewerb gewährleistet werden.

b) Zweckrichtung der Nutzerentscheidung

Wenn es primär dem Nutzer zugebilligt wird, über die Datenverwendung zu entscheiden, muss festgestellt werden, dass der Nutzer und der Gesetzgeber des Data Acts Zwecke verfolgen, die über den bloßen Erhalt von Rohdaten hinausgehen.

Im Data Act wird derzeit davon ausgegangen, dass die Nutzerentscheidung darüber getroffen wird, wer Zugang zu den Rohdaten erhält, die der Nutzer bei der Produkt- oder Dienstenutzung generiert. Die Definition von Daten in Art. 2 Nr. 1 Data Act-E i.V.m. Art. 1 Abs. 1 Data Act-E bezieht sich auf Rohdaten.[62] Rohdaten sind die Daten, wie sie von der Quelle erfasst werden, ohne dass eine Bearbeitung stattgefunden hat.[63] Format und Inhalt der Daten wird durch die jeweilige Einrichtung, mit der die Daten gesammelt werden, bestimmt. Erst in Folgeschritten kommt es zu einer Verarbeitung und Veredelung dieser Rohdaten zu Informationen, die für weitere Kreise nutzbar sind. Ein Interesse an Rohdaten können Datenexperten haben. Weder der Nutzer eines IoT-Produkts noch Unternehmen, die auf nachgelagerten Märkten tätig werden wollen, haben aber in der Regel ein Interesse an Rohdaten.[64] Sie benötigen die Daten tendenziell in einer aufbereiteten Form. Diese Aufbereitung wird typischerweise von

62 Dies wird in Erwägungsgrund 17 klargestellt.

63 *Luber/Litzel*, Was sind Rohdaten?, 9.4.2020, https://www.bigdata-insider.de/was-sind-rohdaten-a-920701/.

64 *Drexl et. al.*, 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), 2022, Rn. 25.

demjenigen geleistet, der die Sammlung der Rohdaten initiiert hat, z.B. der Gerätehersteller.

Der Data Act ist nicht als Verordnung zur Datenteilung um der Datenteilung willen gedacht. Es geht dem europäischen Gesetzgeber um „die optimale Verteilung der Daten zum Nutzen der Gesellschaft" (Erwägungsgrund 2). Das Nutzerinteresse, das im Data Act zentral gesetzt wird, ist nicht oder jedenfalls nicht ausschließlich darauf gerichtet, solche Daten schlicht zu erhalten. Vielmehr ist die Datenteilung zweckgerichtet. Nutzer sollen – so formuliert es Erwägungsgrund 19 – die Daten erlangen, „die erforderlich sind, um Reparatur- und andere Dienste in Anspruch zu nehmen", Unternehmen sollen Daten erhalten, die sie in die Lage versetzen, „innovative, effizientere und bequemere Dienste anzubieten." Die Inanspruchnahme von Reparatur- und anderen Diensten betrifft das Tätigwerden auf dem Sekundärmarkt. Das Anbieten innovativer, effizienterer und bequemerer Dienste ist ebenfalls darauf gerichtet, auf nachgelagerten Marktstufen unternehmerisch tätig zu werden. Diese Zweckrichtung des Data Acts steht in Einklang mit dem übergeordneten Ziel, Innovation und Wettbewerb in der Datenökonomie zu fördern. Die Datenteilung soll Sekundärmärkte beleben. Für dieses Ziel der Zugangseröffnung wird der Zugang zu Rohdaten häufig nicht genügen. Der Zugang zu Daten ist in vielen Fällen ein Zwischenschritt, aber nicht der Zweck.

Kleinere Unternehmen werden häufig nicht in der Lage sein, Rohdaten zu verarbeiten. Sie sind nicht auf Datenanalyse spezialisiert, sondern auf das Erbringen der Leistungen, auf die es dem Kunden eigentlich ankommt. Erhalten sie Rohdaten, wird das für diese Unternehmen unter Umständen wenig hilfreich sein.[65] Sie müssen dann Tools in Anspruch nehmen, um diese Daten lesen oder verarbeiten zu können.[66] Angebote dazu stellen möglicherweise der Hersteller des Produkts oder Dritte zur Verfügung. Damit entstehen potenziell Kosten und Verzögerungen, die in Summe wieder prohibitiv wirken können. So wird für den Kfz-Bereich berichtet, dass die Vielzahl erforderlicher Softwaresysteme zur Bearbeitung für freie Werkstätten oft nicht erschwinglich ist. Die Begrenzung des Anwendungsbereichs der Verordnung auf Rohdaten ohne weitere Tools

65 Vgl. dazu im Kontext von § 20 Abs. 1a GWB *Linsmeier/Haag* in: FS Bechtold, 2021, S. 191.

66 So auch *Drexl et. al.*, 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), 2022, Rn. 25.

wird für viele Nutzungszwecke nicht genügen, um den Sekundärmarktwettbewerb zu ermöglichen. Die Zugangsvereitelung würde nur eine Stufe weiter verschoben.

Innovation und Wettbewerb sind nur möglich, wenn die Unternehmen ihre Leistungen tatsächlich ungehindert erbringen können. Nur dann haben die Nutzer die Möglichkeit, ihre Rolle als „Schiedsrichter im Wettbewerb" wahrzunehmen und auszuspielen. Der die Marktwirtschaft prägende Grundsatz der Konsumentensouveränität setzt eine echte Zugangseröffnung voraus.

c) Erfordernis eines zweckgebundenen Zugangsanspruchs

Zieht man die hier herausgestellten normativen Ausgangspunkte zusammen – keine rechtliche Privilegierung des Dateninhabers, zentrale Rolle des Nutzerinteresses, Belebung der Sekundärmärkte als Zielrichtung der Datenteilung – dann liegt auf der Hand, dass ein nackter Datenzugangsanspruch nicht genügt. Nutzer müssen vielmehr in der Lage sein, Dritten Zugang zu denjenigen Daten und Instrumenten einzuräumen, die für ein Tätigwerden auf dem Sekundärmarkt erforderlich sind. Der Zugangsanspruch muss zweckbezogen sein. Fehlt ein Zugang zu abgeleiteten Daten, zu Software, die benötigt wird, um ein Gerät zu reparieren, oder fehlt der Zugang zu einem Dashboard, dann erhalten Dritte Steine statt Brot: Sie können mit den nackten Daten nichts anfangen und müssen ggf. Zusatzprodukte oder -leistungen erwerben (wenn sie es denn können). Die faktische Kontrolle des Dateninhabers bleibt erhalten, ein freier Zugang zum Sekundärmarkt wird vereitelt.

Im Digital Markets Act (DMA) haben die europäischen Gesetzgeber dieses Problem genau erkannt und gelöst.[67] Im DMA sind verschiedene Zugangsansprüche vorgesehen, die nicht am Zugang zu Rohdaten haften, sondern die Zweckrichtung einkalkulieren. So wird in Art. 6 Abs. 10 DMA Zugang zu aggregierten und nichtaggregierten Daten vorgesehen und ausdrücklich darauf abgestellt, dass die Nutzung der Daten zu ermöglichen ist. In Art. 6 Abs. 8 DMA wird – im Zusammenhang mit Online-Werbung – Zugang zu Instrumenten und Daten gewährt, „die sie [Dritte] benötigen, um ihre eigene unabhängige Überprüfung des Werbeinventars vorzunehmen, einschließlich aggregierter und nichtaggregierter Daten. Diese Daten werden so bereitgestellt, dass Werbetreibende und Herausgeber

67 Siehe dazu unten D.II.

ihre eigenen Überprüfungs- und Messinstrumente einsetzen können". Der Zugangsanspruch weist also eine klare Zweckrichtung auf. Nur am Rande sei hier erwähnt, dass dieser Zugang kostenlos zu gewähren ist. Der europäische Gesetzgeber hat also die Finalität der Datenbereitstellung im Digital Markets Act zutreffend erkannt. Für den Data Act ist eine parallele Wertung erforderlich, wenn dieser Baustein der Datenökonomie die angestrebten Ziele erreichen soll.

2. Zweckgebundener Zugangsanspruch

Das Datenzugangsregime des Data Act ist daher auszubauen, damit das Regelungsziel erreicht werden kann, Dienstleistungen auf nachgelagerten Märkten zu ermöglichen. Um die Eröffnung von Sekundärmärkten für anschließende Dienstleistungen wie Wartung und Reparaturen zu gewährleisten, sollte neben dem bislang im Verordnungsentwurf vorgesehen Datenzugangsanspruch ein weiterer, spezieller Zugangsanspruch vorgesehen werden, der darauf abzielt, das Tätigwerden auf Sekundärmärkten zu ermöglichen. Dieser Zugangsanspruch muss grundlegend am Zweck ausgerichtet sein, den der Nutzer und/oder Zugangspetent legitimerweise erreichen möchte. Der Anspruch muss neben den (Roh-)Daten auch notwendige Hilfsmittel umfassen.

Dies führt nicht dazu, dass Dritte vom Hersteller den Zugang zu beliebigen Daten oder Software verlangen können. Der Zugangspetent müsste darlegen, welche Dienstleistung er auf dem nachgelagerten Markt erbringen möchte und welche Daten, Software und Infrastruktur er dafür benötigt.

Ein Anspruch sollte jedenfalls bestehen, soweit der Dateninhaber selbst über entsprechende Software und Infrastruktur verfügt. So würde auf dem nachgelagerten Markt ein „level playing field" zwischen dem Dateninhaber und Drittunternehmen erzielt und auf diesem nachgelagerten Markt mehr Wettbewerb ermöglicht werden.

Zugangsansprüche zu Waren und Dienstleistungen, die für die Erschließung oder den Zutritt zu nachgelagerten Märkten notwendig sind, werden vereinzelt schon nach kartellrechtlichen Vorschriften, insbesondere Art. 102 AEUV, §§ 19, 20 GWB, gewährt.[68] Auch dort geht der Anspruch

68 Vgl. BGH, 6.10.2015, Az. KZR 87/13, WRP 2016, 229 – Porsche-Tuning; BGH, 26.1.2016, Az. KZR 41/14, NJW 2016, 2504 – Jaguar Vertragswerkstatt. I.Ü. *Podszun*, Handwerk in der digitalen Ökonomie, 2022, S. 76 ff.

über den Zugang zu Rohdaten hinaus und ist darauf gerichtet, den potenziellen Wettbewerber in die Lage zu versetzen, tatsächlich in den Markt einzutreten. Dass es ein ökonomisches Bedürfnis für solche Ansprüche gibt, ist also nicht neu.

Durch die Begrenzung des Zugangsanspruchs auf Daten und sonstige Infrastruktur, die bereits beim Dateninhaber bzw. Hersteller selbst vorhanden ist, würde der Aufwand für diesen nicht unzumutbar groß sein. Insbesondere bliebe ggf. ein Aufwanderstattungsanspruch bestehen.

(1) Empfohlen wird, dass für Dritte, die auf Sekundärmärkten tätig werden wollen, der Zugangsanspruch zweckbezogen definiert wird und diejenigen Daten, Instrumente und Hilfsmittel umfasst, die für das Tätigwerden benötigt werden und die dem Dateninhaber selbst zur Verfügung stehen.

3. Erfasste Daten, Software und Tools

Der vorstehend geforderte zweckorientierte Zugangsanspruch bedarf weiterer Präzisierung. Ist der Zugang grundsätzlich eröffnet, ist damit noch nicht geklärt, auf welche Daten durch wen zugegriffen werden darf und welche Hilfsmittel ggf. zur Verfügung gestellt werden müssen, um den Anspruch praktisch wirksam werden zu lassen.

a) Definition von Daten

Der Begriff wird für die Zwecke von Art. 3-5 Data Act-E nur dahingehend präzisiert, dass „bei der Nutzung erzeugte Daten" umfasst sind. In Erwägungsgrund 17 wird ausgeführt, dass auch absichtlich aufgezeichnete Daten, sowie „Daten, die als Nebenprodukt von Nutzeraktionen, z.B. Diagnosedaten, und ohne jegliche Nutzeraktion, z.B. wenn sich das Produkt im Bereitschaftszustand befindet, erzeugt werden sowie Daten, die aufgezeichnet werden, während das Produkt ausgeschaltet ist". Schon an dieser kleinen Aufzählung zeigt sich, dass der Begriff der erzeugten Daten weit sein und streitanfällig werden kann.[69] Möglicherweise kommt es zu Abgren-

69 Vgl. DIHK, Stellungnahme zum Vorschlag für eine Verordnung über harmonisierte Vorschriften für einen fairen Datenzugang und eine faire Datennutzung (Datengesetz), 2022, S. 4 f; *Ducuing* in: Ducuing/Margoni/Schirru, White Paper

zungsschwierigkeiten, etwa bezüglich Metadaten und Maschinendaten ohne unmittelbaren Personenbezug. Eine Verkomplizierung tritt dadurch ein, dass der Dateninhaber willkürlich entscheiden kann, welche Daten gesammelt werden. Zugangspetenten wiederum können nicht einschätzen, welche Daten überhaupt verfügbar sind. Diese Informationsasymmetrie kann gerade bei der privaten Rechtsdurchsetzung zum Stolperstein werden. Abhelfen würden hier nur eine Auskunftspflicht und eine Prüfungsbefugnis durch externe Sachverständige. Dieser Aufwand wird allerdings nur im Ausnahmefall zu leisten sein.

Daher ist zu empfehlen, nicht die einzelnen Daten in den Blickpunkt zu rücken, sondern den mit dem Datenzugang verfolgten Zweck. Verschiedene Zugangspetenten haben verschiedene Bedarfe: Manche Verbraucherinnen und Verbraucher möchten ggf. nur ihre aktuellen Leistungs- oder Verbrauchsdaten checken. Datenunternehmen möchten möglicherweise Rohdaten erfassen, um damit gänzlich neuartige Anwendungen zu konstruieren oder Forschung zu treiben. Anwender, die Daten für ein Tätigwerden auf dem Sekundärmarkt benötigen, sind eventuell an Rohdaten nicht interessiert und brauchen vielleicht auch nicht alle Nutzerdaten, sondern nur ein bestimmtes Set an Daten. Die Datenweitergabepflicht sollte nach diesen Zwecken bestimmt werden. Das würde dem Dateninhaber die Möglichkeit nehmen, Dritten unterschiedliche Daten in unterschiedlichen Formaten bereitzustellen, die für den entsprechenden Zweck möglicherweise gerade nicht genügen. Welche Daten im Einzelnen benötigt werden, kann allerdings nicht pauschal beantwortet werden. Hier bleibt Raum für individuelle Zugangslösungen. Das Missbrauchspotential für Dateninhaber wird aber durch die Aufnahme der Zweckrichtung in den Datenzugangsanspruch erheblich gesenkt, die Verhandlungsposition der Nutzer und der Dritten wird gestärkt.

b) Abgeleitete Daten

Nach Erwägungsgründen 14 und 17 des Data Act-E ist der Dateninhaber nicht verpflichtet, Zugang zu sog. derivativen oder abgeleiteten Daten zu gewähren.[70] Gemeint sind damit Daten, die erst dadurch entstehen,

---

on the Data Act Proposal, CITIP Working Paper Series, 2022, S. 26; *Staudenmayer*, EuZW 2022, 1037, 1041.

70 Vgl. *Kerber*, Governance of IoT Data: Why the EU Data Act will not Fulfill Its Objectives, 2022, S. 6.

dass die von dem Produkt unmittelbar generierten Daten mittels Software weiterverarbeitet werden. Damit wird klargestellt, dass im Grundsatz nur Rohdaten zur Verfügung gestellt werden müssen. Die Europäische Kommission begründet dies damit, dass dieser Softwareprozess Rechten des geistigen Eigentums unterliegen kann.[71] Die Nutzung bestimmter Software oder einer vom Dateninhaber gestellten Infrastruktur, ggf. entgeltlich, kann für einige Zugangspetenten – gerade aus kleineren und mittleren Unternehmen – eine erhebliche Hürde sein. Der Datenzugangsanspruch bleibt nutzlos, wenn die nutzbaren derivativen Daten erst teuer erworben werden müssen.[72] Es ist davon ausgehen, dass Abgrenzungsprobleme entstehen. Lässt man jede Datenverarbeitung genügen, würden nur noch echte Rohdaten vom Zugangsanspruch umfasst sein. Diese möglicherweise maschinellen Sensordaten dürften für viele Nachfrager, vor allem Verbraucherinnen und Verbraucher, in aller Regel unbrauchbar sein.[73] Nahezu jede sinnvolle, lesbare Darstellung von Informationen ist in irgendeiner Form bereits verarbeitet bzw. umgewandelt worden. Selbst einfache Informationen, z.B. zum Zustand der Batterie eines Elektrofahrzeugs, müssen erst von der Angabe einer elektrischen Spannung in eine geschätzte Kapazität umgerechnet werden. Bei einer engen Auslegung wären selbst diese derivativen Daten bereits vom Zugangsanspruch ausgeklammert. Möglicherweise wollte die Kommission den Anwendungsbereich nicht derart eng ziehen, das lässt sich aber dem Data Act-E nicht mit der erforderlichen Sicherheit entnehmen. Im Ernstfall liegt darin erhebliches Streitpotential, ggf. auch über die Frage, welche Art von Weiterverarbeitung noch zu leisten ist. Ggf. können Hersteller ihre Produkte auch bewusst so designen, dass zunächst für Dritte unlesbare Daten erzeugt werden, die erst in weiteren Schritten in sinnvolle Informationen umcodiert werden. Auch das würde den Datenzugangsanspruch faktisch entwerten.

Neben den praktischen Problemen erscheint auch die Rechtfertigung der Kommission für diese Einschränkung zweifelhaft. Sie stützt sich in den Erwägungsgründen auf möglicherweise bestehende Rechte des geistigen Eigentums an dem Datenverarbeitungsvorgang.[74] Dass derzeit IP-Rechte

71 Erwägungsgrund 17 Data Act-E.

72 Vgl. *Drexl et. al*., 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), 2022, Rn. 24.

73 *Kerber*, Governance of IoT Data: Why the EU Data Act will not Fulfill Its Objectives, 2022, S. 11 f.

74 Erwägungsgrund 17 Data Act-E.

an solchen Datenverarbeitungsvorgängen bestehen können, ist jedoch für sich kein Argument, da der europäische Gesetzgeber gerade diese Rechte auch im erforderlichen Maße einschränken kann. Dies ist partiell im Data Act-E bereits für Rechte an Datenbankwerken vorgesehen, Art. 35 Data Act-E. Der eigentliche Punkt ist daher also nicht ein rechtliches Hindernis, sondern eine Abwägung, die der Verordnungsentwurf zugunsten des hier innovationshemmenden IP-Rechts getroffen hat.

Der mit dem IP-Recht bezweckte Schutz vor Trittbrettfahrern, die von einer Leistung profitieren, ohne an den Kosten beteiligt zu sein, würde im Data Act durch die Pflicht zur Erbringung einer angemessenen Gegenleistung teilweise aufgefangen, wenn dies für nötig erachtet wird. Ob und inwieweit überhaupt IP-Rechte bestehen, ist allerdings äußerst unklar. Im Einzelfall kann dies nicht rasch geprüft werden.[75] Damit das Regelungsziel des Data Act-E erreicht wird, den Zugang zu nachgelagerten Märkten wirksam zu ermöglichen, ist der Zugang zu sinnvoll nutzbaren Daten aber unbedingt notwendig.[76] Aus wettbewerblicher Perspektive und mit Blick auf den Sekundärmarktzugang müssen daher ggf. abgeleitete Daten zur Verfügung gestellt werden.[77] Das muss insbesondere dann gelten, wenn erst dies die Daten überhaupt nutzbar für Fremde macht. Ausgeschlossen werden sollte, dass Hersteller durch geschicktes Produktdesign den Zugangsanspruch faktisch vereiteln kann. Eine geringfügige Umcodierung der Daten, die diese faktisch verschlüsselt, kann dann nicht mehr genügen, um Dritte auszuschließen oder von diesen den kostenpflichtigen Erwerb teurer Entschlüsselungssoftware zu verlangen. Nur wenn die Ableitung Folge einer wesentlichen Investition des Dateninhabers war, sollte eine Kompensation ermöglicht werden.

75 *Drexl et. al.*, 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), 2022, Rn. 29.

76 *Leistner/Antoine*, IPR and the use of open data and data sharing initiatives by public and private actors, 2022, S. 14 ff. So auch *Drexl et. al.*, 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), 2022, Rn. 24.

77 So auch *Specht-Riemenschneider*, ZRP 2022, 137, 140. A.A. *Demary*, Der Data Act - Welchen Rahmen Unternehmen für Data Sharing wirklich brauchen: Beitrag zum Vorschlag der EU-Kommission, 2022, S. 8.

(2) Empfohlen wird, die Beschränkung auf Rohdaten im Grundsatz fallen zu lassen. Stattdessen ist – gerade auch für Dritte – vorzusehen, dass, soweit benötigt, derivative Daten zur Verfügung gestellt werden.

c) Aggregierte Daten

Neben der Beschränkung auf Rohdaten durch den Ausschluss abgeleiteter Datensätze wird die Wirksamkeit des Datenzugangsanspruchs noch durch einen anderen Aspekt eingeschränkt. Für einige datenbasierte Dienstleistungen werden nicht nur individuelle Nutzungsdaten einzelner Nutzer benötigt, sondern aggregierte Daten mehrerer Nutzer.[78] So kann es für die Wartung eines Elektrofahrzeugs zwar ausreichen, dass die Kfz-Werkstatt die Akkuleistung eines bestimmten Akkus auslesen kann. Ein anderes Unternehmen möchte aber ggf. die Fahr- und Akkudaten weiterer Fahrzeuge erfassen, um Folgedienstleistungen erbringen zu können oder Mustervorhersagen treffen zu können. Geschäftsmodelle, die auf aggregierte Daten setzen, sind häufig besonders innovativ, da es nicht mehr um den Einzelfall geht, sondern um eine Art Reihenbetrachtung, die Vorhersagen treffen und neue Zusammenhänge entdecken lässt. Wenn solche Geschäftsmodelle ebenfalls durch den Data Act ermöglicht werden sollen, muss sichergestellt werden, dass diese Unternehmen aggregierte Datensätze erlangen können.

Zugang zu aggregierten Daten kann auf verschiedene Weise gewährt werden. Zum einen können solche Daten vom Dateninhaber bereitgestellt werden. Zum anderen können die Daten durch Dritte, die wiederum auf Nutzerdaten zugreifen, aggregiert werden, beispielsweise Datenintermediäre. Beide Wege sind im aktuellen Verordnungsentwurf nicht ohne Weiteres gewährleistet.

Vom Dateninhaber bzw. Hersteller selbst kann der Datenempfänger aggregierte Datensätze nach der Konzeption des Data Act wohl nicht verlangen, da nach Art. 3 Abs. 1, Art. 5 Abs. 1 Data Act-E nur die Nutzungsdaten herausgegeben werden müssen, die durch die Nutzung des Produkts durch den konkreten Nutzer entstehen, der die Datenfreigabe verlangt. Der Nutzer erhält nur seine eigenen Daten.

78 *Leistner/Antoine*, IPR and the use of open data and data sharing initiatives by public and private actors, 2022, S. 14. Vgl. auch *Kerber*, Governance of IoT Data: Why the EU Data Act will not Fulfill Its Objectives, 2022, S. 13.

Sofern personenbezogene Daten zu den Nutzungsdaten gehören, könnte einer Herausgabe von Daten anderer Nutzer auch die DSGVO entgegenstehen.[79] Nach Art. 1 Abs. 3 Data Act-E bleiben die Vorschriften der DSGVO unberührt, so dass für eine Herausgabe ein Erlaubnistatbestand nach Art. 6 Abs. 1 DSGVO erfüllt sein muss. Zwar kommen nach Art. 6 Abs. 1 lit. b-f DSGVO auch andere Erlaubnistatbestände als eine Einwilligung in Betracht. So könnte der Datenzugangsanspruch des Nutzers eine rechtliche Verpflichtung i.S.d. Art. 6 Abs. 1 lit. c DSGVO darstellen.[80] Ob dies der Fall ist, ist jedoch unklar und bedarf einer Klarstellung. In Erwägungsgrund 24 heißt es:

> „Mit dieser Verordnung wird den Dateninhabern die Pflicht auferlegt, Daten unter bestimmten Umständen bereitzustellen. […] Wenn Nutzer betroffene Personen sind, sollten die Dateninhaber verpflichtet sein, den Nutzern Zugang zu ihren Daten zu gewähren und die Daten vom Nutzer ausgewählten Dritten im Einklang mit dieser Verordnung bereitzustellen. *Mit dieser Verordnung wird jedoch keine Rechtsgrundlage gemäß der Verordnung (EU) 2016/679 geschaffen, die es dem Dateninhaber ermöglicht, Dritten auf Verlangen eines Nutzers, der keine betroffene Person ist, Zugang zu personenbezogenen Daten zu gewähren oder diese bereitzustellen* […]".[81]

Ob diese Formulierung ausschließt, dass das Datenzugangsverlangen eine Rechtsgrundlage für die Herausgabe von personenbezogenen Daten Dritter ist, ist unklar. Teilweise wird darauf hingewiesen, dass nach dem Wortlaut des Erwägungsgrunds nur der Fall erfasst ist, in dem ein Nutzer die Herausgabe von personenbezogenen Daten eines anderen an einen Dritten verlangt.[82] Die Herausgabe solcher Daten an den Nutzer werde dadurch aber nicht ausgeschlossen.[83] Ob die Europäische Kommission tatsächlich zwischen diesen Fällen differenzieren wollte, ist fraglich, da der Nutzer die Daten schließlich auch einfach an den Dritten weitergeben könnte. Allerdings könnte die gesetzliche Verpflichtung zum Datenzugang nach

79 Siehe dazu *Schweitzer/Metzger et al*., Data access and sharing in Germany and in the EU: Towards a coherent legal framework for the emerging data economy, Final Report, 8 July 2022 (Gutachten für das Bundesministerium für Wirtschaft und Klimaschutz), S. 233.

80 Zu dessen Anforderungen siehe *Heberlein* in: Ehmann/Selmayr, DSGVO, 2018, Art. 6 DSGVO Rn. 15 ff.

81 Hervorhebung nur hier.

82 *Specht-Riemenschneider*, MMR 2022, 809, 810 f.

83 *Specht-Riemenschneider*, MMR 2022, 809, 810 f.

dem Data Act ohnehin nur die Datenweitergabe rechtfertigen, nicht aber die weitere Nutzung durch den Datenempfänger, welche einer eigenen Rechtsgrundlage bedarf. Nach Art. 6 Abs. 1 lit. c DSGVO ist die Datenverarbeitung nur zulässig, soweit die Verarbeitung zur Erfüllung einer rechtlichen Verpflichtung erforderlich ist. Folglich wäre die Weitergabe der Daten durch den Dateninhaber möglicherweise aufgrund der Verpflichtung in Art. 5 Data Act-E mit dem Datenschutzrecht vereinbar. Der Datenempfänger benötigt für jede weitere Verarbeitung dieser Daten aber ebenfalls eine Rechtsgrundlage. Er kann sich nicht auf Art. 6 Abs. 1 lit. c DSGVO stützen, da er in keiner Weise, auch nicht durch den Data Act, verpflichtet wird, die Daten zu verarbeiten. Art. 6 Abs. 1 lit. c DSGVO kann also für eine Nutzung von personenbezogenen Daten nicht herangezogen werden.

Darüber hinaus könnte noch der Erlaubnistatbestand aus Art. 6 Abs. 1 lit. f DSGVO (berechtigtes Interesse) einschlägig sein.[84] Wie die dort anzustellende Abwägung ausfällt, lässt sich jedoch nicht rechtssicher pauschal beantworten. Sofern vertreten wird, aus der Normierung des Datenzugangsanspruchs lasse sich ableiten, dass das Interesse des Nutzers am Datenzugang regelmäßig überwiegt,[85] ist dem entgegenzuhalten, dass der Verordnungsentwurf an vielen Stellen eindeutig zum Ausdruck bringt, dass die Vorschriften des Data Act-E komplementär zur DSGVO sein und dessen Schutzniveau nicht absenken sollen (vgl. Art. 1 Abs. 3, Erwägungsgrund 7, 24 Data Act-E). Insbesondere wird in Erwägungsgrund 30 betont, dass der Nutzer, sofern personenbezogene Daten Dritter betroffen sind, sich stets einer ausreichenden datenschutzrechtlichen Rechtsgrundlage vergewissern muss, wobei ausdrücklich auf die Einwilligung und das überwiegende Interesse verwiesen wird. All dies deutet darauf hin, dass durch den Data Act-E die Antwort auf diese Fragen nicht vorgezeichnet werden sollen. Diese Schlussfolgerung wird gestützt durch Art. 5 Abs. 9 Data Act-E, wonach das Recht zur Datenfreigabe an Dritte nicht die Datenschutzrechte anderer Personen beeinträchtigen darf. Jedenfalls aber steht die datenschutzrechtliche Zulässigkeit der Herausgabe von personenbezogenen Daten von Personen, die nicht zugleich der Nutzer sind, auf wackeligen Beinen. Die Problematik sollte durch eine Konturierung der datenschutzrechtlichen Vorschriften im Data Act abgemildert werden.

Aber selbst nicht-personenbezogene Nutzungsdaten dürfen vom Dateninhaber nach Art. 4 Abs. 6 Data Act-E nur mit Einwilligung des jeweiligen

84 Siehe zu dessen Voraussetzungen *Heberlein* in: Ehmann/Selmayr, DSGVO, 2018, Art. 6 DSGVO Rn. 25 ff.

85 Vgl. *Specht-Riemenschneider*, MMR 2022, 809, 811.

Nutzers verwendet werden. Damit ist klar, dass die Datenteilungspflicht gar keine Nutzungsdaten anderer Nutzer umfassen kann, da der Dateninhaber damit deren Rechte verletzen würde. Aus diesen Gründen kommt eine Freigabe aggregierter Nutzerdaten unmittelbar durch den Dateninhaber kaum in Betracht.

Diese Einschränkungen sind geeignet, das Regelungsanliegen des Data Act teilweise zu vereiteln.[86] Viele Dienstleistungen, die Drittunternehmen und insbesondere Handwerker als Anschlussdienstleistung erbringen wollen, sind nur mit Zugang zu aggregierten Daten verschiedener Nutzer denkbar. Als Folge der Empfehlung, für nachgelagerte Dienstleistungen den Zugangsanspruch am angestrebten Nutzungszweck zu orientieren (Empfehlung 1), sollten auch hinsichtlich aggregierter Daten Anpassungen vorgenommen werden. Das ist insofern fair, da der Dateninhaber dank seines Kontakts zu zahlreichen Nutzern aggregierte Daten erhalten kann, Dritte genau diese einfache Möglichkeit aber nicht haben.

Der Zugangsanspruch sollte daher für die Nutzung auf nachgelagerten Märkten auch aggregierte Nutzerdaten umfassen, soweit diese beim Dateninhaber vorliegen.

Um die Rechte von natürlichen Personen an ihren personenbezogenen Daten nicht unverhältnismäßig einzuschränken, müssen geeignete Maßnahmen zur Anonymisierung vorgesehen werden.[87] So könnte der Zugangsanspruch des Zugangspetenten davon abhängen, dass dieser die Daten zunächst einem vertrauenswürdigen Datentreuhänder zur Anonymisierung und Aggregierung überlässt.[88] Sofern der Dateninhaber eine solche Anonymisierung bereits durchgeführt hat, sollte er zur Herausgabe dieser Datensätze verpflichtet sein. Dieser zusätzliche Verarbeitungsschritt könnte im Rahmen einer Gegenleistung vergütet werden. Die datenschutzrechtliche Erlaubnis des Dateninhabers, die Daten herauszugeben ergibt sich aufgrund seiner Verpflichtung aus dem Da-

86 *Schweitzer/Metzger et al.*, Data access and sharing in Germany and in the EU: Towards a coherent legal framework for the emerging data economy, Final Report, 8 July 2022 (Gutachten für das Bundesministerium für Wirtschaft und Klimaschutz), S. 234.

87 So auch *Schweitzer/Metzger et al.*, Data access and sharing in Germany and in the EU: Towards a coherent legal framework for the emerging data economy, Final Report, 8 July 2022 (Gutachten für das Bundesministerium für Wirtschaft und Klimaschutz), S. 234.

88 Für den Kfz-Bereich vzbv, Mobilitätsdatenwächter, 2022; *Reither/Methner/Schenkel*, Einführung eines „Mobilitätsdatenwächters" für eine verbrauchergerechte Datennutzung, 2022.

ta Act aus Art. 6 Abs. 1 lit. c DSGVO. Die Rechtsgrundlage für die Verarbeitung durch einen Datentreuhänder, soweit nach Anonymisierung noch erforderlich, müsste dagegen über die Interessenabwägung nach Art. 6 Abs. 1 lit. f DSGVO gewährleistet werden, sofern man keine zusätzliche Rechtsgrundlage außerhalb des Katalogs von Art. 6 Abs. 1 DSGVO schaffen will. Auch wenn nach der Anonymisierung möglicherweise gar keine personenbezogenen Daten mehr vorliegen, sollten im Sinne der Rechtssicherheit die datenschutzrechtlichen Fragen eindeutig geklärt werden.

(3) Empfohlen wird, klarzustellen, dass der Zugangsanspruch zum Zwecke der Eröffnung von Sekundärmärkten auch die Nutzungsdaten anderer Nutzer umfasst, sofern aggregierte Daten für die Erbringung der Dienstleistung erforderlich sind und dem Dateninhaber zur Verfügung stehen. Eine angemessene Anonymisierung ist bei Weitergabe zu gewährleisten, z.B. über Datentreuhänder. Klargestellt werden sollte, dass bei Anonymisierung ein berechtigtes Interesse i.S.d. Art. 6 Abs. 1 lit. f DSGVO vorliegt, wenn Daten für die weitere Nutzung auf Sekundärmärkten aggregiert werden.

Alternativ könnte das Zusammenführen von Daten mehrerer Nutzer auch in die Sphäre des Datenempfängers verlegt werden. Ein Handwerksunternehmen (oder ein Verband oder die Kammer) könnte die Aggregierung von Daten selbst vornehmen oder von einem beauftragten Unternehmen durchführen lassen. Dafür müsste eine kritische Anzahl Nutzer veranlasst werden, ggf. mit finanziellen Anreizen, die Herausgabe von Nutzungsdaten zum Zwecke der Aggregierung vom Dateninhaber zu verlangen. Sofern der Nutzer einwilligt und ausdrücklich verlangt, dass der Datenempfänger die Daten mit denen anderer aggregieren darf, könnte dieser mittelfristig aggregierte Datensätze aufbauen. Das hätte den praktischen Nachteil, dass den Nutzern nicht direkt die gewünschte Leistung angeboten werden kann, sondern erst dann, wenn genügend andere Nutzer ihre Daten freigegeben haben und eine Aggregierung möglich ist. Gleichwohl mag dieses Modell für bestimmte Anwendungen von Interesse sein, insbesondere wenn Nutzerdaten in einen Datenpool eingespeist werden sollen, in den auch andere Datenquellen einfließen. Hier ergeben sich auch für das Handwerk Chancen.

d) Freigabe für Datenmittler

Besonders effizient wird die Zusammenführung von Nutzerdaten, wenn nicht jedes Unternehmen am Ende der Wertschöpfungskette selbst die Datensätze sammeln und aggregieren müsste, sondern wenn es zwischengeschaltete Datenmittler gibt, die mit Einwilligung der Nutzer wertvolle Datensätze herstellen und diese, mit Einwilligung der Nutzer, mit Drittunternehmen teilen könnten.[89] So könnten zum einen Wettbewerb zwischen mehreren Datenmittlern und zum anderen gleichzeitig ein Datenmarkt entstehen, der weitere Innovationen ermöglicht.[90] So würde die von der Europäischen Kommission angestrebte europäische Datenwirtschaft Kontur erhalten. Zugleich verbliebe beim Nutzer – wie im Data Act-E vorgesehen – die wirtschaftliche Verfügungsgewalt über die Daten.

Unklar ist, ob dieses Modell mit dem vorliegenden Verordnungsentwurf vereinbar ist.[91] Art. 6 Abs. 2 lit. c Data Act-E erschwert die Datenweitergabe vom Datenempfänger an Dritte, z.B. Datenmittler:

> „der [Datenempfänger] darf nicht die erhaltenen Daten einem anderen Dritten in roher, aggregierter oder abgeleiteter Form bereitstellen, es sei denn, dies ist erforderlich, um den vom Nutzer gewünschten Dienst zu erbringen."

Diese Vorschrift untersagt zunächst die Weitergabe der Daten an Dritte, wodurch Datenmittler als Datenhändler für weitere Unternehmen ausgeschlossen wären. Zwar gilt dieses Verbot nicht, wenn die Datenweitergabe vom Nutzer erwünscht wird, allerdings nach dem Wortlaut nur dann, wenn dies erforderlich ist, um „den vom Nutzer gewünschten Dienst zu erbringen". Daraus kann abgeleitet werden, dass eine Datenverarbeitung durch Datenempfänger nur zulässig ist, soweit dies erforderlich ist, um einen vom Nutzer gewünschten Dienst zu erbringen. Mit anderen Worten sind Datenfreigaben losgelöst von einer konkreten gewünschten Dienstleistung für den Nutzer ausgeschlossen. Damit wären jedenfalls Datenfrei-

89 Vgl. *Kerber*, Governance of IoT Data: Why the EU Data Act will not Fulfill Its Objectives, 2022, S. 10 f; *Hennemann/Steinrötter*, NJW 2022, 1481, 1484; *Kempny/Krüger/Spindler*, NJW 2022, 1646, 1647; *Hennemann/von Ditfurth*, NJW 2022, 1905, 1906.

90 *Kerber*, Governance of IoT Data: Why the EU Data Act will not Fulfill Its Objectives, 2022, S. 10.

91 *Kerber*, Governance of IoT Data: Why the EU Data Act will not Fulfill Its Objectives, 2022, S. 10.

gaben zu reinen Verkaufszwecken oder zu Forschung, Weiterentwicklung oder Experiment ausgeschlossen.[92]

Problematisch wird damit auch eine Tätigkeit von Datenmittlern für verschiedene Unternehmen und für verschiedene Dienstleistungen, da der Nutzer nach Art. 6 Abs. 2 lit. c Data Act-E die Datenfreigabe nicht generell, sondern nur zur Ermöglichung *eines* bestimmten Dienstes verlangen kann. Er kann nicht verlangen, dass der Dateninhaber diese freigibt, damit ein Datenmittler diese aufbereiten und mehreren Unternehmen anbieten kann.

Diese Einschränkung auf eine bestimmte Dienstleistung passt zwar auf den ersten Blick zum Ziel, datenbasierte Dienstleistungen auf nachgelagerten Märkten zu erbringen. Übersehen wird dabei aber, dass für einige nachgelagerte Dienstleistungen eine große Menge an Daten verschiedener Nutzer benötigt wird und dass es zu Weiterentwicklungen kommen kann, die bei erster Gestattung noch gar nicht absehbar sind.[93] Zudem widerspricht die Einschränkung auch der Strategie der Europäischen Kommission, einen europäischen Datenmarkt zu schaffen. Es passt außerdem nicht zur erklärten Wertentscheidung, dem Nutzer die wirtschaftlichen Potenziale seiner Nutzungsdaten zuzuweisen.[94] So heißt es in Erwägungsgrund 28, es sollte dem Nutzer freistehen, „die Daten für jeden rechtmäßigen Zweck zu verwenden" und Ziel sei auch die „Entwicklung völlig neuartiger Dienste […] auch auf der Grundlage von Daten aus einer Vielzahl von Produkten oder verbundenen Diensten". Die Kommission versucht also mit dem Data Act sogar eine Zusammenführung von Daten

92 Vgl. Verbraucherzentrale Bundesverband e.V., Verbraucher:innen beim Data Act im Blick behalten, 2022, S. 11 f., die den freien Datenverkauf jedoch ablehnt; a.A. *Drexl et. al.*, 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), 2022, Rn. 14, welche die Vorschrift nicht als ausreichendes Gegenargument ansehen.

93 Vgl. *Kerber*, Governance of IoT Data: Why the EU Data Act will not Fulfill Its Objectives, 2022, S. 10; *Specht-Riemenschneider*, ZRP 2022, 137, 139; *Schweitzer/Metzger et al*., Data access and sharing in Germany and in the EU: Towards a coherent legal framework for the emerging data economy, Final Report, 8 July 2022 (Gutachten für das Bundesministerium für Wirtschaft und Klimaschutz), S. 220.

94 Erwägungsgrund 28. A.A. *Drexl et. al*., 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), 2022, Rn. 16, 18.

aus verschiedenen Quellen zu ermöglichen. Sie beschränkt sich aber auf das Zusammenführen von Daten aus verschiedenen Quellen, um *einen Dienst* zu ermöglichen. Daten aus einer (oder auch mehreren Quellen) für *mehrere Dienste* zu verwenden, scheint auch auf Basis der Erwägungsgründe ausgeschlossen. Festgehalten wird an einer konkreten Zweckbindung im Einzelfall.

Die Zweckbindung bei der Datennutzung, die der Nutzer sowohl dem Dateninhaber gemäß Art. 4 Abs. 6 Data Act-E, als auch dem Datenempfänger nach Art. 6 Abs. 1 Data Act-E auferlegen kann, sollte im Grundsatz beibehalten werden. Der Nutzer sollte weiterhin die Verfügungsgewalt darüber haben, wie seine Nutzerdaten verwendet werden. Eine Klarstellung, dass der Nutzer keinen Einschränkungen dabei unterliegt, zu welchem Zweck er die Daten freigeben möchte, würde aber für größere Kompatibilität mit einer Nutzung für Folgemärkte sorgen.[95]

(4) Empfohlen wird klarzustellen, dass der Nutzer keinen Einschränkungen dabei unterliegt, zu welchem Zweck er die Daten freigeben möchte.

Er sollte verlangen können, dass seine Nutzungsdaten von einem Datenempfänger auch zu Zwecken der Konsolidierung, der Aggregierung, der weiteren Entwicklung und des Weiterverkaufs genutzt werden können, auch wenn er selbst (noch) keine bestimmte Dienstleistung wünscht.[96] Dazu gehört auch die Klarstellung, dass die Lizenzvertragsbedingungen zwischen Dateninhaber und Datenempfänger i.S.d. Art. 8 Data Act-E nur dann angemessen sind, wenn der Datenempfänger, im Einklang mit dem Willen des Nutzers, die Daten kombinieren darf. Für diese Fälle wäre ggf. auch das Wettbewerbsverbot nach Art. 4 Abs. 4 und Art. 6 Abs. 2 lit. e Data Act-E zu modifizieren. Schließlich ließe sich kaum sicherstellen, dass

95 So auch *Kerber*, Governance of IoT Data: Why the EU Data Act will not Fulfill Its Objectives, 2022, S. 10; *Schweitzer/Metzger et al*., Data access and sharing in Germany and in the EU: Towards a coherent legal framework for the emerging data economy, Final Report, 8 July 2022 (Gutachten für das Bundesministerium für Wirtschaft und Klimaschutz), S. 212.

96 *Kerber*, Governance of IoT Data: Why the EU Data Act will not Fulfill Its Objectives, 2022, S. 15; kritisch Verbraucherzentrale Bundesverband e.V., Verbraucher:innen beim Data Act im Blick behalten, 2022, S. 12. A.A. *Drexl* et. al., 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), 2022, Rn. 20.

Daten, die später frei verkauft werden, nicht zu Konkurrenzzwecken verwendet werden.[97] Wie oben gesehen, wäre das aber im Sinne des Wettbewerbs eine hinnehmbare Folge.

e) Zugang zu Hilfsmitteln

Der Zugangsanspruch sollte insgesamt nicht auf Daten im engeren Sinne beschränkt bleiben. Die Zweckbindung legt nahe, dass vielmehr auch der Zugang zu solchen Hilfsmitteln ermöglicht werden muss, die den Zugangspetenten erst in die Lage versetzen, auf Anschlussmärkten tätig zu werden. Das umfasst insbesondere Softwareanwendungen und sonstige Tools sowie ggf. begleitende Daten, die nicht bei der Nutzung generiert werden.

(5) Empfohlen wird, dass für Unternehmen, die auf Folgemärkten tätig werden wollen, der Zugangsanspruch auch den Zugang zu weiteren Hilfsmitteln umfasst, ohne die die Nutzerdaten nicht sinnvoll für den angestrebten Zweck genutzt werden können. Das beinhaltet insbesondere den Zugang zu weiteren, nicht-nutzergenerierten Daten, zu Software und zur Infrastruktur, die für eine sinnvolle und unmittelbare Nutzung der Daten erforderlich sind. Der Zugang zu diesen Hilfsmitteln darf nicht prohibitiv vom Dateninhaber ausgestaltet werden, sondern sollte den selben Vorgaben unterliegen wie der Zugang zu den Daten selbst.

Ohne eine derartige Öffnung können die Daten ggf. nicht verwendet werden. Soweit der Dateninhaber Rechte an Software geltend macht, stellt sich die Frage, ob überhaupt solche Rechte bestehen und ob nicht eine Schranke das entsprechende Schutzrecht zu überwinden vermag. Das IP-Recht an Hilfsmitteln darf nicht dazu führen, dass der Hauptanspruch ökonomisch wertlos wird.

97 Vgl. *Graef/Husovec*, Seven Things to Improve in the Data Act, 2022, S. 2.

II. Ausgestaltung des Dreiecksverhältnisses

Im vorangegangenen Abschnitt wurde empfohlen, einen zweckbezogenen Zugangsanspruch im Data Act zu verankern. Das wäre eine Neuerung, die zahlreiche Probleme beim Zugang zum Sekundärmarkt auflösen würde. Der Vorschlag der Kommission für einen Data Act weist weitere Aspekte auf, bei denen Verbesserungspotential mit Blick auf die Zielerreichung besteht. Im Folgenden werden Empfehlungen gegeben, wie das Dreiecksverhältnis von Dateninhaber, Nutzer und Datenempfänger auf Basis der von der Kommission vorgeschlagenen Zugangsansprüche effektiver ausgestaltet werden kann.

Art. 3, 4 und 5 eröffnen für Nutzer und Dritte Zugang zu Daten, die vom Dateninhaber kontrolliert werden. Die Produkte sind grundsätzlich mit einer Funktion auszustatten, die „access by design" ermöglicht (Art. 3 Abs. 1 Data Act-E). Nutzer sollen unmittelbar auf die Daten zugreifen können (Art. 3 Abs. 2 Data Act-E) oder diese „unverzüglich, kostenlos und gegebenenfalls kontinuierlich und in Echtzeit zur Verfügung" gestellt bekommen (Art. 4 Abs. 1 Data Act-E). Dritte benötigen für den Datenzugang die Vermittlung des Nutzers, der gegenüber dem Dateninhaber erklären muss, dass die vom Nutzer bei der Nutzung generierten Daten dem Dritten zur Verfügung gestellt werden sollen (Art. 5 Abs. 1 Data Act-E).

Mit dieser Ausgestaltung werden zwei Vertragsverhältnisse nötig gemacht, nämlich zwischen Dateninhaber und Nutzer sowie zwischen Dateninhaber und Dritten. Durch dieses Modell wird den Dateninhabern eine faktische Vormachtstellung eingeräumt.[98] Die beiden Vertragsverhältnisse ließen sich noch zugangsfreundlicher ausgestalten (dazu 1. und 2.). So lobenswert der grundsätzliche Anspruch ist, dass „access by design" vorzusehen ist, bleiben bei der Art der Zugangsgewährung noch Fragen offen (dazu 3.). Zudem werden zwei Sonderprobleme angesprochen: Virtuelle Assistenten (4.) und vorausschauende Wartung (5.).

98 Ebenso *Kerber*, Governance of IoT Data: Why the EU Data Act will not Fulfill Its Objectives, 2022, S. 16 ff; *Specht-Riemenschneider*, ZRP 2022, 137. Siehe auch *Podszun/Pfeifer*, GRUR 2022, 953, 956.

1. Vertrag des Dateninhabers mit dem Nutzer

Im Verhältnis zum Nutzer und erst recht zu dritten Datenempfängern behält der Dateninhaber im Data Act-Entwurf eine faktisch starke Position, obwohl er eine solche, wie gesehen, normativ nicht beanspruchen kann.[99]

Der Dateninhaber benötigt zur Datennutzung die Zustimmung des Nutzers. Dieses Zustimmungserfordernis und der entsprechende Vertrag werden im Data Act kaum konturiert. Der Dateninhaber ist dem Grundmodell des Data Acts zufolge in der Regel der Hersteller des Geräts. Dieser behält – so das der Verordnung zugrundeliegende Bild – standardmäßig die Kontrolle über die Daten.[100] Irritierenderweise heißt es in den Erwägungsgründen, es müsse festgelegt werden, „wer – außer dem Hersteller oder einem anderen Dateninhaber – unter welchen Bedingungen und auf welcher Grundlage berechtigt ist, auf die Daten zuzugreifen, die durch Produkte und verbundene Dienste erzeugt werden."[101] Die faktische Kontrolle durch den Dateninhaber wird mit derart unpräzisen Aussagen in eine rechtliche Befugnis des Dateninhabers zur Datennutzung umgewertet. Der Nutzer muss stets den Zugangsanspruch für sich oder Dritte dem Dateninhaber erst abtrotzen.[102] Es liegt ein Ungleichgewicht vor. Nur selten wird es – etwa im Einzelfall bei bedeutsamen Transaktionen im B2B-Bereich – vorkommen, dass ein Nutzer von vornherein den Datenzugriff erhält, ohne dass der Hersteller noch auf die Daten zugreifen kann.

Die Kommission geht offenbar davon aus, dass der Verbraucher die Nutzung stets gestatten wird.[103] Schließlich wird in der Verordnungsbegründung eine angebliche Einschränkung der Grundrechte der Dateninhaber u.a. damit gerechtfertigt, dass diese ja noch immer die Daten nutzen können, wenn nur der Nutzer einwilligt.[104] Einer solchen Rechtfertigung bedarf es nicht, wenn erkannt wird, dass der Dateninhaber sich eben nicht auf ein Recht, sondern auf eine faktische Position stützt. Der erforderliche Aufwand zur Sammlung der Daten wird regelmäßig äußerst gering sein, jedenfalls lässt sich dieser aber notfalls vergüten. Die Konsumentensouveränität, die die Entscheidungen für den Data Act leiten soll, wird nur dann gewahrt, wenn die Verbraucherinnen und Verbraucher echte Aus-

99 Vgl. *Specht-Riemenschneider*, MMR 2022, 809, 818.
100 Erwägungsgrund 19 Data Act-E; Data Act-E – Begründung, S. 16.
101 Erwägungsgrund 4 Data Act-E.
102 *Specht-Riemenschneider*, MMR 2022, 809, 818.
103 Verbraucherzentrale Bundesverband e.V., Verbraucher:innen beim Data Act im Blick behalten, 2022, S. 13.
104 Data Act-E – Begründung, S. 16.

wahlmöglichkeiten haben. Wenn der Nutzer keine echte Wahl hat, bleibt von der Konsumentensouveränität nicht viel übrig.[105] Dann versagt aber in der Folge auch der Wettbewerb auf den nachgelagerten Märkten, da dieser Wettbewerb davon lebt, dass Konsumenten auswählen, wen sie mit der Leistungserbringung beauftragen wollen.

a) Auswahl- und Zustimmungsmöglichkeit

Es ist von vornherein nur schwer vorstellbar, dass Verbraucher in echte Verhandlungen über die Datennutzung mit dem Hersteller eines Geräts treten. Ein Aushandlungsprozess, der zu fairen Ergebnissen führt, wird in den Massengeschäften des Alltags beim Erwerb von smarten Geräten nicht zu leisten sein. Ausdrücklich vorgesehen sind nur einige vorvertragliche Informationspflichten (Art. 3 Abs. 2 Data Act-E), im Übrigen ist davon auszugehen, dass der Grundsatz der Vertragsfreiheit gilt.[106] Es ist zu befürchten, dass die „Richtigkeitsgewähr des Vertragsmechanismus" (*Schmidt-Rimpler*) bei der Einigung zwischen Dateninhabern und Verbrauchern größtenteils versagen wird.[107] Der Dateninhaber wird – nach derzeitiger Fassung des Data Act – häufig keine Schwierigkeiten haben, die Zustimmung des Nutzers einzuholen.[108]

Die Situation ist mit der Einwilligung als Bedingung für die Datenverarbeitung nach Art. 6 Abs. 1 S. 1 lit. a DSGVO vergleichbar. Die Praxis zeigt, dass Verbraucher dieses Recht nur selten mit besonderem Bedacht zuweisen. Vielmehr ist es üblich, durch einen schnellen „OK-Klick" oder die Annahme eines umfassenden Vertragswerks samt „Kleingedrucktem" die Einwilligung in Datenverarbeitungsvorgänge zu erklären.[109] Dass dabei die Tragweite überblickt wird, ist zweifelhaft, zumal das Design der Aus-

105 Vgl. *Specht-Riemenschneider*, MMR 2022, 809, 816.

106 *Kerber*, Governance of IoT Data: Why the EU Data Act will not Fulfill Its Objectives, 2022, S. 21.

107 Zur grundrechtlichen Dimension siehe *Engeler*, NJW 2022, 3398, 3402. Vgl. auch *Hennemann/Steinrötter*, NJW 2022, 1481, 1483; *Specht-Riemenschneider*, MMR 2022, 809, 816; *Podszun/Pfeifer*, GRUR 2022, 953, 960 f.

108 *Ducuing* in: Ducuing/Margoni/Schirru, White Paper on the Data Act Proposal, CITIP Working Paper Series, 2022, S. 26; *Habich*, IIC 2022, 1343, 1347.

109 Vgl. Wissenschaftlicher Beirat beim Bundesministerium für Wirtschaft und Energie, Digitalisierung in Deutschland – Lehren aus der Corona-Krise, 2021, S. 16 f.; *Engeler*, Die Einwilligung ist das Problem, Netzpolitik, 3.8.2021, https://netzpolitik.org/2021/datensouveraenitaet-die-einwilligung-ist-das-problem/.

wahlmöglichkeiten häufig intransparent oder manipulativ ist. Ähnliche Vorgehensweisen der Beteiligten sind hinsichtlich der Datennutzung zu erwarten. Sicherungsmechanismen zum Schutz des Nutzers oder erhöhte Voraussetzungen für die Zustimmung sind nicht vorgesehen.[110] Auch ein neutrales Design, das eine echte Auswahl ermöglicht oder gar eine Standardformulierung sind nicht verpflichtend vorgesehen.[111] Ein einfaches Zustimmungsmanagement, das Nutzern eine echte Auswahl zwischen verschiedenen Zugangsmodellen ermöglicht und zugleich die Fairness für verschiedene Marktakteure wahrt, ist sicherzustellen.[112]

(6) Empfohlen wird, ein Zustimmungsmanagement vorzuschreiben, das Nutzern eine echte Auswahl zwischen verschiedenen Zugangsmodellen ermöglicht.

Vorbildhaft dafür kann die Regelung in Art. 5 Abs. 2 DMA für die Zustimmung zum Aufbau von Nutzerprofilen durch Gatekeeper herangezogen werden. Sie enthält Qualifikationen zum Schutz der Nutzer: Dem Nutzer muss eine spezifische Wahl gegeben werden. Die Zustimmung muss den Anforderungen in Art. 4 Nr. 11 und Art. 7 DSGVO genügen. Das würde bedeuten, dass Nutzer eine bewusste Auswahl aus verschiedenen Möglichkeiten frei treffen können müssen. So wäre etwa vorstellbar, dass beim Erwerb eines datensammelnden Geräts der Nutzer entscheiden muss, was mit den Daten geschehen soll. Dabei sollte – in fairer Weise – abgefragt werden, wer Zugang zu den Sekundärmärkten erhalten soll. Die so erteilte Zustimmung könnte für die Auswahl der Leistungserbringer von absehbaren Folgedienstleistungen (Wartung, Reparatur, Erweiterung usw.) maßgeblich sein, sodass in der Folge für die ausgewählten Betriebe automatisch Zugang gewährt wird. Die Abfrage könnte in regelmäßigen Abständen erneut durchgeführt werden, damit der Nutzer nicht ein für alle Mal an seine erste Auswahlentscheidung gebunden ist. Die Alternativen müssen in Aufmachung und Art gleichwertig präsentiert werden, freilich ohne den Nutzer mit einer Informationsflut zu überfordern. Wichtig ist mit Blick auf Sekundärmärkte insbesondere, dass der Dateninhaber das privilegierte Vertragsverhältnis zum Nutzer nicht unfair missbraucht, um zu seinen Gunsten oder zugunsten seiner autorisierten Vertragspartner Rechtsein-

110 *Specht-Riemenschneider*, MMR 2022, 809, 816.
111 Vgl. *Specht-Riemenschneider*, MMR 2022, 809, 820.
112 ZDH, Bewertung des Kommissionsvorschlags für ein Europäisches Datengesetz KOM(2022) 68 final, 2022, S. 4.

räumungen zu veranlassen oder andere Dritte von kategorisch von der Nutzung auszuschließen. Ein weitgehend vorgegebenes Zustimmungsmanagement (ggf. durch neutrale Dritte, etwa Datenvermittlungsdienste nach Art. 10 Data Governance Acts) würde dieser Gefahr vorbeugen.[113]

b) Verbot der Kopplung

Insbesondere sollte vorgesehen werden, dass die Zustimmung nicht als freiwillig anzusehen ist, wenn sie zur Bedingung eines Vertragsschlusses gemacht wird, für den sie nicht technisch oder rechtlich erforderlich ist.[114] Eine entsprechende Regelung ist im Data Act-E nicht vorgesehen.[115] Der Dateninhaber kann den Erwerb von der uneingeschränkten Zustimmung des Nutzers zu einer bestimmten Datennutzung abhängig machen, wodurch das Einwilligungserfordernis erheblich entwertet wird.[116] Die Untersagung einer solchen Kopplungspraxis müsste auch Umgehungslösungen erfassen, z.B. eine differenzierte Preisgestaltung.

(7) Empfohlen wird, eine Kopplung zu verbieten, die den Erwerb des Produkts von der Zustimmung zu einem bestimmten, nicht erforderlichen Datenzugang für den Dateninhaber oder von ihm beauftragte Personen abhängig macht.

c) Klärung von Unklarheiten im Vertrag

Im Ergebnis wird die Chancenverteilung auch davon abhängen, wie einfach die Klärung von Konflikten über die korrekte Auslegung des Data Acts ist. Das verlangt einerseits möglichst präzise Aussagen in den ma-

113 Vgl. zur Einbindung von Vermittlern *Podszun*, GRUR Int. 2022, 197, 201.

114 Vgl. *Schweitzer/Metzger et al*., Data access and sharing in Germany and in the EU: Towards a coherent legal framework for the emerging data economy, Final Report, 8 July 2022 (Gutachten für das Bundesministerium für Wirtschaft und Klimaschutz), S. 221. Siehe näher dazu *Dammann*, ZD 2016, 307, 311; *Frenzel* in: Paal/Pauly, DS-GVO BDSG, 2021, Art. 7 DS-GVO, Rn. 18 ff.; Verbraucherzentrale Bundesverband e.V., Verbraucher:innen beim Data Act im Blick behalten, 2022, S. 13; *Specht-Riemenschneider*, MMR 2022, 809, 817.

115 Vgl. *Hennemann/Steinrötter*, NJW 2022, 1481, 1483.

116 *Podszun/Pfeifer*, GRUR 2022, 953, 960 f; *Kerber*, Governance of IoT Data: Why the EU Data Act will not Fulfill Its Objectives, 2022, S. 23.

teriellen Vorschriften, andererseits eine klare Rechtsdurchsetzung. Nur wenn die materiellen Vorschriften zügig und effektiv durchgesetzt werden können, entfalten sie Wirkung. Darauf sind gerade diejenigen Marktteilnehmer angewiesen, die die Hilfe des Rechts benötigen, um sich gegen mächtigere Verhandlungspartner durchzusetzen.

Einer effizienten und einfachen Rechtsdurchsetzung stehen zunächst praktische Auslegungsfragen rund um die skizzierten Nutzungsverträge im Weg. Sobald Fragen offen sind, sind sie streitanfällig und können – entsprechend langer Atem vorausgesetzt – von den Parteien jahrelang durch die Instanzen getragen werden.

Das betrifft hinsichtlich des Nutzungsvertrags vor allem die folgenden Punkte:

- Wer ist überhaupt Nutzer i.S.d. Data Acts?[117] Fallen darunter auch kurzzeitige Besitzer? Oder nur Eigentümer? Art. 2 Nr. 5 Data Act-E und Erwägungsgrund 20 lassen diese Frage offen. Was gilt beispielsweise für den Fahrer eines Dienstwagens, den der Arbeitgeber (das Unternehmen) erworben hat? Was gilt, wenn Eltern einen Kühlschrank kaufen, den sie nach einer Weile der Tochter für ihre Studenten-WG schenken? Was gilt bei Gästen, die sich in einem Smart Home aufhalten und dort Daten erzeugen?
- Was gilt, wenn ein smartes Produkt weiterverkauft oder verschenkt wird? Gelten Einwilligungen fort, die der ursprüngliche Erwerber ausgesprochen hat? Müssen sich die neuen Eigentümer selbsttätig darum kümmern, Verträge upzudaten?
- Wie lange ist die einmal erteilte Einwilligung gültig?[118] Gilt sie für unbegrenzte Zeit? Was ist, wenn sich in der Zwischenzeit Parameter für die eine oder andere Seite ändern?[119] Ist eine regelmäßige Erneuerung erforderlich?

---

117 Vgl. *Hennemann/Steinrötter*, NJW 2022, 1481, 1484; *Specht-Riemenschneider*, MMR 2022, 809, 814; *Klink-Straub/Straub*, ZD-Aktuell 2022, 01076; BDI, Stellungnahme zum Legislativvorschlag des EU-Data Act, 2022, S. 10; Bitkom, Position Paper EU Data Act Proposal, 2022, S. 14; DIHK, Stellungnahme zum Vorschlag für eine Verordnung über harmonisierte Vorschriften für einen fairen Datenzugang und eine faire Datennutzung (Datengesetz), 2022, S. 3; ZDH, Bewertung des Kommissionsvorschlags für ein Europäisches Datengesetz KOM(2022) 68 final, 2022, S. 3.

118 Vgl. dazu *Specht-Riemenschneider*, MMR 2022, 809, 817; *Bomhard/Merkle*, RDi 2022, 168, 174.

119 Vgl. dazu BDI, Stellungnahme zum Legislativvorschlag des EU-Data Act, 2022, S. 15 f.

– Was gilt, wenn der Nutzungsvertrag rückabgewickelt wird, unwirksam ist oder eine Leistungsstörung vorliegt?[120] Wann fällt in einer solchen Konstellation eine früher erteilte Einwilligung weg? Ist ggf. eine Rückabwicklung oder Entschädigung vorzusehen? Müssen erlangte Daten vernichtet werden?

Schon diese Fragen deuten darauf hin, dass das Modell „Nutzungsvertrag" noch nicht in allen Konsequenzen bedacht worden ist. Eine erste unverbindliche Abhilfe schaffen möglicherweise die in Art. 34 Data Act-E vorgesehenen Mustervertragsbedingungen. Im Übrigen wäre eine gerichtliche Klärung abzuwarten.

(8) Empfohlen wird, Unklarheiten in der Ausgestaltung des Vertrags zwischen Dateninhaber und Nutzer noch im Gesetzgebungsverfahren aufzulösen. Klärungsbedürftig sind der Nutzerbegriff, insbesondere bei Weitergabe oder Fremdnutzung des Produkts, die Laufzeit und Bindungswirkung der Einwilligung sowie die Konsequenzen einer Vertragsstörung.

Die beste Option für die Verwaltung verschiedener Nutzer dürfte eine technische Lösung über Nutzerprofile sein. Hier könnten auch Zustimmungsmanagement-Systeme zum Einsatz kommen. Möglicherweise kann der Einsatz von Künstlicher Intelligenz die Vertragsgestaltung beflügeln.[121] Für die Einwilligung scheinen eine begrenzte Laufzeit und eine regelmäßige Neu-Abfrage wettbewerbsfördernd. Zu überlegen wäre mit Blick auf Art. 34 Data Act-E, den Anreiz zur Nutzung von Musterverträgen zu erhöhen, indem bei Abweichung von diesen eine Indizwirkung angenommen wird, dass Abweichungen zugunsten des Dateninhabers und zu Lasten von Kleinstunternehmen und KMU missbräuchlich sind.

2. Vertrag des Dateninhabers mit dem Dritten

Dritte erlangen nur Zugang, wenn der Zugang über Nutzer vermittelt wird. Nach dem Leitbild kommt es nach der Aufforderung des Nutzers zu

120 Siehe dazu *Specht-Riemenschneider*, MMR 2022, 809, 814.
121 Vgl. zu Zugangsfragen im DMA *Hacker*, GRUR 2022, 1278.

einem Vertragsschluss zwischen Dateninhaber und Datenempfänger (vgl. Art. 8 Abs. 2 Data Act-E).[122]

a) Grundsatzkritik des vertraglichen Modells

Dieser Weg erhöht die Transaktionskosten für Datenempfänger, die sich nicht unmittelbar über eine offene Schnittstelle die Daten besorgen können, diese auf sonstigem Weg automatisch mit der Nutzerzustimmung erhalten oder in direkten Verhandlungen mit dem Dateninhaber vorgehen können.[123]

Dass die Zustimmung des Nutzers erforderlich ist, mag – wie gesehen – wegen der möglicherweise enthaltenen personenbezogenen Daten, wegen der Stellung des Nutzers als Eigentümer, Mieter usw. des Geräts und aus der Überlegung heraus, dass nur durch die Aktivitäten des Nutzers die Daten generiert wurden, noch nachvollziehbar sein. Wesentlich weniger plausibel ist, warum ein Vertrag mit dem Dateninhaber erforderlich sein soll – dieser Vertrag wird erst nötig, weil sich der Dateninhaber eine faktische Kontrollposition anmaßt. Herstellung und Entwicklung des Geräts sind bereits abgegolten. Die Daten werden dem Dateninhaber normativ gerade nicht zugeordnet. Die faktische Position wird durch das Vertragsmodell vom Verordnungsgeber regelrecht aufgewertet.[124] Sie wird dadurch nicht etwa aufgebrochen, sondern erst begründet. Die einzige Rechtfertigung dafür ist der Bereitstellungsaufwand, der durch die Datenteilung mit dem Datenempfänger entsteht. Dieser Aufwand entsteht aber erst dadurch, dass keine automatische Datenbereitstellung „by design" erfolgt – was der Entwickler des Produkts in der Hand hat.

Der nach dem Leitbild des Data Acts erforderliche Vertrag zwischen Dateninhaber und Datenempfänger birgt verschiedene Probleme, da sich

122 A.A. offenbar *Schweitzer/Metzger et al*., Data access and sharing in Germany and in the EU: Towards a coherent legal framework for the emerging data economy, Final Report, 8 July 2022 (Gutachten für das Bundesministerium für Wirtschaft und Klimaschutz), S. 223, die wohl davon ausgehen, dass ein Vertrag zwischen Dateninhaber und Drittem nicht zwingend erforderlich, aber sinnvoll ist.

123 *Drexl et. al*., 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), 2022, Rn. 72.

124 *Kerber*, Governance of IoT Data: Why the EU Data Act will not Fulfill Its Objectives, 2022, S. 16.

eine fehlende Vertragsparität bei Vergütung und Bedingungen negativ für die schwächere Partei niederschlagen wird.[125] Der Vertrag bietet erhebliches Störungspotenzial für den freien Datenzugang, gerade weil auch über eine Vergütung verhandelt werden soll.[126]

Solche Vertragsverhandlungen können im B2B-Bereich zu effizienten Ergebnissen führen, wenn sich die Unternehmen auf einer Ebene befinden und keine Machtasymmetrien bestehen.[127] Im B2B-Bereich sind auch Situationen denkbar, in denen der Hersteller eines Produkts vom Käufer abhängig ist und eine umgekehrte Verhandlungsmacht besteht, z.B. bei Zulieferern von Kraftfahrzeugherstellern.[128] Hier kann es dazu kommen, dass die Datenhoheit beim Erwerber liegt und der Hersteller Bedingungen akzeptieren muss, unter denen er beispielsweise nicht die Daten zur Verbesserung seiner eigenen Produkte erhalten kann.[129] Im Kontext von B2B-Datenverträgen könnte es sogar effizient sein, beiden Seiten einen unabdingbaren Datenzugang zu gewähren, nicht nur den Nutzern.[130]

Besonders virulent bleibt aber der – etwa handwerkstypische – Fall, dass ein kleineres Unternehmen Zugang zum Sekundärmarkt, z.B. für Folge-

125 *Kerber*, Governance of IoT Data: Why the EU Data Act will not Fulfill Its Objectives, 2022, S. 11 ff.

126 Vgl. *Drexl et. al*., 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), 2022, Rn. 71.

127 *Kerber*, Governance of IoT Data: Why the EU Data Act will not Fulfill Its Objectives, 2022, S. 22.

128 Beispiel nach *Kerber*, Governance of IoT Data: Why the EU Data Act will not Fulfill Its Objectives, 2022, S. 22. Siehe auch BDI, Stellungnahme zum Legislativvorschlag des EU-Data Act, 2022, S. 13 f.

129 *Drexl et. al*., 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), 2022, Rn. 54; DIHK, Stellungnahme zum Vorschlag für eine Verordnung über harmonisierte Vorschriften für einen fairen Datenzugang und eine faire Datennutzung (Datengesetz), 2022, S. 6.

130 *Kerber*, Governance of IoT Data: Why the EU Data Act will not Fulfill Its Objectives, 2022, S. 22. Vgl. *Drexl et. al*., 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), 2022, Rn. 54; *Schweitzer/Metzger et al*., Data access and sharing in Germany and in the EU: Towards a coherent legal framework for the emerging data economy, Final Report, 8 July 2022 (Gutachten für das Bundesministerium für Wirtschaft und Klimaschutz), S. 216. Siehe auch *Specht-Riemenschneider*, MMR 2022, 809, 820.

dienstleistungen oder Reparaturen, anstrebt, aber auf eine Vereinbarung mit dem Dateninhaber angewiesen ist, die vom Nutzer vermittelt wird. Es kann zumindest für Handwerkerleistungen wie Reparaturen erwartet werden, dass in fast allen Fällen ein strukturelles Ungleichgewicht gegeben ist: Dem Handwerksbetrieb, der typischerweise ein kleiner Betrieb ist,[131] stehen Gerätehersteller oder Internetplattformen gegenüber. Selbst wenn die Nutzerzustimmung vorliegt, ist die Vereinbarung noch nicht geschlossen. Dies ließe sich in erster Linie durch einen (kostenlosen), jedenfalls aber effektiven, hochwertigen, permanenten Echtzeitzugang auch für Dritte lösen. Diese sollten zumindest ad hoc nach Zustimmung des Nutzers eine unmittelbare Zugangsmöglichkeit erhalten, ohne dass noch mit dem Dateninhaber verhandelt werden muss.[132] Solche direkte Zugangsmöglichkeiten im Sinne eines „access by design" für Dritte sind bisher nicht vorgesehen. Gerade für Dritte wäre ein direkter Datenzugang sehr viel wichtiger als für Verbraucher.[133] Ein derzeit beim EuGH anhängiger Fall aus der Automobilwirtschaft zeigt, wie anfällig selbst bei Zugangsansprüchen die tatsächliche Zugangsgewährung noch ist, wenn der Dateninhaber seine faktische Überlegenheit ausspielt: In dem Fall wird moniert, dass die Kfz-Hersteller verlangen, dass unabhängige Reparaturwerkstätten, die auf Daten zugreifen wollen, eine Registrierung, einen Login mit permanenter Internetverbindung und ein kostenpflichtiges Abonnement von Tools zum Datenzugriff aufweisen müssen.[134] Da für die Leistungserbringung auf dem Sekundärmarkt rascher Zugang erforderlich ist, wäre ein automatischer Zugang nach Nutzer-Zustimmung die verbraucherfreundlichste Lösung, die geringe Transaktionskosten und geringe Missbrauchsanfälligkeit hätte sowie echten Wettbewerb um den und auf dem Sekundärmarkt ermöglicht. Als Standardmöglichkeit würde dies einen erheblichen Fortschritt bedeuten. Lässt sich dies nicht durchsetzen, wäre zumindest denkbar, Da-

131 Nach den Zahlen des Statistischen Bundesamts für 2019 hatten über die Hälfte der Handwerksbetriebe in Deutschland weniger als 250.000 Euro Umsatz und fast 80 % der Handwerksunternehmen hatten 9 oder weniger Mitarbeitende, siehe https://www.zdh.de/daten-und-fakten/betriebe/beschaeftigte/umsaetze/.

132 Vgl. *Drexl et. al*., 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), 2022, Rn. 69.

133 *Podszun/Pfeifer*, GRUR 2022, 953, 956 f. Vgl. auch *Specht-Riemenschneider*, MMR 2022, 809, 823 f.

134 Im konkreten Fall geht es um Zugang nach Art. 61 Abs. 1, Abs. 4 VO (EU) 2018/858. Das Verfahren ist beim EuGH anhängig unter Az. C-296/22.

teninhaber zu privilegieren, die derartige Lösungen wählen. Sie könnten z.B. weitergehende Rechte bei der Gestaltung von Nutzungsbedingungen haben. Ein solches flexibilisiertes Modell könnte eine Kompromisslinie darstellen.

Der Data Act-E ist für derartige Missbrauchsmöglichkeiten und für die strukturellen Machtungleichgewichte zwischen Dateninhaber und Datenempfänger teilweise blind. Positiv zu erwähnen ist, dass einzelne Relativierungen des Ungleichgewichts bei KMU vorgesehen sind, insbesondere durch die Klauselkontrolle in Art. 13 Data Act-E (zu diesen Bedingungen siehe unten). Die Grundkonstellation bleibt jedoch problematisch.

(9) Empfohlen wird, dass auf Zuruf des Nutzers unmittelbar ein Zugangsrecht für Dritte geschaffen werden muss, ohne dass es noch zu Verhandlungen zwischen Dateninhabern und Dritten kommen muss. Erwogen werden könnte jedenfalls, dass derartige Lösungen im Data Act privilegiert werden.

b) Ausnutzung von Informationsvorteilen

In Art. 5 Abs. 5 Data Act-E ist vorgesehen, dass Dateninhaber ihre überlegene Position nicht verwenden dürfen, um Einblicke in die geschäftlichen Strategien Dritter zu erlangen. Gerade wenn Dateninhaber und Dritte auf denselben Märkten tätig sind, besteht großes Missbrauchspotenzial. Ob die Vorschrift in Art. 5 Abs. 5 Data Act-E in der Praxis dieses Risiko ausreichend zu begrenzen vermag, ist zweifelhaft: Die Klausel ist vorsichtig und konditional formuliert. Häufig wird der Nachweis nicht gelingen. Immerhin wird aber das Problem gesehen, dass die Kontrollmöglichkeit von Informationen, die nicht in den normativen Zuordnungsbereich desjenigen fallen, der sie kontrolliert, zu Wettbewerbsverzerrungen führen kann. Eine strengere Formulierung findet sich für das gleiche Problem in Art. 6 Abs. 2 DMA.[135]

135 In Art. 6 Abs. 2 DMA heißt es: „Der Torwächter darf im Wettbewerb mit gewerblichen Nutzern keine nicht öffentlich zugänglichen Daten verwenden, die von diesen gewerblichen Nutzern im Zusammenhang mit der Nutzung der betreffenden zentralen Plattformdienste oder der zusammen mit den betreffenden zentralen Plattformdiensten oder zu deren Unterstützung erbrachten Dienste generiert oder bereitgestellt werden, einschließlich der von den Kunden dieser gewerblichen Nutzer generierten oder bereitgestellten Daten.

(10) Empfohlen wird, die Klausel in Art. 5 Abs. 5 Data Act-E strenger zu formulieren.

c) Beschädigung des Verhältnisses von Dritten zum Nutzer

Soweit der Verbraucher im Dreiecksverhältnis zu Dateninhaber und Drittem aktiviert wird, ist zu beachten, dass das Verhältnis des Dritten zu seinem (potenziellen) Kunden nicht beschädigt werden darf. Dem Nutzer dürfen keine aufwändigen Handlungen aufgebürdet werden, die zur Verärgerung über den Dritten führen. Wird die Datenweitergabe aus Sicht der Verbraucher „umständlich", leidet darunter die Geschäftsbeziehung zum Leistungserbringer: Der Kunde nimmt den Service dann als schwerfällig wahr und setzt beim nächsten Mal möglicherweise auf einen vom Dateninhaber direkt empfohlenen Vertragspartner des Dateninhabers. Für den fairen wettbewerblichen Zugang zu Sekundärmärkten ist daher unerlässlich, dass Datenempfänger einen möglichst einfachen Zugang zu Daten erhalten.

Das gilt schon für die notwendige Zustimmung des Verbrauchers nach dem Modell in Art. 5 Data Act-E. Muss der Nutzer tätig werden, wird dieser möglicherweise mit Rückfragen oder Formalia behelligt, so schadet dies der Beziehung zwischen Nutzer und Dritten. Hält man an der Vermittlung über den Nutzer fest, ist es essenziell, dass keine Hürden oder Transaktionskosten aufgebaut werden, die die Verwendung des Modells aus Nutzersicht unangenehm werden lassen. Ideal wäre ein automatisierter Prozess, dem der Nutzer schon mit Erwerb des Geräts zustimmt oder der sehr einfach aktiviert werden kann. Rückfragen durch den Dateninhaber an den Nutzer würden hier bereits einen Negativeindruck erzeugen. Durch Stellvertretungslösungen mit dem Dritten oder Datenmittlern könnte der individuelle Endverbraucher auch gänzlich aus dem Prozedere herausgehalten werden. Unbedingt zu vermeiden ist, dass die Datenweiter-

---

Für die Zwecke des Unterabsatzes 1 umfassen die nicht öffentlich zugänglichen Daten alle von gewerblichen Nutzern generierten aggregierten und nichtaggregierten Daten, die aus den kommerziellen Tätigkeiten gewerblicher Nutzer oder ihrer Kunden auf den betreffenden zentralen Plattformdiensten oder auf Diensten, die zusammen mit den betreffenden zentralen Plattformdiensten des Torwächters oder zu deren Unterstützung erbracht werden, abgeleitet oder durch diese erhoben werden können, einschließlich Klick-, Anfrage-, Ansichts- und Sprachdaten."

gabe an den Dritten künstlich verzögert, bürokratisiert oder auf sonstige Weise erschwert wird oder seitens des Dateninhabers beim vermittelnden Nutzer ein schlechter Eindruck vom Datenempfänger erzeugt wird.

(11) Empfohlen wird, das Zustimmungsmanagement so auszugestalten, dass weder künstliche bürokratische Hürden zur Zustimmung errichtet werden noch der Nutzer vom Dateninhaber zu Ungunsten des Dritten beeinflusst werden kann. Nutzt der Dateninhaber seine Position, um den Nutzer zum Nachteil Dritter zu beeinflussen, sollte eine Sanktion vorgesehen werden.

3. Format der Zugangsgewährung

Eines Zugangs über den umständlichen Vertragsweg im Dreiecksverhältnis bedarf es grundsätzlich nicht, wenn Nutzer unmittelbar Daten an Dritte weitergeben können oder diese direkt auf die Daten zugreifen können. Das setzt allerdings voraus, dass unkompliziert Zugriff auf die Daten gewährt wird. Das Ziel muss sein, dass Datenempfänger einen hochwertigen Datenzugang erhalten.

a) Format der Daten

Der Data Act-E macht keine Vorgaben dazu, in welchem Format die Daten zugänglich gemacht werden müssen. Hier mangelt es bei der Frage des Datenzugangs an Problembewusstsein. Das überrascht, da an anderer Stelle im Data Act-E davon die Rede ist, dass „alle erzeugten oder gemeinsam erzeugten Daten, einschließlich der relevanten Datenformate und Datenstrukturen, in einem strukturierten, gängigen und maschinenlesbaren Format" exportiert werden sollen (Art. 26 Abs. 4 Data Act-E, siehe auch Art. 28 Abs. 1 lit. b Data Act-E sowie Erwägungsgrund 31). In der Konsultation vor dem Data Act waren als Schwierigkeiten zu 69 % „technische Hindernisse (Formate, fehlende Standards)" genannt worden.[136] Nur wenn die Daten in einem standardisierten Format herausgegeben werden, lässt sich die für Folgedienstleistungen erforderliche technische Interopera-

136 Data Act-E – Begründung, S. 12.

bilität gewährleisten.[137] Sind Daten erst mühsam umzuwandeln, steigen die Transaktionskosten für Sekundärmarktleistungen.

Zwar gibt es in Art. 28 ff. Data Act-E Vorschriften über die Interoperabilität von Datenräumen, in denen Daten sicher geteilt und gemeinsam genutzt werden können. Diese Vorschriften gelten jedoch nicht unmittelbar für die Datenherausgabe von Dateninhaber an Datenempfänger. Es ist zwar möglich, dass diese die Nutzung von Datenräumen vereinbaren, aber nicht verpflichtend. Daher muss davon ausgegangen werden, dass Unternehmen, die zuvor nicht gewillt waren, Daten mit anderen Unternehmen zu teilen, einem Datenteilungsmodell über Datenräume nicht offen gegenüberstehen.

Bei der Wahl des Formats der Daten können möglicherweise proprietäre Lösungen gewählt werden, sodass Daten nicht oder nur mit Hilfe weiterer Tools, die vom Datenkontrolleur erworben werden müssen, gelesen und verwertet werden können.

Dem kann nur eine Lösung entgegenwirken, nach der Daten in einem strukturierten, gängigen und maschinenlesbaren Format oder jedenfalls in branchenüblicher, einfach zugänglicher Weise zur Verfügung gestellt werden.[138] Dies ist so auch in Art. 6 Abs. 10 DMA vorgesehen.[139] Welche Formate genau diese Kriterien erfüllen, kann ggf. außerhalb des Data Act geregelt werden, z.B. durch Brancheninitiativen und/oder delegierte Rechtsakte der Kommission. Allgemeingültige Lösungen für unterschiedliche Branchen und Anwendungsbereiche werden nicht immer möglich sein, obwohl gerade das branchenübergreifende Zusammenwirken eine große Chance der vernetzten Datenökonomie ist. Dieses Problem ließe sich entweder über delegierte Rechtsakte der Kommission gem. Art. 290 AEUV im Wege einer Vereinheitlichung lösen (ähnlich schon vorgesehen in Art. 28 Data Act-E für Betreiber von Datenräumen) oder durch eine Pflicht, die Daten für Intermediäre zugänglich zu machen, die die Interoperabilität dann herstellen.

137 *Kerber*, Governance of IoT Data: Why the EU Data Act will not Fulfill Its Objectives, 2022, S. 12.

138 Vgl. *Schweitzer/Metzger et al*., Data access and sharing in Germany and in the EU: Towards a coherent legal framework for the emerging data economy, Final Report, 8 July 2022 (Gutachten für das Bundesministerium für Wirtschaft und Klimaschutz), S. 228 f.

139 Siehe dazu unten, D.II.

(12) Empfohlen wird, eine Verpflichtung aufzunehmen, dass Daten in einem strukturierten, gängigen und maschinenlesbaren Format oder in branchenüblicher Weise zur Verfügung gestellt werden müssen. Zudem sollte untersagt werden, dass für Lesen, Speichern und Nutzen der Daten weitere Tools kostenpflichtig erworben werden müssen.

Nicht unerwähnt bleiben sollte, dass Standardisierungen immer auch mit einem Verlust an Innovation und Flexibilität einhergehen und den Wettbewerb auch beschränken. Ein gewisser „Wettbewerb der Standards" ist also durchaus wünschenswert. Das hindert aber nicht die Erfüllung der genannten Anforderungen an das Datenformat.

b) Zugriff und in situ-Zugang

Im Verordnungsentwurf heißt es an verschiedenen Stellen, dass Daten „zugänglich" gemacht werden müssen. Genauere Vorgaben oder Erläuterungen finden sich kaum. Was „zugänglich machen" praktisch bedeutet, bleibt unklar.[140] Der Regelfall ist nach Art. 4 Abs. 1 Data Act-E e.c. jedenfalls die Zugänglichmachung auf dem Gerät selbst. Das ist der sog. „in situ"-Zugang. Das ist für Verbraucherinnen und Verbraucher ein in der Regel sinnvolles und ausreichendes Instrument. Unnötige Datentransfers über Server werden überflüssig gemacht, die Daten sind gleich auf dem Gerät einsehbar, soweit eine Benutzeroberfläche vorhanden ist. Das ist insbesondere dann von Relevanz, wenn Daten schlicht abgelesen werden sollen, was für Verbraucherinnen und Verbraucher häufig der Fall sein wird.

Bei einem in situ-Zugang wird der Nutzer nicht in die Lage versetzt, seinerseits mit den Daten zu arbeiten oder über diese zu verfügen. Der Nutzer bleibt auf eine passive Empfängerrolle beschränkt. Zugleich behält der Dateninhaber die Kontrolle darüber, wie auf die Daten zugegriffen,

140 *Drexl et. al.*, 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), 2022, Rn. 65; DIHK, Stellungnahme zum Vorschlag für eine Verordnung über harmonisierte Vorschriften für einen fairen Datenzugang und eine faire Datennutzung (Datengesetz), 2022, S. 8. Siehe schon *Podszun/Pfeifer*, GRUR 2022, 953, 957.

wie diese genutzt, weiterverarbeitet und weitergegeben werden können.[141] Möglicherweise wird das Nutzungsverhalten des Nutzers erneut registriert, sodass eine weitergehende Kontrolle durch den Dateninhaber möglich ist.

Wenn Daten und möglicherweise daraus gezogene Schlüsse hinterfragt werden sollen oder wenn die Daten weiterverwendet und verarbeitet werden müssen, genügt der in situ-Zugang nicht. Zu diesem Zweck ist eine Herausgabe der Daten erforderlich – regelmäßig in Form eines Transfers auf einen anderen Datenträger.[142] Dies ist insbesondere für Folgenutzungen bei Angeboten auf nachgelagerten Märkten relevant.[143]

Der Data Act gibt in der derzeitigen Form lediglich Hinweise, dass ein solcher Zugriff auf die Daten, d.h. insbesondere das Abspeichern auf einem anderen Datenträger, ermöglicht werden soll. Dies lässt sich z.B. aus den Erwägungsgründen schließen, wenn eine umfassende Nutzung von Daten insbesondere auch auf nachgelagerten Märkten als Ziel angegeben wird.[144] Das dürfte in aller Regel eine Speicherung und Weiterverarbeitung der Daten auch außerhalb des Gerätes erfordern. In Art. 4 Abs. 1 Data Act-E heißt es zudem, dass – soweit der Nutzer nicht direkt auf die Daten zugreifen kann – der Dateninhaber dem Nutzer die Daten „zur Verfügung" stellen muss. Die Verfügungsmöglichkeit über Daten schließt deren weitere Verwendung auf anderen Datenträgern ein. Eine Weitergabemöglichkeit für Nutzer an Dritte ist auch nach Erwägungsgrund 28 vorgesehen. Ein Vertrag mit dem Dateninhaber ist für den Datenempfänger nur nötig, wenn der unmittelbare Zugriff (sei es über eine offene Schnittstelle oder über die Datenweitergabe durch Verbraucher) nicht funktioniert.

Für die Datenfreigabe an Dritte nach Art. 5 Abs. 1 Data Act-E wird es in vielen Fällen nicht genügen, wenn der Datenempfänger die Daten nur auf dem Gerät einsehen kann. Wenn also in den Fällen des Art. 4 Abs. 1 und Art. 5 Abs. 1 Data Act-E die Zurverfügungstellung geschuldet ist, kann

---

141 *Kerber*, Governance of IoT Data: Why the EU Data Act will not Fulfill Its Objectives, 2022, S. 9. Vgl. Auch *Podszun/Pfeifer*, GRUR 2022, 953, 956.

142 Vgl. *Specht-Riemenschneider*, MMR 2022, 809, 816; *Drexl et. al.*, 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), 2022, Rn. 66; DIHK, Stellungnahme zum Vorschlag für eine Verordnung über harmonisierte Vorschriften für einen fairen Datenzugang und eine faire Datennutzung (Datengesetz), 2022, S. 8.

143 Vgl. *Podszun/Pfeifer*, GRUR 2022, 953, 957.

144 Data Act-E – Begründung, S. 16.

für den unmittelbaren Zugang des Nutzers nach Art. 3 Abs. 1 Data Act-E nichts anderes gelten. Mit anderen Worten sind diese Vorschriften richtigerweise so zu lesen, dass dem Nutzer stets neben dem Zugang zu den Daten auch deren Übertragung und Weiterverarbeitung auf anderen Geräten möglich sein muss. Werden die Daten nicht unmittelbar transferiert, muss eine Schnittstelle zum Abruf der Daten geschaffen werden.[145]

(13) Empfohlen wird klarzustellen, dass der in-situ-Zugang zu Daten ohne Möglichkeit des Datentransfers den Anforderungen des Data Acts nicht genügt, insbesondere für Dritte.

c) Access by design

Dass der Datenzugang schon „by design" gewährt werden muss, ist eine besondere Stärke des Data Act-E (Art. 3 Abs. 1 Data Act-E). „Access by design" ist als Grundfall der Datenzugangsgewährung vorgesehen. Das ergibt sich aus der systematischen Stellung in Art. 3 Abs. 1 Data Act-E und aus Art. 4 Abs. 1 Data Act-E. Auch in den Erwägungsgründen wird betont, dass die Produkte so konzipiert und hergestellt werden sollen, dass die Daten für den Nutzer stets leicht zugänglich sind.[146] Das Produkt muss also schon von Anfang an so angelegt sein, dass Datenzugang automatisch mitgedacht wird. Das ist ein erheblicher Fortschritt, weil dadurch die „Black Box" des Geräts etwas geöffnet wird.

Dieser Ansatz ist jedoch im vorliegenden Verordnungsentwurf nicht konsequent ausgestaltet worden. Insbesondere wird das Grundprinzip durch die Einschränkung „soweit relevant und angemessen" mit erheblichen Fragezeichen versehen.[147] Wann unmittelbarer Datenzugang by design irrelevant und unangemessen ist, wird nicht näher dargelegt. Ein Mangel an Relevanz wird sich in der Datenökonomie kaum begründen

145 So auch *Specht-Riemenschneider*, MMR 2022, 809, 818. Vgl. auch *Drexl et. al.*, 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), 2022, Rn. 66.

146 Erwägungsgrund 19 Data Act-E.

147 *Drexl et. al.*, 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), 2022, Rn. 73.

lassen, da es nicht vorhersagbar ist, wofür Daten gebraucht werden können. Das dehnbare Wort „angemessen" müsste näher bestimmt werden. Zu denken wäre etwa an die Zumutbarkeit einer Datenanzeige bei Kleinstgeräten. Andernfalls droht, dass das wegweisende Prinzip „access by design" durch Einwände der Dateninhaber ausgehöhlt wird. Nur wenn „access by design" als zwingende Regel ausgestaltet ist, wird sich dieses hilfreiche Konzept auch durchsetzen. Ausnahmen sind auf wenige Fälle zu beschränken, die in der Verordnung auch aufgezählt werden sollten. Diese Ausnahmen könnten für die Fälle gelten, dass access by design tatsächlich unmöglich oder offensichtlich unverhältnismäßig ist.

(14) Empfohlen wird, das Konzept „access by design" zum Regelfall mit enumerativ aufgezählten Ausnahmetatbeständen zu erklären und einen Anspruch darauf vorzusehen.

4. Rolle von virtuellen Assistenten

Eine besondere Schwierigkeit stellt die Einbeziehung von virtuellen Assistenten dar. Wird ein Gerät über ein anderes Gerät gesteuert, das wiederum mit anderen Geräten vernetzt ist, entsteht möglicherweise eine Kaskade an Datenweiterleitungen und notwendigen Verträgen. So könnte beispielsweise ein Roboter innerhalb einer Maschinenanlage tätig werden, die in eine Smart Factory eingebunden ist, die durch eine Steuerungsanlage gesteuert wird. Auf allen Stufen kommt es zu Datensammlungen und -vernetzungen. Will ein Elektriker den Roboter reparieren, könnte es sein, dass die erforderlichen Daten über mehrere Stufen hinweg angefordert werden müssen. Je nach Konstellation können dabei verschiedene Nutzer oder Dateninhaber involviert sein. Auch auf Datenempfängerseite können mehrere Subunternehmer tätig sein. Es ist denkbar, dass eine unübersichtliche Vertragskaskade mit mehreren Behinderungsmöglichkeiten entsteht. Die gleiche Situation entsteht bei privaten Verbrauchern, etwa wenn Geräte nicht direkt bedient werden, sondern über ein Smart Home-Netzwerk, das über ein Smartphone gesteuert wird. Dabei kann sich die Frage stellen, ob ein Dritter Daten von mehreren Geräten benötigt und wer jeweils Ansprechpartner für welche Daten ist. Das kann die Zugangssituation verkomplizieren. Diese Situation stellt sich insbesondere bei virtuellen Assistenten (Art. 2 Nr. 4 Data Act-E), die gem. Art. 7 Abs. 2 Data Act-E ausdrücklich in die Datenteilungspflicht einbezogen sind, soweit sie zur Produktsteuerung verwendet werden. Abgeholfen werden kann der Ver-

tragskaskade durch die Festlegung eines einheitlichen Zugangspunkts (in der Regel vom Endgerät ausgehend), über den die Daten der gesamten Kette abgerufen werden können. Dies setzt eine Interoperabilität der Geräte voraus und eine Weiterleitungspflicht (ggf. ohne Speichermöglichkeit).

(15) Empfohlen wird eine Regelung, nach der bei Nutzung mehrerer hintereinandergeschalteter Geräte an einem zentralen Zugangspunkt der Zugang zu allen Daten der Kette abgefragt werden kann.

5. Sonderproblem „predictive maintenance"

Für Reparaturdienstleistungen wird erwartet, dass „predictive maintenance", vorausschauende Wartung, künftig eine größere Rolle spielen wird.[148] Damit ist gemeint, dass der Reparatur- und Wartungsbedarf durch Datenanalyse bereits frühzeitig erkannt wird, sodass der Ausfall von Maschinen oder Anlagen durch vorausschauende Wartung vermieden wird. Mit anderen Worten: Es kommt nicht mehr dazu, dass der Endnutzer einen Handwerker ruft, weil die Heizung nicht mehr funktioniert, sondern die Heizung geht gar nicht kaputt, da schon rechtzeitig zuvor Teile ausgetauscht oder gewartet wurden.

Das Geschäftsfeld der vorausschauenden Wartung ist für Dritte nur zugänglich, wenn die Daten auch durch sie zeitnah gelesen und ausgewertet werden können. Eine Umwälzung bisheriger Marktprozesse kann darin liegen, dass der Kontrolleur des Datennetzwerks künftig zuteilt, wer welche Dienste erbringen darf: Weiß der Dateninhaber frühzeitig, dass eine Reparatur fällig wird, hat er es in der Hand, den Verbraucher darauf hinzuweisen und auch gleich einen von ihm autorisierten und mit Zugang zur Datenbox ausgestatteten Handwerker vorzuschlagen. Die Entscheidung, wer die Reparaturleistung erbringen soll, wäre dann erheblich vorgeprägt oder dem Kunden ganz entzogen. Es versteht sich von selbst, dass dies auch die finanziellen Ströme verändern würde – der Dateninhaber würde eine Provision erhalten (so nicht eigene Tochterunternehmen tätig werden). Handelt es sich um den Hersteller, wird dieser darauf ach-

148 Vgl. *Peiß*, BayernLB Research, Megatrend Digitalisierung, 10.10.2018, S. 1. Statista ermittelte 2019, dass 37 % der befragten Unternehmen (überwiegend Maschinen- und Anlagebau, Automobilindustrie und Elektroindustrie) predictive maintenance nutzen, siehe https://de.statista.com/statistik/daten/studie/1078451/umfrage/nutzung-von-predictive-maintenance-anwendungen-in-deutschland/.

ten, dass nur Originalersatzteile verwendet werden (können). Unabhängige Handwerksbetriebe würden nicht mehr am Markt reüssieren können, günstigere Lösungen (z.B. mit anderen Ersatzteilen) würden verdrängt. Der Wettbewerb auf dem Sekundärmarkt würde geschädigt, der Verbraucher würde – bei aller Bequemlichkeit dieser Lösung – möglicherweise höhere Kosten haben, dies aber kaum merken. Für Handwerker wäre nicht mehr der Endnutzer der maßgebliche Ansprechpartner für den eigenen Erfolg, sondern der Dateninhaber.

Mit dem derzeitigen Entwurf des Data Acts kann dieses Thema zugunsten bestimmter Betriebe aufgelöst werden, wenn der Nutzer schon präventiv entscheidet, welches Unternehmen im Fall, dass vorausschauende Wartung erforderlich wird, beauftragt werden soll. Allerdings setzt dies voraus, dass frühzeitig das Thema predictive maintenance ins Zustimmungsmanagement aufgenommen wird. Dieses sollte, wie oben dargelegt, bestimmten Fairnessanforderungen genügen müssen. Insbesondere dürfte bei Wahl durch den Nutzer keine Provision vom ausgewählten Dritten an den Dateninhaber zu entrichten sein.

Seine Auswahl müsste der Nutzer stets überprüfen und ändern können (und auch regelmäßig müssen). So würde die Auswahlentscheidung weiterhin beim Nutzer liegen. Zugleich müsste auf Seiten des Herstellers des Produkts ein System installiert werden (jedenfalls ab einer bestimmten Mindestgröße des Herstellers), das unabhängigen Dritten den Zutritt zum Geschäft der vorausschauenden Wartung ermöglicht. Das könnte entweder durch eine access-by-design-Lösung gesichert werden, die z.B. bestimmten Datenmittlern die Analyse der Daten ermöglicht, oder durch eine Art Auktionslösung: Die Wartungsleistung könnte so an den für den Verbraucher günstigsten Anbieter abgegeben werden. Im Zusammenspiel der Akteure lassen sich hier noch weitere Lösungen des Problems im Markt entdecken. Entscheidend ist, dass die Serviceleistung der vorausschauenden Wartung nicht vom Hersteller monopolisiert werden kann. Das würde die jahrzehntelangen Bemühungen um ein Offenhalten der Sekundärmärkte mit einem Mal konterkarieren.

(16) Empfohlen wird, eine gesonderte Regelung für vorausschauende Wartung zu schaffen. Diese sollte darauf gerichtet sein, dass Nutzer explizit der vorausschauenden Wartung zustimmen müssen und auswählen können, wer als Leistungserbringer eingeschaltet wird. Diese Auswahl muss der Kunde jederzeit neu justieren können (und regelmäßig neu justieren müssen).

III. Bedingungen des Datenzugangs

Wenn es keine offene Schnittstelle gibt, über die Daten abrufbar sind, müssen Dateninhaber und Datenempfänger die Bedingungen des Datenzugangs einschließlich der Vergütung vereinbaren. Dass der Dateninhaber Zugang gewähren muss, wenn der Nutzer diesem zustimmt, ist allerdings nicht verhandelbar. Für das Funktionieren der Sekundärmärkte ist es unerlässlich, dass der Zugang einfach umgesetzt wird und die Bedingungen nicht prohibitiv sind. Hier lässt der Data Act in seiner derzeitigen Form den Datenkontrolleuren noch Spielraum.

Wo sich Dateninhaber und Interessenten bislang nicht freiwillig auf Bedingungen für einen Datenzugang einigen konnten, ist es unwahrscheinlich, dass die Vertragsverhandlungen reibungslos laufen. Das ist insbesondere der Fall, wenn erhebliche Machtungleichgewichte zwischen den Parteien bestehen. Als unterlegene Verhandlungspartei wird im Regelfall der Zugangspetent anzusehen sein. Strukturelle Ungleichgewichte müssen jedoch ausgeglichen werden. Dies leistet für den Vertrag zwischen Dateninhaber und -empfänger der Data Act-E in Art. 5-12. In Art. 13 Data Act-E sind zudem Klauselverbote für Verträge mit Kleinstunternehmen, kleinen oder mittleren Unternehmen vorgegeben. Thematisiert werden im Folgenden die Gegenleistungspflicht (1.), die Nutzungsbedingungen (2.) und insbesondere die Konkurrenzklausel (3.).

1. Gegenleistung

Der Verhandlungsweg ist insbesondere für die Bestimmung der Gegenleistung relevant. Auch hier macht Art. 9 Abs. 1 Data Act-E lediglich die Vorgabe, dass diese angemessen sein muss. Die Gegenleistung bei Daten ist ein besonderes Problem, da diese einerseits einen hohen kommerziellen Wert haben können, andererseits die Kosten der Erhebung und Übertragung relativ gering sind. Die Nicht-Rivalität von Daten und ihre einfache Weitergabe erschweren es, mit dem knappheitsorientierten Preismechanismus zu arbeiten. Eine künstliche Verknappung durch die Schaffung von Dateneigentumsrechten wäre die falsche Konsequenz. Stattdessen muss der Mechanismus der Gegenleistung auf den Prüfstand gestellt werden.[149]

149 So auch *Ducuing/Schirru* in: Ducuing/Margoni/Schirru, White Paper on the Data Act Proposal, CITIP Working Paper Series, 2022, S. 36.

a) Hinterlegungslösung zur Vermeidung von Verzögerungen

Die Flexibilität des Begriffs „angemessen" und die weitergehende Forderung nach FRAND-Bedingungen (dazu sogleich) eröffnet viel Verhandlungspotential und damit Verzögerungspotential bei der Gewährung von Datenzugang.[150] Das kann das Tätigwerden auf Sekundärmärkten erschweren. Ein Verbraucher, der eine rasche Handwerkerleistung benötigt, wird nicht warten wollen, bis das Handwerksunternehmen seiner Wahl mit dem Dateninhaber ausgefochten hat, zu welcher Vergütung Datenzugang erteilt wird. Dieses Problem lässt sich lösen, indem sofortiger Zugang gegen Hinterlegung einer Gegenleistung gewährt wird. An die Stelle der Hinterlegung könnten auch Kredit- oder Clearingsysteme treten, die beispielsweise von Verbänden, Kammern oder Datenmittlern bereitgestellt werden. Wesentlich ist gerade für Lösungen auf dem Sekundärmarkt, z.B. für Reparaturen, dass der Zugangspetent unmittelbar zugreifen kann, ohne dass erst Details der Zahlung geklärt werden müssten.

(17) Empfohlen wird, standardmäßig den sofortigen Zugang zu gewähren. Die berechtigten Interessen des Dateninhabers an einer Vergütung – soweit eine solche überhaupt erforderlich ist – sollten durch eine Hinterlegungslösung oder ähnliche Modelle gesichert werden.

b) Vergleichsverträge als Bezugsgröße

Der Dateninhaber muss nach Art. 9 Abs. 4 Data Act-E Informationen zur Verfügung stellen, anhand derer der Datenempfänger überprüfen kann, ob die Gegenleistung angemessen ist. Schon die Kosten der Bereitstellung dürften regelmäßig strittig sein (siehe im nächsten Punkt). Da die Gegenleistung nach Art. 9 Abs. 1 Data Act-E zudem eine Gewinnmarge umfassen darf, dürfte es schwierig werden, die Angemessenheit objektiv nachzuprüfen.[151] Als Indiz für die Angemessenheit ließe sich zumindest der Vergleich mit anderen Zugangsverträgen heranziehen, die freiwillig oder

150 Vgl. auch *Habich*, IIC 2022, 1343, 1350 ff.

151 Vgl. *Graef/Husovec*, Seven Things to Improve in the Data Act, 2022, S. 3 f. Zu möglichen Lösungsansätzen siehe *Picht*, Caught in the Acts – Framing Mandatory Data Access Transactions under the Data Act, further EU Digital Regulation Acts, and Competition Law, 2022, S. 32 f.

mit Blick auf den Data Act geschlossen wurden. Ergibt sich daraus, dass im konkreten Fall jedenfalls keine diskriminierend hohe Gegenleistung verlangt wird, kann dies ein erstes Indiz für die Angemessenheit sein, insbesondere wenn Vergleichsverträge vorliegen, die mit Vertragspartnern „auf Augenhöhe" geschlossen wurden. Dazu müssten die Vergleichsverträge als Bezugsgröße aber zugänglich sein. Eine Veröffentlichung wird wegen geschäftlicher Interessen regelmäßig nicht in Frage kommen. Denkbar wäre aber die Hinterlegung bei einer offiziellen Stelle, die die Verträge vertraulich behandelt. So könnte gefordert werden, dass alle bisherigen Datenzugangsverträge eines Unternehmens gegenüber der Europäischen Kommission oder einem anerkannten Datenmittler oder einer Körperschaft offengelegt werden. Sie könnten auf Verlangen von Schiedsstellen oder Gerichten eingesehen werden. So ließe sich schneller als bei der Durchsetzung von schwierigen Auskunftsansprüchen erfassen, ob eine Diskriminierung vorliegt und die Angemessenheit im Vergleich zu anderen Zugangspetenten gewahrt ist.

Eine Pflicht zur Offenlegung von Verträgen oder zum Angebot von einheitlichen Nutzungsbedingungen („Tarifen") könnte an die Bedeutung des Dateninhabers für die Märkte geknüpft werden. Besonders wichtige Dateninhaber könnten verpflichtet werden, Musterverträge offenzulegen oder Musterbedingungen auszuarbeiten, diese von der Kommission oder einer anderen Instanz prüfen zu lassen und sodann in nicht-diskriminierender Weise Daten zu diesen Bedingungen für alle Nachfrager (ggf. mit Ausnahme von Gatekeepern i.S.d. DMA) bereitzustellen. Das würde das Streitpotential mit diesen Dateninhabern minimieren und für häufig auftretende Situationen Rechtssicherheit garantieren.

Vergleichbar wäre dieses Vorgehen mit der Inpflichtnahme von Gatekeepern im DMA. Welche Unternehmen einem solchen Spezialarrangement unterworfen werden sollten, ist offen. In Betracht kämen beispielsweise Unternehmen, die als Gatekeeper nach dem DMA benannt worden sind, oder Unternehmen, die eine besonders hohe Zahl von smarten Geräten in den Markt bringen, oder Unternehmen, die marktbeherrschend sind oder an zentralen Stellen marktübergreifende Bedeutung erlangt haben, weil ihr Datenzugang für eine Vielzahl von Anwendungen wichtig ist. Es könnte beispielsweise vorgesehen werden, dass die Nominierung eines Unternehmens durch eine besonders hohe Zahl von Nachfragern bei der Kommission eine solche Musterbedingungspflicht auslösen könnte. Dieses Modell würde Transparenz schaffen, denjenigen, die Datenzugang begehren, einen entsprechenden Anker geben, und Rechtsstreitigkeiten abwenden.

(18) Empfohlen wird, dass Vertragsabschlüsse über Zugang bei einer offiziellen Stelle hinterlegt werden müssen, damit Nichtdiskriminierung und Angemessenheit im Einzelfall überprüft werden können. Für bedeutende Unternehmen könnte auch eine Veröffentlichungspflicht von „Tarifen" und Bedingungen vorgesehen werden.

c) Kostenerstattungsanspruch bei KMU

Ist der Datenempfänger ein KMU, darf nach Art. 9 Abs. 2 Data Act-E die Gegenleistung nicht die Kosten übersteigen, die mit der Bereitstellung der Daten unmittelbar zusammenhängen und dem Verlangen zuzurechnen sind. Welche Kosten konkret erfasst sind, ist im Data Act nicht näher definiert. Die Kosten sollten regelmäßig sehr gering ausfallen, da eine Datenübertragung kaum Kosten verursacht.

Unklarheiten bestehen jedoch noch darüber, ob außer den Kosten für die Datenübertragung noch weitere Kosten geltend gemacht werden können, z.B. Kosten für die Datenaussonderung und Bereitstellung, die Bereinigung um Geschäftsgeheimnisse oder für die Datenpflege. Nach Erwägungsgrund 45 gehören zu den Kosten der Bereitstellung die Kosten für die Reproduktion, die elektronische Verbreitung und Speicherung von Daten, nicht aber die Kosten der Datensammlung oder -produktion. Zudem sei zu berücksichtigen, dass der Dateninhaber die erforderlichen technischen Schnittstellen oder die erforderliche Software und Netzanbindung dauerhaft einrichten muss. Daraus ergibt sich, dass auch die Kosten für die Konzeption des Zugangs- und Übertragungsmechanismus erfasst sein können. Allerdings verlangt der Wortlaut eine Beschränkung auf Kosten, die *unmittelbar* mit der Bereitstellung verknüpft sind. Zudem dürfen nur solche Kosten berücksichtigt werden, die dem Datenempfänger zuzurechnen sind. Ein Dateninhaber, der ohnehin Daten sammelt und diese gelegentlich transferiert, kann also dem KMU nicht die Kosten seiner Dateninfrastruktur aufbürden. Das Kriterium der Zurechnung soll auch verhindern, dass der Dateninhaber seinen Aufwand mehrfach erstattet bekommt. Im Ergebnis wird der Kostenerstattungsanspruch bei KMU für den Dateninhaber wenig einbringen und kommerziell uninteressant sein, jedenfalls wenn dieser nur die unmittelbar dem individuellen Empfänger zuzurechnenden Kosten umfasst.

Das wirft erst recht die Frage auf, ob überhaupt eine Kompensation des Dateninhabers erforderlich ist.[152] Möglicherweise ist ein gänzlicher Verzicht auf die Erstattung oder eine pauschale Erstattung in Höhe weniger Euros zielführender als die konkrete Berechnung im Einzelfall. Der Anreiz zur Datensammlung dürfte sich für den Dateninhaber bereits selbst ergeben, sie wird jedenfalls auch nicht durch die geringen Einnahmeaussichten durch die Kompensation inzentiviert. Die Übertragung an Dritte mag den Dateninhaber aus wettbewerblichen Gründen schmerzen, sie ist jedoch im Data Act vorgesehen. Eine Anreizminderung zur Datensammlung geht davon eher nicht aus. Zugleich bietet die Kostenberechnung ein unverhältnismäßig hohes Störpotenzial. Werden hier prohibitiv hohe Kosten angesetzt, müsste regelmäßig erst entschieden werden, welche Kostenpunkte in welcher Höhe berücksichtigungsfähig sind. Das kann Zugangsansprüche erschweren und verzögern.

Darüber hinaus ist nicht nachvollziehbar, wieso der Nutzer selbst die Daten kostenlos erhalten kann (Art. 3, 4 Data Act-E), ein dritter Datenempfänger dafür jedoch an den Dateninhaber zahlen muss (Art. 8, 9 Data Act-E). Ob der Nutzer die Daten selbst weiterverwerten kann, oder ob dafür – der arbeitsteiligen Gesellschaft entsprechend – ein externer Dritter eingeschaltet wird, hat nichts mit der Frage zu tun, ob der Dateninhaber eine Gegenleistung verdient hat.[153] Wenn dem Data Act die Wertung zugrunde liegt, dass dem Nutzer die Potenziale der Nutzungsdaten zugewiesen werden sollen, ist nicht ersichtlich, wieso der Dateninhaber überhaupt berechtigt sein sollte, eine Gegenleistung zu erhalten, die über etwaige Kosten einer Datenübermittlung hinausgehen. Aus diesen Gründen sollte das System der Gegenleistung, zumindest für KMU, überdacht werden.

(19) Empfohlen wird, die Gegenleistungspflicht bei KMU grundsätzlich zu überprüfen. Soll an einer Gegenleistung festgehalten werden, könnte eine geringe pauschale Vergütung sachgerechter sein als die Auswertung der Kosten im Einzelfall.

152 Vgl. *Drexl et. al*., 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), 2022, Rn. 72; *Specht-Riemenschneider*, MMR 2022, 809, 823 f.

153 *Drexl et. al*., 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), 2022, Rn. 72.

2. Nutzungsbedingungen

Der Zugang muss zu fairen, angemessenen und nichtdiskriminierenden Bedingungen (sog. FRAND-Bedingungen) gewährt werden. In den FRAND-Verhandlungen, die im Bereich von standardessenziellen Patenten geführt werden, hat sich der Zeitfaktor als wesentliches Problem herausgestellt.[154] Selbst wenn eine Partei einen grundsätzlichen Zugangsanspruch hat, könnte ein Dateninhaber bis zur tatsächlichen Zugangsgewährung den Dritten in eine längliche vertragliche Verhandlung über Nutzungsbedingungen und Gegenleistung verwickeln. Dann würde der Datenzugangsanspruch ins Leere gehen.[155] Ob das FRAND-System sinnvoll auf die hiesigen Datenzugangsansprüche übertragen werden kann, ist fraglich.[156]

Die Regelungen, die im Data Act bislang vorgesehen sind, treten der Gefahr, dass die Aushandlung von Nutzungsbedingungen zu keinem oder zu unfairen Ergebnissen führt, nicht energisch genug entgegen.

Der Dateninhaber ist nach Art. 8 Abs. 3 Data Act-E einem Diskriminierungsverbot unterworfen, welches an das Missbrauchsrecht nach Art. 102 AEUV angelehnt ist.[157]

Aus Art. 6 Abs. 2 lit. c Data Act-E lässt sich ableiten, dass eine Bedingung unangemessen ist, die dem Datenempfänger verbietet, die Daten – im Einklang mit dem Willen des Nutzers und nur zur Erbringung eines bestimmten Dienstes – einem Dritten bereitzustellen.

Im Übrigen werden keine Vorgaben hinsichtlich der Bedingungen gemacht mit Ausnahme der Sonderregel in Art. 13 Data Act-E. Diese Vor-

154 *Picht*, Caught in the Acts – Framing Mandatory Data Access Transactions under the Data Act, further EU Digital Regulation Acts, and Competition Law, 2022, S. 27.

155 Vgl. *Drexl et. al*., 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), 2022, Rn. 84.

156 Vgl. *Schweitzer/Metzger et al*., Data access and sharing in Germany and in the EU: Towards a coherent legal framework for the emerging data economy, Final Report, 8 July 2022 (Gutachten für das Bundesministerium für Wirtschaft und Klimaschutz), S. 224 ff.

157 *Picht*, Caught in the Acts – Framing Mandatory Data Access Transactions under the Data Act, further EU Digital Regulation Acts, and Competition Law, 2022, S. 21.

schrift ist zu begrüßen.[158] Die Kommission sieht hier eine zwingende, spezifische AGB-Kontrolle vor, die die Verhandlungsgleichgewichte berücksichtigt. An dieser Vorschrift sollte festgehalten werden.

Erwogen werden sollten jedoch drei Ergänzungen:

Erstens sollte eine Sanktion vorgesehen werden, wenn ein Dateninhaber bei Aushandlung der Bedingungen eine Verzögerungstaktik einsetzt, sodass der Datenzugangsanspruch ökonomisch entwertet wird.

Zweitens sollte eine Ausweitung der Regeln in Art. 13 Data Act-E erwogen werden.[159] So könnte beispielsweise untersagt werden, dass an die Datenempfänger bestimmte quantitative oder qualitative Erwartungen gerichtet werden (z.B. dass im Rahmen einer gewissen Laufzeit der Datenzugangsvereinbarung ein bestimmter Umsatz nachgewiesen werden muss). Solche Erwartungen zu erfüllen, würde Kleinstunternehmen besonders schwerfallen. Für weitere Fälle von Missbräuchen gibt es zwar eine Generalklausel in Art. 13 Abs. 2 Data Act-E. Der Nachweis, dass ein Verstoß gegen die Generalklausel vorliegt, ist aber schwierig. Daher könnte eine Befugnis der Europäischen Kommission vorgesehen werden, diese Liste in erleichterter Form zu erweitern. Es bietet sich das Verfahren des delegierten Rechtsakts an, das in Art. 38 Data Act-E bereits für andere Fälle vorgesehen ist.

Drittens ist sicherzustellen, dass die Klauselkontrolle nach Art. 13 Data Act-E keine höheren Voraussetzungen hat als im B2C-Verhältnis. Nach Art. 13 Abs. 5 Data Act-E ist eine Klausel nur dann als einseitig auferlegt anzusehen, „wenn sie von einer Vertragspartei eingebracht wird und die andere Vertragspartei ihren Inhalt trotz des Versuchs, hierüber zu verhandeln, nicht beeinflussen kann". KMU werden durch Art. 13 Data Act-E also nur geschützt, wenn sie auch versucht haben, über den Inhalt einer Klausel zu verhandeln.[160] Anders im B2C-Bereich: Nach Art. 3 Abs. 2 RL 93/13/EWG genügt es, wenn der Verbraucher auf den Inhalt der Klausel keinen Einfluss nehmen konnte, es ist nicht erforderlich,

158 *Drexl et. al.*, 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), 2022, Rn. 120.

159 So auch ZDH, Bewertung des Kommissionsvorschlags für ein Europäisches Datengesetz KOM(2022) 68 final, 2022, S. 5.

160 *Witzel*, CR 2022, 561, 563; *Drexl et. al.*, 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), 2022, Rn. 120.

dass er einen Verhandlungsversuch unternommen hat. Diese Ungleichbehandlung erscheint nicht angemessen.[161] Insbesondere mit Blick auf kleinere Handwerksbetriebe mit ggf. wenigen Mitarbeitenden kann nicht erwartet werden, dass die unterlegene Partei einen offensichtlich aussichtslosen Versuch unternimmt, auf den Inhalt der Klausel Einfluss zu nehmen. Vielmehr sollten diese Unternehmen auch dann geschützt werden, wenn sie die Klausel einfach widerspruchslos hinnehmen, nicht zuletzt, weil sie keine ausreichenden juristischen Kenntnisse haben. Außerdem würde dies eine Klauselkontrolle in allen Fällen ausschließen, in denen die Vertragsbedingungen mit einem einfachen Klick auf „Akzeptieren" vereinbart werden.[162]

(20) Empfohlen wird, für Extremfälle der Verzögerung oder der Abschlussverweigerung eine Sanktion vorzusehen, insbesondere wenn es sich dabei um eine systematische unternehmerische Strategie handelt. Die Liste der verbotenen Klauseln in Art. 13 Data Act-E sollte überprüft und ggf. ergänzt werden. Empfohlen wird zudem, der Europäischen Kommission die Möglichkeit einzuräumen, die Liste der Beispiele in Art. 13 Abs. 3 und 4 Data Act-E durch delegierten Rechtsakt zu erweitern. Die Formulierung in Art. 13 Abs. 5 Data Act-E sollte an die des Art. 3 Abs. 2 RL 93/13/EWG angepasst werden.

3. Konkurrenzklausel

Die Konkurrenzklausel in Art. 4 Abs. 4 und Art. 6 Abs. 2 lit. e Data Act-E schützt den Dateninhaber davor, dass die Daten genutzt werden, um ein Produkt zu entwickeln, „das mit dem Produkt, von dem die Daten stammen, im Wettbewerb steht".

Zunächst ist die Legitimation dieser Konkurrenzschutzklausel fraglich: Da der Dateninhaber, wie mehrfach betont, keinen besseren Anspruch auf die Daten hat als jeder Dritte, ist fraglich, auf welcher Grundlage sich

161 So auch *Drexl et. al*., 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), 2022, Rn. 123 f.

162 *Witzel*, CR 2022, 561, 563; *Drexl et. al*., 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), 2022, Rn. 123.

ein derartiger Schutz ergeben soll. Allerdings ist einzuräumen, dass ohne eine Konkurrenzklausel der Anreiz geringer wäre, Daten zu sammeln und eine Datenteilung überhaupt zu ermöglichen. Insofern mag eine Konkurrenzklausel erwogen werden. Bemerkenswert bleibt jedoch, dass in der Datenzugangsregelung in § 20 Abs. 1a GWB eine solche Konkurrenzklausel weder im Gesetz, noch in der ausführlichen Gesetzesbegründung aufgenommen wurde.[163] Ob die positiven Wirkungen einer Konkurrenzklausel (Anreizsetzung für die Datensammlung) die negativen Wirkungen (fehlender Wettbewerb) überwiegen, lässt sich kaum ermessen. Teilweise wird vor diesem Hintergrund die Konkurrenzklausel in Frage gestellt.[164] Fraglich ist auch, ob anhand der herauszugebenden Daten wirklich relevante Rückschlüsse auf das Produkt im Wege eines „reverse engineering" gezogen werden können.[165]

Selbst wenn man den Schutz vor Wettbewerb für das Ausgangsprodukt akzeptieren mag, ergeben sich erhebliche Abgrenzungsschwierigkeiten und Umsetzungsprobleme.[166] Zunächst besteht die Gefahr, dass jedes Unternehmen, das von Datenzugang profitiert hat, bei künftigen Produktentwicklungen nachweisen muss, dass das Produkt ohne Zuhilfenahme der Daten entwickelt wurde. Die Inanspruchnahme der Daten könnte sich so als Fluch für die eigene künftige Forschung erweisen.[167] Das gilt insbesondere, wenn die Daten in Kooperationen eingebracht werden und mit weiteren Partnern geteilt werden. Es ist nicht kontrollierbar und einer dynamischen Datenwirtschaft auch nicht angemessen, die so verfügbaren Daten mit einem Nutzungsverbot für bestimmte Anwendungen zu versehen.

Überdies ist offen, ob die Abgrenzung von Produkten, die miteinander im Wettbewerb stehen, einfach möglich ist.[168] Das ist insbesondere dann

163 Vgl. BT-Drucks. 19/23492, S. 80 f.

164 *Leistner/Antoine*, IPR and the use of open data and data sharing initiatives by public and private actors, 2022, S. 15.

165 *Schweitzer/Metzger et al.*, Data access and sharing in Germany and in the EU: Towards a coherent legal framework for the emerging data economy, Final Report, 8 July 2022 (Gutachten für das Bundesministerium für Wirtschaft und Klimaschutz), S. 212.

166 *Graef/Husovec*, Seven Things to Improve in the Data Act, 2022, S. 2; DIHK, Stellungnahme zum Vorschlag für eine Verordnung über harmonisierte Vorschriften für einen fairen Datenzugang und eine faire Datennutzung (Datengesetz), 2022, S. 7.

167 Vgl. *Graef/Husovec*, Seven Things to Improve in the Data Act, 2022, S. 2.

168 *Leistner/Antoine*, IPR and the use of open data and data sharing initiatives by public and private actors, 2022, S. 15.

zweifelhaft, wenn die Innovation gerade darin besteht, das Erstprodukt fortzuentwickeln oder die Leistung des Erstprodukts in einen größeren Kontext integriert wird. Werden beispielsweise die Daten eines Roboters genutzt, der eine Tätigkeit x ausüben kann, ist dann die Entwicklung eines Roboters, der x, aber auch Tätigkeit y ausüben kann, mit dem Makel behaftet, dass der ursprüngliche Dateninhaber gefragt werden muss? Und was ist, wenn der Roboter eine Tätigkeit z verrichten kann, die x und y überflüssig macht oder integriert? Die zunächst sinnvoll scheinende Konkurrenzklausel kann bei näherer Betrachtung zu einem Hemmschuh der datengetriebenen Innovation werden, solange die Daten nicht frei genutzt und weitergegeben können und unklar ist, welche Leistungen substituierbar sind. Sie sollte grundsätzlich überdacht werden.

Im Sinne des Schutzes der Innovation auf dem Sekundärmarkt ist aber jedenfalls festzuhalten, dass Weiterentwicklungen des Ausgangsprodukts möglich sind. Der Maßstab für „Weiterentwicklung" sollte dabei nicht strenger sein als der des Europäischen Gerichts im Fall *Microsoft* für die technische Entwicklung.[169] Nicht legitim ist ein Schutz des Dateninhabers vor Wettbewerb auf dem Sekundärmarkt.[170] Konkurrenzprodukte für den Sekundärmarkt können über die Konkurrenzklausel nicht verboten werden, dies sollte klargestellt werden.

(21) Empfohlen wird, die Notwendigkeit der Konkurrenzklausel neu zu bewerten. Klargestellt werden sollte, dass Weiterentwicklungen des Ausgangsprodukts und Konkurrenzprodukte für den nachgelagerten Markt jedenfalls nicht von der Konkurrenzklausel erfasst sind.

IV. Verhältnis zu anderen Rechtsgebieten

Der Data Act-E verhält sich gegenüber anderen Rechtsvorschriften der Union defensiv. Es stellt sich die Frage, ob der Datenzugangsanspruch mit dem Schutz von Geschäftsgeheimnissen Immaterialgüterrechten (dazu 1.), mit Datenschutzrechten (dazu 2.) und Kartellrecht (dazu 3.) zusammenpasst. Im begleitenden Dokument wird zwar die Kohärenz mit beste-

169 EuG, 17.9.2007, Rs. T-201/04, ECLI:EU:T:2007:289, Rz. 647 – Microsoft.

170 So auch ZDH, Bewertung des Kommissionsvorschlags für ein Europäisches Datengesetz KOM(2022) 68 final, 2022, S. 4.

henden Rechtsakten betont.[171] Es fällt angesichts der Hypertrophie von Regelungen inzwischen aber immer schwerer zu beurteilen, ob dies nicht bloß ein frommer Wunsch des europäischen Gesetzgebers ist. Wie sich das regulatorische Puzzle im Detail zusammensetzt und ob dies noch ein einheitliches Bild ergibt, ist unklar. Diese Unklarheiten könnten benutzt werden, um legitime Datenzugangsansprüche zu torpedieren.

1. Geschäftsgeheimnisschutz und Immaterialgüterrechte

Unklarheiten bestehen zunächst hinsichtlich des Schutzes von Geschäftsgeheimnissen. Der Verordnungsentwurf knüpft an die Richtlinie (EU) 2016/943 an. Die in Art. 2 Nr. 1 RL (EU) 2016/943 enthaltene Definition von Geschäftsgeheimnissen ist jedoch sehr weit und legt die Entscheidung, ob ein Geschäftsgeheimnis vorliegt, im Wesentlichen in die Hände des Inhabers der Information. Hält dieser eine Information für schützenswert und werden entsprechende Schutzmaßnahmen ergriffen, wird die Information geschützt.[172] Umstritten ist, ob darüber hinaus auch ein berechtigtes Interesse an der Geheimhaltung bestehen muss.[173]

Ob und inwieweit Daten, die den Herausgabepflichten des Data Acts unterliegen, auch Geschäftsgeheimnisse im Sinne der RL (EU) 2016/943 sein können, ist unklar.[174] Regelungen finden sich in Art. 4 Abs. 3, 5 Abs. 8 und 8 Abs. 6 Data Act-E. Dateninhaber könnten behaupten, dass alle Daten, die sie herausgeben müssen, Geschäftsgeheimnisse sind.[175] Das würde sie zwar nicht von der Pflicht befreien, die Daten herauszugeben, sie könnten aber umfassende Schutzmaßnahmen nach Art. 5 Abs. 8 Data Act-E vom Datenempfänger verlangen, was potenziell die Nutzbarkeit beeinträchtigt oder die Vertragsverhandlungen weiter erschwert.[176] Insbe-

171 Data Act-E – Begründung, S. 4 f.
172 Siehe dazu *Alexander* in: Köhler/Bornkamm/Feddersen, UWG, 2022, § 2 GeschGehG Rn. 24.
173 Siehe dazu *Hauck* in: MüKo-Lauterkeitsrecht, Band 2, 2022, § 2 GeschGehG Rn. 62 ff.
174 DIHK, Stellungnahme zum Vorschlag für eine Verordnung über harmonisierte Vorschriften für einen fairen Datenzugang und eine faire Datennutzung (Datengesetz), 2022, S. 10.
175 ZDH, Bewertung des Kommissionsvorschlags für ein Europäisches Datengesetz KOM(2022) 68 final, 2022, S. 4.
176 *Drexl et. al.*, Position Statement of the Max Planck Institute for Innovation and Competition of 25 May 2022 on the Commission's Proposal of 23 February

sondere Verbraucher und KMU könnten mit weiteren Vertragswerken über die Geheimhaltung entweder überfordert sein – oder ihnen ohne Kenntnisnahme zustimmen.[177] Die Daten, die in erster Linie vom Data Act erfasst sind, nämlich Nutzungsdaten der Geräte, sollten grundsätzlich außerhalb des Zugriffs der Geschäftsgeheimnisrichtlinie stehen. An ihnen hat der Dateninhaber keinen Anteil, der einen besonderen Schutz zu seinen Gunsten legitimieren würde. Ein Dateninhaber kann Daten, die durch seinen Kunden erst generiert werden, nicht gegen diese zum Gegenstand seiner eigenen Geschäftsgeheimnissphäre machen.

Problematisch bleibt freilich die Nutzung von begleitenden Daten und Informationen, die möglicherweise erforderlich sind, um die Daten überhaupt nutzen zu können. Hier könnte über den Geschäftsgeheimnisschutz oder über Immaterialgüterrechte eine Herausgabe vereitelt werden. Angenommen, die Rohdaten eines Produkts können für eine Zusatzleistung auf dem nachgelagerten Markt nur ausgelesen werden, wenn dazu eine Software des Dateninhabers verwendet wird, dann könnten Informationen zu dieser Software als Geschäftsgeheimnis oder mit Hilfe von Schutzrechten aus Urheberrecht o.ä. geschützt werden. Das würde den Zugang de facto erheblich erschweren oder verteuern. Dem ist entgegenzuwirken, indem entweder Zugang zu diesen Hilfsmitteln gewährt wird und/oder ergänzend die missbräuchliche Geltendmachung solcher Nebendienste sanktioniert wird.

Auf den ersten Blick besteht ein Widerspruch zwischen Art. 5 Abs. 8 Data Act-E und Art. 8 Abs. 6 Data Act-E.[178] In Art. 5 Abs. 8 heißt es, dass Geschäftsgeheimnisse insoweit offengelegt werden, wie dies für den zwischen dem Nutzer und dem Dritten vereinbarten Zweck unbedingt erforderlich ist und alle notwendigen Schutzmaßnahmen gewahrt sind. Eine inhaltlich identische Formulierung findet sich auch in Art. 4 Abs. 3 Data Act-E. Daraus lässt sich ableiten, dass auch Daten, die als Geschäftsgeheimnisse anzusehen sind, im Rahmen des Data Acts herauszugeben sind. Der Zugangsanspruch „trumpft" hier sozusagen den Geschäftsgeheimnisschutz. Auf den ersten Blick widersprüchlich heißt es aber dann in Art. 8 Abs. 6 Data Act-E, dass die Pflicht, einem Datenempfänger Daten

---

2022 for a Regulation on harmonised rules on fair access to and use of data (Data Act), 2022, Rn. 283.

177 Vgl. *Hennemann/Steinrötter*, NJW 2022, 1481, 1484.

178 So auch BDI, Stellungnahme zum Legislativvorschlag des EU-Data Act, 2022, S. 14 und *Demary*, Der Data Act - Welchen Rahmen Unternehmen für Data Sharing wirklich brauchen: Beitrag zum Vorschlag der EU-Kommission, 2022, S. 10, die allerdings einen stärkeren Schutz von Geschäftsgeheimnissen fordern.

bereitzustellen, nicht zur Offenlegung von Geschäftsgeheimnissen i.S.d. Richtlinie (EU) 2016/943 verpflichtet. Im nächsten Halbsatz wird klargestellt, dass das nicht gilt, soweit im Data Act etwas anderes vorgesehen ist, wobei ausdrücklich („einschließlich") auf Art. 6 Data Act-E verwiesen wird. Wieso auf Art. 6 Data Act-E und nicht Art. 4, 5 Data Act-E verwiesen wird, leuchtet nicht ein. Da Art. 6 Data Act-E aber die Pflichten des Datenempfängers in den Fällen des Art. 5 Data Act-E regeln, ist davon auszugehen, dass es sich dabei um ein redaktionelles Versehen handelt.

Welchen Zweck Art. 8 Abs. 6 Data Act-E hat, wird nicht klar. Er hat wohl lediglich deklaratorische Funktion, da ohnehin keine Verpflichtung zur Herausgabe von Geschäftsgeheimnissen an Datenempfänger besteht, solange das nicht im Unionsrecht vorgesehen ist (wie etwa in Art. 5 Abs. 8 Data Act-E). Die Regelung stellt daher wohl lediglich klar, dass die Existenz des Data Act nichts daran ändert, dass die Daten grundsätzlich nach wie vor dem Geschäftsgeheimnisschutz unterliegen.[179] Sie schränkt die Datenzugangsansprüche des Data Acts nicht ein. Das sollte klargestellt werden.[180]

(22) Empfohlen wird eine Klarstellung, dass Daten, die durch den Nutzer generiert werden, keine Geschäftsgeheimnisse sein können. Der Zugang zu Hilfsmitteln, die zur Datenentschlüsselung erforderlich sind, darf vom Dateninhaber nicht unter Berufung auf Geschäftsgeheimnisse oder Immaterialgüterrechte verweigert werden. Empfohlen wird, den Widerspruch in Art. 8 Abs. 6 zu Art. 5 Abs. 8 Data Act-E zugunsten der Formulierung in Art. 5 Abs. 8 aufzulösen.

Soweit der oben geforderten Einführung eines zweckorientierten Zugangsanspruchs gefolgt wird, stellen sich verstärkt Fragen zum Geschäftsgeheimnisschutz. Auch wenn unmittelbare (rohe) Nutzungsdaten nicht als Geschäftsgeheimnisse angesehen werden, kann dies bei derivativen und aggregierten Daten sowie erst Recht bei Software und Tools der Fall sein. Dies steht einem verpflichtenden Zugangsanspruch nicht entgegen. Der Schutz von Geschäftsgeheimnissen verleiht dem Inhaber kein Ausschließ-

179 Dafür spricht auch Erwägungsgrund 62, allerdings bezieht sich dieser originär auf die Herausgabepflichten zugunsten öffentlicher Stellen.

180 So auch *Schweitzer/Metzger et al.*, Data access and sharing in Germany and in the EU: Towards a coherent legal framework for the emerging data economy, Final Report, 8 July 2022 (Gutachten für das Bundesministerium für Wirtschaft und Klimaschutz), S. 233.

lichkeitsrecht, dessen Durchbrechen besonders rechtfertigungsbedürftig ist.[181] Vielmehr geht es schon nach Art. 1 Abs. 1 RL (EU) 2016/943 nur darum, bestimmte unlautere Geheimnistransfers zu unterbinden, z.B. Industriespionage.[182] Dem Gesetzgeber, zumal dem europäischen Gesetzgeber, ist damit unbenommen, den Inhaber von Geschäftsgeheimnissen zur Freigabe dieser Geheimnisse zu verpflichten.

Der Data Act-E sieht eine schonende Verpflichtung zur Freigabe von Geschäftsgeheimnissen vor, da nach Art. 5 Abs. 8 Data Act-E Geschäftsgeheimnisse nur unter Vereinbarung angemessener Schutzmaßnahmen offengelegt werden müssen. Dieser Grundsatz erscheint auch für den Schutz von derivativen und aggregierten Daten sowie Software und Tools angemessen.

2. Datenschutzrecht

Für die Datenschutz-Grundverordnung (VO (EU) 2016/679) (DSGVO) wird in Art. 1 Abs. 3 S. 2 Data Act-E festgestellt, dass der Data Act die darin getroffenen Vorgaben nicht berührt, was bedeuten soll, dass die Vorgaben der DSGVO weiterhin einzuhalten sind (siehe auch 4 Abs. 5 und 6, 5 Abs. 6, 7 und 9 Data Act-E). Das bedeutet, dass Daten, die Rückschlüsse auf natürliche Personen zulassen, nur weitergegeben und verarbeitet werden dürfen, wenn einer der Erlaubnistatbestände des Art. 6 DSGVO erfüllt ist.[183] Es genügt insoweit die Einwilligung des Nutzers (Art. 6 Abs. 1 lit. a DSGVO). Allerdings muss die Einwilligung den Kriterien genügen, die für das Datenschutzrecht etabliert sind, und die in der Praxis häufig nicht eingehalten werden. Gleichzeitig stellt das Datenschutzrecht schon bislang ein Hemmnis für die gemeinsame Datennutzung dar.[184]

Während eine Einwilligung vom Nutzer, der das Gerät erworben hat, regelmäßig noch vorliegen dürfte, ist die Frage, ob dies auch für weitere Nutzer gilt, z.B. Familienangehörige, die das Gerät benutzen, Gäste oder

181 Vgl. Erwägungsgrund 16 RL (EU) 2016/943.

182 Vgl. *Alexander* in: Köhler/Bornkamm/Feddersen, UWG, 2022, § 4 GeschGehG Rn. 16.

183 Siehe zum Datenschutzrecht im IoT auch *Krönke*, Öffentliches Digitalwirtschaftsrecht, 2020, S. 236 ff.

184 BDI, Stellungnahme zum Legislativvorschlag des EU-Data Act, 2022, S. 5; DIHK, Stellungnahme zum Vorschlag für eine Verordnung über harmonisierte Vorschriften für einen fairen Datenzugang und eine faire Datennutzung (Datengesetz), 2022, S. 11.

Personen, denen das Gerät überlassen wird.[185] Hier entstehen rechtliche Unsicherheiten.[186] Diese können umgangen werden, wenn durch Profil-Anmeldungen und neue Einwilligungen jeder Nutzer gesondert vom Gerät erfasst wird. Denkbar wäre auch eine Ausdehnung der Einwilligungslösung für den IoT-Bereich als Ergänzung der DSGVO für smarte Geräte bei gelegentlicher Überlassung.[187] Das Zustimmungsmanagement, dessen Orientierung an den DSGVO-Vorgaben oben bereits empfohlen wurde, kann die Probleme ggf. ausräumen.

(23) Empfohlen wird, dass die datenschutzrechtliche Rechtsunsicherheit bei der Nutzung der Geräte durch andere Personen als den ursprünglichen Erwerber aufgelöst wird.

Nur ergänzend ist darauf hinzuweisen, dass die Möglichkeiten in Art. 6 DSGVO zur Berechtigung weiterreichen als gelegentlich suggeriert wird. In Vertragsverhältnissen gibt Art. 6 Abs. 1 lit. b DSGVO die Möglichkeit zur Datenverarbeitung. Wenn eine rechtliche Verpflichtung besteht (etwa im Data Act), kann auch Art. 6 Abs. 1 lit. c DSGVO herangezogen werden. Angesichts der erheblichen Innovationspotentiale einerseits und der eher geringfügigen Bedeutung der Nutzerdaten ist anzunehmen, dass auch die Abwägung der berechtigten Interessen nach Art. 6 Abs. 1 lit. f DSGVO ggf. zugunsten der Datenverarbeitung ausgehen kann. Für anonymisierte Daten, die gerade für Anwendungen genügen werden, die nicht unmittelbar beim Nutzer anknüpfen, ist die DSGVO ohnehin schon nicht anwendbar. Deren „Störpotential" für die Datenteilung nach dem Data Act sollte insoweit nicht überzeichnet werden.

185 BDI, Stellungnahme zum Legislativvorschlag des EU-Data Act, 2022, S. 5. Siehe bereits oben.

186 Zu Unklarheiten im Zusammenspiel mit der DSGVO siehe *Graef/Husovec*, Seven Things to Improve in the Data Act, 2022, S. 1; ZDH, Bewertung des Kommissionsvorschlags für ein Europäisches Datengesetz KOM(2022) 68 final, 2022, S. 3; *Spajic/Lalova-Spinks* in: Ducuing/Margoni/Schirru, White Paper on the Data Act Proposal, CITIP Working Paper Series, 2022, S. 30; *Staudenmayer*, EuZW 2022, 1037, 1040.

187 Vgl. auch *Bomhard/Merkle*, RDi 2022, 168, 176.

3. Kartellrecht

Kartellrechtliche Bedenken können sich eventuell daraus ergeben, dass im Informationsaustausch zwischen Unternehmen ein Verstoß gegen das Verbot wettbewerbsbeschränkender Vereinbarungen (Art. 101 AEUV) gesehen werden kann.[188] Auch die Kommission geht im Vorschlag zum Data Act davon aus, dass in „der gemeinsamen Nutzung von Daten durch Unternehmen" ein Verstoß gegen Wettbewerbsrecht liegen kann oder eine berechtigte Verweigerung des Zugriffs auf Daten aus Wettbewerbsrecht folgen kann.[189] Zu denken ist etwa an die Konstellation, dass sich Wettbewerber gegenseitig über den Data Act Datenzugangsrechte einräumen und damit wettbewerblich sensitive Informationen (z.B. über Kundenbeziehungen) austauschen. Es entstehen Unsicherheiten, wie weitgehend Daten ausgetauscht werden können. Dateninhaber könnten den Verweis auf kartellrechtliche Risiken nutzen, um sich der Datenweitergabe zu entziehen. Das würde möglicherweise Verzögerungen oder Verweigerungen mit sich bringen, die für den Wettbewerb auf dem nachgelagerten Markt schädlich sind. Die Europäische Kommission hat bislang keine Neigung erkennen lassen, Datenkooperationen und Datenpools in stärkerer Weise zuzulassen als bislang. Damit kann das Kartellrecht zum Stolperstein des Datenzugangs werden. Im Data Act-E selbst wird das Problem kaum gelöst werden können, da Art. 101 AEUV als unmittelbar geltendes Primärrecht dem Sekundärakt vorrangig ist. Eine Lösung dafür sollte durch eine Lockerung des kartellrechtlichen Zugriffs auf Datenpools im Kartellrecht gesucht werden.[190]

(24) Empfohlen wird, in den kartellrechtlichen Leitlinien eine klarere Grenzziehung zwischen erlaubter und verbotener Datenweitergabe zu treffen.

188 Siehe dazu im Einzelnen *Brauneck*, WRP 2022, 954, 958 ff. Vgl. zum Informationsaustausch im Kartellrecht grundlegend EuGH, 23.11.2006, Rs. C-238/05, ECLI:EU:C:2006:734 – *Asnef Equifax*; Europäische Kommission, Leitlinien zur Anwendung von Art. 81 Abs. 3 EG-Vertrag, (2004/C 101/08), Rn. 56.

189 Data Act-E – Begründung, S. 5, 12.

190 Ähnlich *Demary*, Der Data Act - Welchen Rahmen Unternehmen für Data Sharing wirklich brauchen: Beitrag zum Vorschlag der EU-Kommission, 2022, S. 10 f.

V. Rechtsdurchsetzung und Streitbeilegung

Der Erfolg des Data Acts hängt letztlich von der Rechtsdurchsetzung ab. Nur eine – im Notfall – effektive Rechtsdurchsetzung kann auch im Vorfeld sinnvolle Verhandlungen ermöglichen.

1. Unklare Rechtsfolgen

Die Durchsetzung bestehender Rechte nach dem Data Act ist unvollständig geregelt. Wenn Hersteller ihre Produkte entgegen Art. 3 Abs. 1 Data Act-E nicht zugangsfreundlich gestalten oder wenn sie Dritten den Datenzugang verweigern, stellt sich die Frage nach den möglichen Abhilfemaßnahmen. Im Data Act ist vorgesehen, dass durch Behörden Bußgelder verhängt werden können (Art. 33 Data Act-E). Bußgelder werden jedoch erst die Folge langfristig angelegter behördlicher Verfahren sein. Zügige Abhilfe schaffen sie im Zweifel nicht.

In diesem Fall sind privatrechtliche Mechanismen (einstweilige Verfügung auf Unterlassung der Zugangsverweigerung, ggf. Schadensersatz) erforderlich. Derartige Rechtsfolgen werden im Entwurf jedoch nicht explizit benannt.[191] Sie können sich zwar aus dem allgemeinen Privatrecht ergeben. Für die Durchsetzung wäre jedoch hilfreich, wenn im Data Act selbst entsprechende Vorkehrungen getroffen werden, um die Rechtsfindung vor den Gerichten auf nationaler Ebene (und in der Kontrolle beim EuGH) zu erleichtern. Dabei dürfte anzunehmen sein, dass die Dringlichkeit des Anspruchs stets zu bejahen ist, was – im deutschen Zivilprozessrecht – damit stets einen Verfügungsgrund geben dürfte.[192]

Der Anspruch müsste dem Datenempfänger selbst zustehen und nicht vom Nutzer abhängen. Es ist nicht zumutbar, dass beispielsweise ein Handwerksbetrieb, der Zugang zu den Daten einer Heizungsanlage begehrt, seinen Kunden (den Inhaber der Heizungsanlage) in eine zugangsrechtliche Klage gegen den Dateninhaber hereinzieht.

---

191 Vgl. *Bomhard/Merkle*, RDi 2022, 168, 175; *Drexl et. al.*, 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), 2022, Rn. 78.

192 Eine entsprechende gesetzliche Regelung im deutschen Recht enthält § 12 Abs. 1 UWG.

(25) Empfohlen wird, die privatrechtlichen Sanktionen und Möglichkeiten im Data Act klarer herauszustellen, ggf. in Erwägungsgründen. Dritte müssen aus eigenem Recht gegen Beschränkungen des Datenzugangs vorgehen können und dazu den Weg des einstweiligen Rechtsschutzes nutzen können.

2. Stärkung des Streitbeilegungsmechanismus

Im Falle privatrechtlicher Auseinandersetzungen steht den Beteiligten gem. Art. 10 Data Act-E der Gang zu Streitbeilegungsstellen offen, die zügig und spezialisiert über Ansprüche nach dem Data Act entscheiden sollen. Der Weg dorthin kann allerdings nur konsensual beschritten werden. Weigert sich ein Dateninhaber oder ein Datenempfänger (Abs. 8), steht nur der ordentliche Rechtsweg zur Verfügung.

Damit droht gerade in konfrontativen Fällen eine Verschleppungstaktik des Dateninhabers. Dieser kann ggf. die Klaviatur der Justiz bespielen, die zuweilen zu lange braucht, um das Problem effizient zu lösen. Will man eine zügige außergerichtliche Kontrolle fördern, kommen folgende Erwägungen in Betracht:

- Die Teilnahme am Streitbeilegungsverfahren könnte verpflichtend gemacht werden.[193] Erst im Anschluss an ein Streitbeilegungsverfahren wäre der Rechtsweg zu den ordentlichen Gerichten eröffnet. Soweit zulässig,[194] könnte dabei ein eingeschränkter Überprüfungsrahmen für die ordentlichen Gerichte vorgesehen werden. Der Streitbeilegungsinstanz wäre dann – wie einer Behörde – ein Beurteilungsspielraum gegeben.
- Die Teilnahme am Streitbeilegungsverfahren könnte attraktiver gestaltet werden, indem Dateninhaber, die sich freiwillig an ein solches schnelles Verfahren binden und dessen Entscheidungen respektieren, nicht in gleicher Weise an andere Regeln gebunden würden. So könnte z.B. eine Bindung an die Streitbeilegung dadurch kompensiert werden, dass bestimmte Verträge nicht offengelegt werden müssen. Da Bedin-

193 Ähnlich *Specht-Riemenschneider*, MMR 2022, 809, 824, die eine Bindungswirkung sowie Kostenneutralität bei Verfahren unter Beteiligung von Verbrauchern oder Kleinst- und Kleinunternehmen fordert.

194 Dem EuGH bleibt die Auslegung europäischen Rechts vorbehalten. Der Weg zu den ordentlichen Gerichten muss aus grundrechtlichen Erwägungen offenstehen. Vgl. dazu *Staudenmayer*, EuZW 2022, 1037, 1042.

gungen zügig überprüfbar sind, könnten diese großzügiger gehandhabt werden.
- Den Mitgliedsstaaten könnten Vorgaben für die Ausgestaltung von Streitverfahren nach dem Data Act gemacht werden, so wie in vergleichbarer Form das Kartellschadensersatzrecht durch eine EU-Richtlinie effektiviert wurde (umgesetzt in §§ 33 ff. GWB).[195] Kläger werden demnach gegenüber dem allgemeinen Zivilrecht erheblich privilegiert. Die Verfahren sind bei besonders kompetenten Spruchkörpern konzentriert (vgl. §§ 87, 89 GWB). Denkbar wäre auch, dass der nationale Gesetzgeber von sich aus die private Rechtsdurchsetzung auf nationaler Ebene erleichtert. So ist für die Rechte von Nutzerinnen und Nutzern aus dem Digital Markets Act (DMA) im Referentenentwurf zur 11. GWB-Novelle eine entsprechende Übernahme der kartellrechtlichen Sonderregeln für das private enforcement auch des DMA geplant.[196]

Wesentlich ist, dass die Zugangsansprüche nicht durch monatelange Rechtsfindung verschleppt werden.

(26) Empfohlen wird, die Mechanismen für eine zügige, wirkungsvolle Lösung von Streitfragen zu verbessern, indem die Teilnahme am Streitbeilegungsmechanismus verpflichtend wird oder Anreize zur Selbstbindung gesetzt werden. Die private Rechtsdurchsetzung könnte auch im nationalen Rahmen – entsprechend den kartellrechtlichen Regeln – erleichtert werden.

3. Ausweitung der Zuständigkeit des Streitbeilegungsmechanismus

Nach Art. 10 Data Act-E entscheidet die Streitbeilegungsstelle nur über Streitigkeiten in Bezug auf die Festlegung fairer, angemessener und nichtdiskriminierender Bedingungen für die Bereitstellung von Daten und die transparente Art und Weise der Bereitstellung von Daten nach Art. 8 und 9. Nötig wäre aber auch ein Streitbeilegungsmechanismus

195 Vgl. Richtlinie 2014/104/EU des Europäischen Parlaments und des Rates vom 26. November 2014 über bestimmte Vorschriften für Schadensersatzklagen nach nationalem Recht wegen Zuwiderhandlungen gegen wettbewerbsrechtliche Bestimmungen der Mitgliedstaaten und der Europäischen Union (sog. Kartellschadensersatzrichtlinie).

196 BMWK, Referentenentwurf zum Wettbewerbsdurchsetzungsgesetz, 26.9.2022, S. 17 f.

zum Umfang der benötigten Daten.[197] Zwischen Dateninhaber und -empfänger könnten auch Streitigkeiten darüber entstehen, welche Daten für den jeweiligen Nutzungszweck überhaupt erforderlich sind. Gerade für solche Fragen bieten sich Streitbeilegungsstellen mit Geheimhaltungsvereinbarungen an.[198] Da die Streitbeilegungsstellen, jedenfalls nach dem Kommissionsentwurf, ohnehin nur mit Einverständnis der Parteien tätig werden, ist nicht ersichtlich, wieso ihr Entscheidungsmandat beschränkt sein sollte.[199] Durch eine Ausweitung auf alle Rechtsfragen wird die Inanspruchnahme der Streitbeilegungsstelle insgesamt attraktiver.[200] Der sachliche Anwendungsbereich der Streitbeilegung sollte also ausgeweitet werden.[201]

(27) Empfohlen wird, die Zuständigkeit der Streitbeilegungsstellen in Art. 10 Data Act-E auf alle Fragen auszudehnen, die im Zusammenhang mit dem Datenzugang auftreten.

197 *Graef/Husovec*, Seven Things to Improve in the Data Act, 2022, S. 4.
198 *Graef/Husovec*, Seven Things to Improve in the Data Act, 2022, S. 4.
199 *Graef/Husovec*, Seven Things to Improve in the Data Act, 2022, S. 4.
200 *Drexl et. al*., 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), 2022, Rn. 108.
201 So auch *Graef/Husovec*, Seven Things to Improve in the Data Act, 2022, S. 4; *Drexl et. al*., 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), 2022, Rn. 108; *Gerpott*, CR 2022, 271, 279.