TRANSPORTRECHT

Zeitschrift für das gesamte Recht der Güterbeförderung, Spedition, Versicherungen des Transports, Personenbeförderung und Reiseveranstaltung

Heft 4 · April 2023
46. Jahrgang · Seiten 157–208

Herausgeber:
Rechtsanwalt Prof. Dr. Rolf Herber †
Rechtsanwalt Dr. Tobias Eckardt
in Soz. Ahlers & Vogel
Hafenstraße 6, 26789 Leer
E-Mail: eckardt@ahlers-vogel.de

# Der neue EU Data Act – Auswirkungen auf Telematikdaten (2)

Professor Dr. Thomas Hoeren und Rechtsreferendarin Jessica Baumann, Münster

Im ersten[1] Teil des Beitrags wurde die Grundstruktur des Data Act samt neuer relevanter Begriffe sowie die sich aus dem Data Act ergebenden Rechte und Pflichten erläutert und die Möglichkeiten und Grenzen der Bereitstellung von Daten dargestellt. Im zweiten Teil werden die Rechte und Pflichten aus dem Data Act auf ein Praxisbeispiel in Form eines die EU-Grenzen überquerenden Kühl-Transports angewendet. Hierbei werden die sich aus dem Data Act ergebenen Möglichkeiten, aber auch die Schwächen des Verordnungsentwurfs dargestellt.

## 1. Einleitung

Wie im ersten Teil des Beitrags bereits festgestellt, könnten die Regelungen des Data Act für viele Unternehmen in der Praxis Belastungen darstellen und weitere Rechtsfragen nach sich ziehen. Dies gilt insbesondere für Transport-Unternehmen im Rahmen der Erzeugung, Speicherung und Verarbeitung von Telematikdaten.

Moderne Trailer sind schon lange keine reinen »Transporthüllen« mehr, sondern im Inneren voller Technik ausgestattet, u.a. zur Datengewinnung. Ein vernetzter Trailer bzw. das eingebaute Telematiksteuerungssystem sammelt bei der Verwendung des Trailers Daten und leitet diese an das Datenmanagementportal des jeweiligen Herstellers weiter (häufig ein »Cloud«-System), von dem aus die Daten zur Bereitstellung auf der jeweiligen Benutzeroberfläche verarbeitet werden. Durch die Auswertung der umfangreichen, durch das Telematiksteuerungssystem erzeugten Daten können die »smarten Trailer« u.a. die internen Prozesse des Transportunternehmens optimieren und auch die digitale Transformation der Auftraggeber unterstützen.

Die erzeugten Daten sind mannigfaltig, können aber grob in drei Kategorien eingeteilt werden: Zunächst werden Daten über das Fahrzeug und den Trailer selbst erhoben, z.B. die Position des Fahrzeugs bzw. des Trailers oder die Fahrgeschwindigkeit. Des Weiteren fallen technische Daten an, bspw. können technische Probleme erkannt werden, die eine Wartung von Fahrzeug und/oder Trailer erfordern. Über dies hinaus können Daten die Ladung betreffend erzeugt werden, insbesondere bei Kühl-Trailern über die Temperaturen der Ladung in den verschiedenen Ladezonen oder auch die Anzahl der Türöffnungen.

Fraglich ist zunächst, ob die durch ein Telematiksteuerungssystem erhobenen Daten überhaupt in den (sachlichen) Anwendungsbereich des Data Act fallen. Gemäß Art. 2 Nr. 1 Data Act sind Daten i.S.d. Data Act grundsätzlich solche, die durch die Nutzung eines Produkts oder verbundener Dienste generiert werden.[2] Daraus folgt, dass der Data Act Daten nicht mit »Informationen« gleichstellt, sondern als »Transporteur« von Informationen versteht.[3] »Produkte« werden in Art. 2 Nr. 2 Data Act als körperliche Gegenstände definiert, welche über ihre Nutzung oder Umgebung Daten erlangen, erzeugen oder übermitteln. Bestimmte Arten von Produkten werden allerdings nicht erfasst: So sind Produkte, deren Hauptfunktion die Speicherung und Verarbeitung von Daten ist, keine Produkte i.S.d. Data Act,[4] ebenso Produkte, die in erster Linie dazu bestimmt sind, Inhalte anzuzeigen oder abzuspielen (wie Tablets, Smartphones, Webcams).[5] Außerdem werden derivative Daten (solche, die durch einen Softwareprozess von den Rohdaten abgeleitet werden) vom Anwendungsbereich ausgeschlossen, mit dem Argument, dass der Prozess durch Datenableitung Rechten des geistigen Eigentums unterliegen kann.[6]

Das Telematiksteuerungssystem eines Kühl-Trailers fällt nicht unter die vom Anwendungsbereich des Data Act ausgeschlossenen Produkte. Die im Telematiksteuerungssystem integrierte Software, die die gesammelten Daten an das Datenmanagementportal des jeweiligen Herstellers weiterleitet, fällt unter den Begriff des »verbundenen Diensts« gem. Art. 2 Nr. 3 Data Act. Somit finden die Regelungen des Data Act auf Telematikdaten, die durch die Durchführung von (Kühl-) Transporten erzeugt werden, Anwendung. Dies führt zu praxisrelevanten Folgefragen bezüglich der sich nun ergebenden Rechte und Pflichten der an der Durchführung eines solchen (Kühl-)Transports beteiligten Personen.

## 2. Ein praktisches Fall-Beispiel: Der Kühl-Trailertransport von der Schweiz nach Deutschland

An einem praktischen Fall-Beispiel soll veranschaulicht werden, welche Pflichten sich aus dem Data Act ergeben und welche weiteren Rechtsfragen auftauchen.

Ein Auftraggeber, z.B. ein in Deutschland ansässiges Unternehmen aus der Lebensmittelbranche, wendet sich an ein ebenfalls in Deutschland ansässiges, weltweit agierendes Transportunter-

1 Hier Quelle des ersten Teils des Beitrags aus der Zeitschrift »Transportrecht«.

2 *Podszun/Pfeifer*, GRUR 2022, 953 (955).

3 *Karsten/Wienroeder*, RAW 2/22, 99 (100); *Hennemann/Steinrötter*, NJW 2022, 1481 (1482).

4 Art. 2 Nr. 2 a.E.

5 Erwägungsgrund 15 Data Act.

6 Erwägungsgrund 17 Data Act; hierzu kritisch: *Specht-Riemenschneider*, MMR 2022, 809 (820).

nehmen und erteilt den Auftrag, eine Ladung Kühlware aus der Schweiz nach Deutschland zu transportieren. Das Transportunternehmen verfügt über sich bereits in der Schweiz befindende Kühltrailer und bereitet den Transport vor. Damit die Ware während des Transports optimal gekühlt werden kann, befindet sich an der Trailerstirnwand ein Kühlgerät. Die Ware wird in dem Kühltrailer durch einen Frachtführer des Transportunternehmens planmäßig aus der Schweiz nach Deutschland transportiert und kommt beim Auftraggeber an.

Ab der Vorbereitung des Transports in der Schweiz und während des Transports nach Deutschland werden durch die Nutzung des Kühlgeräts sowie durch die im Trailer vorhandene Telematik-Hardware Daten erfasst, bspw. Positionsdaten des Kühltrailers, Temperaturdaten aus dem Kühltrailer, Temperaturdaten aus der äußeren Umgebung oder auch die Anzahl der Türöffnungen. Das Transportunternehmen speichert und verwaltet alle Telematikdaten mit Hilfe einer vom Hersteller des Telematikdatensystems zur Verfügung gestellten cloudbasierten Software.

Im Folgenden wenden sich sowohl der Hersteller des an der Trailerstirnwand angebrachten Kühlgeräts als auch der Auftraggeber an das Transportunternehmen, mit der Bitte, die gesamten Telematikdaten des Transports ab der Schweiz zur Verfügung zu stellen.

Für das Transportunternehmen stellen sich nun verschiedene Fragen: Unterliegen auch die in der Schweiz aufgezeichneten Daten den Bestimmungen des Data Act? Wie ist die Rollenverteilung der verschiedenen Akteure gem. Art. 2 Data Act? Wie und unter welchen Bedingungen können der Hersteller des Kühlgeräts sowie der Auftraggeber die gewünschten Datenrechte erhalten? Wie kann sich das Transportunternehmen bezüglich seiner Pflichten rechtlich am besten absichern?

Diesen Fragen soll im Folgenden nachgegangen werden.

## 3. Räumlicher Anwendungsbereich des Data Act: Fallen auch Daten, die außerhalb der EU erzeugt wurden, unter den Data Act?

Zunächst stellt sich die Frage nach dem Anwendungsbereich des Data Act. Dieser wird in Art. 1 Data Act festgelegt, aus dem sich auch das Ziel des Data Act, das bessere Verfügbarmachen von Daten, deutlich herauslesen lässt. Der sachliche Anwendungsbereich gem. Art. 1 Abs. 1 Data Act umfasst Daten i.S.d. Art. 2 Nr. 1 Data Act (s.o.). In Art. 1 Abs. 2 Data Act finden sich sowohl der räumliche als auch der persönliche Anwendungsbereich: Dabei folgt der räumliche Anwendungsbereich – ebenso wie der Data Govenance Act (DGA)[7] und die Datenschutzgrundverordnung (DSGVO)[8] – dem im Datenwirtschaftsrecht üblichen Marktortprinzip, Art. 1 Abs. 2 Data Act.[9] In persönlicher Hinsicht richtet sich der Data Act an die in Art. 1 Abs. 2 genannten Personen und Stellen.

Gemäß des Marktortsprinzips, welches erstmals durch die DSGVO eingeführt wurde (Art. 3 Abs. 2 DSGVO), erstrecken sich die Vorgaben des europäischen Datenschutzrechts auch auf solche Verantwortliche oder Auftragsverarbeiter, die nicht in der Union niedergelassen sind, aber betroffenen Personen in der Union Waren oder Dienstleistungen anbieten oder deren Verhalten beobachten.[10] Sinn und Zweck des Marktortprinzips der DSGVO ist die Sicherstellung des europäischen Datenschutzniveaus: Immer, wenn für ein Produkt oder eine Dienstleistung Daten mit Binnenmarktbezug erhoben und verarbeitet werden, muss ein entsprechendes Datenschutzniveau der DSGVO gewährleistet werden, und zwar unabhängig davon, wo diese Daten lokal verarbeitet werden.[11] Daraus folgt, dass für eine Anwendung des Data Act die Daten nicht zwangsläufig innerhalb der EU erhoben bzw. erzeugt werden müssen, sondern die Daten müssen einen Bezug zum Binnenmarkt haben, etwa weil sich gem. Art. 1 Abs. 2 Buchst. c) Data Act der Datenempfänger, dem Daten bereitgestellt werden, in der EU befindet. Das Augenmerk auf den Binnenmarktbezug zu legen, entspricht auch der Datenstrategie der EU: »*Ziel ist die Schaffung eines einheitlichen europäischen Datenraums, eines echten Binnenmarkts für Daten, der für Daten aus aller Welt offensteht, in dem sowohl personenbezogene als auch nicht-personenbezogene Daten, darunter auch sensible Geschäftsdaten, sicher sind und in dem Unternehmen auch leicht Zugang zu einer nahezu unbegrenzten Menge hochwertiger industrieller Daten erhalten.*«[12] Auf der anderen Seite wird durch das Erfordernis des Binnenmarktbezugs auch ein vollkommen ausufernder Anwendungsbereich verhindert: Ohne die Erfordernis eines Binnenmarktbezugs könnte z.B. Art. 1 Abs. 2 Buchst. d) Data Act derart zu verstehen sein, dass öffentliche Stellen auch auf Dateninhaber ohne Binnenmarktbezug weltweit zugreifen könnten.[13] Auf das o.g. Fall-Beispiel bezogen bedeutet dies, dass die Daten, die der Kühl-Trailertransport ab der Schweiz generiert, in den Anwendungsbereich des Data Act fallen, alle von dem Transport betroffenen Personen haben einen Binnenmarktbezug.

Auffällig ist, dass es keine intertemporale Regelung des Anwendungsbereichs gibt.[14] Der Data Act äußert sich nicht dazu, wie Daten nach Geltungsbeginn des Data Act zu behandeln sind, die bereits vor Geltungsbeginn erhoben wurden. Hier gibt es Nachbesserungsbedarf.

## 4. Die Begriffsbestimmungen des Data Act: Wer ist in welcher Rolle?

Bezüglich des o.g. praktischen Fall-Beispiels stellt sich des Weiteren die Frage, welcher der Akteure in welcher Rolle i.S.d. Art. 2 ff. Data Act ist.

### a) »Nutzer« i.S.d. Art. 2 Nr. 5 Data Act

Gem. Art. 3 Abs. 1 Data Act sollen Produkte so konzipiert und hergestellt und verbundene Dienste so erbracht werden, dass die bei Nutzung erzeugten Daten für den Nutzer direkt zugänglich sind. Es wird somit grundsätzlich von einem direkten Datenzugriff durch den Nutzer ausgegangen. Abgesehen davon, dass ein direkter Datenzugriff der Nutzer auch »relevant und angemessen« sein muss, wird aus Art. 3 Abs. 1

7 *Hennemann/von Ditfurth*, NJW 2022, 1905 Rn. 12.

8 Kühling/Buchner/*Klar*, DS-GVO, Art. 3 Rn. 3; Paal/Pauly/*Ernst*, DS-GVO, Art. 3 Rn. 13.

9 *Hennemann/Steinrötter*, NJW 2022, 1481 (1482); *Specht-Riemenschneider*, MMR 2022, 809 (812).

10 Kühling/Buchner/*Klar*, DS-GVO, Art. 3 Rn. 3; Taeger/Gabel/*Schmidt*, DS-GVO, Art. 3 Rn. 16.

11 Taeger/Gabel/*Schmidt*, DS-GVO, Art. 3 Rn. 16; Sydow/Marsch/*Ennöckl*, DS-GVO, Art. 3 Rn. 13.

12 COM(2020) 66 final S. 5.

13 *Hennemann/Steinrötter*, NJW 2022, 1481 (1482).

14 *Bomhard/Merkle*, RDi 2022, 168 (175).

Data Act nicht deutlich, was »zugänglich« bedeutet. Aus Erwägungsgrund 21 ergibt sich, dass Zugang zu Daten bereits gewährt wird, wenn Daten eingesehen werden können, bspw. innerhalb eines vom Dateninhaber gesteuerten Programms oder eines Cloud-Dienstanbieters.[15] Ob »Zugang« i.S.d. Art. 3 Abs. 1 Data Act etwas anderes bedeuten soll als »Zugriff«, wird durch die Verordnung nicht klargestellt. Das Wort »zugreifen« findet sich erst in Art. 4 Abs. 1 Data Act. Auch hier herrscht somit noch Klarstellungsbedarf.[16]

Art. 4 Abs. 1 Data Act führt den Grundsatz ein, dass Nutzer Zugang zu Daten erhalten, zu deren Erzeugung sie beigetragen haben.[17] Die Daten müssen auf einfaches Verlangen des Nutzers seitens des Dateninhabers unverzüglich, kostenfrei und gegebenenfalls kontinuierlich und in Echtzeit zugänglich gemacht werden. Zu klären ist somit zunächst, wer im o.g. Fall-Beispiel der »Nutzer« ist.

Gem. Art. 2 Nr. 5 Data Act ist »Nutzer« eine natürliche oder juristische Person, die ein Produkt besitzt, mietet oder least oder eine Dienstleistung in Anspruch nimmt. Die Nutzereigenschaft ist somit nicht nur auf Verbraucher beschränkt, sondern umfasst auch sonstige Personen, die das Produkt – hier den Kühl-Trailer – einsetzen bzw. verwenden.[18]

Hier zeigt sich die Ungenauigkeit des Begriffs »Nutzer«: Im Beispiel-Fall hat das in Deutschland ansässige Unternehmen aus der Lebensmittelbranche als Auftraggeber eine Dienstleistung des Transportunternehmens in Anspruch genommen. Somit könnte der Auftraggeber hier Nutzer i.S.d. Art. 2 Nr. 5 Data Act sein. Unklar ist allerdings, welchen Anteil der Nutzer an der Erzeugung der Daten haben muss – im Ausgangsfall wurde nur der Auftrag zum Transport erteilt, durchgeführt wurde der Transport von einem Frachtführer des Transportunternehmens, der Auftraggeber hat den Trailer nicht selbst von der Schweiz nach Deutschland geführt. Art. 4 Abs. 1 Data Act kann durchaus so ausgelegt werden, dass es allein auf die Nutzung des Produkts (also des Kühl-Trailers) ankommt, nicht jedoch auf die Nutzung durch den Nutzer persönlich.[19] Wendet man dieses Verständnis an, würde es ausreichen, wenn ein Dritter, z.B. ein Arbeitnehmer, das Produkt benutzt und so die Daten generiert – »Nutzer« i.S.d. Data Act wäre dann nur der Arbeitgeber.[20] Im vorliegenden Fall wird der Kühl-Trailer von einem Frachtführer als Arbeitnehmer des Auftragnehmers benutzt. Weil der Frachtführer für seinen Arbeitgeber eine Dienstleistung erbringt, die dem Auftraggeber geschuldet ist, wäre der Auftraggeber – ohne selbst das Produkt benutzt zu haben – Nutzer i.S.v. Art. 2 Nr. 5 Data Act. Dies würde auch dem weiten Verständnis von Erwägungsgrund 17 entsprechen, welcher von »Daten, die bei der Nutzung eines Produkts oder verbundenen Dienstes erzeugt werden« spricht und eben nicht von Daten, die durch Nutzung des Produkts seitens des Nutzers erzeugt werden.

### b) »Dateninhaber« i.S.d. Art. 2 Nr. 6 Data Act

Der Anspruch des Nutzers auf Datenzugang aus Art. 4 Abs. 1 Data Act richtet sich gegen den Dateninhaber. Dies ist gem. Art. 2 Nr. 6 Data Act eine juristische oder natürliche Person, die nach dem Data Act, nach anwendbarem anderen Unionsrecht oder nach den anwendbaren nationalen Rechtsvorschriften durch die Kontrolle über die technische Konzeption des Produktes in der Lage ist, bestimmte Daten bereitzustellen, also die tatsächliche Möglichkeit hat, die Daten für den Nutzer zugänglich zu machen.[21] Auch hier ist die Formulierung der Vorschrift nicht eindeutig:

Auf die faktische Möglichkeit des Datenzugangs abzustellen, kann nicht zielführend sein, denn diese rein technische Fähigkeit haben gegebenenfalls auch Arbeitnehmer, IT-Sicherheitsforscher oder sogar Hacker.[22] Außerdem träfe die faktische Möglichkeit des Datenzugangs auch auf Nutzer und Datenempfänger zu, denen selbst erst auf Grundlage des Data Act Datenzugang gewährt wurde.[23] Zu beachten ist somit auch, dass es bezüglich eines Datensatzes mehrere faktische Dateninhaber geben kann.[24] Würde die jetzige Formulierung im Data Act beibehalten, wäre somit nicht eindeutig klar, wer Anspruchsgegner i.S.d. Art. 4 Abs. 1 Data Act wäre. Zu beachten ist außerdem, dass in der Praxis häufig mehrere Dateninhaber existieren, bspw. wenn die Daten automatisch an weitere Datenverarbeiter gesendet werden. Als Beispiel bieten sich hier sog. »Telematik-Versicherungen« an: So gibt es die Möglichkeit von Rabatt-Angeboten, wenn man der Versicherung Zugriff auf seine Fahrdaten gewährt.[25]

Im o.g. Beispiel-Fall speichert und verwaltet das Transportunternehmen alle Telematikdaten mit Hilfe einer cloudbasierten Software. Das Transportunternehmen hat somit die tatsächliche Möglichkeit, auf die Telematikdaten zuzugreifen, und ist daher Dateninhaber i.S.d. Art. 2 Nr. 6 Data Act.

### c) »Datenempfänger« i.S.d. Art. 2 Nr. 6 Data Act

Gem. Art. 2 Nr. 6 Data Act sind Datenempfänger juristische oder natürliche Personen, die auf die bereitgestellten Daten zugreifen, ohne Nutzer des Produkts zu sein.[26] Soweit der Auftraggeber im o.g. Fall-Beispiel als Nutzer angesehen wird (obwohl er selbst den Kühl-Trailer nicht nutzt, sondern durch den Frachtführer nutzen lässt), scheidet er als Datenempfänger i.S.d. Data Act aus, auch wenn ihm die Daten zugänglich gemacht werden. Jedoch wäre der Hersteller des an der Trailerstirnwand angebrachten Kühlgeräts Datenempfänger, sobald ihm vom Transportunternehmen die Daten zugänglich gemacht würden.

### d) »Dritte« und Datenzugang

Gemäß Art. 5 Abs. 1 Data Act kann der Nutzer vom Dateninhaber verlangen, dass dieser die Daten einem Dritten zur Verfügung stellt – und dies unter ähnlichen Umständen (»unverzüglich«, »dieselbe Qualität«, »gegebenenfalls kontinuierlich und in Echtzeit«), unter denen der Dateninhaber

15 *Podszun/Pfeifer*, GRUR 2022, 953 (957).

16 *Podszun/Pfeifer*, GRUR 2022, 953 (957).

17 *Bomhard/Merkle*, RDi 2022, 168 (169); *Karsten/Wienroeder*, RAW 2/22, 99 (101).

18 *Bomhard/Merkle*, RDi 2022, 168 (169); *Karsten/Wienroeder*, RAW 2/22, 99 (101).

19 *Bomhard/Merkle*, RDi 2022, 168 (170).

20 *Bomhard/Merkle*, RDi 2022, 168 (170); *Karsten/Wienroeder*, RAW 2/22, 99 (101).

21 *Karsten/Wienroeder*, RAW 2/22, 99 (102).

22 *Bomhard/Merkle*, RDi 2022, 168 (169).

23 *Bomhard/Merkle*, RDi 2022, 168 (169).

24 *Karsten/Wienroeder*, RAW 2/22, 99 (102); *Bomhard/Merkle*, RDi 2022, 168 (169).

25 Leupold/Wiebe/Glossner/*Eul*, IT-Recht, Teil 10.2 Rn. 41.

26 *Podszun/Pfeifer*, GRUR 2022, 953 (955).

auch dem Nutzer nach Art. 2 Nr. 5 Data Act verpflichtet ist. Der Dritte ist dann, nachdem er den Zugang zu den Daten durch den Dateninhaber erhalten hat, auch Datenempfänger gem. Art. 2 Nr. 6 Data Act. Bezüglich der Umstände, unter denen die Daten seitens des Dateninhabers nach Art. 5 Abs. 1 Data Act an den Datenempfänger bereitgestellt werden sollen, regelt Art. 8 Abs. 1 Data Act, dass dies zu fairen, angemessenen und nichtdiskriminierenden Bedingungen und in transparenter Weise zu erfolgen hat. Hieraus folgt, dass der Dateninhaber insoweit einem Kontrahierungszwang unter sog. »FRAND«-Bedingungen unterliegt.[27] Auffällig ist, dass Art. 5 Abs. 1 Data Act zwar bestimmt, dass die Zurverfügungstellung der Daten an den Dritten für den Nutzer kostenlos sein muss, dies aber nicht ausschließt, dass der Dateninhaber vom Dritten eine »angemessene« Entschädigung verlangen kann, Art. 9 Abs. 1 Data Act. Hier zeigt sich eine weitere Ungenauigkeit: »Angemessenheit« ist als unbestimmter Rechtsbegriff auslegungsbedürftig. In der Praxis kann hier mit erheblichen Unsicherheiten gerechnet werden.[28] Privilegiert werden an dieser Stelle Kleinst- sowie mittlere Unternehmen (KMU): Werden KMU Daten bereitgestellt, beschränkt sich gem. Art. 9 Abs. 2 Data Act die zu leistende finanzielle Entschädigung auf die Kosten der Bereitstellung und nicht der Erzeugung. Durch diese Regelung sollen KMU vor übermäßigen wirtschaftlichen Belastungen geschützt werden, die es ihnen wirtschaftlich zu schwer machen würden, innovative Geschäftsmodelle zu entwickeln und zu betreiben.[29] Die Datenverarbeitung durch einen Dritten i.S.d. Data Act muss gem. Art. 6 Abs. 1 Data Act durch einen Datenlizenzvertrag inhaltlich geregelt werden.[30] Art. 6 Data Act enthält insoweit auch Verbote, insbesondere ist es dem Dritten gem. Art. 6 Abs. 2 Buchst. e) Data Act nicht erlaubt, mit Hilfe der zur Verfügung gestellten Daten ein Konkurrenzprodukt zu entwickeln.[31]

Kein zulässiger »Dritter« i.S.d. Art. 5 Abs. 1 Data Act sind gem. Art. 5 Abs. 2 Data Act die sog. »Gatekeeper«. Dieser Begriff wurde aus der Verordnung des Europäischen Parlaments und des Rates über bestreitbare und faire Märkte im digitalen Sektor (Gesetz über digitale Märkte [DMA]) vom 14.09.2022 (Amtsblatt der europäischen Union vom 12.10.2022, L265/1) übernommen.[32] Adressiert werden insbesondere Online-Plattformen und Suchmaschinen.[33] Gem. Art. 5 Abs. 2 Data Act dürfen Gatekeeper nicht auf Nutzer einwirken, um direkt oder indirekt nutzungsgenerierte Daten zu erhalten. Außerdem ist es Dritten gem. Art. 5 Abs. 2, 6 Abs. 2 Buchst. d) Data Act verboten, solche Daten Gatekeepern bereitzustellen.[34]

Im o.g. Fall-Beispiel finden sich keine »Dritten« i.S.d. Art. 5 Abs. 1 Data Act. In der Praxis könnten vor allem Fälle relevant werden, in denen der Nutzer selbst ein Interesse daran hat, dass ein Dritter nutzergenerierte Daten eines Dateninhabers erhält, etwa wenn es im Rahmen einer Wartung um Reparatur und/oder Instandhaltung des Produkts geht.

### 5. Zugang zu Datenrechten: Wie und unter welchen Bedingungen erhalten Nutzer, Datenempfänger und Dritte vom Transportunternehmen (= Dateninhaber) die Datenrechte?

Innerhalb des Data Act gründet der Datenzugang auf vertraglichen Beziehungen zwischen Dateninhaber und Nutzer, Dateninhaber und Datenempfänger.[35]

#### a) Vertragliche Beziehung zwischen Dateninhaber und Nutzer

Art. 3 Abs. 1 Data greift zunächst technische Voraussetzungen auf: Produkte sollen so hergestellt bzw. Dienste so erbracht werden, dass die nutzergenerierten Daten leicht, sicher und gegebenenfalls direkt für den Nutzer zugänglich sind. Mit einer solchen technischen Lösung könnte einem Streitfall vorgebeugt werden, auch ohne zusätzlicher vertraglicher Vereinbarung.[36] Auch, wenn dies technisch möglich ist, z.B. weil der Dateninhaber (im Beispiel-Fall: das Transportunternehmen) dem Nutzer einen nutzerspezifischen Zugang zur Cloudanwendung zur Verfügung stellt, in der die Nutzerdaten gespeichert werden, sind vertragliche Regelungen dennoch naheliegend: Bspw. sollte vertraglich geregelt werden, wie lange der Dateninhaber die Daten vorhalten und zur Verfügung stellen muss. Der Data Act selbst regelt die Frage der Aufbewahrungspflicht der Daten nicht. Insbesondere bei längerer Lebensdauer des Produkts stellt sich die Frage, ob auch die Datennutzung dynamisch »weiterlebt«. Die Bedeutung des Datenzugangs wird häufig stark von der Lebensdauer des Produkts abhängen.[37] Insgesamt ist eine Aufbewahrungspflicht aber sehr gut abzulehnen, denn eine solche könnte bewirken, dass Daten von vornherein überhaupt nicht mehr erhoben werden – was dem Zweck des Data Act zuwiderliefe.[38]

Ein Lizenzvertrag zwischen Nutzer und Dateninhaber könnte sich in der Ausgestaltung inhaltlich an Art. 13 Data Act anlehnen, auch wenn hier inhaltlich die Verwendung unfairer Vertragsklauseln gegenüber KMU behandelt werden.[39] Denkbar wäre auch ein Mustervertrag nach Art. 34 Data Act.

Art. 3 Abs. 2 Data Act regelt vorvertraglich die Informationspflicht beim Kauf, Leasing oder der Miete eines Produkts oder bei der Zubuchung eines zusammenhängenden Dienstes. Der Nutzer soll vor Vertragsschluss z.B. wissen, wie er auf Daten zugreifen kann und ob der Hersteller, der das Produkt liefert, oder der Dienstleister, der den zusammenhängenden Dienst erbringt, beabsichtigt, die Daten selbst zu verwenden oder einem Dritten die Verwendung der Daten zu gestatten.[40] Die Entscheidungsgrundlage des Nutzers soll so sichergestellt werden.

Hervorzuheben ist Art. 4 Abs. 4 Data Act. Die Norm regelt die Situation, in der der Dateninhaber nicht-personenbezogene Daten, die bei der Nutzung eines Produktes oder verbun-

27 *Bomhard/Merkle*, RDi 2022, 168 (171); *Hennemann/Steinrötter*, NJW 2022, 1481 (1484).

28 *Podszun/Pfeifer*, GRUR 2022, 953 (957).

29 Erwägungsgrund 44 Data Act.

30 *Karsten/Wienroeder*, RAW 2/22, 99 (103).

31 *Bomhard/Merkle*, RDi 2022, 168 (172).

32 COM(2020) 842 final, 2020/0374 (COD).

33 *Bomhard/Merkle*, RDi 2022, 168 (172).

34 *Hennemann/Steinrötter*, NJW 2022, 1481 (1484); *Podszun/Pfeifer*, GRUR 2022, 953 (957); *Karsten/Wienroeder*, RAW 2/22, 99 (103).

35 *Podszun/Pfeifer*, GRUR 2022, 953 (959); *Hennemann/Steinrötter*, NJW 2022, 1481 (1483).

36 *Podszun/Pfeifer*, GRUR 2022, 953 (959).

37 *Podszun/Pfeifer*, GRUR 2022, 953 (959).

38 *Bomhard/Merkle*, RDi 2022, 168 (174).

39 *Podszun/Pfeifer*, GRUR 2022, 953 (959); *Bomhard/Merkle*, RDi 2022, 168 (173).

40 *Hennemann/Steinrötter*, NJW 2022, 1481 (1483).

denen Dienstes erzeugt werden, selbst nutzen möchte. Eine solche Nutzung setzt eine vertragliche Vereinbarung (Datenlizenzvertrag) mit dem Nutzer voraus. Hier ist der Data Act strenger als die DSGVO: Mit dem Erfordernis einer Datenlizenz gehen daher die Anforderungen für nicht-personenbezogene Daten über diejenigen für personenbezogene Daten hinaus,[41] denn die DSGVO lässt teilweise ein »berechtigtes Interesse« (Art. 6 Abs. 1 DSGVO) an der Verarbeitung von personenbezogenen Daten ausreichen und verlangt keine zusätzlichen Lizenzverträge. Die Stellung des Nutzers wird durch diese Regelung gestärkt: Der Dateninhaber ist von einer vertraglichen Vereinbarung mit dem Nutzer abhängig, wenn er den wirtschaftlichen Wert der Daten nutzen möchte.[42] Daher ist es umso überraschender, dass der Data Act keine Normen zur Regelung von durch Verbrauchern eingeräumte Datenlizenzen vorsieht, ähnlich Art. 13 Data Act.[43] Vermutlich kann damit gerechnet werden, dass Dateninhaber den Vertrieb ihrer Produkte und Leistungen davon abhängig machen, dass der betroffene Nutzer eine umfassende, örtlich, zeitlich und inhaltlich unbeschränkte Datenlizenz erteilt.[44] Etwaige Folgeprobleme könnten sich bei der Frage ergeben, mit welcher Wirkung und ganz allgemein unter welchem Rechtsregime der Datenlizenzvertrag gekündigt werden kann, der Data Act regelt eine etwaige Kündigung jedenfalls nicht.[45]

In der Praxis könnte es allerdings sein, dass Streitigkeiten zwischen dem Dateninhaber und dem Nutzer eher selten sind: Gewerbliche Nutzer werden vermutlich vorab vertraglich klären, welche Rechte wem zustehen, wohingegen Endverbraucher häufig nur ein begrenztes Interesse am Datenzugang haben.[46]

### b) Vertragliche Beziehung zwischen Dateninhabern und Datenempfängern bzw. Dritten

Das Konfliktpotenzial innerhalb der vertraglichen Beziehung zwischen Dateninhaber und Dritten bzw. Datenempfängern ist bereits sehr viel höher. Anders als mit Verbrauchern wird es hier eher zu »Konkurrenz«-Situationen kommen, in denen Dateninhaber ein erhebliches Verzögerungs- und Obstruktionspotenzial ausschöpfen können, um die Zugangsansprüche der Datenempfänger bzw. Dritten ins Leere laufen zu lassen.[47] Im Rahmen der Datenlizenzverträge zwischen Dateninhabern und Datenempfängern bzw. Dritten ist Art. 8 Data Act anzuwenden. Insbesondere das Entgelt, welches der Dateninhaber fordern kann, solange Art. 9 Abs. 2 Data Act nicht anzuwenden ist, könnte in dieser Konstellation ein Streitpunkt werden.

Im Beispiel-Fall ist der Hersteller des an der Trailerstirnwand angebrachten Kühlgeräts, der die Daten zwecks eigener Verwertung anfragt, Datenempfänger. Der Hersteller muss somit mit dem Transportunternehmen einen Datenlizenzvertrag schließen, um die gewünschten Daten erhalten zu können. Weil der Hersteller von Kühlgeräten vermutlich nicht in direkter Konkurrenz zum Transportunternehmen steht, kann vermutet werden, dass das Transportunternehmen die gewünschten Daten unproblematisch zugänglich machen wird. Der Datenlizenzvertrag richtet sich dabei nach den Regelungen des Art. 8 Data Act. Sollte der Hersteller ein KMU sein, gelten zusätzlich die Regeln über missbräuchliche Vertragsklauseln aus Art. 13 Data Act.

## 6. Fazit

Aufgrund der umfangreichen Daten, die im Rahmen eines (Kühl-)Trailertransports generiert werden, hat der Data Act für die Transportbranche eine hohe Relevanz. Das Praxisbeispiel hat im Rahmen eines typisch gelagerten Falls gezeigt, welche Fragen die Anwendung des Data Act mit sich bringen kann. Nachdem die Anwendbarkeit des Data Act keine großen Probleme bereitet, müssen in der Praxis zunächst die involvierten Personen der im Data Act beteiligten Personen nach Art. 2 ff. Data Act zugeordnet werden. Dies kann aufgrund der Ungenauigkeit des Data Act durchaus schwierig sein. Bemerkenswert ist, dass auf den ersten Blick der Dateninhaber eine exponierte Stellung innehat, hat er doch den Zugriff auf (potenziell wirtschaftlich wertvolle) Daten. Diese sind für ihn aber nur nutzbar, wenn der Nutzer sich darüber in einer Vereinbarung (= Lizenzvertrag) einverstanden zeigt. Auch die Verpflichtungen, dem Nutzer gegenüber sowie Dritten, die nun Ansprüche auf Daten geltend machen können, könnten aus Sicht des Dateninhabers eher als »Belastung« gewertet werden. Insgesamt ist festzuhalten, dass der Data Act sehr »vertragslastig« ist – und genau hier stellt sich die Frage, ob die betroffenen Akteure die Regelungen des Data Act, die zudem häufig unklar sind und zu Rechtsunsicherheiten führen, nicht als zu belastend empfinden und letztlich lieber gar keine Daten mehr generieren, um den komplexen Regelungen des Data Act nicht zu unterliegen. Dann hätte der Data Act das genaue Gegenteil seiner Zielsetzung erreicht.[48] Negativ wäre dies auch, weil der Data Act Teil der so wichtigen EU-Datenstrategie ist. Durch datengesteuerte Innovationen erhofft sich die EU viel. Daher sollte sie die Zeit des weiteren Gesetzgebungsverfahren nutzen, um die zahlreichen Unklarheiten des Data Act auszuräumen. Bis zur Ratifizierung des Data Act, der bisher nur als Kommissionsentwurf vorliegt, kann es noch zwei Jahre dauern. Zusätzlich sieht Art. 42 Data Act einen 12-monatigen Übergangszeitraum nach Inkrafttreten vor. Die EU hat somit genügend Zeit, den Kommissionsentwurf zu überarbeiten und zu ergänzen.

41 *Hennemann/Steinrötter*, NJW 2022, 1481 (1483).
42 *Hennemann/Steinrötter*, NJW 2022, 1481 (1483).
43 *Hennemann/Steinrötter*, NJW 2022, 1481 (1483).
44 *Bomhard/Merkle*, RDi 2022, 168 (174).
45 *Hennemann/Steinrötter*, NJW 2022, 1481 (1483).
46 *Podszun/Pfeifer*, GRUR 2022, 953 (959).
47 *Podszun/Pfeifer*, GRUR 2022, 953 (959).
48 *Hennemann/Steinrötter*, NJW 2022, 1481 (1486).