VERBRAUCHER:INNEN BEIM DATA ACT IM BLICK BEHALTEN

Stellungnahme des Verbraucherzentrale Bundesverbands zum Vorschlag der Europäischen Kommission für ein Datengesetz (Data Act)

13. Mai 2022

Impressum

Verbraucherzentrale
Bundesverband e.V.

Team
Digitales und Medien

Rudi-Dutschke-Straße 17
10969 Berlin

digitales@vzbv.de

Bundesverband der Verbraucherzentralen und Verbraucherverbände

Verbraucherzentrale Bundesverband e.V.

INHALT

I. ZUSAMMENFASSUNG

Am 23. Februar 2022 veröffentlichte die Europäische Kommission (EU-Kommission) den Vorschlag für einen Data Act, der die Verfügbarkeit von Daten unter Beachtung der europäischen Grundwerte erleichtern soll. Zusammenfassend sollten aus Sicht des Verbraucherzentrale Bundesverbands (vzbv) insbesondere die folgenden Erwägungen im weiteren Gesetzgebungsprozess berücksichtigt werden:

- Der vzbv unterstützt die Ziele der Europäischen Kommission. Kritisch zu hinterfragen ist jedoch, ob die derzeitige Grundkonzeption des Data Act geeignet ist, die mit ihm anvisierten Ziele zu erreichen. In jedem Fall muss der diesbezüglichen politischen und gesellschaftlichen Debatte ausreichend Raum und Zeit eingeräumt werden, um unbeabsichtigte Auswirkungen zu verhindern.
- Es sollte klargestellt werden, dass im Fall eines Konflikts zwischen der Verordnung und den europäischen Datenschutzvorschriften letztere den Vorrang haben und dass der Data Act keine Rechtsgrundlage für die Verarbeitung personenbezogener Daten schafft. Der vzbv empfiehlt daher, Artikel 1 (3) Satz 1 Data Act durch die Formulierung des Artikel 1 (3) Data Governance Act zu ersetzen.
- Der vzbv spricht sich dafür aus, die Definitionen des Data Act den Definitionen bestehender Rechtsakte anzugleichen beziehungsweise auf die Verwendung identischer Termini, die unterschiedliche Sachverhalte bezeichnen, zu verzichten.
- Für eine rechtsklare Anwendung sind klare Definitionen zentraler Begriffe, klare Adressaten, klare Rollenzuweisungen und ein klarer Anwendungsbereich unerlässlich. Viele der derzeitigen Definitionen sind jedoch unverständlich und irritierend. Im weiteren Gesetzgebungsprozess sollte hier dringend nachgebessert werden.
- Der Data Act sollte stärker zwischen personenbezogenen und nicht-personenbezogenen Daten unterscheiden. Insbesondere sollten hinsichtlich personenbezogener Daten die Zwecke stärker eingeschränkt werden, zu denen Dritte diese Daten verwenden dürfen. Dritten sollte untersagt werden, eine direkte Wertschöpfung aus der Kommerzialisierung dieser personenbezogenen Daten zu ziehen. Ihnen sollte lediglich gestattet werden, den Nutzern Dienste auf Basis dieser Daten anzubieten.
- Die Reichweite der Verträge zwischen Dateninhaber und Nutzer in B2C-Situationen sollte im weiteren Gesetzgebungsprozess konkretisiert werden, insbesondere hinsichtlich der Zwecke, zu denen die Daten durch Dateninhaber verarbeitet werden dürfen, hinsichtlich der Zulässigkeit der Übermittlung der Daten an Dritte sowie hinsichtlich der Geltungsdauer der Verträge.
- Durch gesetzgeberische Vorgaben und die Entwicklung von Standards sollten konkrete Anforderungen an die Anonymisierung sowie an die Verwendung anonymisierter Daten definiert werden.
- Der Data Act darf nicht das wettbewerbskritische und verbraucherunfreundliche „extended vehicle“-Konzept und die damit verbundene exklusive Kontrolle über die Daten durch die Autohersteller zementieren.
- Aufgrund der Masse an Mobilitätsdaten und deren potenziell gesellschaftlichen Mehrwert sollte über den Data Act hinaus ein sektorspezifisches Gesetz für Mobilitätsdaten auf europäischer Ebene erarbeitet werden.

II. EINLEITUNG

Am 23. Februar 2022 veröffentlichte die EU-Kommission den Vorschlag für ein Datengesetz (Data Act / DA).[1] Diese Verordnung ist Teil der Europäischen Datenstrategie 2020, deren Ziel es ist, einen Binnenmarkt für Daten zu schaffen und Europa an die Spitze der datengestützten Gesellschaft zu bringen.[2] Neben dem Data Governance Act[3] (DGA) gilt der DA als tragende Säule, um dieses Ziel zu erreichen.

Durch den DA soll die Verfügbarkeit von Daten unter Achtung der europäischen Grundwerte gefördert werden. Durch die Erleichterung des Datenzugangs und der Datennutzung sollen, bei gleichzeitiger Aufrechterhaltung von Anreizen für Investitionen, eine gerechte Verteilung der Wertschöpfung aus Daten auf die Akteure der Datenwirtschaft gewährleistet, die Innovations- und Wettbewerbsfähigkeit von EU-Unternehmen sichergestellt und die Handlungskompetenz der Menschen in Bezug auf ihre Daten gestärkt werden. Nutzer[4] (Verbraucher:innen und Unternehmen) sollen Zugang zu Daten erhalten, die von vernetzten Produkten oder damit verbundenen Dienstleistungen erzeugt werden, die sie gekauft, gemietet oder geleast haben (folgend verkürzt: „Produkte“ / „Daten“). Dateninhaber dürfen die Daten nutzen, soweit dies mit den Nutzern vereinbart wurde. Sie müssen den Nutzern auf Anfrage diese Daten zur Verfügung stellen oder Datenempfängern übermitteln. Die Zugangsmodalitäten, die zwischen Dateninhabern und Datenempfängern ausgehandelt werden, müssen fair und nichtdiskriminierend sein, außerdem soll die Vergütung angemessen sein. Das europäische Datenschutzrecht, wie etwa die Datenschutz-Grundverordnung[5], bleibt unberührt.

Der vzbv unterstützt die Ziele des DA. Vernetzte Geräte werden künftig nicht nur von Unternehmen stärker eingesetzt werden. In den kommenden Jahren werden sie auch immer präsenter in den Alltag aller Verbraucher:innen vordringen. Dabei generieren vernetzte Geräte unablässig große Datenmengen, die – im Falle von personenbezogenen Daten unter Beachtung der datenschutzrechtlichen Vorgaben – im Gemeininteresse und zur Wertschöpfung verarbeitet werden können. Für eine gerechte Verteilung dieser Wertschöpfung ist es entscheidend, wer die Kontrolle über diese Daten hat, welche Zugangsmöglichkeiten bestehen und wie diese ausgestaltet werden. Neue Datennutzungsverträge mit Dateninhabern und Datenempfängern dürfen Verbraucher:innen jedoch nicht überfordern. Eine solche Überforderung könnte leicht ausgenutzt werden, um Verbraucher:innen zu übervorteilen oder Fehlanreize zu bieten und würde dem Ziel der fairen Datennutzung entgegen stehen.

Daher begrüßt der vzbv, dass die EU-Kommission den Austausch mit verschiedenen Interessengruppen sucht und bedankt sich für die Gelegenheit zur Stellungnahme.

---

[1] Vorschlag für eine Verordnung des Europäischen Parlaments und Rates über harmonisierte Vorschriften für einen fairen Datenzugang und eine faire Datennutzung (Data Act). Alle Artikel und Erwägungsgründe ohne Gesetzesangaben beziehen sich auf den vorliegenden Entwurf des Data Act.

[2] Eine Europäische Datenstrategie. Mitteilung der Europäischen Kommission, COM (2020) 66 final.

[3] Vorschlag für eine Verordnung des Europäischen Parlaments und Rates über europäische Daten-Governance (Data Governance Act). Der DGA wurde am 06. April 2022 durch das Europäische Parlament beschlossen (P9_TA(2022)0111), die Zustimmung des EU-Rates steht zum Zeitpunkt der Stellungnahme noch aus.

[4] Da „Nutzer“, „Dateninhaber“ und „Datenempfänger“ in der Verordnung definierte Begriffe sind, wird in diesen Fällen auf gendergerechte Sprache verzichtet.

[5] Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung)

III. POSITIONEN IM EINZELNEN

1. GRUNDSÄTZLICHE ÜBERLEGUNGEN

Die EU-Kommission verfolgt mit dem Data Act eine Reihe von Zielen. So sollen durch die Erleichterung des Datenzugangs und der Datennutzung für Verbraucher:innen und Unternehmen bei gleichzeitiger Aufrechterhaltung von Anreizen für Investitionen unter anderem eine gerechte Verteilung der Wertschöpfung aus Daten auf die Akteure der Datenwirtschaft gewährleistet, die Innovations- und Wettbewerbsfähigkeit von EU-Unternehmen sämtlicher Branchen sichergestellt und die Handlungskompetenz der Menschen in Bezug auf ihre Daten wirksam gestärkt werden.[6] Der vzbv unterstützt die formulierten Ziele, ist allerdings skeptisch, ob diese mit dem vorliegenden Entwurf tatsächlich erreicht werden können.

Eine Befürchtung ist, dass der DA nicht etwa die faktische Verfügungsgewalt der Dateninhaber über die generierten Daten auflöst, sondern dass der DA vielmehr die Position der Dateninhaber stärkt und rechtlich zementiert. Denn Dateninhaber können sich die Rechte an nicht-personenbezogenen Daten recht einfach durch entsprechende vertragliche Vereinbarungen mit den Nutzern sichern. Für die Vertragsgestaltung gibt es abseits der allgemeinen Verbraucherschutzvorschriften[7] keinerlei Vorgaben und keine Grenzen, was besonders im B2C-Bereich dazu führen könnte, dass bestehende Machtungleichgewichte zu Ungunsten der Verbraucher:innen ausgenutzt werden (siehe auch Ausführungen in Kapitel III.4 sowie Kapitel III.6.1). Gleichzeitig sind die Zugangsrechte und Verhandlungspositionen Dritter nur schwach ausgeprägt und der mögliche Nutzen der Daten für Anschlussdienste, wie Reparatur und Wartung, begrenzt.[8]

Auch ist fraglich, ob die Vorschläge tatsächlich geeignet sind, die Rechte betroffener Personen durch die Erweiterung des Rechts auf Datenübertragbarkeit nach Artikel 20 der Datenschutz-Grundverordnung substanziell zu stärken. Denn schließlich bezieht sich der DA lediglich auf Daten, die durch die Verwendung von einigen vernetzten Produkten erzeugt werden; in allen anderen Datenverarbeitungsbereichen, beispielsweise auch hinsichtlich rein digitaler Produkte[9], entfaltet er keine Wirkung. Des Weiteren werden in vielen Fällen die betroffenen Personen gar nicht die Nutzer im Sinne des DA sein (siehe auch Ausführungen in Kapitel III.2.3) und somit auch nicht in den Genuss des erweiterten Datenportabilitätsrechts kommen. Darüber hinaus formuliert der Entwurf[10] lediglich Anforderungen an die Formate der Daten beziehungsweise an die Interoperabilität, wenn die Daten über die künftigen europäischen Datenräume ausgetauscht werden. Dies dürfte jedoch bei einer Vielzahl von vernetzten Produkten im Endkundenbereich nicht der Fall sein. Demgegenüber könnte der DA gar dazu führen, dass

---

[6] Vgl. Ausführungen zu „Gründe und Ziele des Vorschlags“ im Explanatory Memorandum des Data Act

[7] Vgl. Erwägungsgrund 9, der auf die Richtlinien über unlautere Geschäftspraktiken, Rechte der Verbraucher:innen sowie über missbräuchliche Klauseln in Verbraucherverträgen verweist. Zumindest ein Vorziehen in die Artikel sollte klarstellend erwogen werden, wie auch bei Artikel 1 (3) und Artikel 1 (4) erfolgt.

[8] Dieser Aspekt wird in der vorliegenden Stellungnahme nur kurz hinsichtlich von Mobilitätsdaten beleuchtet (Kapitel III.6.1). Vgl. allgemein dazu ausführlich Kerber, Wolfgang: Governance of IoT Data: Why the EU Data Act will not fulfill its objectives (2022), URL: https://dx.doi.org/10.2139/ssrn.4080436 [Zugriff: 14.04.2022].

[9] Vgl. Gerpott, Torsten: Vorschlag für ein europäisches Datengesetz - Überblick und Analyse der Vorgaben für vernetzte Produkte, in: Computer und Recht (CR) (2022), H. 04, S. 274.

[10] Anders als etwa Artikel 20 (1) DSGVO: „[…] in einem strukturierten, gängigen und maschinenlesbaren Format […]“

das Recht auf den Schutz personenbezogener Daten geschwächt wird, indem er Anreize für Hersteller stärkt, mit ihren Produkten Daten zu generieren, die für die Produktfunktionalität gar nicht erforderlich wären.[11]

Erstaunlich ist außerdem die geringe Verzahnung des DA mit dem Data Governance Act. Der DGA etabliert durch eine horizontale Regelung unabhängige Datenvermittlungsdienste und weist ihnen „eine Schlüsselrolle in der Datenwirtschaft“ zu.[12] Im DA hingegen werden Datenvermittlungsdiensten lediglich als Randnotiz[13] behandelt. Dabei könnten Datenvermittlungsdiensten,[14] eine geeignetere Lösungsoption sein, um den Wettbewerb, Innovationen und die Wahlfreiheit der Nutzer zu stärken, als die im DA vorgeschlagenen Mechanismen, die sich teilweise auch als Überforderung der Verbraucher:innen darstellen könnten (siehe auch Ausführungen in Kapitel III.2.3, Kapitel III.4 und Kapitel III.6.1).

> Im weiteren Gesetzgebungsprozess sollte dringend kritisch hinterfragt werden, ob die derzeitige Grundkonzeption des DA geeignet ist, die mit ihm anvisierten Ziele tatsächlich zu erreichen. In jedem Fall muss der diesbezüglichen politischen und gesellschaftlichen Debatte ausreichend Raum und Zeit eingeräumt werden, um unbeabsichtigte Auswirkungen zu verhindern. Eine vorschnelle Verabschiedung des DA, ohne die aufgeworfenen Fragen zu klären, wäre in einem solch für die Datenwirtschaft und für die Wettbewerbsfähigkeit Europas zentralen Gesetzesvorhaben nicht angemessen und potenziell schädlich.

2. ALLGEMEINE BESTIMMUNGEN

2.1 Klarstellung des Vorrangs des europäischen Datenschutzrechts über den DA

Der DA stellt klar, dass die Europäischen Rechtsvorschriften über den Schutz personenbezogener Daten, die Privatsphäre und die Vertraulichkeit der Kommunikation unberührt bleiben.[15] Diese Klarstellungen begrüßt der vzbv.

Jedoch zeigt sich in den folgenden Artikeln, dass diese anvisierte Abgrenzung des Data Act von der DSGVO nicht immer eindeutig vorgenommen wird. So sollen Dritte Daten nur zu den Zwecken verarbeiten dürfen, die sie mit den Nutzern vereinbart haben.[16] Jedoch sieht die DSGVO bei der Verarbeitung von personenbezogenen Daten

---

[11] Vgl. Kerber, Wolfgang: Governance of IoT Data: Why the EU Data Act will not fulfill its objectives (2022), S. 17f, URL: https://dx.doi.org/10.2139/ssrn.4080436 [Zugriff: 14.04.2022].

[12] Erwägungsgrund 27 DGA „Datenvermittlungsdienste dürften eine Schlüsselrolle in der Datenwirtschaft spielen, insbesondere durch die Unterstützung und Förderung freiwilliger Verfahren zur gemeinsamen Datennutzung zwischen Unternehmen oder die Erleichterung zur gemeinsamen Datennutzung im Zusammenhang mit den im Unionsrecht oder im nationalen Recht festgelegten Verpflichtungen […]“

[13] Vgl. Erwägungsgründe 35 und 87

[14] Etwa im Mobilitätsbereich, vgl. Specht-Riemenschneider, Louisa; Kerber, Wolfgang: Datentreuhänder - Ein problemlösungsorientierter Ansatz (2022), S. 59ff, URL: https://www.kas.de/documents/252038/16166715/Designing+Data+Trustees+-+A+Purpose-Based+Approach.pdf/ffadcb36-1377-4511-6e3c-0e32fc727a4d [Zugriff: 28.04.2022].

[15] Artikel 1 (3)

[16] Artikel 6 (1)

die Möglichkeit einer Zweckänderung vor.[17] Geht nun der DA an dieser Stelle der DSGVO vor und berührt sie damit doch oder ist eine Zweckänderung bei der Verarbeitung personenbezogener Daten – entgegen des Wortlauts des DA möglich? Aus Sicht des vzbv muss in jeden Fall klargestellt sein, dass jede Weiterverarbeitung personenbezogener Daten den Anforderungen des Artikel 6 (4) DSGVO folgen muss.

Außerdem könnte der DA so verstanden werden, dass eine solche Vereinbarung zwischen Nutzern und Dritten als Rechtsgrundlage für die Verarbeitung personenbezogener Daten betrachtet werden könnte (und damit beispielsweise den engen Auslegungen des Europäischen Datenschutzausschusses zu Artikel 6 (1) b) DSGVO[18] entgegenlaufen würde). Daher sollte klargestellt werden, dass auch in diesen Fällen eigene, wirksame Rechtsgrundlagen entsprechend der DSGVO erforderlich sind.

Ähnlich dieser Verträge zwischen Nutzern und Dritten sollen Dateninhaber nicht-personenbezogene Daten auf der Grundlage von vertraglichen Vereinbarungen mit den Nutzern verwenden dürfen.[19] Hier sollte aber deutlich werden, dass die ePrivacy-Richtlinie[20] grundsätzlich vorsieht, dass die Speicherung von Informationen oder der Zugriff auf Informationen, die bereits in den Endgeräten des Nutzers gespeichert sind, nur gestattet ist, wenn der Nutzer auf Grundlage von klaren und umfassenden Informationen seine Einwilligung entsprechend der Vorgaben der DSGVO erteilt hat.[21] Dabei ist es unerheblich, ob es sich bei diesen Informationen um personenbezogene oder nicht-personenbezogene Daten handelt.

Vor dem Hintergrund dieser Fragen und Unklarheiten hält der vzbv eine klarere Kollisionsregel für erforderlich, die festlegt, dass in Konfliktfällen die europäischen Datenschutzvorschriften Vorrang genießen – wie sie auch im DGA enthalten ist. Außerdem sollte in dieser für die Abgrenzung zentralen Norm (wie auch im DGA) klargestellt werden, dass der DA weder Rechtsgrundlagen für die Verarbeitung personenbezogener Daten schafft, noch die im europäischen Datenschutzrecht festgelegten Rechte und Pflichten berührt.[22] Darüber hinaus würde es die Komplexität für Rechtsanwender verringern, wenn der DA bei der Regelung identischer Sachverhalte einen identischen Wortlaut wie der DGA verwenden würde.

---

[17] Artikel 6 (4) DSGVO

[18] Vgl. Europäischer Datenschutzausschuss: Leitlinien 2/2019 zur Verarbeitung personenbezogener Daten gemäß Artikel 6 Absatz 1 Buchstabe b DSGVO im Zusammenhang mit der Bereitstellung von Online-Diensten für betroffene Personen (2019), URL: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-22019-processing-personal-data-under-article-61b_de [Zugriff: 25.04.2022]. In diesen Leitlinien vertritt der Europäische Datenschutzausschuss die Auffassung, dass ein Verantwortlicher eine Datenverarbeitung nur auf die Rechtsgrundlage „Vertrag“ nach Artikel 6 Absatz 1 Buchstabe b DSGVO stützen darf, wenn er nachweisen kann, dass die Verarbeitung für die Durchführung des Vertrags objektiv erforderlich ist. Für die Beurteilung der Erforderlichkeit kann demnach nicht alleine auf den Vertragstext abgestellt werden.

[19] Artikel 4 (6)

[20] Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronischer Kommunikation) in der Fassung der Richtlinie 2009/136/EG vom 25. November 2009

[21] Artikel 5 (3) ePrivacy-RL

[22] Artikel 1 (3) DGA: „Das Unionsrecht und das nationale Recht über den Schutz personenbezogener Daten gelten für alle personenbezogenen Daten, die im Zusammenhang mit der vorliegenden Verordnung verarbeitet werden. Insbesondere gilt die vorliegende Verordnung unbeschadet der Verordnungen (EU) 2016/679 und (EU) 2018/1725 und der Richtlinien 2002/58/EG und (EU) 2016/680, einschließlich im Hinblick auf die Befugnisse der Aufsichtsbehörden. Im Fall eines Konflikts zwischen der vorliegenden Verordnung und dem Unionsrecht über den Schutz personenbezogener Daten oder dem entsprechend diesem Unionsrecht erlassenen nationalen Recht soll das einschlägige Unionsrecht bzw. das nationale Recht über den Schutz personenbezogener Daten Vorrang haben. Die vorliegende Verordnung

Es sollte auch im Data Act klargestellt werden, dass im Fall eines Konflikts zwischen der Verordnung und den europäischen Datenschutzvorschriften letztere den Vorrang haben und dass der DA keine Rechtsgrundlage für die Verarbeitung personenbezogener Daten schafft. Der vzbv empfiehlt daher, Artikel 1 (3) Satz 1 durch die Formulierung des Artikel 1 (3) DGA zu ersetzen.

2.2 Angleichung der Definitionen des DA an Definitionen bestehender Rechtsakte

Problematisch ist weiterhin, dass der DA identische Termini anders definiert, als bestehende europäische Rechtsakte, die ähnliche oder angrenzende Sachverhalte regeln, wie beispielsweise der DGA und die DSGVO. So wird etwa der Begriff der „Dateninhaber“ gleichermaßen im DA[23] und dem DGA[24] definiert, allerdings in unterschiedlicher Weise. Auch die Definitionen „Verarbeitung“ im DA[25] unterscheidet sich von der Definition des identischen Begriffs in der DSGVO[26]. Gleiches gilt für den Begriff des „Nutzers“[27] – bereits definiert in der ePrivacy-Richtlinie[28]. Die Verwendung identischer Termini für unterschiedliche Sachverhalte in angrenzenden Rechtsakten stiftet Verwirrung, erschwert das Verständnis und erzeugt Fehlerquellen.

Der vzbv spricht sich dafür aus, die Definitionen des Data Act den Definitionen bestehender Rechtsakte anzugleichen beziehungsweise auf die Verwendung identischer Termini, die unterschiedliche Sachverhalte bezeichnen, zu verzichten.

2.3 Verwendung klarer Definitionen und Rollenzuweisungen

Ungeachtet dieser Problematik sind auch einige Begriffsbestimmungen innerhalb des DA unklar und die Rollen der verschiedenen Akteure nicht ausreichend ausdifferenziert.

Definition des Begriffs „Produkt“

Die Bestimmung des Begriffs „Produkts“ ist unverständlich. So bezeichnet der Ausdruck „Produkt“ einen körperlichen beweglichen Gegenstand, der auch in einem unbeweglichen Gegenstand enthalten sein kann, Daten über seine Nutzung oder Umgebung erlangt, erzeugt oder sammelt und Daten über einen öffentlich zugänglichen elektronischen Kommunikationsdienst übermitteln kann und dessen Hauptfunktion nicht die Speicherung und Verarbeitung von Daten ist“[29]. Laut der Erwägungsgründe sind davon

schafft keine Rechtsgrundlage für die Verarbeitung personenbezogener Daten, noch berührt es die in den Verordnungen (EU) 2016/679 oder (EU) 2018/1725 oder den Richtlinien 2002/58/EG oder (EU) 2016/680 festgelegten Rechte und Pflichten.“

[23] Artikel 2 (6)

[24] Artikel 2 (8) DGA

[25] Artikel 2 (11)

[26] Artikel 4 (2) DSGVO

[27] Artikel 2 (5)

[28] Artikel 2 a) ePrivacy-RL

[29] Artikel 2 (2)

nicht Produkte erfasst, „die in erster Linie dazu bestimmt sind, Inhalte anzuzeigen oder abzuspielen oder diese […] aufzuzeichnen und zu übertragen. Zu diesen Produkten gehören beispielsweise Personalcomputer, Server, Tablets und Smartphones, Kameras, Webcams, Tonaufnahmesysteme und Textscanner“[30]. Wären nach dieser Definition beispielsweise Fitnesstracker von der Verordnung erfasst? Wenn Fitnesstracker aber erfasst wären, würde dies auch für Smartwatches gelten, mit denen Fitnessdaten erhoben werden können? Und was wäre, wenn man mit diesen Smartwatches telefonieren kann? Wären diese dann ausgeschlossen, da sie über dieselben Funktionalitäten wie Smartphones verfügen – über die auch laufend und im Hintergrund Fitnessdaten aufgezeichnet werden können?

Fraglich ist auch, wie ganzheitlich der Begriff des Produkts verstanden werden soll. Gelten vernetzte Fahrzeuge als Produkte, obwohl mit diesen Fahrzeugen telefoniert werden kann und Inhalte über die Entertainmentanlagen abgespielt werden können? Oder werden die Fahrzeuge nach weiteren Funktionen (GPS-Funktion, Komfortfunktionen, Sicherheitsfunktionen, Entertainmentsystem, usw.) unterteilt? Werden also Verbraucher:innen künftig auf Daten aus Teilen ihrer Fahrzeuge auf Basis des Data Act zugreifen können, aber auf andere nicht? Wie kann dies praktisch abgebildet werden, beispielsweise in Verträgen und vorvertraglichen Informationen? Insgesamt erscheint die Definition des Produkts beziehungsweise der Ausschluss bestimmter Geräteklassen willkürlich.

Definition des Begriffs „Nutzer“

Irritierend ist außerdem, dass der Begriff des „Nutzers“ im Sinne des DA nicht unbedingt den Nutzer eines Produktes einschließt, wie er im allgemeinen Sprachgebrauch verstanden wird. Zwar sei „[ein] „Nutzer“ eine natürliche oder juristische Person, die ein Produkt besitzt, mietet oder least oder eine Dienstleistung in Anspruch nimmt“[31] – allerdings wird in den Erwägungsgründen deutlich, dass der Begriff des „owners“ der englischen Sprachfassung nicht als „Besitzer“, sondern viel mehr als „Eigentümer“ beziehungsweise „Mieter“ oder „Leasingnehmer“ zu verstehen ist („Als Nutzer eines Produkts sollte die […] Person […] verstanden werden, die das Produkt gekauft, gemietet oder geleast hat.“[32]). Auch Artikel 4 (5) und Artikel 5 (6) machen dies deutlich.

Dies bedeutet aber zum Beispiel im Falle vernetzter Fahrzeuge, dass die Fahrzeugeigentümer:innen beziehungsweise Mieter:innen oder Leasingnehmer:innen die Nutzer im Sinne des DA sind, nicht aber die vom Fahrzeugeigentümer personenverschiedenen Fahrer – und damit die Nutzer im allgemeinem Sprachgebrauch, wenn diese sich die Fahrzeuge lediglich ausgeliehen haben.

Unklare Rollenzuweisungen

Der DA adressiert sowohl die Hersteller von Produkten als auch Dateninhaber, wobei Hersteller eine Untergruppe der Dateninhaber zu sein scheinen.[33] Allerdings ist das

[30] Erwägungsgrund 15

[31] Artikel 5 (2)

[32] Erwägungsgrund 18

[33] Artikel 1 (2)

Verhältnis zwischen diesen beiden Akteuren unklar. So beziehen sich einzelne Vorschriften allein auf Hersteller, andere nur auf Dateninhaber, teilweise scheinen die beiden Termini aber auch synonym verwendet zu werden.

Etwa müssen Nutzer vor Abschluss eines Vertrags darüber informiert werden, „ob der Hersteller […] beabsichtigt, die Daten selbst zu nutzen […] und falls ja, für welche Zwecke diese Daten genutzt werden sollen“[34]. Entsprechende vorvertragliche Informationspflichten über die geplante Datennutzung durch Dateninhaber werden nicht normiert. Demgegenüber soll „der Dateninhaber [...] nicht personenbezogene Daten, die bei der Nutzung eines Produktes […] erzeugt werden, nur auf der Grundlage einer vertraglichen Vereinbarung mit dem Nutzer nutzen“[35] dürfen. Bedeutet dies, dass Hersteller die anfallenden Daten in unbeschränkter Art und Weise verwenden dürfen, wenn sie die Nutzer lediglich darüber informieren? Oder müssen auch Hersteller Verträge mit den Nutzern schließen, obwohl möglicherweise gar kein direkter Kontakt besteht? Und wie geht die Rolle der Hersteller als Dateninhaber und die damit verbundenen Rechte und Pflichten auf weitere Dateninhaber über? Kann diese Rolle (beliebig oft?) verkauft werden und wäre es damit beispielsweise Gatekeepern möglich, die Rolle eines Dateninhabers von den Herstellern zu erwerben (und damit auch die Beschränkungen des Artikel 5 (2) zu umgehen)?

Ähnlich unklar ist die Abgrenzung zwischen „Datenempfängern“ und „Dritten“[36]. So scheinen Dritte eine Untergruppe der Datenempfänger zu sein („„Datenempfänger“ eine […] Person […] der vom Dateninhaber Daten bereitgestellt werden, einschließlich eines Dritten, dem der Dateninhaber […] Daten bereitstellt“[37]). Eine Abgrenzung erfolgt jedoch nicht. Vielmehr scheinen im Folgenden die beiden Begriffe synonym verwendet zu werden. So ist in Kapitel 2 ausschließlich von „Dritten“ die Rede, während Kapitel 3 durchgängig (bis auf eine Ausnahme) den Begriff des „Datenempfängers“ verwendet.

Insgesamt scheint der DA allein einfache Dreierkonstellationen (Dateninhaber ► Nutzer ► Datenempfänger) im Fokus zu haben. Dies bildet jedoch heutige komplexe und globale Wertschöpfungsketten nicht ausreichend ab. So scheint vorgesehen zu sein, dass mehrere Akteure als Dateninhaber gelten können – bis hin zum Nutzer, wenn er direkten Zugriff auf die Daten auf seinem Produkt hat und bis hin zum Datenempfänger, der mit Empfang der Daten selbst zu einem Dateninhaber werden kann. Dies gilt insbesondere, wenn unterschiedliche Teile eines Produkts von verschiedenen Unternehmen hergestellt werden. Gleichermaßen können auch auf Seite der Datenempfänger mehrere Akteure (wie Zulieferer von Ersatzteilen oder Subunternehmer) an der Wertschöpfung beteiligt sein.

Der DA lässt dabei völlig offen, wie die durch die Verordnung statuierten Rechte und Pflichten den verschiedenen Akteuren handhabbar und nachvollziehbar zugewiesen werden sollen. Beispielsweise haben hinsichtlich der vorvertraglichen Informationspflichten des Artikel 3 (2) die Vertragspartner von Verbraucher:innen (wie Leasing-Unternehmen) möglicherweise gar keine Kenntnisse über die in dem Fahrzeug verbauten Datenverarbeitungssysteme und die Zugriffsmöglichkeiten der in der Wertschöpfungskette vorgelagerten Akteure.

---

[34] Artikel 3 (2) d)

[35] Artikel 4 (6)

[36] Auch ein Begriff, der bereits in Artikel 4 (10) DSGVO definiert wurde

[37] Artikel 2 (7)

Für eine rechtsklare Anwendung des Data Act sind klare Definitionen zentraler Begriffe, klare Adressaten, klare Rollenzuweisungen und ein klarer Anwendungsbereich unerlässlich. Viele der derzeitigen Definitionen sind jedoch unverständlich und irritierend. Im weiteren Gesetzgebungsprozess sollte hier dringend nachgebessert werden.

3. ABGRENZUNG ZWISCHEN PERSONENBEZOGENEN UND NICHT-PERSONENBEZOGENEN DATEN

Der DA unterscheidet zwar formal zwischen personenbezogenen und nicht-personenbezogenen Daten und stellt klar, dass das Datenschutzrecht nicht berührt wird.[38] Allerdings beziehen sich die anschließenden Regelungen (bis auf wenige Ausnahmen) auf beide Datenkategorien, was die Abgrenzung sehr schwierig macht. Dies führt zu Unklarheiten bei der Interpretation der Bestimmungen, die nicht zu Lasten des Datenschutzes und seiner Durchsetzung gehen dürfen. Eine deutlichere Trennung der Begrifflichkeiten und der damit verbundenen Anforderungen würde zu mehr Rechtssicherheit führen.

Bereits in Kapitel III.2.3 wurde die komplizierte Rollenverteilung zwischen den verschiedenen Akteuren dargestellt. Handelt es sich bei den Daten, auf die zugegriffen beziehungsweise die übertragen werden sollen, um personenbezogene Daten, wird diese Komplexität weiter gesteigert. So statuiert der DA das Ziel, das Recht Betroffener auf die Übertragbarkeit ihrer Daten zu stärken. Allerdings sind in vielen Fällen die betroffenen Personen jedoch gar nicht die Nutzer im Sinne des DA, deren Rechte gestärkt würden. Vielmehr können datenschutzrechtlich verantwortliche Stellen die Nutzer sein, die personenbezogene Daten von Betroffenen von weiteren verantwortlichen Stellen (den Dateninhabern) an Dritte verantwortliche Stellen (den Datenempfängern) übertragen möchten. Nutzer mögen also zwar über den DA das Recht haben, auf Daten zuzugreifen, aber dennoch nicht über eine wirksame Rechtsgrundlage nach der DSGVO verfügen. Dateninhaber müssten nun prüfen, ob eine wirksame Rechtsgrundlage vorliegt, was sich bei der Vielzahl von potenziellen Nutzern und Datenempfängern in der Praxis als unmöglich erweisen dürfte. Dadurch besteht die Gefahr, dass personenbezogene Daten in unzulässiger Weise verarbeitet werden und das allgemeine Datenschutzniveau leidet.

Besonders auffällig werden die mit der mangelnden Abgrenzung zwischen personenbezogenen und nicht-personenbezogenen Daten verbundenen Probleme in Artikel 6. Dieser besagt, dass „ein Dritter […] die ihm nach Artikel 5 bereitgestellten Daten nur für die Zwecke und unter den Bedingungen [verarbeitet], die er mit dem Nutzer vereinbart hat, und – soweit personenbezogene Daten betroffen sind – vorbehaltlich der Rechte der betroffenen Person […]“[39]. Eine Einschränkung der Zwecke, zu denen Dritte die Daten verarbeiten dürfen, enthält der DA nicht. Zwar wird Dritten beispielsweise untersagt, die

[38] Artikel 1 (3)

[39] Artikel 6 (1)

erhaltenen Daten für das Profiling zu nutzen[40] oder die Daten anderen Dritten bereitzustellen[41], allerdings jeweils nur unter der Maßgabe, dass dies nicht erforderlich sei, um die von den Nutzern gewünschten Dienste zu erbringen[42]. Auch enthält Artikel 6 (2) beispielsweise nicht das Verbot, Nutzern finanzielle Anreize für die Übermittlung ihrer Daten zu bieten – anders als Artikel 5 (2) mit Blick auf Gatekeeper.

Ein Unternehmen könnte also Verbraucher:innen anbieten, dass sie ihm – gegen eine kleine Entschädigung – die Daten ihrer Produkte kontinuierlich und in Echtzeit übertragen, es aus diesen Daten Profile bildet und diese Profile an weitere Datenhändler verkauft. Während ein solches Geschäftsmodell mit Blick auf nicht-personenbezogene Daten eher unproblematisch scheint,[43] wären entsprechende Praktiken mit Blick auf personenbezogene Daten als höchst kritisch zu beurteilen. Aus einer grundrechtlichen Perspektive ist die Reduzierung von personenbezogenen Daten auf einen wirtschaftlichen Wert abzulehnen. Eine direkte finanzielle Vergütung für Verbraucher:innen, ihre Daten zu kommerzialisieren, setzt darüber hinaus besonders für einkommensschwache Gruppen falsche Anreize. Diese könnten beispielsweise in Versuchung gebracht werden, Produkte wie Fitnesstracker zu verwenden, allein um etwas Geld durch die Bereitstellung ihrer personenbezogenen Daten zu erlösen.

> Der DA sollte stärker zwischen personenbezogenen und nicht-personenbezogenen Daten unterscheiden. Insbesondere sollten hinsichtlich personenbezogener Daten die Zwecke stärker eingeschränkt werden, zu diese Daten verwendet werden dürfen. Dritten sollte untersagt werden, eine direkte Wertschöpfung aus der Kommerzialisierung dieser personenbezogenen Daten zu ziehen, sondern lediglich gestattet werden, den Nutzern Dienste auf Basis dieser Daten anzubieten. Insbesondere sollte ausgeschlossen werden, dass diese Daten zu Zwecken des Scorings oder zu Werbezwecken verarbeitet werden.

4. ABGRENZUNG ZWISCHEN B2B- UND B2C-SITUATIONEN

Problematisch ist jedoch nicht nur, dass der DA nicht ausreichend zwischen personenbezogenen und nicht-personenbezogenen Daten differenziert. Auch die einheitliche Betrachtung von B2B- und B2C-Situationen ist kritisch.

So sollen Dateninhaber nicht-personenbezogene Daten[44] auf der Grundlage von vertraglichen Vereinbarungen mit den Nutzern verwenden dürfen.[45] Die Dateninhaber können sich also jegliche Rechte an nicht-personenbezogenen Daten durch vertragliche Vereinbarungen mit den Nutzern sichern. Die faktische Verfügungsgewalt über die Daten kann so auf Basis eines einfachen Vertrags rechtlich zementiert werden. Fraglich

---

[40] Artikel 6 (2) b)

[41] Artikel 6 (2) c)

[42] Wobei unklar ist, ob „nur für die Zwecke und unter den Bedingungen, die er mit dem Nutzer vereinbart hat“ mit „um den vom Nutzer gewünschten Dienst zu erbringen“ gleichzusetzen ist.

[43] Beziehungsweise eine angemessene Verfügung der Nutzer für die Bereitstellung ihrer nicht-personenbezogenen Daten im Sinne der Fairen Verteilung der Wertschöpfung aus Daten gar angebracht sein könnte.

[44] Unter nicht-personenbezogene Daten fallen auch anonymisierte Daten, weswegen auch diese Datenkategorie im B2C-Kontext eine Rolle spielt.

[45] Artikel 4 (6)

ist darüber hinaus, ob die Nutzungsmöglichkeiten der Daten durch Dateninhaber auch deren Weitergabe beziehungsweise deren Verkauf beinhalten. Der DA scheint diese Nutzungsform nicht auszuschließen. Dabei kann auch beispielsweise ein Verkauf der Daten durch den Dateninhaber an Gatekeeper den Interessen der Nutzer entgegenstehen und die Marktmacht der Gatekeeper weiter stärken.[46] Es verwundert, dass mit Artikel 5 (2) zwar die Interessen der Dateninhaber gegenüber den Gatekeepern gesichert werden sollen, aber ein direkter Verkauf der Daten durch die Dateninhaber an Gatekeeper nicht zum Schutz der Nutzerinteressen eingeschränkt wird.

Verträge zur Nutzung nicht-personenbezogener Daten mögen zwar im B2B-Kontext tatsächlich ausgehandelt werden. Im B2C-Kontext wird es sich aber meist um vorformulierte Verträge handeln, mit allen Problemen, die bereits beispielsweise aus dem Datenschutzbereich bekannt sind: Durch die ungleichen Machtverhältnisse besteht die Gefahr, dass die Verträge zum Nachteil der Verbraucher:innen ausgestaltet werden und Dark Patterns und ähnliche Strategien wie die Kopplung der Zustimmung zur Datennutzung an die Erfüllung der Hauptleistung des Vertrags eingesetzt werden. Eine Konkretisierung der möglichen zulässigen Inhalte der Verträge findet sich im DA nicht wieder, sondern richtet sich alleine nach den allgemeinen Verbraucherschutzvorschriften.[47] Auch scheint der DA davon auszugehen, dass der Nutzer die Datennutzung stets gestatten wird.

Kaufen Verbraucher:innen also beispielsweise ein Fahrzeug, könnte der Kaufvertrag eine Art „total-buyout-Klausel“ enthalten, dass der Dateninhaber diese Daten ohne größere Einschränkung im Umfang, für beliebige Zwecke, auf unbestimmte Zeit verwenden und ohne Kompensation nutzen darf (siehe auch Ausführungen in Kapitel III.6.1). Das Ziel, einer ausgewogeneren Verteilung der Wertschöpfung aus den gemeinsam erzeugten Daten, würde so nicht erreicht werden. Unklar ist außerdem, wie beispielsweise im Falle eines Verkaufs des Produkts verfahren wird. Werden die Verträge mit Dateninhabern und Dritten aufgelöst oder weitergeführt? Unter welchen Bedingungen?

Daher sollte im weiteren Gesetzgebungsprozess eine Konkretisierung dieser Verträge im B2C-Kontext erfolgen, um von vorneherein große Rechtsunsicherheit zu vermeiden:

- Beschränkung der Datennutzung: Nicht-personenbezogenen Daten im B2C-Kontext sollten durch Dateninhaber nur für legitime Zwecke wie Produktfunktionalität / -sicherheit und Produktentwicklung verarbeitet werden dürfen. Weitere Verarbeitung der Daten sollte nur zu von den Verbraucher:innen granular ausgewählten Zwecken erlaubt sein. Es sollte verboten sein, Verbraucher:innen in irgendeiner Weise zur Zustimmung zu zwingen, zu täuschen oder zu manipulieren, indem etwa die Erbringung der Hauptleistung an die Zustimmung gekoppelt wird, die Daten für weitere Zwecke verwenden zu dürfen.
- Beschränkung der Datenübermittlung: Nicht-personenbezogenen Daten im B2C-Kontext sollten nur für legitime Zwecke wie Produktfunktionalität / -sicherheit und Produktentwicklung an Dritte übermittelt werden dürfen. Weitere Übermittlungen

[46] Vgl. Kerber, Wolfgang: Stellungnahme zur öffentlichen Anhörung zum Thema „Digital Markets Act“ am 27. April 2022 (2022), S. 4, URL: https://www.bundestag.de/resource/blob/891306/578dd8a1a09df8a565e269e160f1651f/ADrs-20-9-58_Stellungnahme-Prof-Dr-Kerber-data.pdf [Zugriff: 27.04.2022].

[47] Vgl. Erwägungsgrund 9, der auf die Richtlinien über unlautere Geschäftspraktiken, Rechte der Verbraucher:innen sowie über missbräuchliche Klauseln in Verbraucherverträgen verweist. Zumindest ein Vorziehen in die Artikel sollte klarstellend erwogen werden, wie auch bei Artikel 1 (3) und Artikel 1 (4) erfolgt.

sollten nur zu von den Verbraucher:innen gewünschten Zwecken erlaubt sein. Werden die Daten an Dritte vermarktet, sollten Verbraucher:innen angemessen an der Wertschöpfung beteiligt werden.

- Zeitliche Begrenzung der Verträge: Die Geltungsdauer der Verträge sollte befristet sein, beispielsweise auf zwei Jahre. Anschließend sollten Verbraucher:innen stets die Möglichkeit haben, die Verträge zu kündigen. Im Falle eines Verkaufs des Produktes, sollten die Verträge neu abgeschlossen werden müssen.

> Die Reichweite der Verträge zwischen Dateninhaber und Nutzer in B2C-Situationen sollte im weiteren Gesetzgebungsprozess konkretisiert werden, insbesondere hinsichtlich der Zwecke, zu denen die Daten durch Dateninhaber verarbeitet werden dürfen, hinsichtlich der Zulässigkeit der Übermittlung der Daten an Dritte sowie hinsichtlich der Geltungsdauer der Verträge.

5. ERGÄNZUNG VON REGELUNGEN ZUR ANONYMISIERUNG

Die Weiterentwicklung von Anonymisierungstechniken ist ein wesentlicher Baustein, um das Ziel des DA zu erreichen, die Verfügbarkeit von Daten zu verbessern. Eine einwandfreie Anonymisierung stellt jedoch eine überaus anspruchsvolle Herausforderung dar, insbesondere wenn Daten über einen unbestimmten Zeithorizont mit unbestimmten Empfängern geteilt oder gar veröffentlicht werden und somit aus verschiedenen Quellen zusammengeführt werden können. Seit einigen Jahren wird verstärkt daran geforscht, wie mit entsprechenden Sicherheitskonzepten eine starke Anonymisierung erreichen werden kann, ohne dass die Analysequalität leidet. Diese Forschung an Anonymisierungsverfahren sollte verstärkt und gefördert werden.

Weiterhin hat der europäische Gesetzgeber in der DSGVO Abstand von einem absoluten Anonymisierungsbegriff genommen. Anonymisierung ist demnach nicht binär zu verstehen, vielmehr gibt es ein Spektrum verschiedener Anonymisierungsmaßnahmen, die unterschiedliche Qualitäten aufweisen und somit für verschiedene Zwecke unterschiedlich angemessen und geeignet sind. Die DSGVO gibt jedoch keine Auskunft darüber, unter welchen Umständen eine Anonymisierung als hinreichend erachtet werden kann. Hierfür bedarf es gesetzgeberischer Vorgaben und die Entwicklung von Standards, die konkrete Anforderungen an die Anonymisierung festlegen.

Darüber hinaus bedarf es weiterer Schutzkonzepte, mit denen das Risiko einer De-Anonymisierung verringert werden kann. Beispiele für solch weiterführende Schutzkonzepte finden sich im außereuropäischen Ausland. So wurde beispielsweise in Japan das Konzept der „anonymously processed information“ eingeführt.[48] Für die Erstellung solcher Informationen gelten weitreichende Anforderungen, die eine De-Anonymisierung unmöglich machen oder zumindest wesentlich erschweren sollen. Auch nach der Anonymisierung müssen die Verantwortlichen weitere Sicherheitsmaßnahmen ergreifen. Darüber hinaus wurde es verboten, anonymisierte Daten mit anderen Daten zusammenzuführen, um den Personenbezug wiederherzustellen sowie im Anonymisierungsverfahren entfernte, aber noch andernorts vorhandene Merkmale zu erwerben.

[48] Vgl. Geminn, Christian; Laubach, Anne; Fujiwara, Shizuo: Schutz anonymisierter Daten im japanischen Datenschutzrecht (2018), in: ZD, S. 413–420, URL: https://beck-online.beck.de/Bcid/Y-300-Z-ZD-B-2018-S-413-N-1 [Zugriff: 22.04.2022].

Ferner wurden Informationspflichten gegenüber der Öffentlichkeit eingeführt, unter anderem in Bezug auf die Kategorien von Informationen, die in den anonymisierten Daten enthalten sind. Ähnliche Vorgaben sollten auch Eingang in die europäische Gesetzgebung finden.

> Durch gesetzgeberische Vorgaben und die Entwicklung von Standards sollten konkrete Anforderungen an die Anonymisierung sowie an die Verwendung anonymisierter Daten definiert werden.

6. SPEZIFISCHE BETRACHTUNG DES MOBILITÄTSSEKTORS

Im Bereich Mobilität vermag der DA aus den nachfolgend beschriebenen Gründen nicht, verbrauchergerechte und für „Nutzer“ faire Grundlagen zu schaffen. Eine „Gatekeeper“-Funktion durch Fahrzeughersteller oder Beförderungsunternehmen muss vermieden werden. Die Menschen in Deutschland sind noch am ehesten bereit, ihre Mobilitätsdaten weiterzugeben, wenn es der Allgemeinheit bei der Verkehrsinfrastrukturplanung hilft. Ein gutes Drittel der Deutschen ist hingegen gar nicht dazu bereit.[49] Insofern ist es entscheidend, dass die Nutzung von Mobilitätsdaten in einer möglichst transparenten und für Nutzer vollständig kontrollierbaren Weise geschieht. Das ist zwingende Voraussetzung dafür, dass Verbraucher:innen bereit sind, Mobilitätsdaten zu teilen.

6.1 Problem des „extended vehicle“

Wie bereits unter Kapitel III.4 beschrieben, sieht der DA bei nicht-personenbezogenen Daten vor, dass diese vom Dateninhaber auf der Grundlage einer vertraglichen Vereinbarung mit dem Nutzer genutzt werden dürfen. Dateninhaber sind nach dem DA die Autohersteller, während Verbraucher:innen lediglich Bereitstellungsrechte zugestanden wird. Der vzbv sieht eine große Gefahr, dass Autohersteller Fahrzeugkäufer:innen und –halter:innen bereits beim Autokauf mit Allgemeinen Geschäftsbedingungen oder buy-out-Klauseln jede beliebige Datennutzung abverlangen könnten und damit das nutzer- und wettbewerbsfeindliche Konzept des „extended vehicle“[50] auf Dauer zementiert würde. Artikel 8 bietet keinen ausreichenden Schutz vor der Manifestierung der Autohersteller als „Gatekeeper“ mit Hilfe des „extended vehicle“-Konzepts, da Verbraucher:innen keine alternativen Zugangsmöglichkeiten zu den Mobilitätsdaten zur Verfügung stehen – auch in dem Falle, dass sich Hersteller und Dritte nicht einigen können. Verbraucher:innen sollten immer die Möglichkeit haben Intermediäre frei auszuwählen. Eine quasi standardmäßige Weiterleitung der Daten an einen nur zum Schein neutralen Treuhänder („Trust-Center“ nach dem Adaxo-Modell der Autohersteller[51]) erst nach vorheriger Kanalisierung über die Backends der Hersteller stellt nach Ansicht des vzbv

[49] Vgl. vzbv: Repräsentative Bevölkerungsbefragung zum autonomen Fahren (2021), URL: https://www.vzbv.de/sites/default/files/2021-10/vzbv%20-%20Autonomes%20Fahren%20-%20Infografiken.pdf [Zugriff: 02.05.2022].

[50] Der Vorschlag der Autohersteller läuft darauf hinaus, Autodaten in der Obhut der Industrie zu belassen und ein sog. „Trust Center“ einzurichten, das deren Integrität gewährleisten soll. Vgl. VDA: VDA-Konzept für den Zugriff auf fahrzeuggenerierte Daten ADAXO: Automotive Data Access – Extended and Open (2022), URL: https://www.vda.de/vda/de/aktuelles/publikationen/publication/adaxo--automotive-data-access---extended-and-open [Zugriff: 26.04.2022].

[51] Vgl. vorige Fußnote.

keine neutrale Datenbereitstellung dar. Leider sieht der DA keine Regelungen für den Einsatz von Treuhandmodellen vor. Für den Mobilitätsbereich ist das besonders problematisch.

Wenn Nutzer überhaupt nicht wissen, an wen ihre Daten fließen und wozu die Daten genutzt werden, können sie keine informierte – und damit auch keine souveräne – Entscheidung treffen, ob und unter welchen Bedingungen sie ihre Daten teilen möchten. Das würde dem Grundgedanken des DA unmittelbar widersprechen.

Schließlich birgt die Kanalisierung über das Backend der Autohersteller die Gefahr, den freien Wettbewerb zwischen Autoherstellern und Drittanbietern einzuschränken. Denn nach Artikel 5 müssen Autohersteller ihre Daten nur auf Verlangen eines Nutzers für diesen bereitstellen. Die Nutzer wissen aber gar nicht, welche Daten relevant sind oder welche Dienstleistungen überhaupt möglich wären, wenn relevante Daten bereitgestellt würden.

Ohne die Kooperation der Automobilhersteller können weder Verbraucher:innen noch andere Akteure wie beispielsweise Reparaturwerkstätten auf Mobilitätsdaten zugreifen. Auch wenn die Autohersteller grundsätzlich bereit sind, den Zugang zu bestimmten Arten von Mobilitätsdaten gegen Entgelt zu verschaffen, können sie die Bedingungen diktieren, das heißt sie können frei darüber entscheiden, welche Daten sie zur Verfügung stellen wollen und zu welchen Preisen und Bedingungen.

Wenn zum Beispiel eine freie Werkstatt ihren Kund:innen anbieten will, dass die Werkstatt bei kritischen Messwerten sofort benachrichtigt wird, müsste die Werkstatt mit dem Autohersteller die Modalitäten für die Datenbereitstellung in Echtzeit vertraglich vereinbaren. Mit dieser Bitte dürfte ein Unternehmen noch nicht einmal an seine Kund:innen herantreten, wenn es sich nicht um eine freie Werkstatt handelt, sondern um ein Unternehmen, das als Gatekeeper zentrale Plattformdienste erbringt.[52] Google ist es daher verboten, seine Kunden aufzufordern, vom Autohersteller Wetterdaten (etwa von den Regensensoren) übermittelt zu bekommen. Ein regionaler Wetterdienstanbieter dürfte das zwar, hätte aber keinen Einfluss auf wichtige Umstände, wie etwa Schnittstellen oder Relevanz der bereitzustellenden Daten. Um den Nutzern von Autos nachfrageorientierte und möglichst umfängliche Dienste anbieten zu können, sind Drittanbieter aber auf relevante Daten angewiesen. So könnten Daten von den Regensensoren zu einer verbesserten, standortgenauen Regen- oder sogar Glättewarnung führen.

Zwar existieren im Sektor Mobilität verschiedene europarechtliche Vorgaben zum Datenteilen[53], aber es verbleibt ein großer Widerspruch zum DA: Dieses Datenteilen ist letzten Endes nicht kostenlos für den Nutzer. Wenn es um das Datenteilen zwischen Dateninhabern und Dritten geht, müssen die Dritten für die Bereitstellung der Daten grundsätzlich zahlen. Der Zweck des DA ist hingegen, dem Nutzer ein Recht auf kostenlose Bereitstellung der Daten zu geben. Warum sollte der Nutzer aber für eine standortgenaue Regenwarnung mehr Geld ausgeben, weil der Dritte (zum Beispiel Betreiber einer Wetterwarn-App) seinerseits den Autohersteller entlohnen muss für dieselben Daten, die der Nutzer nach dem DA unentgeltlich bereitgestellt verlangen darf?

---

[52] Artikel 5 (2)

[53] Z.B.: Richtlinie 2010/40/EU des europäischen Parlaments und des Rates vom 7. Juli 2010 zum Rahmen für die Einführung intelligenter Verkehrssysteme im Straßenverkehr und für deren Schnittstellen zu anderen Verkehrsträgern (IVS-Richtlinie); Richtlinie 2010/40/EU des Europäischen Parlaments und des Rates hinsichtlich der Bereitstellung EU-weiter multimodaler Reiseinformationsdienste.

Zwar sieht der DA das Bereitstellen von Daten an Nutzer grundsätzlich vor, aber nicht die Modalitäten, wie das zu geschehen hat, etwa nicht den zwingenden Einsatz eines Treuhänders. Es stellt sich die Frage, wie neutral Autohersteller sein können, wenn es beispielsweise um eine Unfallaufklärung geht. Wenn es um bürgerliche Freiheitsrechte geht, die unter anderem den Einzelnen und seine Entscheidungen gegenüber dem Staat schützen sollen, darf die Entscheidung, welche Daten zum Beispiel an Strafverfolgungsbehörden gehen, nicht den Herstellern überlassen bleiben.

> Der Data Act darf nicht das wettbewerbskritische und verbraucherunfreundliche „extended vehicle“-Konzept und die damit verbundene exklusive Kontrolle über die Daten durch die Autohersteller zementieren.

6.2 Notwendigkeit einer sektorspezifischen Regulierung für den Mobilitätsbereich

Die vorstehend aufgeführten Probleme lassen sich nicht alleine durch eine horizontale Regelung im DA beheben. Daher sind sektorspezifische Regelungen für den Mobilitätsbereich vorzugsweise auf europäischer Ebene erforderlich, die unter anderem eine neutrale Mobilitätsdatentreuhand[54] verpflichtend vorsehen und für den Mobilitätsbereich spezialisierte Personal Information Management Systeme (PIMS) mit der Funktion eines „Einwilligungsassistenten“ ermöglichen. Der DA sollte um eine Generalklausel erweitert werden, wonach Daten, die nach dem DA für Verbraucher:innen kostenlos bereitzustellen sind, nicht durch sektorspezifische Rechtsvorschriften mittelbar doch wieder kostenpflichtig werden.

> Der vzbv fordert eine sektorspezifische Regelungen für den Mobilitätsbereich in einem vorzugsweise europäischen Mobilitätsdatengesetz, um die Position der Verbraucher:innen gegenüber der Marktmacht der Verkehrsunternehmen zu stärken sowie eine effiziente und an Gemeinwohlzielen orientierte Nutzung der sehr großen Mengen von Mobilitätsdaten zu gewährleisten.

[54] Vgl. zu den Vorteilen: Specht-Riemenschneider, Louisa; Kerber, Wolfgang: Datentreuhänder - Ein problemlösungsorientierter Ansatz (2022), S. 59ff, URL: https://www.kas.de/documents/252038/16166715/Designing+Data+Trustees+-+A+Purpose-Based+Approach.pdf [Zugriff: 28.04.2022].