REGELUNGEN DER DSGVO IM SPANNUNGSVERHÄLTNIS ZUM DATA ACT?

und anderen neuen Ansätzen, die eine größere Verkehrsfähigkeit von Daten erreichen wollen[1]

I. Einführung

Die EU habe den Anschluss an den Wettbewerb verloren, 80% der europäischen Daten seien ungenutzt. Es bestünden eine Vielzahl an Hindernissen für das Teilen von Daten im B2B-Sektor. Würde das volle Potential der Datenwirtschaft genutzt, würde das europäische BIP um über 270 Billionen Euro bis 2028 steigen, meint René Schneider[2]. Um die EU im Bereich der Datenwirtschaft zu fördern, werden im Rahmen der Datenstrategie der EU-Kommission eine Vielzahl an Rechtsakte vorgestellt. Diese umfassen neben der bereits eine Weile in Kraft befindlichen DSGVO, das Free Flow of Data Act, den Data Governance Act, das Digital Markets Act und das Digital Services Act.[3] Die genannten Rechtsakte haben die Verbreitung von Daten zum Ziel. Hierbei scheint es zu Spannungen zwischen dem Datenschutz als Ausdruck des Schutzes des Einzelnen und Datenverbreitung bzw. Datennutzung für den womöglich gesamtgesellschaftlichen Wohlstand und Fortschritt zu kommen. „*Der EDSA und der EDSB sind der Ansicht, dass dieser politische Trend hin zu einem datengesteuerten wirtschaftlichen Rahmen ohne ausreichende Berücksichtigung der Aspekte des Schutzes personenbezogener Daten aus der Sicht der Grundrechte ernsthafte Bedenken aufwirft. […] [Sie] weisen darüber hinaus darauf hin, dass das Modell der Europäischen Union auf der durchgängigen Berücksichtigung ihrer Werte und Grundrechte bei den Entwicklungen ihrer Politik beruht und dass die DSGVO als Grundlage betrachtet werden muss, auf der ein europäisches Daten-Governance-Modell aufzubauen ist.*“[4] Dem scheint sich die EU-Kommission in ihrer Vorstellung zur „Digitalen Dekade“ anzuschließen. Denn ihr Ansatz für die nächsten zehn Jahre soll eine auf den Menschen ausgerichtete und nachhaltige Vision für die digitale Gesellschaft sein, um Bürger und Unternehmen zu stärken. Im Rahmen der Vorstellung der Digitalen Dekade hat die Kommission auch eine Erklärung Europäische Digitale Rechte und Grundsätze vorgestellt.[5] Die Kommission möchte sicherstellen, dass die Menschen voll befähigt sind die Möglichkeiten der Digitalen Dekade zu genießen.[6] Der aktuelle Entwurf des Data Acts scheint der Schauplatz dieses

---

[1] Der Beitrag entstand im Rahmen von Recherchetätigkeiten des Autors, Nicolas Kutschera, von Juli bis September 2022 als wissenschaftlicher Mitarbeiter am Lehrstuhl für Strafrecht, Strafprozessrecht, Rechtstheorie, Informationsrecht und Rechtsinformatik bei Prof. Dr. Dr. Eric Hilgendorf. Der Text wurde im August 2023 überarbeitet. Der Autor ist für den Inhalt allein verantwortlich.

[2] René Schneider ist Legal Director bei CGI, Senior Privacy Consultant bei DataGuard, sowie freiberuflicher Rechtsanwalt und Datenschutzbeauftragter.

[3] *Schneider, René,* „EU Data Act Draft – selected challenges for switching data processing services and international data transfers.” EPIC Summit 2022, Mai 2022, Web, 31.08.2023, https://lp.dataguard.de/hubfs/EPIC/EPIC%202022/EPIC%20on%20Demand%20Desktop/Stage%203%20_%20EU%20Data%20Act%20Draft%20%E2%80%93%20selected%20challenges%20for%20switching%20data%20processing%20services%20and%20international%20data%20transfers_150102_HQ.mp4.

[4] *EDSA/EDSB,* Gemeinsame Stellungnahme 03/2021 des EDSA und des EDSB zum Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über europäische Daten-Governance (Data-Governance-Gesetz). Version 1.1 vom 09.06.2021, S. 9.

[5] *Europäische Kommission,* Europe‘s Digital Decade. Digital-Strategy.ec.europa.eu, zuletzt geupdatet am 24.08.2022, https://digital-strategy.ec.europa.eu/en/policies/europes-digital-decade, abgerufen am 01.09.2022.

[6] *Europäische Kommission,* European Digital Rights and Principals. Digital-Strategy.ec.europa.eu, Zuletzt geupdatet am 04.05.2022, https://digital-strategy.ec.europa.eu/en/policies/digital-principles, abgerufen am 01.09.2022.

Zwiespalts der Kommission zu sein. Denn dieser müsste eigentlich das größte Potenzial für die Datenwirtschaft haben. Aus diesem Grund erfolgt auch eine sehr detaillierte Auseinandersetzung mit dem aktuell noch in erster Lesung befindlichen Kommissionsentwurf.[7]

INHALTSVERZEICHNIS

I. Einführung ***1***

II. Das Data Act und die DSGVO ***4***

1. Kurzfassung mit Verweisen **5**

2. Allgemeine Bestimmungen (Kapitel I) **6**

a) Art. 1 - Anwendungsbereich 6

aa) Personenbezogen oder nicht? 6

bb) Produkt im Data-Act 7

cc) Datenschutzklausel 8

b) Art. 2 – Definitionen 9

3. Zugangsrechte zu Daten – Art. 3 bis 7 (Kapitel II) **10**

a) Art. 3 – Konzeption und Informationspflicht 10

b) Art. 4 – Recht auf Zugang der erzeugten Daten 11

aa) Art. 4 Abs. 1 - Zugangsrecht 11

bb) Art. 4 Abs. 2 - Spezifizierungsverlangen 11

cc) Art. 4 Abs. 3 - Geschäftsgeheimnisse 12

dd) Art. 4 Abs. 4 - Konkurrenzprodukt 12

ee) Art. 4 Abs. 5 – nicht von der Datenverarbeitung betroffener Nutzer 13

(1) Das Kopplungsverbot 14

(2) Berechtigte Interessen 15

(3) Besondere Kategorien 15

(4) Zweck der Verarbeitung 15

(5) Anonymisierte Daten 16

ff) Art. 4 Abs. 6 – Vertrag über Nutzung nicht-personenbezogener Daten 17

c) Art. 5 – Weitergabe an Dritte 17

d) Art. 6 – Pflichten Dritter, die Daten i.A. des Nutzers erhalten 19

e) Art. 7 – KMU-Ausnahme und virtuelle Assistenten 20

4. Pflicht Daten Dritten bereitzustellen – Art. 8 bis 12 (Kapitel III) **20**

5. Missbräuchliche Klauseln für Datenzugang und Datennutzung (Kapitel IV) **22**

6. Pflichten Daten öffentlichen Stellen bereitzustellen – Art. 14 bis 22 (Kapitel V) **23**

7. Wechsel zwischen Datenverarbeitungsdiensten – Art. 23 bis 26 (Kapitel VI) **26**

8. Internationaler Zugang und internationale Übermittlung für nicht-personenbezogene Daten – Art. 27 (Kapitel VII) **27**

9. Interoperabilität – Art. 28 bis 30 (Kapitel VIII) **28**

10. Anwendung und Durchsetzung – Art. 31 bis 34 (Kapitel IX) **28**

a) Art. 31 – Zuständige Behörden 28

[7] Mittlerweile liegt laut einer Pressemitteilung der Kommission eine politische Einigung zwischen den drei Häusern vor: *EU-Kommission,* Datengesetz: Kommission begrüßt politische Einigung über Vorschriften für eine faire und innovative Datenwirtschaft. Pressemitteilung der EU-Kommission vom 28.06.2023, https://ec.europa.eu/commission/presscorner/detail/de/ip_23_3491, zuletzt abgerufen am 30.08.2023.

b) Art. 32 – Recht auf Beschwerde 30
c) Art. 33 – Sanktionen 30
d) Art. 34 – Mustervertragsbedingungen 30

11. Art. 35 – Sui-Generis-Recht im Rahmen der RL 1996/9/EG (Kapitel X) 31

12. Art. 36 bis 42 – Schlussbestimmungen (Kapitel XI) 31

13. Kohärenz mit anderen EU-Rechtsakten 31

III. Data Governance Act – Verordnung (EU) 2022/868 32

IV. Free Flow of Data Act – VO(EU) 2018/1807 34

V. Open Data und Public Sector Information Directive – RL(EU) 2019/1024 34

VI. ePrivacy-Richtlinie und ePrivacy-Verordnung 35

VII. Strafverfolgungsrechtsakte 37

1. Verwendung von Fluggastdatensätzen zur Strafverfolgung – RL(EU) 2016/681 37

2. Agentur zur Zusammenarbeit auf dem Gebiet der Strafverfolgung – VO(EU) 2016/794 37

3. Verstärkte Zusammenarbeit zur Errichtung der Europäischen Staatsanwaltschaft – VO(EU) 2017/1939 38

VIII. Rechtsakte im Wettbewerbs-, Urheber- und digitalen Vertragsrecht 38

1. Digital Markets Act – COM(2020) 842 final 38

2. Richtlinie Urheberrecht und verwandten Schutzrechten im digitalen Binnenmarkt – RL(EU) 2019/790 38

3. Digitale Inhalte Richtlinie – RL(EU) 2019/770 40

IX. Kollision von EU-Rechtsakten 40

II. Das Data Act und die DSGVO[8]

Das Data Act ist Teil der EU-Strategie für eine gemeinsame digitale Zukunft. Sie ist das Schlüsselinstrument, um mehr Daten verfügbar zu machen und diese im Einklang mit dem Recht und den Werten der EU zu verwenden.[9] Der Europäische Datenschutzausschuss (EDSA) und der Europäische Datenschutzbeauftragte (EDSB) warnen in einer gemeinsamen Stellungnahme, dass der aktuelle Data-Act-Vorschlag eine Entwicklung zu einer Kommerzialisierung personenbezogener Daten vorantreibt und personenbezogene Daten als bloße Handelsware betrachtet werden könnten. Dies würde das Konzept der Menschenwürde und den auf Menschen ausgerichteten Ansatz, die die EU in ihrer Datenstrategie als wesentliches Ziel angibt, untergraben.[10]

Das Data Act soll einen Rechtsrahmen für den Zugriff auf Daten und das Teilen und Wiederverwenden von Daten im Bereich B2C, B2B und B2G schaffen. Daneben soll auch das Wechseln zwischen Anbietern gefördert und Interoperabilitätsstandards geschaffen werden. Während Gatekeeper (Digital Markets Act) Beschränkungen unterliegen sollen, sollen KMUs privilegiert werden. Die öffentliche Hand (B2G) soll bei Vorliegen von Öffentlichem Interesse, Notfällen oder Krisen die Möglichkeit haben auf Daten von Unternehmen zuzugreifen.[11]

All dies soll im Einklang mit den bisherigen datenschutzrechtlichen Vorgaben funktionieren, insbesondere der Datenschutzgrundverordnung. Doch schafft der Verordnungsvorschlag das und schafft er es überhaupt seine deklarierten Ziele zu erreichen? Prof. Wolfgang Kerber von der Universität Marburg meint zwar, dass das wesentliche Problem, die defacto Kontrolle über alle generierten Daten aufgrund des technischen Designs, vom Entwurf erfasst wird. Die Lösungsvorschläge des Vorschlags seien aber bei weitem nicht ausreichend. Der Mechanismus für die Nutzerrechte leide unter zahlreichen schwerwiegenden Problemen, die ihn schwach und weitgehend unwirksam machen würden. So sei der Umfang an Daten unzureichend, die Transaktionskosten hoch, insbesondere durch das Aushandeln der fairen, angemessenen und nichtdiskriminierenden Bedingungen. Die Nutzer würden durch die vertragliche Grundlage auch nicht mehr Kontrolle über die Nutzung der IoT-Daten erhalten, da es weiterhin ungelöste schwerwiegende Probleme des Marktversagens in B2C-Situationen gebe, sodass alle Nutzungsrechte bei den Dateninhabern verbleiben werden. Der Hauptgrund für dieses Fazit sei das Beharren des Vorschlags auf den Schutz der exklusiven De-facto-Kontrollposition der Dateninhaber, obwohl es sehr zweifelhaft sei, ob im Falle von IoT-Geräten aufgrund kostendeckender Preise, überhaupt ein Anreizproblem für Investitionen bestehe. Eine Neugewichtung zugunsten einer einfacheren und umfassenderen gemeinsamen Nutzung von Daten und einer stärkeren Befähigung der Nutzer sei erforderlich, insbesondere um mehr Innovationen in der Datenwirtschaft zu ermöglichen.[12] Auch Prof. Louisa Specht-Riemenschneider attestiert dem Entwurf, dass er die politischen Ziele, denen er sich verpflichtet

---

[8] Der Abschnitt befasst sich ausschließlich mit dem Data Act in der Fassung der Kommission.

[9] *Europäische Kommission,* Shaping Europe´s digital future, https://digital-strategy.ec.europa.eu/en/policies/data-act, abgerufen am 04.07.2022.

[10] *EDSA/ EDSB,* EDPB-EDPS Joint Opinion 2/2022 on the Proposal of the European Parliament and of the Council on harmonized rules on fair access to and use of data (Data Act). Brüssel 04.05.2022, S. 2-8.

[11] *Schneider, René,* „EU Data Act Draft – selected challenges for switching data processing services and international data transfers." EPIC Summit 2022, Mai 2022, Web, 31.08.2023, https://lp.dataguard.de/hubfs/EPIC/EPIC%202022/EPIC%20on%20Demand%20Desktop/Stage%203%20_%20EU%20Data%20Act%20Draft%20%E2%80%93%20selected%20challenges%20for%20switching%20data%20processing%20services%20and%20international%20data%20transfers_150102_HQ.mp4.

[12] Vgl. ausführlich *Kerber, Wolfgang,* Governance of IoT Data. Why the EU Data Act will not fulfill its objectives (2022), S. 1, URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4080436 (abgerufen am 22.08.2022).

hat, nicht erreicht. Nachschärfen müsste der Entwurf u.a. bei vielen offenen Rechtsbegriffen, der Differenzierung zwischen gewerblichen Nutzern und Verbrauchern, dem Datenzugangsanspruch der Wissenschaft und der Nutzer, einer adäquaten Ausgestaltung der Vertragsbeziehung nach Art. 4 VI mit dem Kopplungsverbot und zwingenden Regelungen zugunsten von Verbrauchern, einer Schrankenregelung wie Art. 20 IV DSGVO und einer Datentreuhandlösung, bei der etwa eine staatliche Stelle Datenzugangsverlangen prüft und ggf. Maßnahmen ergreift.[13]

1. Kurzfassung mit Verweisen

Der Entwurf des Data Act gefährdet die effektive Durchsetzung der Betroffenenrechte und könnte das Datenschutzniveau der DSGVO absenken. Der aktuelle Entwurf kann ausgehend zweier Analysen nicht die gesetzten Ziele erreichen (S. 4f). Allein dieser Kritikpunkt lässt die zu befürchtenden Einschränkungen im Datenschutz in einem dramatischeren Licht erscheinen.

Besonders kritisch hervorzuheben sind m.E. die Einschränkungen aufgrund der Unterschiede zwischen personenbezogenen und nicht-personenbezogenen Daten. Der Entwurf erweckt den Eindruck, als sei die Mehrzahl der durch ein Gerät aufgrund der Nutzung generierten Daten keine personenbezogenen Daten, was den Anwendungsbereich der datenschutzrechtlichen Bestimmungen in den Hintergrund rückt. Dies scheint aber höchst zweifelhaft. Zwar unterscheidet die Definition und die einzelnen Nutzeranspruchsnormen nicht zwischen personenbezogenen und nicht-personenbezogenen Daten (S. 6-7). Allerdings erfolgt keine Unterscheidung zwischen Betroffenen und Nutzern. Mögliche datenschutzrechtliche Subjekte gehen bei den Rechten, die das Data Act gewährt nur nicht leer aus, wenn sie auch Nutzer im Sinne des Data Acts sind (S. 17-21). Daneben verpasst der Vorschlag die Chance den Betroffenen durch die Spiegelung von Privacy by Design und Default eine möglichst anonyme, pseudonymisierte oder sonst datensparsame Nutzung zu ermöglichen (S. 10). Der in Art. 4 angesprochene Nutzungsvertrag, den der Dateninhaber mit dem Nutzer abschließen muss, der auch Verbraucher sein kann, lässt entsprechende verbraucherschützende Regelungen vermissen (S. 4, 11, 17ff). Dauerprobleme wie das Kopplungsverbot werden durch diese Konstellationen nicht gelöst, sondern neu angefacht (S. 14-15). Auch eine klare Unterscheidung zwischen Daten, pseudonymisierten oder anonymisierten Daten gelingt nicht (S. 6f, 16f). Der Verordnungsvorschlag spricht mal von nicht personenbezogenen und mal von pseudonymisierten Daten, ohne dies zu definieren. Der Entwurf vermisst es klare Vorgaben für die Pseudonymisierung und Anonymisierung zu machen. Schließlich verweist er in einzelnen Vorschriften stets auf die Unberührtheit der datenschutzrechtlichen Bestimmungen (S. 8-9). Dadurch ergeben sich zwei unterschiedliche Lager von Kritikern. Die einen befürchten eine Ausweitung des Anonymisierungsproblems der DSGVO auf nicht-personenbezogene Daten, die anderen befürchten ein Absinken des Datenschutzniveaus, da der Entwurf durch die vielen Unklarheiten dazu beiträgt, dass Unternehmen selbst entscheiden müssen, wo sie das Datenschutzrecht beachten und wo nicht (S. 6f, 8f). Die Regelungen rund um die fairen Bedingungen zur Bereitstellung von Daten führen zu einer Monetarisierung personenbezogener Daten, auch wenn die Nutzer selbst diese kostenlos erhalten (S. 20-23). Den Regelungen zur Bereitstellung von Daten an öffentliche Stellen fehlt es an Rechtmäßigkeit, Erforderlichkeit und Angemessenheit der Verpflichtungen (S. 23-26). Kritikwürdig ist auch die Regelung der Sanktionen und Aufsichtsbehörden (S. 28-31). Die Datenschutzbehörden sollen – obwohl es stets um personenbezogene Daten gehen könnte – nach dem Entwurf nicht mal zwangsweise die koordinierende Behörde eines Mitgliedstaats darstellen. Stattdessen soll es möglich sein, neue Behörden einzurichten. Die nach dem Entwurf vorgesehene Zuständigkeit der Datenschutzaufsichtsbehörden wirft zudem weitere Fragen auf

[13] *Specht-Riemenschneider, Louisa,* Der Entwurf des Data Act: Ein großer Wurf in die falsche Richtung? In: GRUR 2022, 937 (938).

(S. 28-29). Das Beschwerderecht ist zu unklar hinsichtlich der Anlaufstelle für Beschwerdeführer und der Anwendbarkeit der Norm (S. 29f) und die Sanktionen erwecken eher den Eindruck einer Richtlinie ohne klare Vorgaben und ohne Harmonisierungswirkung (S. 30).

2. Allgemeine Bestimmungen (Kapitel I)

a) Art. 1 - Anwendungsbereich

Die Verordnung gilt nach Art. 1 Abs. 2 für Hersteller und Nutzer von Produkten und Erbringer verbundener Dienste, solange diese in der Union in Verkehr gebracht werden (a), Dateninhaber, die Empfängern in der Union Daten bereitstellen (b), Datenempfänger in der Union, denen Daten bereitgestellt werden (c), öffentliche Stellen und Organe, Einrichtungen und sonstige Stellen der Union, die von Dateninhabern die Bereitstellung von Daten verlangen (d) und Anbieter von Datenverarbeitungsdiensten, die Kunden in der Union Dienste anbieten (e). Damit handelt es sich um einen umfassenden Anwendungsbereich, der den gesamten Binnenmarkt abdeckt, also auch ausländische Unternehmen erfasst, solange diese im konkreten Fall europäische Kunden haben oder entsprechend in Europa ihre Produkte oder Dienstleistungen anbieten. Das Data Act ist insoweit auch anwendbar, als öffentliche Stellen aufgrund einer außergewöhnlichen Notwendigkeit zur Wahrnehmung einer Aufgabe von öffentlichem Interesse die Bereitstellung von Daten verlangen. Zu denken ist insbesondere an die Bereitstellung von Standortdaten, wie sie die Telekom 2020 der Bundesregierung zur Eindämmung des Corona-Virus zur Verfügung gestellt hatte.[14]

Teil des Anwendungsbereichs ist auch der sachliche Gegenstand des Datengesetzes. Nach Art. 1 Abs. 1 geht es um die Bereitstellung von Daten. Der Verordnungsentwurf betrifft grundsätzlich personenbezogene und nicht-personenbezogene Daten von Produkten oder mit diesen verbundenen Dienstleistungen bzw. Software. Denn Art. 2 Nr. 1 definiert Daten als „*jede digitale Darstellung von Handlungen, Tatsachen oder Informationen sowie jede Zusammenstellung solcher Handlungen, Tatsachen oder Informationen auch in Form von Ton-, Bild- oder audiovisuellem Material*“. Ob Daten personenbezogen sind oder nicht ist für die Anwendbarkeit des Datengesetzes irrelevant. Das Datenschutzrecht ist aber stets bei der Anwendung des Data Act mitzuberücksichtigen. Denn werden nicht-personenbezogene Daten geteilt muss aus Sicht des Datenschutzes zunächst geprüft werden, ob wirklich kein Personenbezug gegeben ist. Daneben knüpft sich daran u.a. auch die Zuständigkeit von Aufsichtsbehörden an (S. 28f).

aa) Personenbezogen oder nicht?

René Schneider kritisiert in einem Vortrag beim EPIC Summit 2022 am 25.05.2022, dass die Differenzierung zwischen personenbezogenen und nicht personenbezogenen Daten nicht klar und eine Trennung innerhalb desselben Cloudspeichers möglicherweise technisch gar nicht möglich sei. Bspw. können auch Telemetriedaten personenbezogene Daten sein, gerade solche (Nutzungs-, Diagnose- und Verbindungsdaten) sind aber vom Entwurf erfasst.[15] Wie das Beispiel vernetzter Fahrzeuge zeigt, können die meisten von einem solchen generierten Daten als

---

[14] Die Bereitstellung erfolgte damals freiwillig und war wohl je nach verwandter Anonymisierungstechnik rechtmäßig. Mehr dazu: *Piltz, Carlo/ Zwerschke, Johannes,* Telekom gibt Handy-Standortdaten weiter. Daten dürfen Leben retten. Legal Tribune Online vom 19.03.2020, https://www.lto.de/recht/hintergruende/h/telekom-corona-krise-daten-weitergabe-rki-datenschutzrecht-dsgvo/, abgerufen am 04.08.2022.

[15] *Schneider, René,* „EU Data Act Draft – selected challenges for switching data processing services and international data transfers.” EPIC Summit 2022, Mai 2022, Web, 31.08.2023, https://lp.dataguard.de/hubfs/EPIC/EPIC%202022/EPIC%20on%20Demand%20Desktop/Stage%203%20_%20EU%20Data%20Act%20Draft%20%E2%80%93%20selected%20challenges%20for%20switching%20data%20processing%20services%20and%20international%20data%20transfers_150102_HQ.mp4.

personenbezogen betrachtet werden. Der EDSA schrieb dazu in seinen Leitlinien zu vernetzten Fahrzeugen: *„Auch wenn die von einem vernetzten Fahrzeug erhobenen Daten nicht direkt mit einem Namen, sondern mit technischen Aspekten und Merkmalen des Fahrzeugs verknüpft sind, betreffen sie den Fahrer oder die Insassen des Fahrzeugs. Zur Veranschaulichung: Daten über den Fahrstil oder die zurückgelegte Strecke, Daten über die Abnutzung von Fahrzeugteilen, Standortdaten oder von Kameras erhobene Daten können das Verhalten des Fahrers ebenso betreffen wie Informationen über andere Personen, die sich im Fahrzeug aufhalten, oder über betroffene Personen, an denen das Fahrzeug vorbeifährt. Solche technischen Daten werden von einer natürlichen Person erzeugt und ermöglichen ihre direkte oder indirekte Identifizierung durch die Person, die für die Verarbeitung der Daten verantwortlich ist (im Folgenden „Verantwortlicher"), oder durch eine andere Person.*"[16]

Personenbezogene und nicht personenbezogene Daten könnten nicht getrennt werden, die Herstellung von echten anonymen Daten sei nur schwer möglich. Daneben fielen die Anforderungen an die Datenverwendung auseinander. Während Art. 18 Abs. 5 des Data Act pseudonymisierte Daten ausreichen lässt, setzt die DSGVO weitgehend auf anonymisierte Daten, bspw. Art. 89 Abs. 1 DSGVO[17]. Das Trennungsproblem könnte jedoch die unterschiedlichen Ansatzpunkte und damit eine Bevorzugung der Pseudonymisierung erklären. Schneider sieht im weiteren Verlauf eine Ausweitung des Anonymisierungsproblems der DSGVO hin zu nicht-personenbezogenen Daten.[18] Allerdings ist insoweit zu entgegnen, dass nicht von einer Ausweitung gesprochen werden kann. Vielmehr liegen stets personenbezogene Daten vor, wenn die Anonymisierungs- oder Pseudonymisierungsversuche trotzdem einen Personenbezug erlauben, da damit gerade personenbezogene Daten vorliegen.[19] Das Problem wird also durch den Data Act nicht neu geschaffen, sondern lediglich aufgrund möglicher neuer Nutzungsmöglichkeiten von Daten in den Vordergrund gerückt. Die Ausführungen des EDSA zu vernetzten Fahrzeugen werfen die Frage auf, ob es sich bei von Nutzern generierten Daten überhaupt um nicht-personenbezogene Daten handeln kann.

bb) Produkt im Data-Act

Unter Produkt ist eine körperliche, bewegliche Sache zu verstehen, die Daten betreffend die Nutzung und Umgebung sammelt und mit öffentlicher elektronischer Kommunikation weiterleitet, Art. 2 Nr. 2 Datengesetz. Umfasst sein kann dabei auch ein in unbewegliche Sachen eingebautes Produkt. Die Hauptfunktion des Produkts darf nicht das Speichern oder Verarbeiten von Daten sein. Verbundene Dienstleistungen sind digitale Dienstleistungen oder Software, die in das Produkt eingebaut oder damit vernetzt und für eine Funktion erforderlich sind.[20]

Insoweit ist eine Vielzahl an Produkten erfasst wie Smart-Home-Systeme, Autos, Maschinen, Roboter, Traktoren, Baumaschinen, medizinische Geräte oder Systeme mit Künstlicher Intelligenz. Nicht erfasst werden damit Geräte, die vor allem für das Anzeigen, Abspielen,

---

[16] *EDSA*, Leitlinien 01/2020 zur Verarbeitung personenbezogener Daten im Zusammenhang mit vernetzten Fahrzeugen und mobilitätsbezogenen Anwendungen. Version 2.0, 09.03.2021, S. 5.
[17] *Schneider, René,* „EU Data Act Draft – selected challenges for switching data processing services and international data transfers." EPIC Summit 2022, Mai 2022, Web, 31.08.2023, https://lp.dataguard.de/hubfs/EPIC/EPIC%202022/EPIC%20on%20Demand%20Desktop/Stage%203%20_%20EU%20Data%20Act%20Draft%20%E2%80%93%20selected%20challenges%20for%20switching%20data%20processing%20services%20and%20international%20data%20transfers_150102_HQ.mp4.
[18] Ebd.
[19] Paal/Pauly/Ernst, 3. Aufl. 2021, DS-GVO Art. 4 Rn. 48f.
[20] Art. 2 Nr. 2 Data Act Entwurf.

Aufnehmen oder Übermitteln von Inhalten spezifiziert sind. Fragezeichen kommen dabei aber bei klassischen Fax-Multifunktionsgeräten auf, bei denen die Speicherung und Verarbeitung von Daten und die Übermittlung gleichermaßen relevant ist.[21] Genauso problematisch ist die Anwendung auf Fitnesstracker, wobei die Folgefrage sich sodann auf Smartwatches erweitert, die Fitnessdaten erheben können, sowie Smartwatches die zusätzlich dazu noch Telefonie ermöglichen. Genauso ist es mit Fahrzeugen, als scheinbar klassisch von der Verordnung erfasste Produkte. Diese bieten neben Telefonie auch Entertainmentmöglichkeiten. Ist es Verbraucher:innen in Zukunft nur möglich auf einen Teil ihrer Daten zuzugreifen, auf andere nicht?[22]

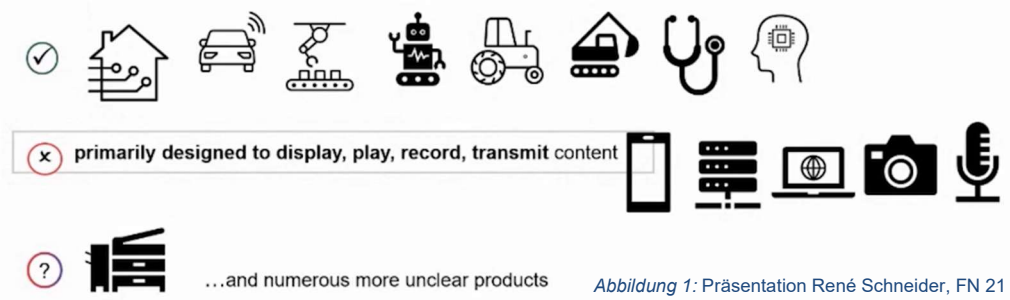

Abbildung 1: Präsentation René Schneider, FN 21

EDSA und EDSB sehen in der Definition von Produkt nach Art. 2 Nr. 2, verbundenen Dienst nach Art. 2 Nr. 3 und virtuellen Assistenten nach Art. 2 Nr. 4 Überschneidungen mit dem Begriff „Endeinrichtungen“ aus Art. 1 Nr. 1 lit. a der Richtlinie 2008/63/EG der Kommission aus bzw. „Endgerät“ im Sinne von Art. 5 Abs. 3 ePrivacy-Richtlinie. Denn die ePrivacy-Richtlinie sieht die Zustimmung des Teilnehmers oder Nutzers vor der Speicherung von Informationen oder dem Zugriff auf bereits gespeicherte Informationen im Endgerät eines Teilnehmers oder Endnutzers vor, es sei denn der Zugriff wäre unbedingt erforderlich, um einen ausdrücklich angeforderten Dienst zu erbringen.[23] Daneben ist auch stets eine Rechtsgrundlage nach Art. 6 DSGVO notwendig. Zwar stellt Erwägungsgrund 15 klar, dass Produkte wie private Computer, Server, Tablets, Smartphones, Kameras, Webcams, Tonaufzeichnungssysteme und Textscanner nicht unter den Vorschlag fallen würden, EDSA und EDSB sind aber dennoch der Ansicht, dass Art. 2 Nr. 2 nach dem Wortlaut solche Geräte trotzdem erfasst. Deshalb sollte die Definition von Produkt entsprechend angepasst werden.[24]

cc) Datenschutzklausel

Besonders hinzuweisen ist auf Art. 1 Abs. 3 Datengesetz. Hier wird explizit auf die die DSGVO und die ePrivacy-Richtlinie verwiesen, deren Anwendbarkeit durch das Data Act nicht berührt sein soll. Sollte es sich aber bei den Nutzern um von der Verarbeitung personenbezogener Daten betroffene Personen handeln, ergänzen die Bestimmungen des Kapitel II das Recht auf Datenübertragbarkeit nach Art. 20 DSGVO. Dem Verbraucherzentrale Bundesverband e.V. und dem Europäischen Datenschutzbeauftragten und Datenschutzausschuss gehen diese Klarstellung nicht weit genug, weshalb sie eine Ersetzung durch eine ähnliche Vorschrift des Data Governance Act fordern.[25] Denn die Vorschrift des Art. 1 Abs. 3 des Data Governance Act gibt

---

[21] Abbildung aus *Schneider, René,* „EU Data Act Draft – selected challenges for switching data processing services and international data transfers.” EPIC Summit 2022, Mai 2022, Web, 31.08.2023, https://lp.dataguard.de/hubfs/EPIC/EPIC%202022/EPIC%20on%20Demand%20Desktop/Stage%203%20_%20EU%20Data%20Act%20Draft%20%E2%80%93%20selected%20challenges%20for%20switching%20data%20processing%20services%20and%20international%20data%20transfers_150102_HQ.mp4.

[22] *Verbraucherzentrale Bundesverband e.V.,* Verbraucher:innen beim Data Act im Blick behalten. Stellungnahme des Verbraucherzentrale Bundesverbands zum Vorschlag der Europäischen Kommission für ein Datengesetz (Data Act). Berlin, 13. Mai 2022, S. 9.

[23] Art. 5 Abs. 3 ePrivacy-Richtlinie ist in § 25 TTDSG umgesetzt.

[24] *EDSA/ EDSB,* EDPB-EDPS Joint Opinion 2/2022 on the Proposal of the European Parliament and of the Council on harmonized rules on fair access to and use of data (Data Act). Brüssel 04.05.2022, S. 13-14.

[25] *Verbraucherzentrale Bundesverband e.V.,* Verbraucher:innen beim Data Act im Blick behalten.

klar an, welcher Rechtsakt im Konfliktfall Vorrang genießt und das das DGA keine Rechtsgrundlage für die Verarbeitung personenbezogener Daten schafft. Das Data Act spricht dagegen allein vom Unberührt-bleiben und ergänzenden Bestimmungen des Kapitel 2 (Art. 3 bis 7) mit Blick auf Art. 20 DSGVO. Legt man die aktuelle Formulierung des Art. 1 Abs. 3 Data Act zugrunde, dass u.a. die Anwendbarkeit der Verordnung (EU) 2016/679 unberührt bleiben soll, ist fraglich, ob das Schutzniveau durch mögliche durch das Data Act geschaffene Rechtsgrundlagen nicht unter das der DSGVO absinken darf oder ob es eben „unberührt bleibt".

Der EDSA und der EDSB kritisieren an der Klausel des Art. 1 Abs. 3 weiter, dass der Eindruck entsteht, dass Anfragen von Einrichtungen und Organen der Union die Rechtsakte im Bereich des Datenschutzes nicht einhalten müssen. Dies folgern sie daraus, dass Art. 1 Abs. 2 lit. d zwar öffentliche Stellen nennt, sie aber nicht von der Stellung als Nutzer oder Datenempfänger ausschließt. Hier wünschen sich die Beiden eine Einbeziehung der Verordnung (EU) 2018/1725.[26]

b) Art. 2 – Definitionen

Die Definitionen des Data Act in Art. 2 fallen nach Ansicht der Verbraucherzentrale Bundesverband e.V. mit denen anderer EU-Rechtsakte auseinander. Insbesondere die in der DSGVO bekannte Definition der Verarbeitung wird im DA anders definiert.[27]

Die Definition von Daten in Art. 2 Nr. 1 sollte nach Ansicht von EDSA und EDSB in personenbezogene und nicht-personenbezogene Daten aufgeteilt werden. Denn insbesondere die Erläuterung in Erwägungsgrund 24, dass nutzergenerierte Daten auf vertraglicher Grundlage verwendet werden können, stelle nicht klar, ob auch die Verpflichtungen für Verantwortliche nach der DSGVO greifen sollen. Aus den gleichen Gründen sollten auch die Definitionen des Betroffenen und der Einwilligung aufgenommen werden, da diese Begriffe im Vorschlag und den Erwägungsgründen genutzt werden.[28]

Das Auseinanderfallen des alltäglichen Verständnisses der Definition des Nutzers mit der Auffassung des Data Act ist problematisch. Dieses scheint unter Nutzer den Eigentümer, Mieter oder Leasingnehmer zu verstehen, nicht den direkten Nutzer, im Fall eines Autos also den Fahrer. Ebenfalls unklar erscheint die Rollenverteilung. Das Data Act geht von einer einfachen Dreierkonstellation aus mit dem Dateninhaber, dem Nutzer und dem Dritten. Letztere wird aber zwischendurch auch Datenempfänger genannt, während das Verhältnis von Dateninhaber und Hersteller nicht geklärt wird. Bestehen hier auch Verträge zwischen Hersteller und Nutzer? Können Gatekeeper die Rolle eines Dateninhabers von einem Hersteller erwerben, um gegebenenfalls den Beschränkungen des Art. 5 Abs. 2 zu entgehen?[29] EDSA und EDSB

Stellungnahme des Verbraucherzentrale Bundesverbands zum Vorschlag der Europäischen Kommission für ein Datengesetz (Data Act). Berlin, 13. Mai 2022, S. 7-8; *EDSA/ EDSB,* EDPB-EDPS Joint Opinion 2/2022 on the Proposal of the European Parliament and of the Council on harmonized rules on fair access to and use of data (Data Act). Brüssels 04.05.2022, S. 2 und 9.

[26] *EDSA/ EDSB,* EDPB-EDPS Joint Opinion 2/2022 on the Proposal of the European Parliament and of the Council on harmonized rules on fair access to and use of data (Data Act). Brüssels 04.05.2022, S. 9-10.

[27] *Verbraucherzentrale Bundesverband e.V.,* Verbraucher:innen beim Data Act im Blick behalten. Stellungnahme des Verbraucherzentrale Bundesverbands zum Vorschlag der Europäischen Kommission für ein Datengesetz (Data Act). Berlin, 13. Mai 2022, S. 8

[28] *EDSA/ EDSB,* EDPB-EDPS Joint Opinion 2/2022 on the Proposal of the European Parliament and of the Council on harmonized rules on fair access to and use of data (Data Act). Brüssel 04.05.2022, S. 12-13.

[29] *Verbraucherzentrale Bundesverband e.V.,* Verbraucher:innen beim Data Act im Blick behalten. Stellungnahme des Verbraucherzentrale Bundesverbands zum Vorschlag der Europäischen Kommission für ein Datengesetz (Data Act). Berlin, 13. Mai 2022, S. 9.

kritisieren an dieser Stelle, dass es wie auch der vzvb angesprochen hat, Fälle gibt, in denen der Nutzer nicht das Subjekt der Datenverarbeitung ist.[30] Dem Data Act erscheint dieser Unterschied entweder nicht bekannt zu sein oder es ist diesem egal. Möglicherweise gingen die Autoren des Data Act auch davon aus, dass Betroffene einer Datenverarbeitung nicht erfasst werden müssen, da sie bereits ausreichend von der DSGVO geschützt werden.

Der Begriff „Dateninhaber", der in Art. 2 Nr. 6 definiert ist, bedarf nach Auffassung von EDSA und EDSB einer genaueren Formulierung. So sei nicht klar, was unter „*durch die Kontrolle über die technische Konzeption des Produkts und damit verbundener Dienste*" verstanden werden könne.[31]

3. Zugangsrechte zu Daten – Art. 3 bis 7 (Kapitel II)

Kapitel II des Data Act Entwurfes ermöglicht es Nutzern Zugang zu Daten, die bei der Nutzung eines vernetzten Produkts oder eines damit verbundenen Dienstes erzeugt, gesammelt oder empfangen wurden, zu erhalten und sie weiterzugeben. Der Nutzer soll entscheiden können, ob, wie und wofür Dritte Zugang erhalten können. Trotzdem handelt es sich dabei nicht um Dateneigentum. Der Europäische Wirtschafts- und Sozialausschuss hat sich in seiner Stellungnahme dafür ausgesprochen: „*Der EWSA ist der Auffassung, dass der Schutz personenbezogener Daten zusammen mit dem Schutz der digitalen Identität und der Privatsphäre grundlegende Aspekte der „Daten-Governance" sind und unmittelbar mit der Achtung der Menschenwürde und der Grundrechte zusammenhängen. Deshalb ist es wichtig, die Eigentumsrechte an personenbezogenen Daten anzuerkennen und zu wahren, damit die Unionsbürgerinnen und -bürger die Kontrolle über die Nutzung ihrer Daten haben.*"[32]

a) Art. 3 – Konzeption und Informationspflicht

Art. 3 verpflichtet Hersteller Produkte so zu konzipieren und herzustellen, dass der Nutzer einfach auf erzeugte Daten zugreifen kann (Abs. 1). Im Vorfeld soll er klar und verständlich über Art und Umfang der Daten, die Art der Erzeugung und Nutzung durch wen, die Art und Weise wie er auf die Daten zugreifen kann und wie er den Dateninhaber kontaktieren oder zur Weitergabe veranlassen, sowie Beschwerde einlegen kann, informiert werden (Abs. 2). Die Vorgaben des Art. 3 erinnern somit stark an Art. 13 DSGVO, der ebenfalls Informationspflichten festlegt.

EDSA und EDSB fordern, dass Art. 3 Abs. 1 und Art. 4 Abs. 1 des DA das Prinzip der Datenminimierung fördert und Produkte so designt werden sollten, dass Betroffene die Möglichkeit erhalten die vom Vorschlag erfassten Produkte und Dienstleistungen anonym oder mit so wenig Eingriff in die Privatsphäre wie möglich zu nutzen. Dateninhaber sollen auch die Menge an Daten, die das Gerät verlässt bspw. durch Anonymisierung verringern. Die Pflicht nach Art. 3 Abs. 2 lit. a den Nutzer über Art und Umfang der Daten zu informieren, dürfe nicht als Einschränkung des Datenminimierungsgrundsatzes der DSGVO verstanden werden. Außerdem sollte Art. 3 klar angeben, wer den Pflichten nachkommen muss.[33]

---

[30] *EDSA/ EDSB,* EDPB-EDPS Joint Opinion 2/2022 on the Proposal of the European Parliament and of the Council on harmonized rules on fair access to and use of data (Data Act). Brüssel 04.05.2022, S. 2-3.
[31] Ebd. S. 11.
[32] *Mureşan, Marinel Dănuț/ Mensi, Maurizio,* Stellungnahme des Europäischen Wirtschafts- und Sozialausschusses zum Datengesetz. INT/978, S. 6.
[33] *EDSA/ EDSB,* EDPB-EDPS Joint Opinion 2/2022 on the Proposal of the European Parliament and of the Council on harmonized rules on fair access to and use of data (Data Act). Brüssel 04.05.2022, S. 15.

b) Art. 4 – Recht auf Zugang der erzeugten Daten

aa) Art. 4 Abs. 1 - Zugangsrecht

Art. 4 enthält das Recht der Nutzer Zugang zu den erzeugten Daten zu erhalten. Abs. 1 verbrieft das Recht des Nutzers auf die Daten zuzugreifen, auch wenn er dies nicht innerhalb des Produkts bereits kann, kostenlos, unverzüglich und gegebenenfalls kontinuierlich und in Echtzeit. Ein einfaches Verlangen auf elektronischem Wege muss dafür ausreichend sein. Im Vergleich zur DSGVO ist die direkte Nennung des elektronischen Wegs neu, das bedeutet aber nicht, dass die Datenbereitstellung nach Art. 20 DSGVO nicht elektronisch möglich oder nicht elektronische Anfragen ausreichend wären, dies ist vielmehr die Praxis. Der elektronische Weg in Art. 4 Abs. 1 Satz 2 Datengesetz ist demnach aus Klarheitsgründen eingefügt worden. Jedoch sollte beachtet werden, dass es sich dabei nicht um eine Formvorschrift nach deutschem Verständnis i.S.v. § 126a BGB handelt, sondern hier wie bei Art. 28 Abs. 9 DSGVO das elektronische Format sogar Textform ausreichen kann, solange dadurch ausreichend den Dokumentations-, Beweissicherungs- und Authentizitätssicherungszwecken Geltung verschafft werden kann.[34] *Martini* vertritt bei Art. 28 Abs. 9 DSGVO zwar die Auffassung, dass eine einfache E-Mail dem nicht genügen könne, dabei geht es aber explizit um die Einigung hinsichtlich eines Vertrages über die Auftragsverarbeitung, während bei Art. 4 Abs. 1 S. 2 Datengesetz ein „einfaches Verlangen auf elektronischem Wege“ ausreichen soll. Solange die E-Mailadresse dem Dateninhaber bereits bekannt ist, sollte damit eine ausreichende Authentifizierung gegeben sein. Im Übrigen verbleibt ihm die Vorschrift des Abs. 2 zur Klärung der Identität des anfragenden Nutzers.

bb) Art. 4 Abs. 2 - Spezifizierungsverlangen

In Art. 4 Abs. 2 wird der Dateninhaber daran gehindert zur Erfüllung eines Herausgabeverlangens mehr Daten als zur Identifikation des Nutzers erforderlich, zu verlangen und keine Daten über den Zugang zu den verlangten Daten aufzubewahren, was nicht für das Zugangsverlangen und die Sicherheit und Pflege der Dateninfrastruktur erforderlich ist. Dies entspricht dem Prinzip der Datensparsamkeit nach Art. 5 Abs. 1 lit. c DSGVO und steht auch nicht mit den Art. 20, 11 DSGVO im Widerspruch. Denn die Situation des Art. 11 DSGVO ist so, dass personenbezogene Daten vorliegen, diese aber nicht zur Identifikation einer Person ausreichen und deshalb nicht neue Daten erhoben werden müssen. „*Identifizierbar ist eine Person, wenn der Verantwortliche verschiedene Mittel zur Identifizierung besitzt und damit zu rechnen ist, dass er von diesen Gebrauch macht. Dies ist insbesondere dann anzunehmen, wenn der damit verbundene Aufwand zumutbar ist. In Erwägungsgrund 26 der Datenschutzrichtlinie hieß es diesbezüglich, dass die Mittel zu berücksichtigen seien, die vernünftigerweise eingesetzt würden, während in Erwägungsgrund 26 der Datenschutzgrundverordnung davon die Rede ist, dass die Mittel zu berücksichtigen seien, die nach allgemeinem Ermessen wahrscheinlich genutzt würden.*“[35] Kontaktiert ein Nutzer den Dateninhaber mit der E-Mail, mit der dieser einen Account beim Dateninhaber besitzt sollte der Dateninhaber alle erforderlichen Informationen besitzen, da mit der übereinstimmenden E-Mailadresse bereits von einer Identifizierbarkeit ausgegangen werden könnte. Je nach Sensibilität der in Rede stehenden Daten sollte über das Ergreifen zusätzlicher Authentifizierungsmaßnahmen nachgedacht werden. Insbesondere bei Zahlungsgeschäften ist dies mit der Zahlungsdiensterichtlinie PSD2 für notwendig erachtet worden. EDSA und EDSB fordern allerdings, dass im Normtext klargestellt werden sollte, dass sich aus Art. 4 Abs. 2 keine Einschränkungen der Verpflichtungen nach der DSGVO ergeben.[36]

---

[34] Vgl. Paal/Pauly/Martini, 3. Aufl. 2021, DS-GVO Art. 28 Rn. 75.
[35] BeckOK DatenschutzR/Wolff, 40. Ed. 1.11.2021, DS-GVO Art. 11 Rn. 12.
[36] *EDSA/ EDSB,* EDPB-EDPS Joint Opinion 2/2022 on the Proposal of the European Parliament and of

cc) Art. 4 Abs. 3 - Geschäftsgeheimnisse

René Schneider wirft in seinem Vortrag Fragen hinsichtlich Geschäftsgeheimnisse und dem europäischen Kartellrecht auf. Er kritisiert, dass die Regelung zu einer Offenlegung verpflichtet, auch wenn dies nur mit einem NDA passieren würde.[37] Art. 4 Abs. 3 des Entwurfs beschäftigt sich mit Geschäftsgeheimnissen. Dieser stellt klar, dass diese nur offengelegt werden, „*wenn alle besonderen Maßnahmen getroffen worden sind, die erforderlich sind, um die Vertraulichkeit der Geschäftsgeheimnisse, insbesondere gegenüber Dritten, zu wahren. Der Dateninhaber und der Nutzer können Maßnahmen vereinbaren, um die Vertraulichkeit der gemeinsam genutzten Daten, insbesondere gegenüber Dritten, zu wahren.*“ Darüber hinaus legt auch Art. 8 Abs. 6 fest, dass keine Pflicht besteht, einem Datenempfänger Geschäftsgeheimnisse im Sinne der Richtlinie (EU) 2016/943 herauszugeben. Ausnahmen bewegen sich im Rahmen des Data Act und Umsetzungsgesetzen des EU-Rechts.[38] Im deutschen Recht sind bei der Beurteilung der Art. 4 Abs. 3, 8 Abs. 6 Datengesetz damit das die Richtlinie umsetzende Gesetz zum Schutz von Geschäftsgeheimnissen (GeschGehG) zu berücksichtigen. Um die Offenlegung von Geschäftsgeheimnissen in einem Fall, in dem sie durch die Datenweitergabe betroffen sind, zu verhindern werden Unternehmen Klauseln vereinbaren, die bei dem geringsten Anzeichen der Weitergabe oder Nutzung von Geschäftsgeheimnissen hohe Vertragsstrafen nach sich ziehen. Diese Lösung ist mit Blick auf eine mögliche Verbrauchereigenschaft eines Nutzers mit Vorsicht zu genießen, insbesondere können Vertragsstrafen gegenüber Verbrauchern gegen die AGB-Kontrolle verstoßen. Daneben kann die Datenweitergabe auch nicht deshalb versagt werden, weil ein Dateninhaber den Begriff des Geschäftsgeheimnisses umfassender verstehen möchte und insbesondere die erzeugten Daten für ein Geschäftsgeheimnis hält. Insofern kann nur eine solche Regel wie sie Art. 4 Abs. 3 vorsieht einen angemessenen Ausgleich zwischen dem Datenzugangsanspruch des Nutzers und dem Interesse des Dateninhabers seine Geschäftsgeheimnisse zu schützen schaffen. Aus Sicht des Datenschutzes gibt es hinsichtlich Geschäftsgeheimnisse keine besonderen Erwägungen. Letztlich ist aber die besondere Vertraulichkeit, auch gegenüber Dritten, wie es Abs. 3 vorschreibt aus Sicht des Grundsatzes der Integrität und Vertraulichkeit nach Art. 5 Abs. 1 lit. f, Erwägungsgrund 39 DSGVO zu begrüßen.

dd) Art. 4 Abs. 4 - Konkurrenzprodukt

Auch hinsichtlich des von René Schneider in der Abbildung auf der folgenden Seite angesprochenen Problems „No competitive product“ trifft Art. 4 in Absatz 4 eine Regelung: „*Der Nutzer darf die aufgrund eines Verlangens nach Absatz 1 erlangten Daten nicht zur Entwicklung eines Produktes nutzen, das mit dem Produkt, von dem die Daten stammen, im Wettbewerb steht.*“ Die Auswirkungen der theoretischen Möglichkeit des Datenempfängers zur Entwicklung eines Produkts anhand der erhaltenen Daten und des Verbots des Art. 4 Abs. 4 in der Praxis sind jedoch abzuwarten. Die Frage, ob ein Empfänger sich an solchen Daten bei der Entwicklung eines Konkurrenzprodukts bedient hat, wird in der Folge stets im Raum stehen können. Die grundsätzliche Problematik ist zwar aus anderen Geschäftsbereichen bekannt und wird dort mit vertraglichen Wettbewerbsverboten gelöst. Auch bei einem Wechsel zur Konkurrenz ist ein solches Wettbewerbsverbot offensichtlich nicht passend, gegenüber dem Nutzer aber durchaus möglich. Trotzdem bestehen insoweit große Unsicherheiten: Denn es ist nicht klar, was ein

---

the Council on harmonized rules on fair access to and use of data (Data Act). Brüssel 04.05.2022, S. 15.

[37] Vgl. *Schneider, René,* „EU Data Act Draft – selected challenges for switching data processing services and international data transfers.” EPIC Summit 2022, Mai 2022, Web, 31.08.2023, https://lp.dataguard.de/hubfs/EPIC/EPIC%202022/EPIC%20on%20Demand%20Desktop/Stage%203%20_%20EU%20Data%20Act%20Draft%20%E2%80%93%20selected%20challenges%20for%20switching%20data%20processing%20services%20and%20international%20data%20transfers_150102_HQ.mp4.

[38] Art. 8 Abs. 6 Data Act Entwurf.

solches Konkurrenzprodukt nach Art. 4 Abs. 4 Datengesetz ist. Daneben kritisiert Schneider noch die gleichzeitige Einhaltung des Data Act und des Kartellrechts: Zum einen müssten Daten und damit gegebenenfalls Geschäftsgeheimnisse und Erfindungen geteilt werden und zum anderen ist dies ausdrücklich verboten.[39]

ee) Art. 4 Abs. 5 – nicht von der Datenverarbeitung betroffener Nutzer

Schneider kritisiert weiter fehlende Regelungen für den Nachfolger des erstmaligen Nutzers. Dieser habe nach dem Entwurf Anspruch auf alle Daten, auch betreffend den Vorbesitzer, was mit geltendem Datenschutzrecht nicht im Einklang stehe.[40] Allerdings regeln Art. 4 Abs. 5 und Art. 5 Abs. 6 des Data Act Entwurfs gerade den Fall, dass der Nutzer nicht die von der Datenverarbeitung betroffene Person ist. Sodann soll er nur die Daten erhalten oder weitergeben können, wenn eine Rechtsgrundlage nach Art. 6 Abs. 1 oder Art. 9 der DSGVO vorliegt. Von einem uneingeschränkten Anspruch auch auf die Daten des Vorbesitzers kann somit nicht die Rede sein. EDSA und EDSB fordern, dass der Verweis den gesamten Art. 6 DSGVO erfassen und Art. 5 Abs. 3 ePrivacy-Richtlinie (§ 25 TTDSG in Deutschland) berücksichtigen soll.[41]

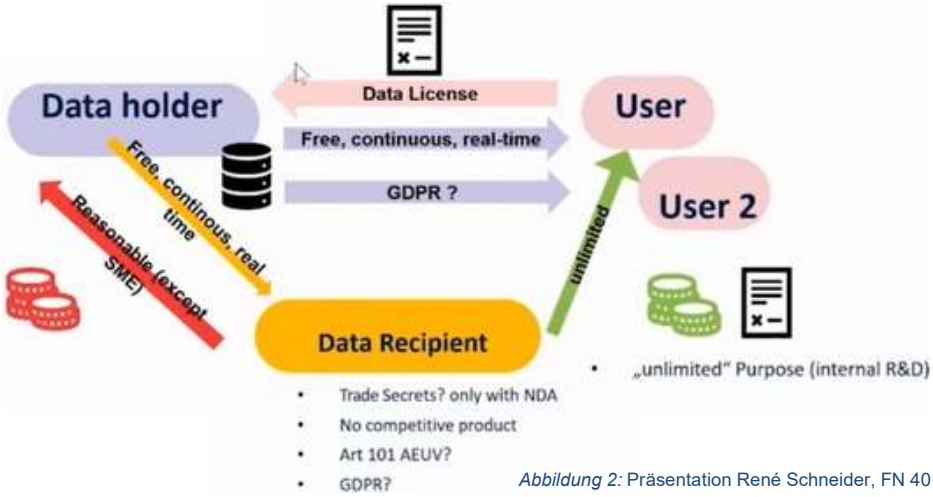

Abbildung 2: Präsentation René Schneider, FN 40

Problematisch ist weiter, dass die Dateninhaber zur Prüfung einer Rechtsgrundlage berufen zu sein scheinen, was aufgrund der Vielzahl potenzieller Nutzer und Datenempfängern in der Praxis eher zur Verarbeitung von personenbezogenen Daten in unzulässiger Weise führen könnte und die Gefahr eines Absinkens des allgemeinen Datenschutzniveaus im Raum steht.[42] Dies erscheint deshalb überzeugend, da in den Art. 3, 4, 5, 6 und 8 des Vorschlags nicht klar genug hervorgeht, dass es sich um die geschäftliche Verpflichtung des Herstellers/ Dateninhabers handelt, dem Unternehmen Zugang zu den Daten zu gewähren, vorbehaltlich aller Bedingungen und Grenzen der DSGVO und nicht um ein „Recht", personenbezogene Daten zu übertragen und verarbeiten zu lassen.[43] Genau diesen Eindruck erweckt aber Art. 1 Abs. 3 S. 3, der ausführt, dass Kapitel II des Vorschlags den Art. 20 DSGVO ergänzt.

---

[39] *Schneider, René,* „EU Data Act Draft – selected challenges for switching data processing services and international data transfers." EPIC Summit 2022, Mai 2022, Web, 31.08.2023, https://lp.dataguard.de/hubfs/EPIC/EPIC%202022/EPIC%20on%20Demand%20Desktop/Stage%203%20_%20EU%20Data%20Act%20Draft%20%E2%80%93%20selected%20challenges%20for%20switching%20data%20processing%20services%20and%20international%20data%20transfers_150102_HQ.mp4.
[40] Abbildung aus *Ebd.*
[41] *EDSA/ EDSB,* EDPB-EDPS Joint Opinion 2/2022 on the Proposal of the European Parliament and of the Council on harmonized rules on fair access to and use of data (Data Act). Brüssel 04.05.2022, S. 14.
[42] *Verbraucherzentrale Bundesverband e.V.,* Verbraucher:innen beim Data Act im Blick behalten. Stellungnahme des Verbraucherzentrale Bundesverbands zum Vorschlag der Europäischen Kommission für ein Datengesetz (Data Act). Berlin, 13. Mai 2022, S. 11.
[43] *EDSA/ EDSB,* EDPB-EDPS Joint Opinion 2/2022 on the Proposal of the European Parliament and of the Council on harmonized rules on fair access to and use of data (Data Act). Brüssel 04.05.2022, S. 10.

Hinsichtlich der Rechtsgründe, insbesondere der vertraglichen Ausgestaltung der „Data Licence“ können sich Folgeprobleme eröffnen. Die Frage beispielsweise, ob erstmalige Nutzer mit dem Verkauf ihres Gerätes automatisch in die Nutzung ihrer personenbezogenen Daten einwilligen können, ob dies Gegenstand eines Kaufvertrages gemacht werden kann, ob die Verarbeitung auch mit berechtigten Interessen gelingt oder wie es mit Zweckvereinbarungen und anonymisierten Daten aussieht.

(1) Das Kopplungsverbot

Hinsichtlich der Frage, ob personenbezogene Daten Gegenstand eines Kaufvertrages gemacht werden können, ist auf die §§ 312 Abs. 1a, 327ff. BGB zu verweisen, die die Richtlinie (EU) 2019/770 umsetzen. Die Richtlinie stellt klar, dass personenbezogene Daten nicht als Ware betrachtet werden können, Verbraucher aber im Zusammenhang mit solchen Geschäftsmodellen Anspruch auf vertragliche Rechtsbehelfe haben.[44] Die Praxis fasst das zunehmend so auf, dass personenbezogene Daten Gegenstand eines Vertrages sein können und bieten im Gegenzug zu den Daten bspw. ihre redaktionellen, journalistischen Inhalte an. Das Datengesetz umgeht diese Problematik, indem es in Art. 4 Abs. 6 allein von „nicht personenbezogene Daten“ spricht. Diese dürften nur auf Grundlage eines Vertrages verarbeitet werden, wobei der Dateninhaber Beschränkungen hinsichtlich der Verwertung der Daten unterliegt. Für personenbezogene Daten gilt dagegen nach Art. 4 Abs. 5 die DSGVO, dies wurde bereits in Art. 1 Abs. 3 Datengesetz klargestellt. Hierzu sind also weiter die Rechtsgrundlagen der Art. 6, 9 DSGVO erforderlich. Personenbezogene Daten zum Gegenstand eines Vertrages zu machen ist umstritten. Denn das sogenannte Kopplungsverbot des Art. 7 Abs. 4 DSGVO geht davon aus, dass personenbezogene Daten, die für die Erfüllung des Vertrages nicht erforderlich sind, die Freiwilligkeit der Einwilligung zur Verarbeitung der personenbezogenen Daten entfallen lässt. Insoweit ist der Streitpunkt, ob die Positionierung personenbezogener Daten als ein Vertragsgegenstand sie zur Erfüllung des Vertrages erforderlich machen. Insbesondere Verlage und journalistische Onlineplattformen argumentieren, dass die Daten die Gegenleistung der Nutzer sind und des Weiteren wirtschaftlich zur (besseren) Finanzierung der Inhalte mit personalisierter Werbung erforderlich seien. Datenschützer argumentieren, dass die Werbung auch unpersonalisiert möglich sei und das Kopplungsverbot durch die Gestaltung als Vertragsgegenstand stets leerlaufen würde. Die Regelungen zur Freiwilligkeit der Einwilligung fänden daneben Eingang über die Willenserklärung für den Vertrag. Hat der Nutzer keine Alternative zur Hingabe seiner personenbezogenen Daten als Gegenstand des Vertrages (bspw. ein angemessenes Entgelt) soll es an der Freiwilligkeit fehlen, sodass die Einwilligung – in die Verarbeitung im Rahmen des Vertrages – unwirksam ist.[45] Diese Grundsätze spielen nun eine Rolle, sobald ein Nutzer eines Produkts oder eines damit verbundenen Dienstes mit dem Kauf auch aktiv in die Verarbeitung seiner personenbezogenen Daten einwilligen soll oder dies als Gegenleistung neben den Kaufpreis tritt. Ausgehend der Meinung der Datenschützer, die ein absolutes Kopplungsverbot vertreten, ist im Rahmen einer Abwägung insbesondere darauf zu achten, ob die Freiwilligkeit durch ein alternatives angemessenes Entgelt gewahrt ist.[46] Vertreter eines relativen Kopplungsverbotes stellen das Recht des Einzelnen aus Art. 8 Abs. 1, 2 EuGRCh,

[44] Vgl. Richtlinie (EU) 2019/770, Erwägungsgrund 24.

[45] Vgl. *Forster, Thomas/ Kutschera, Nicolas*, Das Kopplungsverbot und Daten als Geldwert – Das Ende von „kostenlosen“ digitalen Inhalten? Datenschutz-notizen vom 16.09.2021, https://www.datenschutz-notizen.de/das-kopplungsverbot-und-daten-als-geldwert-das-ende-von-kostenlosen-digitalen-inhalten-0631211/, abgerufen am 08.08.2022.

[46] Vgl. BeckOK DatenschutzR/Stemmer, 40. Ed. 1.5.2022, DS-GVO Art. 7 Rn. 45-50; EuArbRK/Franzen, 4. Aufl. 2022, EU (VO) 2016/679 Art. 7 Rn. 9; *DSK,* Kurzpapier Nr. 3, Verarbeitung personenbezogener Daten für Werbung. 17.12.2018. S. 2; *EDSA,* Leitlinien 05/2020 zur Einwilligung gemäß Verordnung 2016/679. Version 1.1, angenommen am 04. Mai 2020, S. 11.

die Freiheit über die eigenen personenbezogenen Daten disponieren zu können, in den Vordergrund und fordern eine Abwägung hinsichtlich aller Umstände, insbesondere auch ob eine Monopolstellung des Datenverarbeiters gegeben ist. Erwägungsgrund 43, der ein absolutes Kopplungsverbot formuliert lehnen sie ab, da er gerade nicht Teil des Art. 7 Abs. 4 DSGVO geworden ist.[47] Ob Grundrechte aber dazu bemüht werden können, das Schutzniveau für Grundrechtsträger abzusenken ist fraglich. Besitzt ein Nutzer entsprechend des Art. 8 Abs. 1, 2 EuGRCh den klaren Willen in die Verarbeitung einzuwilligen besteht kein Anlass über ein Kopplungsverbot nachzudenken. Ebenfalls kritisch zu hinterfragen ist der fehlende Wille von *Heckmann* und *Paschke* Erwägungsgrund 43 bei der Auslegung von Art. 7 Abs. 4 DSGVO zu berücksichtigen. Erwägungsgründe stellen als in den Rechtsakt aufgenommene Überlegungen des Gesetzgebers Quellen dar, die im Rahmen der Auslegung berücksichtigt werden können. Der Ansicht des absoluten Kopplungsverbots gebührt der Vorzug, da dieses den Einzelnen vor untergeschobenen Einwilligungen im Rahmen eines Vertrages angemessener schützt.

(2) Berechtigte Interessen

Zu beachten ist, dass Art. 6 Abs. 1 UAbs. 1 lit. f, die Verarbeitung aufgrund berechtigter Interessen ohne überwiegende entgegenstehende Interessen des Betroffenen, ebenfalls ein Rechtsgrund nach Art. 4 Abs. 5 darstellen kann. Diese Rechtsgrundlage kann voraussichtlich lediglich in seltenen Fällen vom Nachfolger geltend gemacht werden, bspw. falls der nachfolgende Nutzer Gründe für Fehlfunktionen oder Schäden am Produkt mittels der während der Nutzungszeit des Vorbesitzers angefallenen Daten aufklären möchte. Die Interessen müssen jedoch ein vergleichbares Übergewicht wie das der Rechtsverfolgung gewährleisten, andernfalls kann nicht einfach eine Datenübermittlung erfolgen, Art. 4 Abs. 5. Daneben sollten für eine ausreichend begründetes Interesse auch Anhaltspunkte für die Aussagekraft bereits erzeugter Daten durch andere Nutzer gegeben sein.

(3) Besondere Kategorien

Im Falle von personenbezogenen Daten, die die besonderen Kategorien des Art. 9 Abs. 1 DSGVO erfüllen ist zusätzlich eine Rechtsgrundlage nach Art. 9 Abs. 2 DSGVO erforderlich.

(4) Zweck der Verarbeitung

Nach dem Rechtsgrund der Verarbeitung schlägt René Schneider in die Kerbe des Zwecks der Verarbeitung. Denn der Grundsatz der Speicherbegrenzung nach Art. 5 Abs. 1 lit. e DSGVO, der besagt, dass personenbezogene Daten nur so lange gespeichert werden dürfen, „*wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist*“, könne seiner Auffassung nach im Rahmen der „Data License“ durch denjenigen, der die Daten vom Nutzer übertragen bzw. zur Verfügung gestellt bekommt durch eine einfache Zweckbestimmung „Internal R&D“, also interne Forschung und Entwicklung, ausgehebelt werden, was zu einer unbeschränkten Verarbeitung führe.[48] Zunächst ist darauf hinzuweisen, dass der die wissenschaftliche oder historische Forschung privilegierende Art. 89 DSGVO sich nur auf Forschung bezieht und nicht jede Analyse oder Aufbereitung von personenbezogenen Daten erfasst.[49] Die Zweckbindung des Art. 5 Abs. 1 lit. b DSGVO gilt also auch hier. Unabhängig davon, ob Nutzer:innen bei Vertragsschluss oder

[47] Vgl. Ehmann/Selmayr/Heckmann/Paschke, 2. Aufl. 2018, DS-GVO Art. 7 Rn. 95-99; Paal/Pauly/Frenzel, 3. Aufl. 2021, DS-GVO Art. 7 Rn. 21.
[48] Vgl. *Schneider, René,* „EU Data Act Draft – selected challenges for switching data processing services and international data transfers.” EPIC Summit 2022, Mai 2022, Web, 31.08.2023, https://lp.dataguard.de/hubfs/EPIC/EPIC%202022/EPIC%20on%20Demand%20Desktop/Stage%203%20_%20EU%20Data%20Act%20Draft%20%E2%80%93%20selected%20challenges%20for%20switching%20data%20processing%20services%20and%20international%20data%20transfers_150102_HQ.mp4.
[49] Vgl. BeckOK DatenschutzR/Eichler, 40. Ed. 1.11.2021, DS-GVO Art. 89 Rn. 6.

Einwilligung zur Verarbeitung für „interne Forschung und Entwicklung“ wirksam entsprechende Willenserklärung abgeben konnten, da möglicherweise nicht die Anforderungen an die Informiertheit der Einwilligung vorgelegen haben, muss eine unbeschränkte Verarbeitung auch für Forschungs- und Entwicklungszwecke gegen den Grundsatz der Datenminimierung und Speicherbegrenzung nach Art. 5 Abs. 1 lit. c und e DSGVO verstoßen. Der Verbraucherzentrale Bundesverband e.V. fordert bei der Änderung des Zwecks eine deutliche Klarstellung, ob eine Zweckänderung nach Art. 6 Abs. 4 DSGVO trotz des Wortlauts des Data Act möglich ist. Denn Art. 4 Abs. 5 spricht von Rechtsgrundlagen gemäß Art. 6 Abs. 1 und Art. 9, nicht von Art. 6 Abs. 4.[50]

(5) Anonymisierte Daten

Anders kann das gesehen werden, wenn die Daten anonymisiert worden sind. „*In der Literatur ist bislang die Ansicht herrschend, wonach die Löschung eine vollständige Unkenntlichmachung der personenbezogenen Daten verlangt. Der BfDI und die Datenschutzbehörde Österreichs (öDSB) gehen demgegenüber davon aus, dass bereits die Aufhebung des Personenbezugs durch Anonymisierung ausreichend ist.*“[51] Wesentlich bei der Herleitung dieser Ansicht ist die Verbindung des Grundsatzes der Speicherbegrenzung mit dem Löschanspruch: Denn dieser Grundsatz stellt ausdrücklich auf den Personenbezug ab. Er verlangt eine Speicherung, „*die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist*“. Der Löschanspruch, der in der Folge mit Wegfall des Zwecks besteht, stellt damit auf die Identifizierung ab. Es müssen damit nicht alle personenbezogenen Daten i.S.v. Art. 4 Nr. 1 DSGVO gelöscht werden, sondern nur solche die die Identifizierbarkeit ermöglichen. Das Restrisiko der Re-Identifizierbarkeit ist bei ordnungsgemäßer Anonymisierung der Daten genauso hoch wie das Risiko der Identifizierbarkeit von nicht-personenbezogenen Daten. Nicht ordnungsgemäß wäre offensichtlich die alleinige Entfernung direkt identifizierender Merkmale, dies würde lediglich zu einer Pseudonymisierung führen.[52] Es ist jedoch darauf zu achten, dass nach dem Zusammenführen mehrerer personenbezogener Daten zu einem Gruppendatensatz keine Zuordnung von Einzeldaten zu Personen mehr möglich sein darf. Die frühere Anforderung für eine Zuordnung nur mit einem unverhältnismäßig großen Aufwand an Zeit und Kosten ist aufgrund der stetig zunehmenden Möglichkeiten mit technischen Mitteln scheinbar anonyme Daten dennoch den Betroffenen zuordnen zu können eigentlich eine Absage zu erteilen. Eine Erschwerung der Re-Identifizierung ist damit eher eine Pseudonymisierung. Die Art. 29-Datenschutzgruppe hat in ihrer Stellungnahme 5/2014 bereits ausgeführt, dass eine wirksame Anonymisierung voraussetzt, dass „*keine Partei in der Lage sein darf, eine Person aus dem Datenbestand herauszugreifen, eine Verbindung zwischen zwei Datensätzen eines Datenbestandes oder zwischen zwei unabhängigen Datenbeständen herzustellen oder durch Inferenz Informationen aus einem solchen Datenbestand abzuleiten.*“[53] Zwar stellt die Anonymisierung eine Verarbeitung i.S.v. Art. 4 Nr. 2 DSGVO dar, eine Verarbeitung zu einem anderen Zweck nach Art. 6 Abs. 4 DSGVO liegt nicht vor, da diese ersichtlich personenbezogenen Daten betrifft, während bei den anonymisierten Daten gerade keine (mehr) vorhanden sind. Als Rechtsgrundlage für eine Anonymisierung bzw. Löschung wird dagegen Art. 6 Abs. 1 UAbs. 1 lit. c i.V.m. Art. 17 DSGVO vorgeschlagen. Im Fall von besonderen Kategorien personenbezogener Daten darf die Löschung nicht vom Verbot des

[50] *Verbraucherzentrale Bundesverband e.V.,* Verbraucher:innen beim Data Act im Blick behalten. Stellungnahme des Verbraucherzentrale Bundesverbands zum Vorschlag der Europäischen Kommission für ein Datengesetz (Data Act). Berlin, 13. Mai 2022, S. 7.
[51] Vgl. *Stürmer, Verena,* Löschen durch Anonymisieren? Mögliche Erfüllung der Löschpflicht nach Art. 17 DS-GVO. In: ZD 2020, 626 (626).
[52] Ebd. S. 628-629.
[53] Paal/Pauly/Ernst, 3. Aufl. 2021, DS-GVO Art. 4 Rn. 49-51.

Art. 9 Abs. 1 DSGVO erfasst werden, da sonst die DSGVO sich selbst widerspräche, „*wenn sie die Löschung auch besonderer Kategorien personenbezogener Daten zwar verlangte, diese aber mangels Rechtsgrundlage nicht durchführbar wäre.*“ [54] Der Schutz des Art. 9 Abs. 1 ist im Fall der Anonymisierung nicht erforderlich, da dies gerade dem Schutz der Betroffenen dient.[55] Der Verbraucherzentrale Bundesverband e.V. fordert die Weiterentwicklung der Anonymisierungstechniken, die Förderung entsprechender Forschungsansätze und die Entwicklung von Standards, da es sich dabei um einen wesentlichen Baustein handele, um das Ziel des Data Act, die Verfügbarkeit von Daten, zu verbessern.[56]

ff) Art. 4 Abs. 6 – Vertrag über Nutzung nicht-personenbezogener Daten

Das gleiche wie bei anonymisierten Daten gilt bei Art. 4 Abs. 6 auch hinsichtlich nicht-personenbezogener Daten. Dort kann mangels Anwendbarkeit der DSGVO nicht auf die Grundzüge des Art. 5 DSGVO zurückgegriffen werden, das Datenschutzrecht stünde damit einer unendlichen Speicherung nicht-personenbezogener Daten nicht im Wege. Die Verbraucherzentrale Bundesverband e.V. weist an dieser Stelle aber auf die Vorgaben der ePrivacy-Richtlinie hin, die „*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.*“[57] Ob es sich dabei um personenbezogene oder nicht-personenbezogene Daten handelt, sei unerheblich.[58]

Zusammenfassend muss klargestellt werden, dass Art. 4 Datengesetz entsprechend dem Verweis in Art. 1 Abs. 3 das Recht auf Datenübertragbarkeit aus Art. 20 DSGVO erweitert (s. S. 5f).

c) Art. 5 – Weitergabe an Dritte

Art. 5 Abs. 1 verpflichtet den Dateninhaber auf Verlangen des Nutzers die bei der Nutzung eines Produkts oder verbundenen Dienstes erzeugten Daten unverzüglich einem Dritten, für den Nutzer kostenlos und in derselben Qualität, kontinuierlich und in Echtzeit, bereitzustellen. Für zentrale Plattformanbieter, die auch für mindestens einen Dienst als Gatekeeper im Sinne des Digital Markets Acts gelten, trifft Art. 5 Abs. 2 besondere Vorgaben hinsichtlich des Ziels der Übertragung, also der Position des Dritten. Die Buchstaben a-c des Art. 5 Abs. 2 enthalten hierzu das Verbot von Aufforderungen, geschäftlichen Anreizen und das grundsätzliche Erhalten der Daten nach Art. 4 Abs. 1.

Gänzlich unbeachtet scheint aber die Konstellation der Übertragung der Daten durch den Dateninhaber oder den Dritten an einen zentralen Plattformanbieter mit der Stellung eines Gatekeepers zu sein. Allein Art. 5 Abs. 1 erfasst noch die „*im Namen eines Nutzers handelnden Partei*“, sodass eine direkte Umgehung auf Verlangen des Nutzers ausgeschlossen scheint. Der direkte Verkauf der Daten durch den Dateninhaber an den Gatekeeper wird aber nicht beschränkt. Daneben werden zwar Verträge von Unternehmen mit KMUs mit Art. 13 einer Missbrauchskontrolle unterzogen. Verträge von Unternehmen mit Nutzern bzw. Nutzern, die Verbraucher sind, werden dem bisherigen Verbraucherrechtsregime überlassen.[59] Eine solche

---

[54] Vgl. *Stürmer, Verena,* Löschen durch Anonymisieren? Mögliche Erfüllung der Löschpflicht nach Art. 17 DS-GVO. In: ZD 2020, 626 (630).
[55] Ebd.
[56] *Verbraucherzentrale Bundesverband e.V.,* Verbraucher:innen beim Data Act im Blick behalten. Stellungnahme des Verbraucherzentrale Bundesverbands zum Vorschlag der Europäischen Kommission für ein Datengesetz (Data Act). Berlin, 13. Mai 2022, S. 16-17.
[57] Ebd. S. 7.
[58] Ebd.
[59] Ebd. S. 13.

wäre jedoch aufgrund der besonderen Rechtsmaterie wünschenswert. Denn inwieweit bspw. Art. 13 als vergleichbare gesetzliche Grundlage im Sinne von § 307 Abs. 2 Nr. 1 BGB für B2C-Verträge herangezogen werden kann ist noch nicht absehbar. Darüber hinaus wäre mit Blick auf die Richtlinienherkunft des § 307 Abs. 2 Nr. 1 BGB und der nicht wortgleichen Regelung in Art. 3 Abs. 1 der Richtlinie 93/13/EWG des Rates vom 05.04.1993 eine Regelung diesbezüglich für alle Mitgliedsstaaten wünschenswert.

Die Verbraucherzentrale Bundesverband e.V. fordert klarere Vorgaben im B2C-Kontext, um eine mögliche „total-buyout-Klausel" zu verhindern. So sollte die Datennutzung für nicht-personenbezogene Daten im B2C-Kontext auf legitime Zwecke wie Produktfunktionalität/ -sicherheit und Produktentwicklung oder von Verbraucher:innen granular ausgewählten Zwecken erlaubt sein. Eine Koppelung einer Zustimmung mit der Hauptleistung, Manipulation oder Täuschung zur Verwendung für weitere Zwecke solle verboten sein. Daneben solle die Datenübermittlung beschränkt sein. Auch hier soll dies bei nicht-personenbezogenen Daten nur für bereits genannte legitime Zwecke gehen oder gewünschte Zwecke. Bei einer Vermarktung sollten Verbraucher:innen angemessen beteiligt werden. Außerdem sollten die Verträge zeitlich befristet sein und Verbraucher:innen stets die Möglichkeit haben die Verträge zu kündigen. Ein Verkauf soll auch zum Neuabschluss der Verträge führen.[60] Im Rahmen einer Betrachtung des Problems des „extended vehicle" befürchtet der vzbv aufgrund der Möglichkeit umfangreicher buy-out-Klauseln und des fehlenden Schutzes der Manifestierung der Autohersteller als Gatekeeper eine Zementierung dieses wettbewerbsfeindlichen Konzepts. Ein Problem ist die Tatsache, dass Nutzer:innen zwar die Daten selbst kostenlos erhalten könnten, Datenempfänger für die Daten aber bezahlen müssen. Google als Gatekepper könnte zwar nicht Wetterdaten vom Autohersteller erhalten und standortgenaue Regen- oder Glättewarnungen anbieten, das könnte aber gegebenenfalls ein kleineres Unternehmen. Dieses müsste aber für die Datenbereitstellung bezahlen und das obwohl Nutzer:innen die Daten selbst kostenlos erhalten könnten. Damit wäre der Dienst für Nutzer:innen nur schwer kostenlos erhältlich. Außerdem ist fraglich wie neutral Autohersteller sein können, wenn es um eine Unfallaufklärung geht. Hier liegt die Entscheidung welche Daten Strafverfolgungsbehörden erhalten beim Hersteller, obwohl bürgerliche Freiheitsrechte im Raum stehen. Letztlich wissen Nutzer:innen auch nicht an wen alles die Daten fließen, denn das Data Act enthält keine Informationspflicht, die den Dateninhaber verpflichtet dies mitzuteilen. Diese Information enthält der Katalog des Art. 3 Abs. 2 gerade nicht.[61] Insoweit ist jedoch mit Blick auf Art. 1 Abs. 3 Data Act bei personenbezogenen Daten auch auf Art. 13 Abs. 1 lit. e DSGVO zu verweisen, der die Nennung von Empfängern bzw. Kategorien von Empfängern vorsieht.

Art. 5 Abs. 3 schränkt ähnlich Art. 4 Abs. 2 die im Rahmen einer Identifizierung verlangten Daten auf das erforderliche ein (S. 1). Außerdem darf der Dateninhaber keine Information über den Zugang des Dritten aufbewahren, die nicht zur Ausführung des Zugangsverlangens und der Sicherheit und Pflege der Dateninfrastruktur erforderlich ist (S. 2). Dies entspricht dem Prinzip der Datensparsamkeit nach Art. 5 Abs. 1 lit. c DSGVO. EDSA und EDSB fordern allerdings, dass im Normtext klargestellt werden sollte, dass sich genauso wie bei Art. 4 Abs. 2 aus Art. 5 Abs. 3 keine Einschränkungen der Verpflichtungen nach der DSGVO ergeben.[62] Der Dritte wird durch Art. 5 Abs. 4 daran gehindert sich ohne Zutun des Dateninhabers Zugang zu den Daten des Nutzers zu verschaffen, denn er darf keine Zwangsmittel oder „offensichtliche Lücken" in der technischen Infrastruktur ausnutzen. Warum Art. 5 Abs. 4 aber von offensichtlichen Lücken

[60] Ebd. S. 13-14.
[61] Ebd. S. 15-17.
[62] *EDSA/ EDSB,* EDPB-EDPS Joint Opinion 2/2022 on the Proposal of the European Parliament and of the Council on harmonized rules on fair access to and use of data (Data Act). Brüssel 04.05.2022, S. 15.

spricht wird nicht im Entwurf erörtert. Insoweit ist auch nicht hinlänglich klar, ob die Lücken an sich offensichtlich und damit bekannt sein müssen oder es aus den Umständen offensichtlich ist, dass Lücken ausgenutzt wurden.

Die Art. 5 Abs. 5 und 6 sind identisch mit denen des Art. 3 Abs. 4 und 5. Hier gilt das dort geschriebene. EDSA und EDSB haben in ihrer Stellungnahme nochmals ausdrücklich gefordert, dass Daten, die durch ein Produkt oder einen verbundenen Service erzeugt wurden nur zur Verfügung gestellt werden dürfen, wenn alle Bedingungen und Regelungen des Datenschutzrechts eingehalten werden, insbesondere wenn eine gültige Rechtsgrundlage gemäß Art. 6 besteht und ggf. die Bedingungen von Art. 9 DSGVO sowie Art. 5 Abs. 3 ePrivacy-Richtlinie erfüllt sind. Dazu gehört auch die Information der Betroffenen über den Zugang der für die Verarbeitung Verantwortlichen und der Erleichterung der Ausübung der Betroffenenrechte.[63]

Art. 5 Abs. 7 möchte Betroffene nach der DSGVO schützen. Deren Rechte sollen durch Versäumnisse seitens Dateninhaber oder des Dritten, Vorkehrungen für die Übermittlung der Daten zu treffen, nicht behindert, verhindert oder beeinträchtigt werden. Zwar werden hier erstmal Betroffenenrechte nach der DSGVO angesprochen, sodass der Eindruck entstehen könnte, dass auch Betroffenenrechte wie Auskunfts-, Lösch- oder Widerspruchsrecht umfasst sein könnten. Allerdings beschränkt sich die Nennung auf Art. 20 DSGVO. Eine echte Verpflichtung der einzelnen Akteure bleibt aus.

Für Art. 5 Abs. 8, der Geschäftsgeheimnisse betrifft, gelten die Ausführungen zu Art. 4 Abs. 3 entsprechend.

Art. 5 Abs. 9 legt fest, dass das Übertragungs- oder Weitergaberecht von Daten nach Art. 5 Abs. 1 nicht die Datenschutzrechte anderer Personen beeinträchtigen kann. Diese Formulierung ist dem EDSA und dem EDSB nicht klar genug. Sie fordern eine Klarstellung hinsichtlich des Umfangs und der Bedeutung dieses Absatzes und empfehlen die Kriterien für die Abwägung des Rechts auf Übertragbarkeit mit den Datenschutzbelangen anderer Personen anhand der Leitlinien des EDSB zur Datenübertragbarkeit in einem Erwägungsgrund aufzugreifen.[64]

d) Art. 6 – Pflichten Dritter, die Daten i.A. des Nutzers erhalten

Art. 6 Abs. 1 verpflichtet den Dritten zur Verarbeitung der bereitgestellten Daten nur nach den mit dem Nutzer vereinbarten Zwecken, bei personenbezogenen Daten „*vorbehaltlich der Rechte der betroffenen Personen*“. Die Verbraucherzentrale Bundesverband e.V. kritisiert, dass hier die mangelnde Abgrenzung personenbezogener und nicht-personenbezogener Daten am prägnantesten zu Tage trete. Es fehle an einer Einschränkung der Zwecke, zu denen der Dritte die Daten verarbeiten dürfte und der Dritte könne grundsätzlich Nutzern finanzielle Anreize für die Übermittlung der Daten anbieten. Deshalb sei es möglich, dass ein Unternehmen es Verbraucher:innen anbiete, gegen eine Entschädigung die Daten der Produkte kontinuierlich und in Echtzeit zu übertragen, daraus Profile zu bilden und diese an weitere Datenhändler zu verkaufen. Bei personenbezogenen Daten wäre diese Praktik als problematisch zu bewerten, da hierbei personenbezogene Daten auf ihren wirtschaftlichen Wert reduziert würden und einkommensschwachen Gruppen durch Verkauf ihrer Daten über bspw. Fitnesstracker falsche Anreize gesetzt würden.[65]

---

[63] Ebd. S. 14.
[64] Ebd. S. 15.
[65] *Verbraucherzentrale Bundesverband e.V.,* Verbraucher:innen beim Data Act im Blick behalten. Stellungnahme des Verbraucherzentrale Bundesverbands zum Vorschlag der Europäischen Kommission für ein Datengesetz (Data Act). Berlin, 13. Mai 2022, S. 11-12.

Daneben befürchtet der Verbraucherverband, dass die Vereinbarung nach Art. 6 Abs. 1 als eine Rechtsgrundlage für die Verarbeitung personenbezogener Daten betrachtet werden könnte, was den engen Auslegungen des EDSA in den Leitlinien 2/2019 zuwiderlaufen würde, sodass auch hier eine Klarstellung gewünscht ist.[66] EDSA und EDSB empfehlen für den Fall, dass der Nutzer nicht Betroffener nach der DSGVO ist, sicherzustellen, dass jede weitere Verarbeitung im Einklang mit Art. 6 Abs. 4 DSGVO erfolgt, bzw. bei der Profilerstellung des Art. 6 Abs. 2 lit. b unter Berücksichtigung des Art. 22 DSGVO. Auch die Verweise auf Art. 9 DSGVO und die Vorgaben des Art. 5 Abs. 3 ePrivacy-Richtlinie sollen Berücksichtigung finden. Immer wenn es sich beim Nutzer, Dateninhaber oder dem Dritten nicht um einen Betroffenen handelt, sollte die Verarbeitung personenbezogener Daten klar eingeschränkt werden, insbesondere wenn sich aus diesen präzise Rückschlüsse auf das Privatleben ziehen ließen. Der Einschub in Art. 6 Abs. 1 „soweit personenbezogene Daten betroffen sind“ sollte mit dem Wortlaut „*und wenn alle in den Datenschutzvorschriften vorgesehenen Bedingungen und Regeln eingehalten werden, insbesondere wenn eine gültige Rechtsgrundlage gemäß Artikel 6 besteht und gegebenenfalls die Bedingungen von Artikel 9 der DSGVO und Artikel 5 Absatz 3 der Datenschutzrichtlinie für elektronische Kommunikation erfüllt sind, und vorbehaltlich der Rechte der betroffenen Person, soweit personenbezogene Daten betroffen sind.*“[67] ersetzt werden.[68] Abs. 1 Buchstabe a, der Täuschung oder Manipulation durch den Dritten verbietet, sollte anstatt dem Nutzer den Betroffenen im Sinne der DSGVO erfassen. Das gleiche gilt hinsichtlich der Profilerstellung nach Buchstabe b, auch hier können Nutzer und natürliche Person auseinanderfallen, sodass bspw. ein Unternehmen die Profilbildung der eigenen Mitarbeiter wünschen könnte – mit erheblichen Beeinträchtigungen für die Rechte und Freiheiten der eigentlich Betroffenen.[69] Auch der Dritte sollte als Verantwortlicher dem Prinzip der Datenminimisierung verpflichtet sein und Anonymisierungstechniken anwenden, wann immer es möglich ist.[70]

e) Art. 7 – KMU-Ausnahme und virtuelle Assistenten

Die Tatsache, dass mit Art 7 Abs. 1 KMU im Sinne von Art. 2 des Anhangs der Empfehlung 2003/361/EG, nicht den Pflichten des Kapitels unterliegen, ist problematisch. Es ist unweigerlich zu begrüßen, dass KMU gefördert werden, um ihnen Chancen am Markt zu ermöglichen. Dies könnte jedoch auf Kosten des Datenschutzrechts einhergehen. Zwar ist Art. 1 Abs. 3 von dieser Ausnahme nicht erfasst. Die explizite Ausnahme könnte jedoch zu einem praktischen Defizit bei der Anwendung des Datenschutzrechts durch KMU führen, da wesentliche Verbote wie Art. 6 Abs. 2 lit. a – das Nudging-Verbot – und b – die Profileinschränkung – in diesem Kapitel ausgesprochen wurden. Daneben gibt Art. 1 Abs. 3 inhaltlich nicht genug her, um den Vorrang des Datenschutzrechts zu gewährleisten (s.o.).

4. Pflicht Daten Dritten bereitzustellen – Art. 8 bis 12 (Kapitel III)

Kapitel III legt fest, dass die Bereitstellung von Daten zu fairen Bedingungen und transparent erfolgen muss. Etwaige Gegenleistungen müssen angemessen ausgestaltet sein. EDSA und EDSB kritisieren, dass Betroffene in Fällen, in denen sie nicht Nutzer sind, nicht Vertragspartner werden, was die Effektivität der Datenschutzrechte einschränkt. Darüber hinaus besteht das Risiko, dass durch Datenvermittlungsdienste und -tauschbörsen aus Daten, die zuvor als nicht-personenbezogen klassifiziert wurden aufgrund der Kombination mit anderen zur Verfügung

[66] Ebd. S. 7.
[67] *EDSA/ EDSB,* EDPB-EDPS Joint Opinion 2/2022 on the Proposal of the European Parliament and of the Council on harmonized rules on fair access to and use of data (Data Act). Brüssel 04.05.2022, S. 15-16.
[68] Ebd.
[69] Ebd. S. 16.
[70] Ebd. S. 17.

stehenden Informationen zu personenbezogenen wandeln. Art. 8 Abs. 3 und 4 würden das Recht auf informationelle Selbstbestimmung gefährden. Denn diese Absätze verbieten es Dateninhabern zwischen Datenempfängern zu diskriminieren oder einem Datenempfänger exklusiv Daten zur Verfügung zu stellen. Dies wäre jedoch das Recht eines Betroffenen, insbesondere dann, wenn die Verarbeitung auf einer Einwilligung nach Art. 6 DSGVO oder Art. 5 Abs. 3 ePrivacy-Richtlinie beruhe. Der kurze Hinweis auf die DSGVO in Erwägungsgrund 41 reiche insoweit nicht aus.[71] Dieser lautet lediglich „*Diese Pflichten gelten unbeschadet der Verordnung (EU) 2016/679.*"

Art. 9, der die Gegenleistung für die Bereitstellung von Daten regelt, erlaubt es zusammen mit Erwägungsgrund 42 gegenüber KMU nur ein Entgelt hinsichtlich der Kosten und Investitionen für die Bereitstellung zu verlangen. EDSA und EDSB befürchten, dass dies im Zusammenspiel mit Erwägungsgrund 46 so verstanden wird, dass bei großen Unternehmen bzw. einem großen Unternehmen als Empfänger es das Recht des Dateninhabers ist, eine „angemessene Entschädigung" festzulegen, die ein Anreiz für die Monetarisierung personenbezogener Daten sein könnte. Dies sei aber nicht mit Art. 8 EuGrCh vereinbar.[72]

Art. 10 sieht die Möglichkeit vor „*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 gemäß den Artikeln 8 und 9*" durch die Mitgliedstaaten zertifizierte Streitbeilegungsstellen beizulegen. EDSA und EDSB empfehlen dringend in Abs. 5 und 9 des Art. 10 Vorschriften aufzunehmen, die die Rechte des Betroffenen und die Pflichten des Verantwortlichen achten. Dazu gehört auch explizit die Möglichkeit des wirksamen Rechtsmittels, was nach Abs. 9 allein den Parteien zusteht, was den Betroffenen ausschließen könnte oder die Möglichkeit selbst eine Beschwerde bei einer Aufsichtsbehörde einzureichen.[73]

Art. 11 Abs. 1 schlägt zur Einhaltung der Pflichten der Art. 5, 6, 9 und 10 die Anwendung geeigneter Schutzmaßnahmen, insbesondere „intelligente Verträge" vor. EDSA und EDSB fordern, dass klargestellt werden sollte, wie „Smart Contracts" Dateninhabern und Empfängern adäquate Garantien gegen unautorisierte Weitergabe oder unbefugte Zugriffe sowie der Einhaltung der Vereinbarungen bereitstellen können. Außerdem wünschen sie sich Kohärenz mit Art. 32 DSGVO, sodass in Art. 11 Abs. 1 eine Verpflichtung zur Umsetzung geeigneter technischer und organisatorischer Maßnahmen entsprechend dem jeweiligen Risiko der Datenverarbeitung, eingefügt werden sollte. Die Verpflichtung des Datenempfängers im Fall einer Erlangung der Daten durch ungenaue oder falsche Informationen, Täuschungen, Zwangsmittel oder dem Ausnutzen von Lücken, die Nutzung für nicht genehmigte Zwecke oder ohne Zustimmung des Dateninhabers nach Art. 11 Abs. 2 sollte das Erfordernis einer Rechtsgrundlage nach der DSGVO und die Rechte des Betroffenen wahren. Daneben lassen die Ausnahmetatbestände des Art. 11 Abs. 3 die Interessen und Schäden des Betroffenen unberücksichtigt.[74]

Die Verpflichtung des Dateninhabers zur Bereitstellung von Daten an Datenempfänger nach Art. 5 in Art. 12 Abs. 1 kann nach Ansicht von EDSA und EDSB als Rechtsgrundlage nach Art. 6 Abs. 1 UAbs. 1 lit. c DSGVO, der rechtlichen Verpflichtung, verstanden werden. Zwar möchte Erwägungsgrund 24 dies ausschließen, dessen Formulierung sei jedoch unzureichend. Art. 12 Abs. 2, der die Unwirksamkeit von Klauseln, die zum Nachteil einer Partei oder eines

[71] Ebd.
[72] Ebd. S. 18.
[73] Ebd.
[74] Ebd. S.18-19.

Nutzers die Anwendung des Kapitels ausschließen, abweichen oder abändern, festlegt, sollte dies auch für nachteilige Abweichungen und Änderungen für die Rechte der Betroffenen vorsehen.[75]

5. Missbräuchliche Klauseln für Datenzugang und Datennutzung (Kapitel IV)

Die Vertragsbedingungen, die Regelungen über die Nutzung der zu übertragenden Daten erlauben, sind in einigen selbst im Data Act geregelten Fällen nicht bindend. Die Fälle sind in Art. 13 aufgeführt. Art. 13 Abs. 1 stellt klar, dass einseitig auferlegte Vertragsklauseln von einem Unternehmen gegenüber einem Kleinstunternehmen oder einem kleinen oder mittleren Unternehmen für Letztere nicht bindend sind, wenn sie missbräuchlich sind.

Art. 13 Abs. 2 definiert den allgemeinen Missbrauchstatbestand, der dann vorliegt, wenn die Vertragsklausel in grober Weise von guten Geschäftsgepflogenheiten beim Datenzugang und der Datennutzung abweicht und gegen Treu und Glauben und die guten Sitten verstößt. EDSA und EDSB weisen an dieser Stelle darauf hin, dass die gute Geschäftspraxis, das Gebot von Treu und Glauben und der redliche Geschäftsverkehr, die in Art. 13 Abs. 2 genannt werden, weder definiert noch sonst einheitlich festgelegt sind.[76] In der Umsetzung droht hier eine unterschiedliche Anwendung in der Union.

Abs. 7 legt fest, dass sich die Missbräuchlichkeit des Art. 13 allein auf Regelungen zum Datenzugang und der Datennutzung, der Haftung oder Rechtsbehelfe bei datenbezogenem Pflichten bezieht (Abs. 1), nicht aber auf den Hauptgegenstand des Vertrags, noch auf für den Preis betreffende Klauseln. Art. 13 Abs. 3 besagt, dass die Klausel missbräuchlich ist, wenn sie bezweckt oder bewirkt, dass die Klauselstellerin die Haftung für Vorsatz oder grobe Fahrlässigkeit ausschließt (a); sie Rechtsbehelfe einseitig im Fall von Nichterfüllung vertraglicher Verpflichtungen oder der Haftung im Falle der Verletzung dieser Verpflichtungen beschränkt oder ausschließt (b) oder sie sich einseitig das ausschließliche Recht einräumt zu bestimmen, ob die gelieferten Daten mit dem Vertrag übereinstimmen oder eine Vertragsklausel auszulegen (c). Nach Art. 13 Abs. 4 gilt als missbräuchlich, wenn die Vertragsklausel bezweckt oder bewirkt, dass Rechtsmittel bei Nichterfüllung oder Haftung im Rahmen des Vertrages unangemessen beschränkt werden (a); dass die Klauselstellerin sich einseitig ein Datenzugangs- und Nutzungsrecht in einer Weise einräumt, die den berechtigten Interessen der Vertragspartei erheblich schadet (b); dass sie der anderen die Nutzung der bereitgestellten oder erzeugten Daten untersagt oder diese in verhältnismäßiger Weise zu nutzen, zu erfassen, zuzugreifen, zu kontrollieren oder zu verwerten (c); dass die stellende Partei die andere daran hindert, eine Kopie der von ihr bereitgestellten oder erzeugten Daten zu erhalten (d) oder dass die stellende Partei mit unangemessen kurzer Frist kündigen darf, wobei die realistischen Möglichkeiten zum Wechsel zu einer anderen Vertragspartei oder gleichbaren Dienst und eines finanziellen Nachteils berücksichtigt werden (e). Sind die übrigen Bedingungen abtrennbar von der missbräuchlichen Klausel, sind sie bindend, Art. 13 Abs. 6.

Komplikationen mit dem Datenschutzrecht ergeben sich an dieser Stelle, sobald eine Klausel gegen Art. 13 verstößt. Liegt kein Verstoß vor, dienen die Vertragsbedingungen als vertragliche Grundlage für die Verarbeitung der personenbezogenen Daten nach Art. 6 Abs. 1 UAbs. 1 lit. b DSGVO. Ist eine Klausel unwirksam und die wesentliche Regelung, die Grundlage für die Verarbeitung darstellt ist abtrennbar, bleibt es bei der datenschutzrechtlichen Verarbeitungsgrundlage. Ist diese dagegen betroffen, die Bedingungen also nicht abtrennbar von einer missbräuchlichen Klausel, fehlt es an einer Rechtsgrundlage. Keine Komplikationen mit

[75] Ebd. S. 19.
[76] Ebd.

dem Datenschutzrecht ergeben sich dagegen, wenn es sich nicht um personenbezogene Daten handelt. Pseudonymisierte Daten würden hier nicht ausreichen.[77] Offen bleibt, ob ein Nutzer oder Dritter, der Betroffener bzw. Verbraucher ist sich auch auf die Missbräuchlichkeit von Klauseln nach Art. 13 Abs. 2-4 berufen kann und warum er dies nicht tun können sollte.

6. Pflichten Daten öffentlichen Stellen bereitzustellen – Art. 14 bis 22 (Kapitel V)

Die Art. 14 bis 22 regeln die Pflicht von Dateninhabern Daten auf Anfrage von öffentlichen Stellen oder Organen, einer Einrichtung oder sonstigen Stelle der Union herausgeben zu müssen. EDSA und EDSB haben ernsthafte Bedenken in Bezug auf die Rechtmäßigkeit, Erforderlichkeit und Angemessenheit der Verpflichtung Daten an Öffentliche Stellen und EU-Institutionen, Agenturen oder Organe herausgeben zu müssen.[78]

Art. 14 Abs. 1 ordnet die Pflicht an, Absatz 2 schließt KMU aus. EDSA und EDSB haben den Eindruck, dass der Data Act Entwurf Art. 6 Abs. 1 UAbs. 1 lit. c DSGVO als Rechtsgrundlage für die Verarbeitung personenbezogener Daten für einen solchen Fall ansieht. Trotzdem sei aber nicht klar, für welche besondere Aufgabe im öffentlichen Interesse und welche Öffentlichen Stellen dazu berufen sein werden. Außerdem sollten die Kategorien von personenbezogenen Daten, auf die durch öffentliche Stellen zugegriffen werden sollen, spezifiziert werden. Sie befürchten, dass Standortdaten darunterfallen könnten, die intime Rückschlüsse erlaubten.[79]

Art. 15 beschreibt die außergewöhnliche Notwendigkeit die für eine Anfrage vorliegen muss. EDSA und EDSB vermissen hinsichtlich der Buchstaben a und b, die beide den öffentlichen Notstand betreffen, die Anforderung „*ausdrücklich im Gesetz vorgesehen*“, da jede Einschränkung des Rechts auf personenbezogene Daten „gesetzlich vorgesehen“ sein muss, Art. 52 Abs. 1 EuGrCh. Einschränkungen müssen eine gesetzliche Grundlage haben, die hinreichend zugänglich und vorhersehbar sowie hinreichend präzise formuliert ist. Sie muss im Einklang mit den Grundsätzen der Notwendigkeit und Verhältnismäßigkeit auch Umfang und Art und Weise der Ausübung der Befugnisse durch die zuständigen Behörden festlegen und mit ausreichenden Garantien zum Schutz des Einzelnen vor willkürlichen Eingriffen versehen sein. In ihrer Stellungnahme gehen EDSA und EDSB sodann auf die die Anfrage legitimierenden Begriffe „außergewöhnliche Notwendigkeit“ und „öffentlicher Notstand“ ein. Die Definition von letzterem in Art. 2 Nr. 10 sei viel zu ungenau. Erwägungsgrund 57 spezifiziere zwar in einem gewissen Rahmen den öffentlichen Notstand, durch den Verweis auf einschlägige Verfahren der Mitgliedstaaten oder internationaler Organisationen. Diese Präzisierung sollte jedoch in den verfügenden Teil des Vorschlags aufgenommen werden und hinsichtlich beider Begriffe viel strengere Definitionen verwandt werden. So könne die Definition des öffentlichen Notstands so geändert werden, dass sie die Arten von Situationen darstellen, in denen ein solcher vorliegt. Hinsichtlich des Buchstaben c in Art. 15 sei die Norm nicht vorhersehbar, sodass sich Komplikationen mit Grundrechten ergeben würden und die Frage im Raum steht, wie sich durch die Verringerung von Verwaltungsaufwand die Auswirkungen auf die Grundrechte und -freiheiten der betroffenen Personen aufwiegen lässt. Die Eingriffe über Buchstabe c erscheinen EDSA und EDSB nicht als erforderlich.[80]

Art. 16 Abs. 1 stellt klar, dass die Pflichten für Berichterstattung, Beantworten von Auskunftsersuchen oder die Überprüfung der Einhaltung rechtlicher Pflichten unberührt bleibt. Art. 16 Abs. 2 verbietet die Anwendung der Datennutzungsanfrage für die Zwecke „*der*

---

[77] *Schild*, BeckOK DatenschutzR, DS-GVO Art. 4 Rn. 78,
[78] *EDSA/ EDSB,* EDPB-EDPS Joint Opinion 2/2022 on the Proposal of the European Parliament and of the Council on harmonized rules on fair access to and use of data (Data Act). Brüssel 04.05.2022, S. 20.
[79] Ebd. S. 20-21.
[80] Ebd.

Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder Ordnungswidrigkeiten oder der Strafvollstreckung oder der Zoll- oder Steuerverwaltung". Übriges anwendbares Unionsrecht für diese Zwecke bleibt unberührt. EDSA und EDSB kritisieren hier zunächst, dass die genannten Bereiche von denen des Art. 1 Abs. 4 unterscheiden. Daneben stelle bereits Erwägungsgrund 60 dar, dass in diesen Bereichen sich die Stellen auf sektorale Rechtsvorschriften stützen sollten. Solche Einrichtungen sollten aus dem Anwendungsbereich des Kapitel V ausgenommen sein, denn Dateninhaber sollten allein im Einklang mit den sektoralen Rechtsvorschriften verpflichtet werden können. Hinsichtlich der Organe, Agenturen und Einrichtungen der Union sollten im verfügenden Text ausdrücklich die berechtigten Stellen genannt werden.[81]

Art. 17 gibt in den Absätzen 1 und 2 Vorgaben hinsichtlich der Art und Weise des Datenbereitstellungsverlangens. EDSA und EDSB kritisieren hinsichtlich des Datenbereitstellungsverlangens allgemein, dass die öffentliche Stelle einen breiten Ermessensspielraum verfügt, da sie in ihrem Antrag selbst festlegt, welche Daten benötigt werden und was den außergewöhnlichen Bedarf darstellt. Nur im Fall eines öffentlichen Notstands soll es dazu ein festgelegtes Verfahren geben. Umfang und Art und Weise der Ausübung der Befugnisse sollten klarer definiert werden, um Betroffene gegen willkürliche Eingriffe zu schützen. Die vorliegende Regelung entspricht nicht den Voraussetzungen einer Eingriffsgrundlage wie sie der EuGH fordere. Dabei zitieren EDSA und EDSB die Rechtssache C-623/17[82] und nennen die wesentlichen Voraussetzungen: klare und präzise Regeln für den Anwendungsbereich und die Anwendung der Maßnahmen sowie Mindestgarantien für Personen deren personenbezogene Daten betroffen sind, die Angabe unter welchen Umständen und Bedingungen eine Maßnahme erlassen werden kann, so dass sichergestellt ist, dass der Eingriff auf das unbedingt erforderliche Maß beschränkt ist. Bei Daten besonderer Kategorien seien derartige Garantien noch notwendiger.[83]

Hinsichtlich der Angabe der Rechtsgrundlage nach Art. 17 Abs. 1 lit. d fordern EDSA und EDSB, dass klargestellt werden soll, dass die Rechtsgrundlage angegeben werden muss, die der öffentlichen Stelle die Aufgabe zuweist.[84] Die Sicherheitsvorkehrungen für Betroffene seien nicht ausreichend im Vorschlag ausformuliert. Insbesondere Art. 17 Abs. 2 Buchstabe c bezieht zwar die rechtmäßigen Ziele des Dateninhabers mit ein, nicht aber die Risiken für die Rechte und Freiheiten des Betroffenen.[85]

Absatz 2 Buchstabe d ordnet an, dass „*soweit wie möglich nur nicht personenbezogene Daten*" betroffen sein sollen. Das diese Einschränkung gegeben ist, ist datenschutzrechtlich zu begrüßen. Denn es entspricht dem Datenminimierungsgrundsatz des Art. 5 Abs. 1 lit. c DSGVO. EDSA und EDSB sehen den Buchstabe d als Teil der Pseudonymisierungs- und Anonymisierungsbemühen, von denen ersteres in Art. 18 Abs. 5 angesprochen wird (Ausführungen dazu dort).[86]

In Art. 17 Abs. 3 wird darauf hingewiesen, dass die Daten gerade nicht zur Weiterverwendung im Rahmen der Richtlinie (EU) 2019/1024[87] („Offene Daten und die Weiterverwendung von

[81] Ebd. S. 23-24.
[82] EuGH, C-623/17, Privacy International gegen Secretary of State for Foreign and Commonwealth Affairs, ECLI:EU:C:2020:790, Rn. 68.
[83] *EDSA/ EDSB,* EDPB-EDPS Joint Opinion 2/2022 on the Proposal of the European Parliament and of the Council on harmonized rules on fair access to and use of data (Data Act). Brüssel 04.05.2022, S. 22.
[84] Ebd. S. 20.
[85] Ebd. S. 21.
[86] Ebd.
[87] Mit der „Open-Data-Richtlinie", können bspw. geografische Informationen, Grundbuchinformationen, statistische oder juristische Informationen im Besitz öffentlicher Stellen oder öffentlicher Unternehmen

Informationen des öffentlichen Sektors“) verwendet werden dürfen. Absatz 4 erlaubt aber die Teilung von derart erlangten Daten mit anderen öffentlichen Stellen im Einklang mit der außergewöhnlichen Notwendigkeit nach Art. 15 und ordnet in UAbs. 2 die Pflicht an, den Dateninhaber über eine Weiterübermittlung bzw. -bereitstellung zu informieren. Erwägungsgrund 65 schränkt die Weiterverwendung auf den ursprünglichen Zweck ein. EDSA und EDSB weisen insoweit darauf hin, dass jede Verarbeitung personenbezogener Daten für einen anderen Zweck als den der Erhebung von Art. 6 Abs. 4 DSGVO bzw. Art. 6 Verordnung (EU) 2018/1725 gedeckt sein muss. Die Vorschriften sollten dahingehend angepasst werden.[88]

Art. 18 regelt die Art und Weise der Erfüllung des Datenzugangsverlangens. EDSA und EDSB fordern, dass die in Abs. 2 genannten sektorspezifischen Rechtsvorschriften spezifiziert werden sollten.[89] Aus der Ablehnungsbefugnis des Absatz 2 Buchstabe b könnte sich eine Ablehnung aufgrund Unvereinbarkeit mit Datenschutzrecht ergeben. Insoweit ist allerdings zu beachten, dass Art. 17 Abs. 2 lit. d nicht per se den Zugriff auf personenbezogene Daten ausschließt. Es erfolgt lediglich eine Anordnung des Datenminimierungsgrundsatzes (s.o.). Deshalb ist es fraglich, ob sich aus Anfragen, die personenbezogene Daten fordern, obwohl sie nach dem angegebenen Zweck nicht erforderlich sind, eine Ablehnungsbefugnis aus Art. 18 Abs. 2 lit. b aufgrund Verstoßes gegen Art. 17 Abs. 2 lit. d ergibt. Hier wird dann die Einschätzungsprärogative der Behörde und der verfolgte Zweck gegen den Datenminimierungsgrundsatz stehen und gegeneinander abgewogen werden müssen. Insoweit ist auch Art. 18 Abs. 5 zu beachten, der anordnet, dass der Dateninhaber, sofern das Verlangen auch mit pseudonymisierten Daten erfüllt werden kann, die personenbezogenen Daten pseudonymisieren muss. Inwieweit eine öffentliche Stelle explizit verlangen kann, dass nicht einmal Pseudonymisierungsversuche unternommen werden sollen bleibt abzuwarten. Die explizite Forderung von personenbezogenen Daten könnte jedoch einen Verdacht hinsichtlich des Zweckverbots des Art. 16 Abs. 2 eröffnen. Denn werden explizit nicht pseudonymisierte Daten gefordert besteht zumindest eine erhöhte Wahrscheinlichkeit, dass diese einem Strafverfahren abhelfen könnten. Letztlich darf durch das Herausgabeverlangen keine Anwendung oder Auslegung einer Bestimmung der Verordnung in der Art und Weise erfolgen, „*dass das Recht auf Schutz personenbezogener Daten oder das Recht auf Privatsphäre und Vertraulichkeit der Kommunikation geschwächt oder eingeschränkt wird.*“[90] EDSA und EDSB halten die Einschränkung der „angemessenen Anstrengungen“ für die Pseudonymisierung für nicht ausreichend. Pseudonymisierung mindert die Risiken für die Betroffenen, indem sie die Menge der verarbeiteten personenbezogenen Daten und die Auswirkungen einer eventuellen Datenschutzverletzung reduziert. Daneben könnten noch andere geeignete Garantien der DSGVO vom Dateninhaber umgesetzt werden.[91] Art. 18 Abs. 6 verweist für den Widerspruch auf die Ablehnung des Dateninhabers der anfragenden öffentlichen Stelle bzw. für den Einspruch des Dateninhaber gegen das Verlangen auf die nach Art. 31 zuständige Behörde. EDSA und EDSB fordern, dass Art. 31 den EDSB und einen Verweis auf die Verordnung (EU) 2018/1725 einbezieht sowie in Art. 18 Abs. 6 auch den Betroffenen als widersprechende Person und dessen Recht auf ein effektives Rechtsmittel gegen diese Anfrage berücksichtigt.[92]

---

und öffentlich finanzierte Forschungsdaten weiterverwendet werden.

[88] *EDSA/ EDSB,* EDPB-EDPS Joint Opinion 2/2022 on the Proposal of the European Parliament and of the Council on harmonized rules on fair access to and use of data (Data Act). Brüssel 04.05.2022, S. 22

[89] Ebd. S. 23.

[90] Erwägungsgrund 7, S. 5 des Datengesetzes.

[91] *EDSA/ EDSB,* EDPB-EDPS Joint Opinion 2/2022 on the Proposal of the European Parliament and of the Council on harmonized rules on fair access to and use of data (Data Act). Brüssel 04.05.2022, S. 21-22.

[92] Ebd. S. 23.

Art. 19 Abs. 1 ordnet eine Zweckbindung, die Einhaltung technischer und organisatorischer Maßnahmen und eine Vernichtungsverpflichtung nach Ablauf des Zwecks an. Dies entspricht den Vorgaben der Art. 5 Abs. 1 lit. b und c DSGVO (Zweckbindung und Datenminimierung), den datenschutzfreundlichen Voreinstellungen des Art. 25 DSGVO und den Technischen und Organisatorischen Schutzmaßnahmen der Art. 32 DSGVO, § 64 BDSG. Erwägungsgrund 8 führt dazu aus, dass zu solchen Maßnahmen „*nicht nur die Pseudonymisierung und Verschlüsselung, sondern auch der Einsatz zunehmend verfügbarer Technik, die es ermöglicht, Algorithmen direkt am Ort der Datenerzeugung einzusetzen und wertvolle Erkenntnisse zu gewinnen, ohne dass die Daten zwischen den Parteien übertragen bzw. die Rohdaten oder strukturierten Daten selbst unnötig kopiert werden*“ zählen. Dem EDSA und dem EDSB halten die Verortung der Einhaltung technischer und organisatorischer Maßnahmen in Art. 19 für falsch. Dies müsse bereits bei der Erhebung der Daten beachtet werden, sodass dies ein Fall der Informationspflichten von Art. 17 sein soll.[93] Die in Art. 19 Abs. 1 lit. a angeordnete Zweckbindung wird allerdings dadurch konterkariert, dass die öffentlichen Stellen selbst in ihrer Anfrage den Zweck festlegen können. Dabei könnten sie weite Zwecke angeben, was auch die Löschverpflichtung beeinträchtigt. Hier sollte von Anfang an ein Zeitraum festgelegt werden.[94]

Auch die Weitergabe von Daten an Organisationen für wissenschaftliche Forschungstätigkeiten, nationale statistische Ämter und Eurostat unterliegen der Zweckbindung, Art. 21 Abs. 1, Abs. 3. Die Zweckbindung besteht auch bei der gegenseitigen Unterstützung, auch im Rahmen der Amtshilfe, Art. 22 Abs. 2. EDSA und EDSB fordern angemessene Garantien gemäß Art. 89 DSGVO und Art. 13 der Verordnung (EU) 2018/1725, die den potenziell sensiblen Charakter der fraglichen Daten berücksichtigen. Ein besonderes Augenmerk solle auf die Garantien für die Verarbeitung zu wissenschaftlichen Forschungszwecken gelegt werden, die einen rechtmäßigen, verantwortungsvollen und ethischen Umgang mit den Daten gewährleisten.[95]

Art. 22 regelt die Amtshilfe und grenzüberschreitende Zusammenarbeit.

7. Wechsel zwischen Datenverarbeitungsdiensten – Art. 23 bis 26 (Kapitel VI)

Auch wenn die Vorschriften der Art. 23 bis 26 hinsichtlich des Abbaus von Wechselhindernissen zwischen Datenverarbeitungsdiensten keine datenschutzrechtliche Relevanz aufweisen, möchte ich Ihnen die hierzu gelagerte Kritik von Herrn Schneider nicht vorenthalten. Er sieht in Art. 23 grundsätzlich einen Eingriff in die Vertragsfreiheit. Die kürzeren Vertragslaufzeiten aufgrund der kurzen Kündigungsfrist von 30 Kalendertagen nach Art. 23 Abs. 1 lit. a des Datengesetzes würden Rabatte und Preisreduzierungen für Langzeitverträge erschweren, da die Investitionskosten und Drittanbietersoftwarelizenzen nicht mehr so einfach amortisiert werden könnten.[96] Erwägungsgrund 52 sieht dieses Problem, weshalb der Grundsatz der Vertragsfreiheit als wesentliches Konzept in den Geschäftsbeziehungen zwischen Unternehmen berücksichtigt werden soll. Einer weiteren Kritik von Herr Schneider, dass die Pflicht des Art. 23 gravierende Herausforderungen für europäische XaaS (Anything as a Service) Provider schaffen würde, ist der Anwendungsbereich des Art. 1 Abs. 2 Datengesetz entgegenzuhalten. Genauso wie die DSGVO beschränkt sich der Anwendungsbereich nicht allein

[93] Ebd. S. 21.
[94] Ebd. S. 23.
[95] Ebd. S. 22-23.
[96] *Schneider, René,* „EU Data Act Draft – selected challenges for switching data processing services and international data transfers.” EPIC Summit 2022, Mai 2022, Web, 31.08.2023, https://lp.dataguard.de/hubfs/EPIC/EPIC%202022/EPIC%20on%20Demand%20Desktop/Stage%203%20_%20EU%20Data%20Act%20Draft%20%E2%80%93%20selected%20challenges%20for%20switching%20data%20processing%20services%20and%20international%20data%20transfers_150102_HQ.mp4.

auf europäische Firmen, sondern er bezieht sich auf europäische Daten bzw. „*Anbieter von Datenverarbeitungsdiensten, die Kunden in der Union solche Dienste anbieten*“, Art. 1 Abs. 2 lit. e Datengesetz. Aus dem Anwendungsbereich gelangt ein Anbieter damit nur, wenn er seine Dienstleistungen nicht auf europäische Kunden ausrichtet und nicht die weiteren Buchstaben a-d einschlägig sind. Die Nachteile treffen damit nicht nur europäische XaaS-Anbieter, sondern alle gleichermaßen. Bei Art. 24 Abs. 1 kritisiert Schneider die Vorgabe der uneingeschränkten Kontinuität bei der Erbringung der jeweiligen Funktionen oder Dienste. Dies sei unrealistisch und in der Praxis nur gegen zusätzliche Vergütung machbar. Daneben würden die Kosten in Zukunft nicht vorhersehbar sein, die Inflation müsse mit einkalkuliert werden. Dies würde die Preise erhöhen und die Wettbewerbsfähigkeit europäischer Anbieter verringern. Große Fälle bräuchten einen alternativen Übergangszeitraum wie ihn Art. 24 Abs. 2 benennt.[97] Hinsichtlich der Wettbewerbsnachteile ist wiederum auf Art. 1 Abs. 2 Datengesetz zu verweisen. Die einheitliche Durchsetzung des Datengesetzes für europäische Nutzer mit nicht-europäischen Dateninhabern ist jedoch essenziell, ansonsten werden die europäischen Dateninhaber benachteiligt sein. Inwieweit die Vorgaben des Art. 24 unrealistisch sind, bleibt abzuwarten. Schließlich dauert es noch ein bisschen, bis die Verordnung in Kraft tritt und Geltung erlangt. Die Vorschrift des Art. 24 Abs. 2, die in ihrem Satz 2 auch ein verringertes Entgelt während der Überschreitung der 30 Tage vorsieht wird die Unternehmen jedenfalls entsprechend motivieren einheitliche Schnittstellen und Standards einzusetzen bzw. mitzuentwickeln, da das Überschreiten allein bereits Umsatzausfälle bedeutet.

Art. 25 regelt die Reduktion und Abschaffung der Wechselentgelte. Art. 26 befasst sich mit technischen Aspekten des Wechsels.

8. Internationaler Zugang und internationale Übermittlung für nicht-personenbezogene Daten – Art. 27 (Kapitel VII)

Art. 27 möchte die Übermittlung bzw. den Zugriff auf nicht-personenbezogene Daten außerhalb der EU verhindern. Dazu sollen Anbieter nach Art. 27 Abs. 1 „*alle angemessenen technischen, rechtlichen und organisatorischen Maßnahmen, einschließlich vertraglicher Vereinbarungen [treffen], um eine internationale Übermittlung oder einen internationalen staatlichen Zugriff zu in der Union gespeicherten nicht personenbezogenen Daten zu verhindern, wenn dies im Widerspruch zum Unionsrecht oder zum nationalen Recht des betreffenden Mitgliedstaats stünde.*“ Abs. 2 erlaubt den Zugriff bei Vorliegen internationaler Übereinkünfte, Abs. 3 stellt dar, wann ohne internationale Übereinkünfte Daten übermittelt werden dürfen. Hierzu ist insbesondere eine Begründung und Verhältnismäßigkeit des Urteils, eine Rechtsmittelmöglichkeit und die Berücksichtigung der Interessen durch das Unionsrecht oder das nationale Recht geschützten Daten nötig.

René Schneider sieht hier eine Schlechterstellung von nicht-personenbezogenen Daten zu personenbezogenen Daten und keinen Grund für das veraltete Prinzip der Datenlokalisierung. Diese Regelungen würden den internationalen Datentransfer, der für den Alltag internationaler Unternehmen erforderlich ist, nicht berücksichtigen. In der Regelung sieht er eine Ausweitung von „Schrems II“ auf nicht-personenbezogene Daten mit damit einhergehenden Compliance-Aufgaben.[98]

EDSA und EDSB begrüßen dagegen Art. 27, der ihrer Auffassung nach Art. 48 DSGVO spiegelt. Da Art. 27 eigentlich nur Zugangsanfragen und keine Übermittlung betrifft und der Begriff anscheinend abweichend von der Bedeutung der DSGVO verwendet wird, empfehlen sie den

[97] Ebd.
[98] Ebd.

Begriff aus Art. 27 zu entfernen.[99] Unter Übermittlung im Sinne der DSGVO wird man aber nach Pauly „*jede Offenlegung personenbezogener Daten ggü. einem Empfänger in einem Drittland oder einer int. Organisation verstehen müssen, wobei es weder auf die Art der Offenlegung, noch auf die Offenlegung ggü. einem Dritten ankommt*“[100]. Deshalb sollte m.E. an dieser Stelle trotzdem der Begriff der Übermittlung beibehalten werden. Art. 27 Abs. 1 sei hinsichtlich der Formulierung „*Unbeschadet des Absatzes 2 oder 3*“ unklar. EDSA und EDSB wollen verhindern, dass der Eindruck entsteht, dass die in Abs. 1 angeführten Maßnahmen nur bei einer Anfrage eingehalten werden müssen und nicht standardmäßig. Auch der Begriff „angemessen“ birgt die Gefahr, dass die Effektivität der Maßnahmen verringert sein könnte, sodass vielmehr „erforderlich“ verwendet werden sollte. Die Wirkung der eingeholten Stellungnahme der zuständigen Behörde nach Art. 27 Abs. 3 sollte bei Feststellung der Beeinträchtigung der genannten Interessen der Union oder ihrer Mitgliedstaaten verpflichtend für den Adressaten sein.[101]

9. Interoperabilität – Art. 28 bis 30 (Kapitel VIII)

Kapitel VIII enthält mit den Art. 28 bis 30 Regelungen zu Anforderungen an Interoperabilität, die Interoperabilität von Datenverarbeitungsdiensten und Anforderungen an intelligente Verträge. Daraus ergeben sich keine Bezüge zum Datenschutzrecht.

10. Anwendung und Durchsetzung – Art. 31 bis 34 (Kapitel IX)

EDSA und EDSB kritisieren grundsätzlich an der Anwendung und Durchsetzung, dass die Überwachung der Anwendung der Verordnung zwischen den Mitgliedstaaten nicht harmonisiert wird, kein europäisches Kohärenzverfahren vorgesehen ist, was die kohärente Anwendung im Binnenmarkt gewährleisten könnte. Fehlende harmonisierten Sanktionen ließen ein Forum Shopping befürchten.[102]

a) Art. 31 – Zuständige Behörden

Art. 31 Abs. 1 verpflichtet jeden Mitgliedstaat eine oder mehrere zuständige Behörden zu errichten oder zu benennen, die verantwortlich sind. EDSA und EDSB kritisieren hieran, dass die Benennung von mehr als einer zuständigen Behörde zu operativen Schwierigkeiten kommen könnte, da die aktuelle Governance-Architektur zu Komplexität und Verwirrung führen würde.[103]

Art. 31 Abs. 2 legt fest, dass die für die Überwachung der DSGVO zuständigen Datenschutzbehörden bzgl. personenbezogener Daten auch für die Überwachung des Data Acts zuständig sind und die Kapitel VI und VII der DSGVO sinngemäß Anwendung finden sowie sektoral Fachbehörden zuständig bleiben, die zuständige Behörde aber zumindest Erfahrungen auf dem Gebiet der Daten und der elektronischen Kommunikationsdienste verfügen muss. EDSA und EDSB kritisieren die vage Festlegung des Art. 31 Abs. 2 lit. b hinsichtlich der sektoralen Behörden. Hier gibt es große Überschneidungen und Zuständigkeitskonflikte, auch mit der in Erwägungsgrund 82 und den Art. 36, 37 genannten Verbraucherschutzbehörden. Es sollte festgelegt werden, welche Behörde konkret für die Anwendung und Durchsetzung von Kapitel IV, den missbräuchlichen Klauseln, zuständig ist. Das Governance-Modell des Vorschlags muss klarer und detaillierter mit dem in den sektoralen Rechtsvorschriften vorgesehenen Modellen (z.B.

---

[99] *EDSA/ EDSB,* EDPB-EDPS Joint Opinion 2/2022 on the Proposal of the European Parliament and of the Council on harmonized rules on fair access to and use of data (Data Act). Brüssel 04.05.2022, S. 24.
[100] Paal/Pauly/Pauly, 3. Aufl. 2021, DS-GVO Art. 44 Rn. 4.
[101] *EDSA/ EDSB,* EDPB-EDPS Joint Opinion 2/2022 on the Proposal of the European Parliament and of the Council on harmonized rules on fair access to and use of data (Data Act). Brüssel 04.05.2022, S. 24.
[102] Ebd.
[103] Ebd. S. 25.

die Behörden der Gesundheitsdatenraumverordnung) abgestimmt werden. Die Benennung der Datenschutzbehörden als zuständige Behörden für den Schutz personenbezogener Daten wird begrüßt. Allerdings sehen EDSA und EDSB einen möglichen Konflikt mit den sektoralen Behörden, da die Formulierung „Unbeschadet des Absatzes 1“ diese nicht mit einbezieht.[104] Die alleinige Erwähnung des Europäischen Datenschutzbeauftragten in Art. 33 Abs. 4 wird kritisiert. Er sollte in Art. 31 Abs. 2 lit. a explizit als zuständige Behörde für die Organe, Einrichtungen und Agenturen der EU genannt werden, da diese auch als Nutzer oder Dateninhaber im Sinne des Vorschlags auftreten können.[105]

Art. 31 Abs. 3 gibt Vorgaben hinsichtlich der einzelnen durch die Mitgliedstaaten vorzugebenen Aufgaben und Befugnisse für die zuständigen Behörden. Hinsichtlich Abs. 3 stellen EDSA und EDSB fest, dass die festgelegten Befugnisse und Aufgaben nahezu denen des Art. 58 DSGVO entsprechen. Es fehlt jedoch an einer Harmonisierung der Aufgaben und Befugnisse der zuständigen Behörden und einem besseren Zusammenspiel mit der DSGVO. Schließlich sei nicht klar, wie sich die Aufgaben und Befugnisse des Art. 31 Abs. 3 auf die der Datenschutzbehörden bei Überwachung und Anwendung des Data Act auswirken (Art. 31 Abs. 2 lit. a). Es könne aus Art. 31 Abs. 2 lit. a der Eindruck gewonnen werden, dass sich die Aufgaben und Befugnisse aus den Kapiteln VI und VII der DSGVO ergeben. Unklar sei jedoch, ob der Vorschlag selbst auch Aufgaben und Befugnisse zuweise und wie diese in einem solchen Fall mit den Aufgaben der DSGVO zusammenwirken würden.[106] Das Abstimmungsgebot mit Behörden anderer Mitgliedstaaten in Art 31 Abs. 3 lit. f sei nicht klar genug, um ein echter europäischer Kooperationsrahmen zu sein.[107]

Abs. 4 ordnet die Zusammenarbeit von mehreren zuständigen Behörden, sowie die Zusammenarbeit mit der Datenschutzbehörde an. EDSA und EDSB ist das Verhältnis von Abs. 1 zu Abs. 4 nicht klar genug. Sie fordern das Streichen des „Unbeschadet des Absatzes 1“ in Art. 31 Abs. 2 und eine klarere Formulierung und eindeutige Bestimmung über die Benennung der zuständigen Behörden, der Datenschutzbehörde, der sektoralen Behörde und der koordinierenden Behörde sowie über die Aufteilung der Zuständigkeiten und den Kooperationsmechanismus.[108] Als koordinierende Behörde wünschen sie sich die Datenschutzbehörden, da diese ein einzigartiges rechtliches und technisches Know-how bei der Überwachung der Datenverarbeitung, der Beratung von digitalen Akteuren und betroffenen Personen sowie bei der Nutzung von Interregulierungsmechanismen verfügen würden, was sie zum Kernstück der digitalen Regulierungslandschaft mache. Zur Gewährleistung der Prävalenz des in Art. 16 AEUV und Art. 8 EuGrCh verankerten Grundsatzes auf den Schutz personenbezogener Daten sollte die Rolle der Datenschutzbehörden in der Governance-Architektur des Vorschlags überwiegen. Die Benennung von Behörden als koordinierende zuständige Behörden, die keine Datenschutzbehörden sind, könnte zu echter Komplexität für digitale Akteure und betroffene Personen führen und die Überwachung der Bestimmungen der DSGVO behindern.[109]

Abs. 5 enthält die Mitteilungspflicht der Behörden und ggf. koordinierenden Behörden und die Angabe, dass die Kommission ein öffentliches Register dieser führt. Abs. 6 enthält eine die indirekte oder direkte Einflussnahme von außen, auch von Weisungen, durch Behörden oder privaten Stellen der Behörden verbietende Vorschrift. Dies wird von EDSA und EDSB begrüßt,

[104] Ebd.
[105] Ebd. S. 28.
[106] Ebd. S. 25.
[107] Ebd. S. 27.
[108] Ebd. S. 25-26.
[109] Ebd. S. 27.

allerdings wünschen diese sich eine ausdrücklich die Unabhängigkeit erwähnende Formulierung.[110]

b) Art. 32 – Recht auf Beschwerde

Art. 32 Abs. 1 erlaubt es natürlichen oder juristischen Personen – unbeschadet eines verwaltungsrechtlichen oder gerichtlichen Rechtsbehelfs – bei der jeweils zuständigen Behörde des gewöhnlichen Aufenthaltsorts, Arbeitsplatzes oder Niederlassung Beschwerde einzulegen. EDSA und EDSB befürchten operative Schwierigkeiten, da unklar ist, wie Beschwerdewillige feststellen, ob personenbezogene Daten betroffen sind und welche Behörde für die Bearbeitung ihrer Beschwerde zuständig ist. Hier sollte ein präziser Mechanismus für die Zusammenarbeit bei der Bearbeitung der Beschwerden und eine klare Anlaufstelle für Beschwerdeführer eingerichtet werden.[111]

Art. 32 Abs. 2 verpflichtet die Behörde den Beschwerdeführer zu unterrichten. Art. 32 Abs. 3 ordnet die Zusammenarbeit bei der Bearbeitung von Lösungen an, insbesondere auch auf elektronischem Wege. Dies soll aber nicht die Zusammenarbeit nach den Kapiteln VI, VII der DSGVO betreffen. Die Absätze 2 und 3 sind nach Ansicht von EDSA und EDSB unzureichend und geben weder Beschwerdeführern noch den Aufsichtsbehörden genügend Informationen. Die koordinierenden Behörden sollten als Anlaufstelle für alle Beschwerden benannt werden und diese weiterleiten. Außerdem sollte ausdrücklich erwähnt werden, dass Kapitel VIII der DSGVO (Rechtsbehelfe, Haftung und Sanktionen) nicht berührt ist. Auch hinsichtlich der federführenden Aufsichtsbehörde bei grenzüberschreitender Verarbeitung nach Art. 56 DSGVO sei unklar, was hier vorgesehen ist. Es fehle ebenfalls an Regelungen hinsichtlich der Untätigkeit zuständiger Behörden nach eingereichten Beschwerden, die die parallele und einheitliche Durchsetzung auch mit der DSGVO gewährleisten könnten.[112]

c) Art. 33 – Sanktionen

Art. 33 Abs. 1 verpflichtet die Mitgliedstaaten zum Erlass von Vorschriften über Sanktionen. Abs. 2 verpflichtet die Mitgliedstaaten der Kommission die Vorschriften und Maßnahmen mitzuteilen und spätere Änderungen unverzüglich zu melden. Abs. 3 legt fest, dass die Aufsichtsbehörden nach Art. 51 DSGVO in ihrem Zuständigkeitsbereich bei Verstößen gegen die Kapitel II, III und V im Einklang mit Art. 83 DSGVO ebenfalls Geldbuße erteilen dürfen. Hierin ist nach EDSA und EDSB keine Harmonisierung der Sanktionen für Verstöße zu sehen. Es sei auch unklar, wie welche Behörde für die Durchsetzung von Art. 5 Abs. 2 zuständig wäre, den Gatekeepern das Auftreten als Dritte zum Datentausch untersagt und welche Sanktionen hierfür berufen wären. Das Zusammenspiel zwischen Data Act und DSGVO hinsichtlich Sanktionen und Durchsetzung müsse klargestellt werden. Ohne harmonisierte Sanktionen und einheitlicher Anwendung dieser bestünde die Gefahr des Forum Shoppings, was dem Ziel, der Fairness bei der Aufteilung des Wertes von Daten zwischen den Akteuren in der Datenwirtschaft zu gewährleisten, zuwiderläuft.[113]

d) Art. 34 – Mustervertragsbedingungen

Die Kommission erstellt nach Art. 34 unverbindliche Mustervertragsbedingungen für den Datenzugang und die Datennutzung. EDSA und EDSB empfehlen der Kommission, dass sie den

[110] Ebd. S. 26.
[111] Ebd.
[112] Ebd.
[113] Ebd. S. 27.

EDSA konsultiert, wenn sie Mustervertragsbedingungen erarbeitet, soweit es sich um personenbezogene Daten handelt.[114]

11. Art. 35 – Sui-Generis-Recht im Rahmen der RL 1996/9/EG (Kapitel X)

Das in Art. 7 der Richtlinie 96/9/EG festgelegte spezifische Schutzrecht für Datenbanken kann die Rechte der Nutzer nach Art. 4 und 5 des Entwurfs nicht einschränken.

12. Art. 36 bis 42 – Schlussbestimmungen (Kapitel XI)

Die Art. 36 und 37 verweisen auf die Verordnung (EU) 2017/2394 (Zusammenarbeit der nationalen Behörden zur Durchsetzung der Verbaucherschutzgesetze) und Richtlinie (EU) 2020/1828 (Verbandsklagenrichtlinie für Verbraucher), bei denen jeweils im Anhang das Data Act eingefügt wird. EDSA und EDSB sehen diese Änderung zusammen mit Erwägungsgrund 82 als Möglichkeit das EU-Kooperationsnetz für den Verbraucherschutz zu nutzen. Allerdings sei es unklar, wie und in welchem Umfang der Verbraucherschutz-Mechanismus mit dem in dem Artikel 32 vorgesehenen Beschwerderecht zusammenwirkt.[115]

13. Kohärenz mit anderen EU-Rechtsakten

Die Verbraucherzentrale Bundesverband e.V. ist erstaunt über „die geringe Verzahnung des Data Act mit dem Data Governance Act. Der DGA etabliert durch eine horizontale Regelung unabhängige Datenvermittlungsdienste und weist ihnen „*eine Schlüsselrolle in der Datenwirtschaft zu. Im DA hingegen werden Datenvermittlungsdienste lediglich als Randnotiz behandelt. Dabei könnten Datenvermittlungsdiensten, [sic!] eine geeignete Lösungsoption sein, um den Wettbewerb, Innovation und die Wahlfreiheit der Nutzer zu stärken, als die im DA vorgeschlagenen Mechanismen, die sich teilweise auch als Überforderung der Verbraucher:innen darstellen könnten*“.[116]

Der EDSA und der EDSB vermissen eine bessere Abstimmung des Data Act Entwurfs mit dem Digital Markets Act (DMA) und dem DGA. Es ist nicht klar, wie die Vorschriften des Data Act mit Blick auf Art. 6 Abs. 1 lit. h und i des DMA zu verstehen sind, die Gatekeeper zur Bereitstellung von Tools verpflichten, die Datenportabilität im Einklang mit den Vorgaben der DSGVO ermöglichen. Der Entwurf sollte deshalb an den finalen Text des DMA angepasst werden, auf den sich die Gesetzgeber bereits geeinigt hatten.[117] Im DGA gibt es Anbieter eines Datenvermittlungsdienstes. Erwägungsgrund 35 greift die Möglichkeit auf, dass ein Dritter im Sinne des Data Act Anbieter eines solchen Dienstes ist, sodann sollen die Schutzvorkehrungen des DGA gelten. Darauf erfolgt aber keine Wiedergabe dieser Problematik im verfügenden Teil des Texts. EDSA und EDSB empfehlen, dass die spezifischen Garantien für betroffene Personen aus der DSGVO hier spezifiziert werden sollten, die für die Weitergabe von Daten von Dateninhabern an Dritte als Vermittler gelten würden. Diese Garantien sollten klarstellend neben die Garantien der DSGVO und der ePrivacy Richtlinie treten unter besonderer Beachtung der Einwilligung des Endnutzers in die Datenverarbeitung durch Dritte.[118]

Zur Kollision mit EU-Recht ab S. 40.

---

[114] Ebd.
[115] Ebd. S. 26-27.
[116] *Verbraucherzentrale Bundesverband e.V.,* Verbraucher:innen beim Data Act im Blick behalten. Stellungnahme des Verbraucherzentrale Bundesverbands zum Vorschlag der Europäischen Kommission für ein Datengesetz (Data Act). Berlin, 13. Mai 2022, S. 6.
[117] *EDSA/ EDSB,* EDPB-EDPS Joint Opinion 2/2022 on the Proposal of the European Parliament and of the Council on harmonized rules on fair access to and use of data (Data Act). Brüssel 04.05.2022, S. 11.
[118] Ebd. S. 11-12.

III. Data Governance Act – Verordnung (EU) 2022/868

Das DGA wurde nach Zustimmung des Rats am 16.05.2022 am 30.05.2022 durch Rat und Parlament beschlossen und tritt am 24.09.2023 in Kraft. Der DGA behandelt im Schwerpunkt die Bereitstellung von Daten der öffentlichen Hand, das Konzept der Datenvermittlungsdienste und den sogenannten Datenaltruismus.[119] Das Data Governance Act bezieht sich im Gegensatz zur Richtlinie (EU) 2019/1024, der OD-PSI, auf Daten, an denen Rechte Dritter bestehen und als solche nicht uneingeschränkt freigegeben werden können. Die OD-PSI-Richtlinie bezieht sich dagegen auf „Open (Government) Data".[120]

In seinem Art. 1 Abs. 3 stellt das Data Governance Act klar, dass Datenschutzbestimmungen der Union gegenüber dem DGA Vorrang genießen und es keine Rechtsgrundlage zur Verarbeitung personenbezogener Daten schafft und auch nicht in den Datenschutzrechtsakten festgelegten Rechte und Pflichten berührt. Die Begriffsbestimmungen des Art. 2 erscheinen kohärent. Die Definition von Daten ist mit der des Data Act identisch. Daneben enthält das DGA aber auch Definitionen zu personenbezogenen Daten, nicht personenbezogenen Daten, der Einwilligung, der Erlaubnis, betroffenen Personen uvm., die regelmäßig Bezug auf die Definitionen der DSGVO nehmen.

Der ursprüngliche Kommissionsvorschlag enthielt keine richtige das Datenschutzrecht bevorzugende Klausel. Hier hieß es nur, dass „*diese Verordnung […] die Verpflichtung der Anbieter von Diensten für die gemeinsame Datennutzung zur Einhaltung der Verordnung (EU) 2016/679 und die Verantwortung der Aufsichtsbehörden, die Einhaltung dieser Verordnung sicherstellen, unberührt lassen. Handelt es sich bei den Anbietern von Diensten für die gemeinsame Datennutzung um für die Verarbeitung Verantwortliche oder Auftragsverarbeiter im Sinne der Verordnung (EU) 2016/679, so sind sie an die Bestimmungen der genannten Verordnung gebunden.*" Diese Klarstellung, die mit seinem S. 2 noch klarer war als die aktuelle Fassung von Art. 1 Abs. 3 des Data Acts, fand sich jedoch in Erwägungsgrund 28 des Kommissionsentwurfs. Die in Kraft getretene Fassung ist zu begrüßen, da sie mit dem angesprochenen Art. 1 Abs. 3 DGA eine Klarstellung zur Anwendbarkeit des Datenschutzrechts besitzt, die die Gefahr des Absinkens des Datenschutzniveaus wesentlich verringert. Hier ist eindeutig dargelegt, dass im Konfliktfall zwischen dem Data Governance Act und den datenschutzrechtlichen Bestimmungen der Union bzw. Umsetzungsgesetze der Mitgliedstaaten letztere stets Vorrang haben. Auch die Problematik der Rechtsgrundlage nach Art. 6 Abs. 1 UAbs. 1 lit. c oder e DSGVO fällt mit Art. 1 Abs. 3 S. 4 DGA weg. Denn das DGA selbst kann mit diesem Satz 4 keine Rechtsgrundlage für die Verarbeitung personenbezogener Daten darstellen.

EDSA und EDSB kritisierten aber auch die Formulierung der Definition des Dateninhabers nach Art. 2 Nr. 5 des Kommissionsentwurfs, wonach dieser „*berechtigt ist, Zugang zu bestimmten, unter ihrer Kontrolle befindlichen*" Daten weiterzugeben. Die DSGVO kenne kein entsprechendes Recht, vielmehr „*bescheinigt die DSGVO jeder natürlichen Person das Recht auf Schutz der sie betreffenden Daten, was sich auf eine umfassende Reihe von Vorschriften für die Verarbeitung personenbezogener Daten bezieht, die für jede Stelle verbindlich sind, die die Daten verarbeitet*".[121] Die Definition des Dateninhabers wurde für die finale Fassung noch geändert. In

---

[119] *Rücker, Daniel/ Hartl, Korbinian,* Der „Data-Governance-Act" – (Über-)Regulierung oder Motor für den europäischen Datenraum? Noerr-Newsroom vom 08.04.2022, https://www.noerr.com/de/newsroom/news/der-data-governance-act, abgerufen am 25.08.2022.

[120] *Falkhofen, Benedikt,* Infrastrukturrecht des digitalen Raums. Data Governance Act, Data Act und Gaia-X. In: EuZW 2021, 787, 789.

[121] *EDSA/ EDSB,* Gemeinsame Stellungnahme 03/2021 des EDSA und des EDSB zum Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über europäische Daten-Governance (Data-Governance-Gesetz). Version 1.1 vom 09.06.2021, S. 11-12.

Art. 2 Nr. 8 wird klar bestimmt, dass der Dateninhaber nicht Betroffener im Sinne der DSGVO sein kann, aber nach geltendem Unionsrecht oder nationalem Recht berechtigt ist, Zugang zu gewähren. Damit scheint zumindest eine Rechtsgrundlage nach der DSGVO nötig zu sein, um die Rolle eines Dateninhabers inne haben zu dürfen. Ob diese Vorgabe aber etwas an dem faktischen Problem und dem Bewusstsein von Dateninhabern etwas ändert bleibt offen. Schließlich kann ein Nutzungsvertrag nach Ansicht vieler auch eine Rechtsgrundlage zur Verarbeitung personenbezogener Daten bieten, auch wenn Vertreter des Kopplungsverbots das anders sehen (S. 14f). Dass die Kommission bzw. der europäische Gesetzgeber die Daten Personen zuordnen wollen lässt sich auch dem Entwurf des Data Acts entnehmen. Zum Nachteil für den Datenschutz scheint es aber nicht um die betroffenen Individuen, sondern um die datenerhebenden Unternehmen und öffentlichen Stellen zu gehen.

EDSA und EDSB befürchteten in Art. 11 Nr. 2 des Kommissionsvorschlags, dass eine Rechtsgrundlage für die Verarbeitung von Metadaten zur eigenen Entwicklung eingeführt würde. Dies ist deshalb problematisch, da es sich dabei um personenbezogene Daten handeln kann.[122] Im finalen Gesetz findet sich die Norm in Art. 12 lit. c. Die Definition von Metadaten, die sich zuvor in Art. 2 Nr. 4 fand, wurde hier aufgenommen. Es heißt zwar weiterhin, dass die Daten „*nur für die Entwicklung dieses Datenvermittlungsdienstes verwendet*“ werden. In der Fassung von Art. 11 Nr. 2 hieß es aber noch „*dürfen nur für die Entwicklung dieses Dienstes verwendet werden*“. Das Streichen des Wortes dürfen müsste eine mögliche Qualität als Rechtsgrundlage ausgeräumt haben.

Auch wenn datenschutzrechtliche Regelungen in der finalen Fassung des Data Governance Act stets vorgehen, bleibt die Problematik, dass anonymisierte und damit nicht-personenbezogene Daten aufgrund der Kombination einer Vielzahl von nicht-personenbezogenen Daten miteinander und der sich entwickelnden „Big Data“-Mustererkennung schnell wieder eine Identifizierung ermöglichen könnten. Trotzdem wurden diese Daten zunächst geteilt. Sollten die anonymisierten Daten später wieder einen Personenbezug erlauben ist äußerst fraglich, wie überprüft werden könnte, inwieweit Verantwortliche sich an geltendes Datenschutzrecht halten.[123] Hier schmerzt die Nichtbenennung der Datenschutzbehörden als zuständige Stellen beim Data Act besonders. Diese wären als einheitlicher Ansprechpartner deutlich schneller involviert und könnten derartige Re-Identifizierungen erkennen.

Ungehört blieb die Kritik von EDSA und EDSB hinsichtlich der zuständigen Stellen, die die öffentlichen Stellen unterstützen und für die Datenvermittlungsdienste und die Registrierung von datenaltruistischen Organisationen zuständig sind. Deren Aufgaben beträfen voraussichtlich auch die Verarbeitung personenbezogener Daten. Die Benennung von zuständigen Stellen bzw. Behörden, die keine Datenschutzbehörden sind, könnte für Betroffene als auch digitale Akteure sehr verwirrend sein und die kohärente Überwachung und Anwendung der Bestimmungen der DSGVO beeinträchtigen.[124] Die in Kraft tretende Fassung enthält in seinen Regelungen zu den zuständigen Stellen in den Art. 7, 26-28 keine Verweise auf die Datenschutzbehörden. Die Verpflichtung zur Abstimmung mit den Datenschutzbehörden in Art. 13 Abs. 3 DGA ist für die kohärente Umsetzung des Datenschutzes unzureichend. Erwägungsgrund 4 sagt an seinem Ende: „*Es sollte möglich sein, Datenschutzbehörden als gemäß dieser Verordnung zuständige Behörden zu betrachten. Wenn andere Behörden als zuständige Behörden gemäß dieser Verordnung handeln, sollten sie dabei die Aufsichtsbefugnisse und –zuständigkeiten der Datenschutzbehörden gemäß der Verordnung (EU) 2016/679 davon unberührt bleiben.*“ Dieser Erwägungsgrund ist mehr als nur unzureichend. Denn mit Blick auf Art. 1 Abs. 3 DGA ist völlig

[122] Ebd. S. 14-15.
[123] Ebd. S. 18.
[124] Ebd. S. 20.

unzweifelhaft, dass eine Datenschutzbehörde nach der DSGVO auch über personenbezogene Daten Aufsicht hat, die im Rahmen des DGA von einer öffentlichen Stelle zur Weiterverwendung zur Verfügung gestellt werden. Warum das DGA aber nicht explizit zur kohärenten Anwendung des Datenschutzrechts diese als mögliche „koordinierende Stelle“ oder einfach als die zu benennende zuständige Stelle deklariert ist nicht nachvollziehbar. Auch fehlen Lösungen für den Konfliktfall. Die Datenschutzbehörde eines Landes kann schlecht der zuständigen Stelle oder einer öffentlichen Stelle ein Bußgeld erteilen. Denn Deutschland hat mit § 43 Abs. 3 BDSG explizit die Öffnungsklausel des Art. 83 Abs. 7 DSGVO nicht angewandt. Allein öffentlich-rechtliche Unternehmen, die im Wettbewerb stehen, bleiben der Gefahr eines Bußgeldes ausgesetzt.[125] Auch Österreich und Kroatien haben dies ausgeschlossen, während Polen die Höhe der Geldbußen auf 23.000 € beschränkt hat.[126] Dies soll zwar aufgrund der Rechtstreue öffentlicher Stellen und der Möglichkeit der verwaltungsgerichtlichen Klärung kein Problem darstellen, es verringert jedoch die Einwirkungsmöglichkeiten der Datenschutzbehörden. In der Stellungnahme zum Kommissionsentwurf schrieben EDSA und EDSB bereits: „*Sollten darüber hinaus spezielle Stellen benannt werden, die öffentliche Stellen und Weiterverwender von Daten unterstützen sollen und mit der Gewährung des Zugangs für die Weiterverwendung von Daten, einschließlich personenbezogener Daten, betraut werden, können diese Stellen nicht als „zuständig“ bezeichnet werden, da sie nicht als Aufsichtsbehörde fungieren würden, die die Bestimmungen über die Verarbeitung personenbezogener Daten zu überwachen und durchzusetzen vermag. Um die Rechtssicherheit und die einheitliche Anwendung des EU- Besitzstands im Bereich des Schutzes personenbezogener Daten zu gewährleisten, müssen die Tätigkeiten und Pflichten dieser benannten Stellen auch der unmittelbaren Zuständigkeit und Aufsicht der Datenschutzbehörden unterliegen, wenn personenbezogene Daten betroffen sind.*“[127]

IV. Free Flow of Data Act – VO(EU) 2018/1807

Das Free Flow of Data Act soll sicherstellen, dass elektronische Daten, die keine personenbezogenen Daten sind, in der gesamten EU frei verarbeitet werden können. Damit sollten Lokalisierungsauflagen der EU-Mitgliedstaaten abgebaut werden. Die neun Artikel umfassende Verordnung sieht eine reine Anwendung hinsichtlich nicht-personenbezogener Daten vor. Art. 2 Abs. 2 sagt deutlich: „*Bei einem Datensatz, der aus personenbezogenen und nicht-personenbezogenen Daten besteht, gilt diese Verordnung für die nicht-personenbezogenen Daten des Datensatzes. Sind personenbezogene und nicht-personenbezogene Daten in einem Datensatz untrennbar miteinander verbunden, berührt diese Verordnung nicht die Anwendung der Verordnung (EU) 2016/679.*“ In Erwägungsgrund 9 werden auch technische Entwicklungen im Hinblick auf anonymisierte Daten berücksichtigt: „*Ist es durch technologische Neuentwicklungen möglich, anonymisierten Daten wieder in personenbezogene Daten umzuwandeln, müssen diese Daten als personenbezogene Daten behandelt werden, und die Verordnung (EU) 2016/679 muss entsprechend gelten.*“

V. Open Data und Public Sector Information Directive – RL(EU) 2019/1024

Diese Richtlinie, die OD-PSI, möchte den gesetzlichen Rahmen für die Weiterverwendung von öffentlichen Informationen wie geografische Informationen, Grundbuchinformationen, statistischer oder juristischer Informationen im Besitz der öffentlichen Stellen oder der öffentlichen Unternehmen und von öffentlich finanzierten Forschungsdaten festlegen.

---

[125] *Frenzel,* Paal/Pauly DSGVO. BDSG § 43 Rn. 3f.
[126] *Holländer,* BeckOK Datenschutzrecht. DS-GVO Art. 83 Rn. 81.1.
[127] *EDSA/ EDSB,* Gemeinsame Stellungnahme 03/2021 des EDSA und des EDSB zum Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über europäische Daten-Governance (Data-Governance-Gesetz). Version 1.1 vom 09.06.2021, S. 32, 45.

Praktisch ergibt sich damit die Pflicht für Öffentliche Stellen Anträge zur Weiterverwendung von Dokumenten ggf. mit elektronischen Mitteln zu verarbeiten, in angemessen Zeit verfügbar zu machen, Vorkehrungen zu treffen, um die Online-Suche nach Dokumenten in ihrem Besitz zu erleichtern und über die in der Richtlinie genannten Rechte informieren und Hilfe bereitstellen.

Die Wechselwirkungen der OD-PSI mit der DSGVO sind nicht klar. Denn sie hat nicht konkret personenbezogene oder nicht-personenbezogene Daten zum Gegenstand. Art. 1 Abs. 4 erweckt den Eindruck, dass diese Richtlinie der DSGVO vorgeht: „*Diese Richtlinie gilt unbeschadet des Unionsrechts und des nationalen Rechts über den Schutz personenbezogener Daten, insbesondere der Verordnung (EU) 2016/679 und der Richtlinie 2002/58/EG sowie dem entsprechenden nationalen Recht.*“ Erwägungsgrund 52 nimmt dem den Wind aus den Segeln, indem er darstellt, dass sich die Richtlinie „*nicht auf den Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten gemäß dem Unionsrecht und dem nationalen Recht*“ auswirkt. Eine Weiterverwendung personenbezogener Daten seien nur unter Einhaltung des Grundsatzes der Zweckbindung nach Art. 5 Abs. 1 lit. b und Art. 6 DSGVO zulässig. Art. 4 Abs. 4 bietet die Möglichkeit auch die Entscheidung zur Weiterverwendung von Daten durch eine unabhängige Überprüfungsinstanz überprüfen zu lassen. Dazu soll auch eine nach der DSGVO errichtete Aufsichtsbehörde oder ein nationales Gericht zählen.

VI. ePrivacy-Richtlinie und ePrivacy-Verordnung

Die ePrivacy-Richtlinie legt spezifische Standards „*für alle Akteure fest, die auf einem Endgerät eines Teilnehmers oder eines Nutzers im Europäischen Wirtschaftsraum (EWR) gespeicherte Informationen speichern oder darauf zugreifen möchten.*“[128] Innerhalb der ePrivacy-Richtlinie gilt Art. 5 Abs. 3 für alle privaten oder öffentlichen Einrichtungen, die Informationen auf einem Endgerät ablegen oder lesen, unabhängig von der Art der gespeicherten oder abgerufenen Daten. Endeinrichtungen sind nach Art. 1 Nr. 1a der Richtlinie 2008/63/EG „*direkt oder indirekt an die Schnittstelle eines öffentlichen Telekommunikationsnetzes angeschlossene Einrichtungen zum Aussenden, Verarbeiten oder Empfangen von Nachrichten; sowohl bei direkten als auch bei indirekten Anschlüssen kann die Verbindung über Draht, optische Faser oder elektromagnetisch hergestellt werden; bei einem indirekten Anschluss ist zwischen der Endeinrichtung und der Schnittstelle des öffentlichen Netzes ein Gerät geschaltet; b) Satellitenfunkanlagen mit ihren Einrichtungen*“.[129] Bei klassischen IoT-Geräten und vernetzten Fahrzeugen handelt es sich dabei dann wohl um Endeinrichtungen, die den Zugriff auf Informationen gestatten und damit eine Einwilligung erfordern. § 25 TTDSG ist die deutsche Umsetzungsnorm, die eine Einwilligung bei Speicherung von Informationen auf den Endeinrichtungen erfordert, die gemäß der DSGVO, also unter Beachtung von Art. 7f, zu erfolgen hat.

Die ePrivacy-Verordnung sollte als ursprünglich zeitgleich mit der DSGVO in Kraft tretende Verordnung speziell die elektronische Kommunikation als lex specialis zur DSGVO regeln und dabei die ePrivacy-Richtlinie ersetzen. Abzuwarten ist, ob die ePrivacy-Verordnung den Datenschutz durch sektorspezifische Regelungen stärken oder schwächen wird. Letzteres könnte im Interesse der Kommission sein, mit der Datenstrategie mehr und mehr Daten der Nutzung zu öffnen.

Schon im Februar 2021 hat der Rat einen gemeinsamen Standpunkt entwickelt. Diesen hat u.a. der BfDI kritisiert. Kritisch betrachtet er die Wiedereinführung der Vorratsdatenspeicherung, die Zulässigkeit von „Cookie Walls“, Ausbleibende Garantien für Nutzer (Widerspruchsrecht und Datenschutz-Folgenabschätzung gestrichen, Rückgriff auf Garantien der DSGVO

[128] *EDSA*, Leitlinien 01/2020 zur Verarbeitung personenbezogener Daten im Zusammenhang mit vernetzten Fahrzeugen und mobilitätsbezogenen Anwendungen. Version 2.0, 09.03.2021, S. 7.
[129] Ebd.

ausgeschlossen) und die Weiterverarbeitung personenbezogener Daten ohne Einwilligung zu anderen Zwecken.[130] Die kritisierte Vorratsdatenspeicherung findet sich in Art. 7 Abs. 4 des aktuellen Entwurfs. Die Verordnung macht die Speicherung allein von der Erforderlichkeit für die Strafverfolgung und die Öffentliche Sicherheit abhängig unter Berücksichtigung der Grundrechte und Grundfreiheiten, die für eine demokratische Gesellschaft erforderlich und angemessen sind. Die Länge der Speicherung soll zwar begrenzt sein, kann aber verlängert werden. Der Text macht keine Vorschläge für eine solche Speicherfrist. Allerdings verweist Erwägungsgrund 26 auf die Interpretation des EuGH und des EGMR. Die Kritik des BfDI hinsichtlich der Cookie-Wall begründet sich in „Erwägungsgrund 20aaaa", während Erwägungsgrund 20a Endnutzern die Möglichkeit eröffnet ihre Einwilligung im Vorfeld durch eine Software generalisierend abzugeben. Hinsichtlich der Abschaffung von Datenschutz-Folgeabschätzungen muss allerdings auf Erwägungsgrund 17 verwiesen werden, der dessen Möglichkeit ausdrücklich vorsieht, sollte es bei der Verarbeitung von Kommunikations-Metadaten zu einem hohen Risiko für die Rechte und Freiheiten natürlicher Personen kommen können. Auch in Art. 6a Abs. 2 ist ein solches vorgesehen. Ein Widerspruchsrecht ist zumindest in Art. 15 Abs. 4a und Art. 16 Abs. 4 zu finden. Die Verarbeitung zu anderen Zwecken findet sich ausschließlich in Erwägungsgrund 17aa und Art. 8 Abs. 1 lit. g. Hierbei sieht der Entwurf die Prüfung durch die Person, die Daten erhebt oder Speichermöglichkeiten auf Endgeräten nutzt vor, ob die geplante Verarbeitung mit dem ursprünglich erhobenen Zweck vereinbar ist. Dabei handelt es sich bei Art. 8 Abs. 1 lit. g des Entwurfs um eine identische Vorschrift zu Art. 6 Abs. 4 DSGVO. Die Unterabsätze (i) bis (v) des Art. 8 Abs. 1 lit. g des Entwurfs entsprechen den Buchstaben a bis e des Art. 6 Abs. 4 DSGVO. Hinsichtlich der Rechtsgrundlage zur Verarbeitung von bereits erhobenen Daten zu anderen Zwecken ändert sich damit nichts zur DSGVO. Problematischer ist, dass Art. 8 Abs. 1 lit. d eine neue Rechtsgrundlage schafft die Daten des Endnutzers zum Zwecke der „audience measuring", also zur Publikumsmessung, zu verarbeiten. In die gleiche Kerbe schlägt Art. 8 Abs. 2 lit. c, der die Verarbeitung von Daten, die Endgeräte aussenden, zu statistischen Zwecken erlaubt, solange diese anonymisiert oder so früh wie möglich gelöscht werden. Daneben folgen in Absatz 1 Tatbestände zur Sicherheit, u.a. zur Betrugsverhinderung, Software-Updates oder dem Lokalisieren eines Endnutzers beim Absetzen eines Notrufs.[131]

Trotzdem sollen mit dem aktuellen Stand des Textes eine Vielzahl an neuen datenschützenden Regelungen kommen. Datenschutz.org zählt hierbei auf, dass Anbieter verpflichtet werden Daten nach dem Stand der Technik zu sichern, wozu auch Verschlüsselung sowie das Verbot des Backdoor-Handels zählt. Das räumliche Tracking durch Programme soll illegal werden, auch soll der Schutz vor Tracking im Rahmen der elektronischen Kommunikation effektiviert werden. Auch soll es keine Verarbeitung mehr ohne Einwilligung des Nutzers mehr geben, was bereits für Telefonanbieter gelte, soll jetzt auch für WhatsApp und andere Messenger gelten. Neben verpflichtenden datenschutzfreundlichen Voreinstellungen – privacy by default, was bereits in der DSGVO klar normiert war – sollen Strafverfolger neuen Transparenz- und Dokumentationspflichten unterliegen, sodass staatliche Anfragen durch Anbieter offengelegt werden müssen.[132]

---

[130] *BfDI,* E-Privacy-Verordnung. Übersichtsseite Fachthemen. https://www.bfdi.bund.de/DE/Fachthemen/Inhalte/Telemedien/ePrivacy_Verordnung.html, zuletzt abgerufen am 31.08.2023.

[131] Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) - Mandate for negotiations with EP (6087/21, 10.02.2021), abrufbar auf Eur-Lex.

[132] *Datenschutz.org,* ePrivacy-Verordnung: Die Ergänzung zur EU-Datenschutzverordnung. Datenschutz.org vom 21.12.2017, zuletzt aktualisiert am 22.08.2022, https://www.datenschutz.org/eprivacy-verordnung/, zuletzt abgerufen am 31.08.2023.

Den Standpunkt, den der LIBE-Ausschuss und das Parlament bereits Ende 2017 entwickeltet hatten, fand bei Medienverbänden keine Gegenliebe. Im Gegenteil sprachen einige von einer Gefahr für die Finanzierung der Freien Presse. Dies stand im eklatanten Widerspruch zu den Äußerungen von Bürgerrechtlern, die sich über mehr Datenschutz für EU-Bürger freuten.[133] Im Jahr 2021 konnte der Rat schließlich eine gemeinsame Position finden. Seitdem steht das Trilog-Verfahren aufgrund der fehlenden Transparenz in der Kritik.[134]

VII. Strafverfolgungsrechtsakte

1. Verwendung von Fluggastdatensätzen zur Strafverfolgung – RL(EU) 2016/681

Die Richtlinie (EU) 2016/681 verpflichtet die Mitgliedstaaten Daten aus den Buchungs- und Abfertigungssystemen der Fluggesellschaften für die Dauer von fünf Jahren in einer Zentralstelle eines Mitgliedstaats vorzuhalten. Dabei müssen in der EU ankommende als auch aus der EU ausgehende Flüge berücksichtigt werden. Verarbeitungszwecke sind die Verhütung, Aufdeckung, Ermittlung und Verfolgung von terroristischen Straftaten und schwerer Kriminalität. Dabei können Fluggäste vor ihrer Ankunft anhand im Voraus festgelegter Kriterien und anhand der Datenbanken der Strafverfolgungsbehörden, die Daten für konkrete Ermittlungs- bzw. Strafverfolgungszwecke und als Beitrag bei der Entwicklung von Kriterien zur Risikobewertung verwendet werden. Die Daten müssen in der Zentralstelle eines Mitgliedstaats zwar für fünf Jahre vorgehalten werden. Sechs Monate nach der Übermittlung durch die Fluggesellschaft müssen sie aber entpersonalisiert werden. Danach ist ein Offenlegen der vollständigen Daten nur mit einem Gerichtsbeschluss oder einer „hinreichenden Grundlage gebührend begründeten Anfrage zuständiger Behörden“ bei terroristischen Straftaten oder schwerer Kriminalität möglich, Art. 12 Abs. 3, 6 Abs. 2 lit. b der Richtlinie. Art. 13 enthält spezielle Datenschutzvorschriften, die sich insbesondere auf die Datenschutzrichtlinie und den Rahmenbeschluss des Rates 2008/977/JI zur polizeilichen und justiziellen Zusammenarbeit in Strafsachen stützen.[135] An deren Stelle traten die DSGVO und die Richtlinie (EU) 2016/680.

Von der Fluggastdatenstrafverfolgungsrichtlinie ist damit keine Absenkung des bestehenden Datenschutzniveaus in der EU zu erwarten. Allerdings ist sie als Hintergrund für bereits bestehende staatliche Datennutzungsrechte hilfreich.

2. Agentur zur Zusammenarbeit auf dem Gebiet der Strafverfolgung – VO(EU) 2016/794

Die am 11. Mai 2016 beschlossene Verordnung über die Agentur der Europäischen Union für die Zusammenarbeit auf dem Gebiet der Strafverfolgung (Europol) und zur Ersetzung und Aufhebung der Beschlüsse 2009/371/JI, 2009/934/JI, 2009/935/JI, 2009/936/JI und 2009/968/JI des Rates wurde mit der Verordnung (EU) 2022/991 am 08.06.2022 geändert.

Die Verordnung legt Bestimmungen für Europol und auch Kontrollmöglichkeiten durch das Europäische Parlament und den nationalen Parlamenten fest. Die Befugnisse von Europol gehen mit Datenschutzgarantien und parlamentarischer Kontrolle einher. Europol kann insbesondere Daten an Unionseinrichtungen (Art. 24) und Drittstaaten und internationale Organisationen (Art.

---

[133] *Sonneborn, Martin,* Herr Sonneborn geht nach Brüssel. Abenteuer im Europaparlament. 11. Auflage 2019. S. 321-331.

[134] *Dachwitz, Ingo,* NGOs fordern mehr Transparenz über Geheimverhandlungen. Netzpolitik.org vom 07.02.2023, https://netzpolitik.org/2023/eu-trilog-ngos-fordern-mehr-transparenz-ueber-geheimverhandlungen/, zuletzt abgerufen am 30.08.2023.

[135] Vgl. Zusammenfassung der Richtlinie (EU) 2016/681 auf Eur-Lex, https://eur-lex.europa.eu/legal-content/DE/LSU/?uri=CELEX:32016L0681, zuletzt abgerufen am 31.08.2022.

25) übermitteln sowie mit privaten Parteien (Art. 26f) austauschen. Hierzu sind Abkommen und Kommissionsbeschlüsse und gegenüber Unionseinrichtungen nur verhältnismäßige und erforderliche Wahrnehmung von Aufgaben erforderlich. Art. 27a ordnet die Anwendbarkeit der Verordnung (EU) 2018/1725 an, der „DSGVO für EU-Organe". Darüber hinaus finden sich in Kapitel VI weitergehende Datenschutzbestimmungen. Neben der Bewertung der Zuverlässigkeit der Quellen und der Richtigkeit von Informationen müssen besondere Kategorien personenbezogener Daten und verschiedene Kategorien von Betroffenen sowie Speicher- und Löschfristen beachtet werden. In Art. 33a ist sogar die Verarbeitung zum Zwecke der Forschungs- und Innovationsprojekte vorgesehen. Dabei soll es sich aber um interne Projekte handeln, die vom Exekutivdirektor, dem EDSB und vom Verwaltungsrat abgesegnet werden müssen. In Art. 34 und 35 ist die Meldung von Verletzungen an die Behörden und die Benachrichtigung der Betroffenen vorgesehen. Im Anschluss folgen weitere Betroffenenrechte entsprechend der genannten Datenschutzverordnung für Organe der EU.

3. Verstärkte Zusammenarbeit zur Errichtung der Europäischen Staatsanwaltschaft – VO(EU) 2017/1939

Die Verordnung (EU) 2017/1939 wurde mit delegierter Verordnung (EU) 2020/2153 der Kommission vom 14.10.2020 mit Wirkung vom 10.01.2021 geändert. Ziel ist es eine Europäische Staatsanwaltschaft zu errichten, die Straftaten gegen die finanziellen Interessen der EU verfolgt und gliedert die Zuständigkeit zwischen den nationalen Behörden, der zentralen Stelle in Luxemburg und den Delegierten Europäischen Staatsanwälten.

Die genannte delegierte Verordnung nennt die Kategorien operativer personenbezogener Daten und die Kategorien betroffener Personen, deren operative personenbezogene Daten von der EUStA im Register der Verfahrensakten verarbeitet werden dürfen. In Kapitel VIII enthält die Verordnung spezifische Datenschutzbestimmungen, beginnend mit den aus Art. 5 DSGVO bekannten Datenschutzgrundsätzen in Art. 47 und der Verpflichtung der EUStA zur Einhaltung dieser.

VIII. Rechtsakte im Wettbewerbs-, Urheber- und digitalen Vertragsrecht

1. Digital Markets Act – COM(2020) 842 final

Das Digital Markets Act pocht bei der Verwendung von personenbezogenen Daten auf die Einhaltung der datenschutzrechtlichen Bestimmungen. Ausführungen dazu erfolgen in Erwägungsgrund 11, 40, 45, 55 und 58. Auch im Normtext wird dies deutlich. Die Definitionen (nicht-)personenbezogener Daten knüpft an der DSGVO an, Art. 2 Nr. 20-21. Gatekeeper dürfen nach Art. 5 nur nach freier und mit Alternative versehener Einwilligung des Betroffenen Daten ihrer Dienste zusammenführen, Art. 5 lit. a. Neben Pflichten hinsichtlich Endnutzern in Art. 6 Abs. 1 lit. h-i muss nach Art. 7 Abs. 1 sichergestellt werden, dass alle Maßnahmen u.a. im Einklang mit der DSGVO und der ePrivacy-Richtlinie stehen. Art. 11 Abs. 2 normiert ein Umgehungsverbot und trifft Maßnahmen, damit gewerbliche Nutzer die Einwilligung nach DSGVO und ePrivacy-VO erhalten können.

2. Richtlinie Urheberrecht und verwandten Schutzrechten im digitalen Binnenmarkt – RL(EU) 2019/790

Die umstrittene sogenannte Urheberrechterichtlinie oder auch DSM-Richtlinie wurde am 17.04.2019 beschlossen. Der BfDI, Ulrich Kelber, warnte im Februar 2019 davor, dass trotz Nichtvorkommens von Uploadfiltern im Wortlaut des Gesetzesentwurfs es in der praktischen Anwendung auf sie hinauslaufen würde. Kleinere Plattform- und Diensteanbieter würden gar nicht die Möglichkeit haben, mit allen erdenklichen Rechteinhabern Lizenzverträge abzuschließen oder

eigene Uploadfilter zu erstellen, sodass diese auf Angebote großer IT-Unternehmen zurückgreifen müssten. Dies könnten wie bei Analysetools Meta, Amazon oder Google sein. Kelber forderte konkrete Schritte, um das skizzierte Szenario der Konzentration von Daten bei einem Oligopol von Anbietern abzuwenden. Ein modernes Leistungsschutzrecht sei zwar sicher notwendig, dies dürfe aber nicht auf dem Rücken und zu Lasten des Datenschutzes der Internetnutzerinnen und -nutzer erfolgen.[136] Die Richtlinie gibt in Erwägungsgrund 85 explizit die Vereinbarkeit der Verarbeitung nach dieser Richtlinie mit der DSGVO und der ePrivacy-Richtlinie vor. Auch in Art. 17 Abs. 3 UAbs. 3 stellt sie klar, dass sie keine Rechtsgrundlage für die Verarbeitung personenbezogener Daten sein kann, außer dies erfolge im Einklang mit DSGVO und ePrivacy-RL. Dies greift Art. 28 nochmals auf, der vorschreibt, dass die Verarbeitung personenbezogener Daten nach den beiden genannten Rechtsakten zu erfolgen hat.

Die Befürchtungen des BfDI konnte die finale Fassung der Richtlinie nicht ausräumen. Aus Art. 17 Abs. 4 lit. b lässt sich schließen, dass Diensteanbieter Uploadfilter einsetzen müssen. Denn die Vorschrift verpflichtet „*nach Maßgabe hoher branchenüblicher Standards für die berufliche Sorgfalt alle Anstrengungen [zu unternehmen] […], dass bestimmte Werke und sonstige Schutzgegenstände […] nicht verfügbar sind.*“ Allerdings wird die Problematik für kleinere Unternehmen mit Art. 17 Abs. 6 abgedämpft. Dieser besagt, dass Diensteanbieter, die erst seit drei Jahren ihre Dienste in der Union anbieten und deren Jahresumsatz 10 Mio. Euro nicht übersteigt, nur die Pflicht nach Art. 17 Abs. 4 lit. a, alle Anstrengungen zu unternehmen, um eine Erlaubnis einzuholen, umfasst. Die dreijährige Lebensdauer eines Dienstes kann jedoch kleine Anbieter nicht wirksam schützen. Wichtiger ist vielmehr der Jahresumsatz von 10 Mio. Euro, der eigentlich eine kumulative Voraussetzung sein müsste. Relevanter ist Art. 17 Abs. 7, der die Gefahr des Overblockings abfedern möchte. Nutzer sollen sich nach Art. 17 Abs. 7 UAbs. 2 auf die Ausnahmen des Zitats, der Kritik, der Rezension sowie Karikaturen, Parodien oder Pastiches berufen können. Art. 17 Abs. 8 UAbs. 1 sieht außerdem vor, dass hieraus keine allgemeine Überwachung resultiert.

Am 20.05.2021 verabschiedete der Bundestag das Umsetzungsgesetz, Gesetz zur Anpassung des Urheberrechts an die Erfordernisse des digitalen Binnenmarkts. Wesentliche Inhalte der Richtlinie finden sich im Urheberrechts-Diensteanbieter-Gesetz (UrhDaG).

Prof. Dr. Ansgar Ohly von der LMU hält das UrhDaG nicht wie Prof. Dr. Louisa Specht-Riemenschneider (Bonn) für „*das Beste, was dem Urheberrecht passieren konnte*“[137], sondern für „*eine faire Abwägung von Urheberrechtsschutz und Kommunikationsfreiheiten […] und einen praktikablen Rahmen für ein weitgehend automatisiertes Umfeld*“.[138] Specht-Riemenschneider ist deshalb der Auffassung, da der Unterschutz der Urheber „*durch eine stetige Stärkung seiner Rechtsdurchsetzungsbefugnisse entgegengewirkt wurde […]. Damit der Unterschutz aber nun nicht auf der Seite der Nutzer aufklafft, waren die Schrankenbestimmungen zu stärken.*“[139]

Ein gutes Jahr nach Inkrafttreten scheint ein positives Fazit möglich. Prof. Dr. Christian-Henner Hentsch von der TH Köln hat keinen Fall von Oberblocking in der Presse mitbekommen und stellt fest, dass auch das Angebot bei den Diensteanbietern nicht abgenommen hat. „*Damit scheint*

---

[136] *BfDI:* Reform des Urheberrechts birgt auch datenschutzrechtliche Risiken. Pressemitteilung 10/2019 des BfDI vom 26.02.2019, https://www.bfdi.bund.de/SharedDocs/Pressemitteilungen/DE/2019/10_Uploadfilter.html, abgerufen am 31.08.2022.

[137] *Specht-Riemenschneider, Louisa:* Das Beste, was dem Urheberrecht passieren konnte. In: WRP 2021, Heft 8, Editorial.

[138] *Ohly, Ansgar:* Urheberrecht im digitalen Binnenmarkt – Die Urheberrechtsnovelle 2021 im Überblick. In: ZUM 2021, 745 (755).

[139] *Specht-Riemenschneider, Louisa:* Das Beste, was dem Urheberrecht passieren konnte. In: WRP 2021, Heft 8, Editorial.

das oberste Ziel des deutschen Gesetzgebers, Rechtsfrieden zu schaffen und die Richtlinie mit möglichst wenig Kollateralschäden durch Uploadfilter umzusetzen, erreicht worden."[140] Positiv zu bewerten sei daneben auch, dass private Nutzer nicht nach dem UrhDaG haften. Allein kommerzielle Influencer oder Let's Player würden nicht vom UrhDaG enthaftet. Problematisch erscheine die sehr unterschiedliche Umsetzung in den EU-Mitgliedstaaten, die eine Herausforderung für die einheitliche Auslegung des Art. 17 darstellt.[141]

3. Digitale Inhalte Richtlinie – RL(EU) 2019/770

Die Digitale Inhalte Richtlinie regelt bestimmte vertragsrechtliche Aspekte der Bereitstellung digitaler Inhalte und digitaler Dienstleistungen. Die Vorgaben der Richtlinie waren bis 01.07.2021 umzusetzen. Im Deutschen Recht wurden hierzu ein neuer § 312 Abs. 1 und Abs. 1a und neue §§ 327 ff. in das BGB eingefügt. Die Richtlinie äußert sich hinsichtlich der Anwendung der datenschutzrechtlichen Bestimmungen eindeutig in den Erwägungsgründen 37 bis 39, 48 und 69. Erwägungsgrund 37 stellt klar, dass im Zweifel der Schutz personenbezogener Daten Vorzug gegenüber der Richtlinie genießt. Dies wird durch Art. 3 Abs. 8 im verfügenden Text wiederholt. Erwägungsgrund 38 stellt klar, dass die Richtlinie keine Rechtsgrundlage zur Verarbeitung personenbezogener Daten begründet, sondern dies von der DSGVO abhängig ist und stellt ab S. 5 zusammen mit Erwägungsgrund 39 dar, dass auch die Betroffenenrechte der DSGVO unbeschränkt anwendbar sind. Erwägungsgrund 48 stellt ausführlich dar, dass das Nichteinhalten von Pflichten aus der DSGVO auch einen Mangel begründen kann. Erwägungsgrund 69 verpflichtet Unternehmen bei Bereitstellung von personenbezogenen Daten durch den Verbraucher die Pflichten der DSGVO einzuhalten, unabhängig davon, ob der Verbraucher eine Geldzahlung leistet. Nach dem Ende des Vertrages solle er die Daten nicht nutzen dürfen, es sei denn sie hätten außerhalb des Kontexts keinen Nutzen. Art. 16 Abs. 2 enthält diese Verpflichtung sich im Fall der Beendigung des Vertrages die Pflichten aus der DSGVO einzuhalten. Außerdem besitzen nach Art. 21 Abs. 2 lit. d Einrichtungen, Organisationen oder Vereinigungen ohne Gewinnerzielungsabsicht, die im Bereich des Datenschutzes wie in Art. 80 DSGVO tätig sind, das Recht auf Beschwerde zu Gerichten und Verwaltungsbehörden. Werden die vielen Ausführungen der Richtlinie zur Anwendung der DSGVO berücksichtigt kann nicht davon ausgegangen werden, dass personenbezogene Daten so einfach eine Gegenleistung in einem Vertrag sein können. Denn hierzu müsste stets eine Rechtsgrundlage vorliegen. Dabei kann es sich damit also nicht um Art. 6 Abs. 1 UAbs. 1 lit. b DSGVO – die Verarbeitung aufgrund Vertrags – handeln, denn der Vertrag kann nicht die Rechtsgrundlage für die eigenen Vertragsinhalte sein. Rein aus Sicht der DSGVO bleibt es damit im Regelfall bei der Einwilligung, die das Problem des Kopplungsverbots mit sich bringt (s. S. 14f). Trotzdem möchte die Richtlinie die Verbraucher nicht schutzlos stellen und trifft deshalb Regelungen zum Gewährleistungsrecht in einem solchen Fall.

IX. Kollision von EU-Rechtsakten

Niederrangiges EU-Recht darf nicht gegen höherrangiges EU-Recht verstoßen. Dies kann jeder Einzelne nach Ansicht des EuGH auch vor diesem oder jedem mitgliedstaatlichen Gericht nach Art. 47 EuGrCh i.V.m. Art. 277 AEUV überprüfen lassen (, wobei die Verwerfungskompetenz beim EuGH liegt). In Betracht kommt für ein nationales Gericht die Vorlage nach Art. 267 AEUV zur Vorabentscheidung. Die Vereinbarkeit des Sekundär- mit dem Primärrecht ist stets vorrangig

[140] *Hentsch, Christian-Henner:* Erstes Jubiläum des UrhDaG. Die Gewinner und Verlierer der Urheberrechtsreform. Legal Tribune Online vom 01.08.2022, https://www.lto.de/recht/hintergruende/h/ein-jahr-urheberrechtsreform-urhdag-bilanz-uploadfilter-overblocking-social-media-plattformen-haftung-urheberrechtsverletzungen/, abgerufen am 05.09.2022.
[141] Ebd.

durch primärrechtskonforme Auslegung herzustellen. Besondere Bedeutung hat hier die Auslegung in Konformität mit der EuGrCh erlangt.[142]

Relevant für die vorliegende Betrachtung der möglichen Beeinflussung der Datenschutzgrundverordnung durch entsprechende Datennutzungsrechtsakte, die ebenfalls in Form einer Verordnung oder einer Richtlinie ergehen, ist aber die Rangfrage innerhalb des Sekundärrechts: Gilt auf der EU-Ebene ebenfalls der Grundsatz „lex posterior derogat legi priori"? Der Literatur zu der Kommentierung des Art. 288 AEUV, der die Rechtsakte der Union behandelt, lässt sich entnehmen, dass die allgemeinen Regeln juristischer Methodenlehre mit leichten unionsrechtlichen Modifikationen angewandt werden.

So gilt der Grundsatz lex posterior derogat legi priori (das spätere Gesetz verdrängt das frühere) *„mit der Maßgabe, dass die Rechtsakte vom gleichen Organ im gleichen Verfahren erlassen wurden, damit weder die grundsätzliche Gleichberechtigung der Organe noch die besondere Funktion einzelner Verfahren beeinträchtigt werden. Außerdem ist zwischen einzelnen Sekundärrechtsakten das Prinzip lex specialis derogat legi generali (das spezielle Gesetz verdrängt das allgemeine) anwendbar. […] Wegen der Gleichrangigkeit sind die verschiedenen Rechtsformen untereinander abänderbar, d. h. eine Richtlinie kann durch eine Verordnung und eine Verordnung kann durch eine Richtlinie geändert werden.*"[143] Etwas anders sieht dies Kotzur, der der Auffassung ist, dass sich die Rangordnung aus der Reihenfolge und Bedeutung der in Art. 288 AEUV aufgezählten Rechtsakte ergibt, sodass die Verordnung der Richtlinie und dem Beschluss vorgeht und beides implizit abändern könne. Sieht eine Kompetenznorm den Erlass von Verordnungen vor, könne auch eine Richtlinie erlassen werden.[144] Ganz klar lässt sich dies hinsichtlich delegierter Rechtsakte und Durchführungsrechtsakten beantworten, deren Unterscheidbarkeit aus dem Vergleich von Art. 288 mit Art. 290, 291 ergibt. Hier ist klar, dass ein neuer Rechtsakt nach Art. 288 einem delegierten bzw. Durchführungsrechtsakt vorgeht. Dies gilt nach Ruffert nicht für Durchführungsrecht, das unmittelbar auf dem Vertragswerk beruht. Relevant sind hier insbesondere Ermächtigungen aus dem Wettbewerbsrecht, Art. 103 AEUV.[145]

Letztlich ist aber – wie Nettesheim noch hinweist – stets zu prüfen, *„ob überhaupt eine Kollision besteht. Weicht eine spätere Verordnung von einer gleichrangigen früheren ab, so kann darin eine konkludente Abänderung liegen. Das gleiche gilt, wenn in demselben Regelungsbereich eine Verordnung zeitlich nach einer Richtlinie erlassen wird, nicht aber umgekehrt. Diese Rangregel muss gelten, da Verordnung und Richtlinie regelmäßig unterschiedliche Regelungsadressaten aufweisen. Während die Verordnung unmittelbar in jedem Mitgliedstaat Geltung beansprucht und in allen ihren Teilen verbindlich ist, verpflichtet die Richtlinie die Mitgliedstaaten zur Anpassung ihrer Rechtsordnung. Entschließt sich die EU zum Erlass einer Verordnung, so ist darin zugleich eine implizite Aufhebung der früheren Richtlinie zu sehen; entschließt sich die EU demgegenüber zum Erlass einer Richtlinie, so bewirken die an die Mitgliedstaaten gerichteten Richtlinienbestimmungen nicht automatisch eine Aufhebung der in ihrer Rechtswirkung in den mitgliedstaatlichen Raum hineinreichenden Verordnungsbestimmungen; diese Feststellung gilt sowohl für den Zeitpunkt des Inkrafttretens der Richtlinie als auch für den Zeitpunkt des Ablaufs der Umsetzungsfrist.*"[146]

---

[142] *Stelkens, Ulrich:* Stelkens/Bonk/Sachs, Verwaltungsverfahrensgesetz. 9. Auflage 2018, Rn. 38f.
[143] *Ruffert, Matthias:* Calliess/Ruffert, EUV/AEUV. AEUV, Art. 288 Rn. 14; *Geismann, Maria,* von der Groeben/Schwarze/Hatje, Europäisches Unionsrecht. 7. Auflage 2015. AEUV, Art. 288, Rn. 30; *Nettesheim, Martin:* Grabitz/Hilf/Nettesheim, Das Recht der Europäischen Union. 75. Auflage. AEUV, Art. 288, Rn. 228.
[144] *Kotzur, Markus:* Geiger/Khan/Kotzur, EUV/AEUV. AEUV, Art. 288, Rn. 5.
[145] *Ruffert, Matthias:* Calliess/Ruffert, EUV/AEUV. AEUV, Art. 288 Rn. 13
[146] *Nettesheim, Martin:* Grabitz/Hilf/Nettesheim, Das Recht der Europäischen Union. 75. Auflage. AEUV, Art. 288, Rn. 229.

Die EU-Kommission baut in der Regel in ihre Entwürfe stets entsprechende Aufhebungsvorschriften ein. Oft findet sich dies sogar in der Überschrift des Rechtsakts. Die bisherigen Hinweise in Bezug auf die Geltung der DSGVO sind jedoch im Data Act als im Zweifel als ausdrückliche Abänderung zu verstehen. Denn auch wenn die DSGVO „unberührt“ bleiben soll, finden sich im Verlauf der Verordnung zuhauf Regelungen, die von der DSGVO abweichen. Damit ist eine Kollision gegeben, die es im weiteren Gesetzgebungsverfahren zu verhindern gilt. Anders ist dies beim Data Governance Act, bei dem es im Gegensatz zum ursprünglichen Kommissionsentwurf eine ausdrückliche Vorrangregelung gibt, die eine Kollision verhindert.