EuZ
ZEITSCHRIFT FÜR EUROPARECHT

AUSGABE:
01|2023

LEITARTIKEL:

Bernd Holznagel / Benedikt Freese
EU Data Act: Ein wichtiger Baustein in der Europäischen Datenstrategie

EU Data Act

Ein wichtiger Baustein in der Europäischen Datenstrategie

Bernd Holznagel/Benedikt Freese*

Inhalt

* Prof. Dr. Bernd Holznagel, LL.M. (McGill) ist Direktor des Instituts für Informations-, Telekommunikations- und Medienrecht an der Westfälischen Wilhelms-Universität Münster. Benedikt Freese ist dort Doktorand.

A. Einleitung

Wie viele Filme in 4K-Auflösung müssten Sie streamen, um das weltweit für das Jahr 2025 zu erwartende Datenvolumen zu erreichen? Schätzen Sie, bevor Sie weiterlesen. Obwohl die Frage mit ihrem suggestiven Charakter zu einer hohen Schätzung verleitet, dürfte die Antwort verblüffen. Im Jahre 2025 soll das weltweite Datenvolumen bei 175 Zettabyte liegen.[1] Das entspricht rund 2,15 Billionen Filmdateien in 4K-Auflösung,[2] oder 368.000 Jahren ununterbrochenen Streamings. Manche möchten gar ausgerechnet haben, dass die Höhe des Stapels an DVDs, auf denen 175 Zettabyte gespeichert wären, über das 23-fache der Entfernung zwischen Erde und Mond beträgt.[3] Diese grossen Datenmengen bringen ein wirtschaftliches Potenzial mit sich: Wenn etwa gewerblich genutzte Maschinen und Haushaltsgeräte immer genauere Auskunft über ihre Nutzung und Umwelt geben, lassen sich hieraus Muster ableiten, die zu nützlichen Innovationen beitragen können. Auch auf gesellschaftlicher Ebene kann die Auswertung der Datenmengen zu Verbesserungen beitragen.

---

1 Seagate, Rethink Data. Bessere Nutzung von mehr Unternehmensdaten - vom Netzwerkrand bis hin zur Cloud, 2022, 10.

2 Vgl. <https://www.ionos.de/digitalguide/websites/web-entwicklung/was-ist-ein-zettabyte/>.

3 <https://blog.wiwo.de/look-at-it/2018/11/27/weltweite-datenmengen-sollen-bis-2025-auf-175-zetabyte-wachsen-8-mal-so-viel-wie-2017/>.

Ein Beispiel bot bereits die Pandemiebekämpfung: Behörden liessen sich von Telekommunikationsdienstleistern anonymisierte Standortdaten der Mobiltelefone der Bürger übermitteln, um pandemiefördernde Bewegungsströme analysieren zu können.[4]

Um das ökonomische und gesellschaftliche Potenzial dieser Datenmengen anzuheben, hat die Europäische Kommission rechtspolitischen Handlungsbedarf angemeldet, den sie in jüngster Zeit schrittweise umsetzt. Den Zugang zu Daten der öffentlichen Hand (Government-to-Business und Government-to-Consumer, G2B und G2C)[5] regelt vor allem die Open Data-Richtlinie.[6] Diese Materie ist auch Gegenstand des Data Governance Act (DGA)[7], der Vorgaben für die Weiternutzung von sensiblen Daten durch öffentliche Stellen enthält. Beispielhaft sind die Daten zu nennen, die dem Gemeinhaltungsschutz unterliegen. Zudem regelt der DGA Anforderungen an Datenvermittlungsdienste (Art. 10 ff. DGA). Er fördert die freiwillige gemeinsame Datennutzung für gemeinwohlorientierte Zwecke (sog. „Datenaltruismus", Art. 2 Nr. 16, 16 ff. DGA) und schützt nicht personenbezogene Daten im internationalen Umfeld (Art. 31 DGA). Das Funktionieren des Wettbewerbs in der Datenwirtschaft soll der Digital Markets Act (DMA) sicherstellen.[8] Dem Grundrechtsschutz dienen der kürzlich in Kraft getretene Digital Services Act (DSA)[9] und der Verordnungsentwurf zur Festlegung harmonisierter Vorschriften für künstliche Intelli-

---

4 Wilken Timo/Rammos Thanos, Der Data Act - Chancen und Risiken für Unternehmen durch das geplante europäische Datengesetz, DER BETRIEB 2022, 1241, 1244.

5 Die Beschreibung folgt dem Datenfluss, sodass beispielsweise bei „Government-to-Business" die Datenweitergabe von einer öffentlichen Stelle an ein Unternehmen erfolgt.

6 Richtlinie (EU) 2019/1024 des Europäischen Parlaments und des Rates vom 20. Juni 2019 über offene Daten und die Weiterverwendung von Informationen des öffentlichen Sektors (Neufassung), ABl L 172 vom 26. Juni 2019, 56 ff.

7 Verordnung (EU) 2022/868 des Europäischen Parlaments und des Rates vom 30. Mai 2022 über europäische Daten-Governance und zur Änderung der Verordnung (EU) 2018/1724 (Daten-Governance-Rechtsakt), ABl L 152 vom 3. Juni 2022, 1 ff.

8 Verordnung (EU) 2022/1925 des Europäischen Parlaments und des Rates vom 14. September 2022 über bestreitbare und faire Märkte im digitalen Sektor und zur Änderung der Richtlinien (EU) 2019/1937 und (EU) 2020/1828, ABl L 265 vom 12. Oktober 2022, 1 ff.

9 Verordnung (EU) 2022/2065 des Europäischen Parlaments und des Rates vom 19. Oktober 2022 über einen Binnenmarkt für digitale Dienste und zur Änderung der Richtlinie 2000/31/EG (Gesetz über digitale Dienste), ABl L 277 vom 27. Oktober 2022, 1 ff.

genz.[10] Instrumente des Schutzes personenbezogener Daten sind die Datenschutz-Grundverordnung (DS-GVO)[11] und die E-Privacy-Richtlinie[12], die sich weiterhin im Prozess der Überarbeitung zu einer Verordnung befindet.[13]

In dieses Gefüge will die Europäische Kommission ihren Verordnungsvorschlag für einen Data Act (DA-E)[14] einpassen. Dieser soll den fairen Datenzugang und die faire Datennutzung im Business-to-Business- (B2B), Business-to-Consumer- (B2C) und Business-to-Government-Bereich (B2G) regeln, den Wechsel zwischen Datenverarbeitungsdiensten und die Interoperabilität bei der Datenbereitstellung vereinfachen sowie nicht personenbezogene Daten im internationalen Umfeld schützen.[15] Zugleich will die Kommission mit dem Verordnungsentwurf noch bestehende Lücken in der Umsetzung ihrer Europäischen Datenstrategie[16] schliessen. Es gibt also Grund genug, den DA-E im Rahmen dieses Beitrags kritisch zu untersuchen.

Die Darstellung nimmt folgenden Gang: Zunächst wird ein Überblick über die Bestimmungen des Verordnungsentwurfs gegeben und eine Abgrenzung zu anderen Rechtsakten vorgenommen (siehe B.). Es folgt eine Analyse der zentralen Regelungskomplexe des DA-E (siehe C.). Der Beitrag schliesst mit einem Fazit (siehe D.).

---

10 Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zur Festlegung harmonisierter Vorschriften für Künstliche Intelligenz (Gesetz über künstliche Intelligenz) und zur Änderung bestimmter Rechtsakte der Union, COM (2021) 206 final vom 21. April 2021.

11 Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), ABl L 119 vom 4. Mai 2016, 1 ff.

12 Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation), ABl L 201 vom 12. Juli 2002, 37 ff.

13 Siehe dazu Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über die Achtung des Privatlebens und den Schutz personenbezogener Daten in der elektronischen Kommunikation und zur Aufhebung der Richtlinie 2002/58/EG (Verordnung über Privatsphäre und elektronische Kommunikation), COM (2017) 10 final vom 10. Januar 2017.

14 Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über harmonisierte Vorschriften für einen fairen Datenzugang und eine faire Datennutzung (Datengesetz), COM (2022) 68 final vom 23. Februar 2022.

15 Komprimiert zusammengefasst in DA-E, 3 f.

16 Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen Eine europäische Datenstrategie, COM (2020) 66 final vom 19. Februar 2020.

B. Aufbau des Entwurfs und Abgrenzung zu anderen Rechtsakten

I. Aufbau

Der Verordnungsentwurf gliedert sich in elf Kapitel.

Gliederung des Data Act-Entwurfs

Kapitel I Allgemeine Bestimmungen	Artikel 1 – 2
Kapitel II Datenweitergabe von Unternehmen an Verbraucher und zwischen Unternehmen	Artikel 3 – 7
Kapitel III Pflichten der Dateninhaber, die rechtlich verpflichtet sind, Daten bereitzustellen	Artikel 8 – 12
Kapitel IV Missbräuchliche Klauseln in Bezug auf den Datenzugang und die Datennutzung zwischen Unternehmen	Artikel 13
Kapitel V Bereitstellung von Daten für öffentliche Stellen und Organe, Einrichtungen und sonstige Stellen der Union wegen aussergewöhnlicher Notwendigkeit	Artikel 14 – 22
Kapitel VI Wechsel zwischen Datenverarbeitungsdiensten	Artikel 23 – 26
Kapitel VII Schutzvorkehrungen für nicht personenbezogene Daten im internationalen Umfeld	Artikel 27
Kapitel VIII Interoperabilität	Artikel 28 – 30
Kapitel IX Anwendung und Durchsetzung	Artikel 31 – 34
Kapitel X Sui-generis-Recht im Rahmen der Richtlinie 1996/9/EG	Artikel 35
Kapitel XI Schlussbestimmungen	Artikel 36 – 42

Diese Kapitel lassen sich in eine Reihe von Oberkategorien zusammenfassen.

Erstens sind das erste und das letzte Kapitel mit ihren allgemeinen Bestimmungen und Schlussbestimmungen *rechtstechnisch geboten*. Kapitel I regelt Gegenstand und Anwendungsbereich der geplanten Verordnung (Art. 1 DA-E). Gemäss Art. 1 Abs. 2 DA-E soll die Verordnung „in der Union" gelten. Damit

gilt für den DA-E das sog. Marktortprinzip.[17] Dies setzt den Regelungsansatz für den territorialen Anwendungsbereich aus anderen europäischen Datenregelwerken fort (Art. 11 Abs. 3 Data Governance Act [DGA][18] und Art. 3 Abs. 2 Datenschutz-Grundverordnung [DS-GVO])[19]. In Art. 2 DA-E finden sich ferner vor die Klammer gezogene Begriffsbestimmungen.

Zweitens will die Europäische Kommission mit dem DA-E den *Datenzugang und die Datennutzung im B2B- und B2C-Bereich* regeln (Kapitel II, III, IV, X – siehe C.I.). In Kapitel II verleiht der DA-E einem Nutzer einen Anspruch, die bei der Nutzung eines Produkts oder verbundenen Dienstes entstehenden Daten vom Dateninhaber anzufordern (Art. 4 DA-E). Dies braucht es nur, wenn die begehrten Daten nicht ohnehin direkt für den Nutzer zugänglich sind, was nach Art. 3 DA-E künftig der Standard sein soll. Die Datenweitergabe kann auf Geheiss des Nutzers auch an einen Dritten erfolgen (Art. 5 DA-E). Mit diesem horizontalen – d.h. nicht auf einen bestimmten Sektor zugeschnittenen – Datenzugangsrecht würde der DA-E ein echtes Novum darstellen. So bestanden bislang lediglich sektorale Datenzugangsrechte.[20] Darüber hinaus wird in Kapitel III die verpflichtende Datenweitergabe ausgestaltet. Damit die Regelungen von Datenzugang und Datennutzung nicht durch das sui-generis-Recht an Datenbanken aus Art. 7 Richtlinie 1996/9/EG[21] torpediert werden, soll in Kapitel X hierzu abgegrenzt werden. Des Weiteren werden Vertragsklauseln im Zusammenhang mit dem Datenzugang und der Datennutzung in Kapitel IV des Verordnungsentwurfs einer neuen Kontrollnorm unterzogen (Art. 13 DA-E).

---

17 Specht-Riemenschneider Louisa, Der Entwurf des Data Act. Eine Analyse der vorgesehenen Datenzugangsansprüche im Verhältnis B2B, B2C und B2G, MMR-Beil. 2022, 809, 812; Hennemann Moritz/Steinrötter Björn, Data Act – Fundament des neuen EU-Datenwirtschaftsrechts?, NJW 2022, 1481, 1482, Rz 6.

18 Vgl. zum Marktortprinzip im DGA Hennemann/Steinrötter, 1482, Rz 6; der DGA hat generell eine grosse Aufmerksamkeit erfahren, siehe etwa Schildbach Roman, Zugang zu Daten der öffentlichen Hand und Datenaltruismus nach dem Entwurf des Daten-Governance-Gesetzes. Datenwirtschaftsrecht IV: Mehrwert für das Teilen von Daten oder leere Hülle?, ZD 2022, 148; Tolks Daniel, Die finale Fassung des Data Governance Act. Erste Schritte in Richtung einer europäischen Datenwirtschaft, MMR 2022, 444.

19 Vgl. zum Marktortprinzip in der DS-GVO Ernst Stefan, in: Paal Boris/Pauly Daniel (Hrsg.), Datenschutz-Grundverordnung Bundesdatenschutzgesetz, 3. A., München 2021 (zit.: Paal/Pauly-Bearbeiter), Art. 3 DS-GVO, Rz 13 ff.; Ennöckl Daniel, in: Sydow Gernot/Marsch Nikolaus (Hrsg.), DS-GVO | BDSG, 3. A., Baden-Baden 2022 (zit.: Sydow/Marsch-Bearbeiter), Art. 3 DS-GVO, Rz 11 ff.

20 DA-E, 6 f.; Specht-Riemenschneider (Fn. 17), 810.

21 Richtlinie 1996/9/EG des Europäischen Parlaments und des Rates vom 11. März 1996 über den rechtlichen Schutz von Datenbanken, ABl L 77 vom 27. März 1996, 20 ff.

Diese soll missbräuchliche Vertragsbestandteile, die Kleinstunternehmen sowie kleinen und mittleren Unternehmen i. S. d. Art. 2 des Anhangs der Empfehlung 2003/361/EG[22] einseitig auferlegt werden, verhindern.

Drittens sollen künftig neben dem B2B- und B2C-Bereich auch Träger öffentlicher Gewalt vermehrt an den immensen Datenmengen im europäischen Binnenmarkt partizipieren. In Kapitel V DA-E werden daher *Datenzugang und Datennutzung im B2G-Bereich* geregelt (siehe C.II.). Nach Art. 14 DA-E erhalten öffentliche Stellen und Organe, Einrichtungen und sonstige Stellen der Union bei Vorliegen einer aussergewöhnlichen Notwendigkeit Zugang zu von der jeweiligen Stelle begehrten Daten. Das durch diesen Zugang entstehende Rechtsverhältnis zwischen den berechtigten Stellen und den verpflichteten Dateninhabern erfährt in dem Kapitel eine umfassende Ausformung.

Viertens stellt der Verordnungsentwurf *Verhaltensregeln für zentrale Marktakteure im Digitalwettbewerb* auf. (siehe C.III.). Kapitel VI enthält Vorgaben für einen erleichterten Wechsel zwischen Datenverarbeitungsdiensten (Cloud- und Edge-Anbieter). Zudem möchte die Europäische Kommission nicht personenbezogene Daten in internationalen Verarbeitungskontexten besser schützen und sieht dafür in Kapitel VII ein entsprechendes Pflichtenprogramm für Anbieter von Datenverarbeitungsdiensten vor. Auch die Interoperabilität zwischen Datenräumen wird in Kapitel VIII neuen Anforderungen unterworfen.

Schliesslich nimmt sich Kapitel IX DA-E der Anwendung und Durchsetzung an. Hier regelt Art. 31 DA-E die in den jüngsten Rechtsakten im Digitalbereich stets für politischen Zündstoff sorgende Frage, wie die *Aufsicht über die Einhaltung des DA-E* gestaltet werden soll (siehe C.IV.). Dies ist ein Thema, dass in den Mitgliedstaaten naturgemäss auf ein besonderes Interesse stösst.

Diese Inhalte liegen ganz auf der Linie der Europäischen Datenstrategie der Europäischen Kommission. Mit dieser Strategie soll die Europäische Union als gewichtiger internationaler Player der Digitalwirtschaft etabliert werden. Hier droht die Union angesichts des enormen Einflusses der USA und Chinas, an Bedeutung einzubüssen.[23] Den Weg zu mehr internationalem Gewicht sieht die Kommission in einem gegenüber diesen Ländern eigenständigen Ansatz: Wie in den USA und in China soll auch in der Union das Potenzial von Daten genutzt werden.[24] Während in den USA nach Ansicht der Kommission aller-

---

22 Empfehlung 2003/361/EG der Kommission vom 6. Mai 2003 betreffend die Definition der Kleinstunternehmen sowie der kleinen und mittleren Unternehmen, ABl L 124 vom 20. Mai 2003, 36 ff.

23 <https://www.deutschlandfunk.de/china-usa-eu-digitalisierung-technologie-100.html>.

24 Vgl. COM (2020) 66 final, 7 ff.

dings wenige Privatakteure über den wertschöpfenden Umgang mit Daten entscheiden und in China diese Entscheidung staatlich kontrollierten Akteuren unterliege, soll das Wachstumspotenzial in der Union *wertegeleitet* ausgeschöpft werden.[25] Dies lässt sich für die Kommission durch eine demokratische Ausgestaltung des Datenzugangs und der Datennutzung sowie der Regelung eines hohen Grundrechts-, Sicherheits- und Ethik-Niveaus erreichen.[26] In diese Ziele fügt sich der DA-E ein, indem er Datenzugang und Datennutzung regelt (Kapitel II, III, IV, V, X), die Datensicherheit im internationalen Umfeld angeht (Kapitel VII) und Fairnessstandards im Digitalmarkt schafft (Kapitel VI, VIII).

Schon dieser kurze Überblick verdeutlicht, wie grossflächig der Bereich ist, den der DA-E abdecken soll. Zwangsläufig überlappen die Regelungsmaterien des Entwurfs damit aber auch mit denen anderer europäischer Rechtsakte. In diesen Spannungsfeldern muss sich der DA-E behaupten, um seine Wirkung entfalten zu können.

II. Abgrenzung zu anderen Rechtsakten

1. Verhältnis zum Schutz personenbezogener Daten

Nach Art. 1 Abs. 3 DA-E bleiben die Regeln zum Schutz personenbezogener Daten unberührt, insbesondere die DS-GVO und die E-Privacy-Richtlinie. Daher muss sich vor allem der Datenzugang für den Nutzer oder Dritte auf Anfrage des Nutzers (Art. 4 u. 5 DA-E) sowie für Träger hoheitlicher Gewalt (Art. 14 DA-E) im Falle personenbezogener Daten anhand dieser Vorgaben messen lassen. Nach Art. 6 u. 9 DS-GVO müssen die Verarbeitungen personenbezogener Daten also von einem Rechtfertigungsgrund gedeckt sein.

Bezüglich des Datenzugangs nach Art. 4 u. 5 DA-E ist zu unterscheiden, ob der Nutzer betroffene Person der personenbezogenen Daten ist oder nicht (Art. 4 Nr. 1 DS-GVO). Ist er die betroffene Person, liegt in der Geltendmachung der Ansprüche seine Einwilligung in die Verarbeitung der begehrten personenbezogenen Daten, sodass die Verarbeitung von Art. 6 Abs. 1 lit. a, Art. 9 Abs. 2 lit. a DS-GVO gedeckt ist.[27] Ist der Nutzer nicht die betroffene Person, muss für die Datenweitergabe ein anderer Rechtfertigungsgrund nach Art. 6 Abs. 1 DS-GVO und ggf. Art. 9 Abs. 2 DS-GVO vorliegen.

---

25 COM (2020) 66 final, 4.

26 COM (2020) 66 final, 4.

27 Specht-Riemenschneider (Fn. 17), 810.

Eine anderer Rechtfertigungsgrund könnte sich aus Art. 6 Abs. 1 lit. c DS-GVO ergeben. Dieser setzt voraus, dass der Dateninhaber bei Weitergabe von Daten nach Art. 4 u. 5 DA-E einer rechtlichen Verpflichtung zur Datenweitergabe unterliegt. Diese rechtliche Verpflichtung könnten die Zugangsansprüche in Art. 4 u. 5 DA-E selbst darstellen. In der Folge wäre die Bereitstellung personenbezogener Daten nach Art. 4 u. 5 DA-E stets von Art. 6 Abs. 1 lit. c DS-GVO gedeckt.[28]

Gegen diese Konstruktion könnte systematisch sprechen, dass der DA-E nach Erwägungsgrund 24 keine datenschutzrechtliche Grundlage für die Weitergabe personenbezogener Daten an den Nutzer als nicht betroffene Person schaffen soll.[29] Dies lässt sich aber teilweise mit dem Wortlaut des Erwägungsgrunds entkräften, nach dem diese Einschränkung nur gelten soll, wenn der Nutzer als nicht betroffene Person den Zugang zu personenbezogenen Daten für Dritte (Art. 5 DA-E) verlangt.[30] Systematisch sind allerdings auch Art. 4 Abs. 5, 5 Abs. 6 DA-E zu beachten. Hiernach ist für die Datenweitergabe im Rahmen von Art. 4 u. 5 DA-E erforderlich, dass im Falle des Auseinanderfallens von Nutzer und betroffener Person eine Rechtsgrundlage nach Art. 6 Abs. 1 DS-GVO und ggf. Art. 9 DS-GVO vorliegt. Hätte die Kommission in den Ansprüchen aus Art. 4 u. 5 DA-E selbst rechtliche Verpflichtungen zur Datenweitergabe nach Art. 6 Abs. 1 lit. c DS-GVO gesehen, hätte es dieser Regelungen nicht bedurft. Dies unterstreicht der Verweis auf den Schutz personenbezogener Daten in Art. 5 Abs. 9 DA-E.[31] Es muss somit ein ausserhalb von Art. 4 u. 5 DA-E liegender Rechtfertigungsgrund gefunden werden, um die Weitergabe personenbezogener Daten an nicht betroffene Personen im Rahmen von Art. 4 u. 5 DA-E zu ermöglichen,[32] etwa eine Einwilligung der betroffenen Person (Art. 6 Abs. 1 lit. a, 9 Abs. 2 lit. a DS-GVO). Angesichts der schon im frühen Sta-

---

28 Specht-Riemenschneider (Fn. 17), 811.

29 Bomhard David/Merkle Marieke, Der Entwurf eines EU Data Acts. Neue Spielregeln für die Data Economy, RDi 2022, 168, 172, Rz 27.

30 Specht-Riemenschneider (Fn. 17), 811.

31 Hennemann/Steinrötter, 1482 f., Rz 9.

32 Hennemann/Steinrötter, 1482 f., Rz 9; Wilken/Rammos, 1242; Bomhard/Merkle, 172, Rz 27 ff.; Klink-Straub Judith/Straub Tobias, Data Act als Rahmen für gemeinsame Datennutzung, ZD-Aktuell 2022, 01076.

dium bestehenden Meinungsverschiedenheiten hinsichtlich des Verhältnisses des DA-E zur DS-GVO ist indes eine Klarstellung im weiteren Verfahren zu erwägen.[33]

Immerhin können die Art. 4 u. 5 DA-E mangels Konfliktfall reibungslos neben das Recht auf Datenübertragbarkeit nach Art. 20 DS-GVO treten.[34] Einfacher liegt auch der Fall des Datenzugangs der Träger hoheitlicher Gewalt nach Art. 14 DA-E. Da dieser Zugang eine aussergewöhnliche Notwendigkeit erfordert, wird die Gewährung des Datenzugangs in wohl allen Fällen im öffentlichen Interesse erforderlich sein (Art. 6 Abs. 1 lit. e Alt. 1 DS-GVO, Art. 9 Abs. 2 lit. g DS-GVO).[35]

2. Verhältnis zum Schutz geistigen Eigentums

Nach Art. 35 DA-E soll das sui-generis-Recht an Datenbanken aus Art. 7 Richtlinie 1996/9/EG nicht für Datenbanken gelten, die Daten enthalten, die bei der Nutzung eines Produkts oder verbundenen Dienstes erlangt oder erzeugt wurden. Damit soll verhindert werden, dass das Datenbankrecht den Ansprüchen aus Art. 4 u. 5 DA-E entgegengesetzt wird. Das Schrifttum lehnt die Anwendung des Datenbankrechts auf Sätze maschinengenerierter Daten bereits weitgehend ab.[36] Die Kommission schafft mit Art. 35 DA-E nun klare Verhältnisse.

3. Verhältnis zum Wettbewerbsrecht

Der DA-E soll die Art. 101 ff. AEUV nicht berühren.[37] Dieser Hinweis ist deklaratorisch, da sich die Verordnung als Sekundärrecht ohnehin in den primärrechtlichen Grenzen der Art. 101 ff. AEUV bewegen müsste. Dies wird dazu

---

33 Specht-Riemenschneider (Fn. 17), 810; European Data Protection Board/European Data Protection Supervisor, EDPB-EDPS Joint Opinion 2/2022 on the Proposal of the European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act), Brüssel 2022 (zit: EDPB/EDPS, Joint Opinion 2/2022), 8, Rz 13 ff.; Wilken/Rammos, 1247.

34 Erwägungsgrund 31 DA-E; dies steht auch in Einklang mit der Datenstrategie, die eine Erweiterung des Rechts auf Datenübertragbarkeit nach Art. 20 DS-GVO anregte, siehe dazu COM (2020) 66 final, 25; zu den Unterschieden zwischen Art. 20 DS-GVO und Art. 4 u. 5 DA-E im Einzelnen Wilken/Rammos, 1246 f.

35 Specht-Riemenschneider (Fn. 17), 811.

36 Ensthaler Jürgen/Üge Duygu, Wem gehören die durch die Nutzung von Maschinen generierten Daten?, BB 2022, 2051; Hessel Stefan/Leffer Lena, Rechtlicher Schutz maschinengenerierter Daten. Schutz durch das GeschGehG, MMR 2020, 647, 648.

37 Erwägungsgrund 88 DA-E.

führen, dass Unternehmen ihre Handlungen im Rahmen des DA-E randscharf zwischen der Einhaltung des DA-E und der Schwelle der Art. 101 ff. AEUV abgrenzen müssen. Stellt sich eine Massnahme – etwa die Gewährung von Datenzugang durch ein Unternehmen an ein anderes nach den Art. 3 ff. DA-E – als wettbewerbswidrig heraus, hat sie nach den Art. 101 ff. AEUV zu unterbleiben. Ist die Massnahme wettbewerbskonform, muss sie im Rahmen des DA-E erfolgen.[38] Dies kann zu Rechtsunsicherheiten führen. Mithin sollte im weiteren Verfahren das Verhältnis zu den Art. 101 ff. AEUV klarer umrissen werden.[39]

Ferner können neben das Datenzugangsregime des DA-E auch wettbewerbsrechtliche Datenzugangsvorschriften nach nationalem Recht treten. Ein Beispiel bietet § 19 Abs. 2 Nr. 4 des deutschen Gesetzes gegen Wettbewerbsbeschränkungen (GWB)[40], der die Weigerung eines marktbeherrschenden Unternehmens, einem anderen Unternehmen Datenzugang zu verschaffen, unter bestimmten Voraussetzungen als missbräuchlich einstuft.[41] Eine Verdrängung des Datenzugangsregimes des DA-E durch diese nationalen Vorschriften findet allerdings aufgrund ihres niedrigeren Standes in der europäischen Normenhierarchie nicht statt. Umgekehrt soll der DA-E den Datenzugang erweitern, nicht einschränken, sodass er keine Sperrwirkung auf derlei spezifisch wettbewerblich geprägte Datenzugänge entfalten dürfte.

4. Verhältnis zu weiteren Vorschriften

Datenbezogene Vorgaben in den Bereichen des Strafverfahrensrechts, der Bekämpfung von Geldwäsche und der Terrorismusfinanzierung sowie im Bereich des Geldtransfers werden nach Art. 1 Abs. 4 S. 1 u. 2 DA-E nicht berührt. Unklar ist, ob dies eine subsidiäre Anwendung des DA-E im Falle fehlender Spezialregelungen offenhält. Zu denken wäre etwa an eine subsidiäre Aktivierung des Datenzugangs nach Art. 14 ff. DA-E. Systematisch ist hierfür Art. 16 Abs. 2 S. 1

---

38 Pointiert zusammengefasst durch Bomhard/Merkle, 172, Rz 25 f.

39 In diese Richtung auch Podszun Rupprecht/Pfeifer Clemens, Datenzugang nach dem EU Data Act: Der Entwurf der Europäischen Kommission, GRUR 2022, 953, 954; Weiterführend zur Vereinbarkeit des DA-E mit Wettbewerbsrecht Brauneck Jens, Zur Vereinbarkeit des Data Act-Entwurfes mit dem Europäischen Wettbewerbsrecht, WRP 2022, 954.

40 Gesetz gegen Wettbewerbsbeschränkungen in der Fassung der Bekanntmachung vom 26. Juni 2013 (BGBl. I 2013, 1750), zuletzt geändert durch Art. 2 des Gesetzes zur Änderung des Energiewirtschaftsrechts im Zusammenhang mit dem Klimaschutz-Sofortprogramm und zu Anpassungen im Recht der Endkundenbelieferung vom 19. Juli.2022 (BGBl. I 2022, 1214).

41 Vgl. im Einzelnen Wolf Maik, in: Säcker Franz Jürgen/Meier-Beck Peter (Hrsg.), Münchener Kommentar zum Wettbewerbsrecht Band 2: Gesetz gegen Wettbewerbsbeschränkungen §§ 1–96, 185, 186, 4. A., München 2022, § 19 GWB, Rz 170b f.

DA-E zu berücksichtigen. Dieser sperrt Art. 14 DA-E im Bereich des Strafverfahrensrechts, des Ordnungswidrigkeitsverfahrensrechts und in der Zoll- und Steuerverwaltung. Im Umkehrschluss könnte Art. 1 Abs. 4 DA-E so verstanden werden, dass er keine generelle Sperrwirkung des DA-E für die aufgelisteten Bereiche normiert. Auch hier wäre eine Klarstellung durch den Gesetzgeber wünschenswert.[42]

C. Zentrale Regelungskomplexe

I. Datenzugang und Datennutzung im B2B- und B2C-Bereich nach dem DA-E

1. Regelungssystematik

Die Europäische Kommission zögerte zunächst, bestimmten Marktakteuren verbindliche Datenzugangsansprüche einzuräumen.[43] In Marktforschungen stellte sie jedoch fest, dass es im Binnenmarkt an einer freiwilligen Datengewährung mangelt, was die Fairness der Datenverteilung und das Wachstumspotenzial der datenbasierten Wirtschaft in Zweifel rückte.[44] Daher schlägt die Kommission nun verpflichtende Datenzugänge im B2B- und B2C-Bereich vor, die sektorübergreifend angelegt sind. Nach dem DA-E erfolgt der Datenzugang auf Anfrage eines Nutzers an ihn selbst (siehe C.I.2.) oder auf Anfrage eines Nutzers an einen Dritten (siehe C.I.3.). Ferner sind bei der Ausgestaltung rechtlich verpflichtender Datenweitergaben künftig die Regeln der Art. 8 – 12 DA-E zu beachten (siehe C.I.4.). Bei verpflichtenden und freiwilligen Datenzugängen und Datennutzungen soll ferner in Zukunft eine Missbrauchskontrolle von Verträgen stattfinden (siehe C.I.5.).

2. Datenzugangsanspruch des Nutzers an ihn selbst (Art. 4 DA-E)

Art. 4 DA-E normiert einen Datenzugangsanspruch des Nutzers gegenüber Dateninhabern.[45]

---

42 Zweitzitat: EDPB/EDPS, Joint Opinion 2/2022, 12, Rz 36.

43 COM (2020) 66 final, 15 f.

44 DA-E, 12 f.

45 DA-E, 3.

Anspruch des Nutzers auf Zugang und Nutzung von Produkt- und Dienstdaten, Art. 4 DA-E

Tatbestand

a) Anspruchsteller ist Nutzer, Art. 4 Abs. 1, 2 Nr. 5, DA-E

b) Anspruchsteller verlangt Produkt- oder Dienstdaten, Art. 4 Abs. 1, 2 Nr. 1-3, 7 Abs. 2 DA-E

c) Anspruchsteller kann auf diese Daten nicht ohnehin nach Art. 3 Abs. 1 DA-E zugreifen

d) Anspruchsgegner ist tauglicher Dateninhaber, Art. 4 Abs. 1, 2 Nr. 6, 7 Abs. 1 DA-E

e) Geschäftsgeheimnisschutz steht nicht entgegen, Art. 4 Abs. 3 DA-E

f) Personenbezogene Daten: Rechtsgrundlage, Art. 6 u. 9 DS-GVO, Art. 4 Abs. 5 DA-E

Rechtsfolge

g) Bereitstellung im Umfang des Art. 4 DA-E

a) Anspruchsteller ist Nutzer, Art. 4 Abs. 1, 2 Nr. 5, DA-E

Art. 2 Nr. 5 DA-E definiert den Nutzer als „eine natürliche oder juristische Person, die ein Produkt besitzt, mietet oder least oder eine Dienstleistung in Anspruch nimmt". In Erwägungsgrund 18 Satz 1 DA-E ist statt von „besitzt" von „gekauft" die Rede. Fraglich ist daher, ob der Nutzer das Produkt rechtmässig nutzen dürfen muss, oder auch rechtswidrige Nutzer erfasst sind.[46] Letztere könnten unter den Wortlaut „besitzt" in Art. 2 Nr. 5 DA-E fallen. Ein Indiz geben Erwägungsgrund 18 Sätze 2 und 3 DA-E, die den Datenzugangsanspruch des Nutzers damit begründen, dass er je nach Rechtstitel, unter dem er das Produkt nutzt, die Risken des Produkts trägt, sodass es konsequent ist, ihm im Gegenzug ein Datenzugangsrecht zu gewähren. Dieses Telos schlägt bei einem rechtswidrigen Nutzer nicht durch. Art. 2 Nr. 5 DA-E ist damit nur auf den rechtmässigen Nutzer anwendbar. Dies können Verbraucher wie Unternehmen sein. Je nach Ausgestaltung dieser rechtlichen Grundlage können auch

[46] Specht-Riemenschneider (Fn. 17), 814.

mehrere Personen gleichzeitig Nutzer sein.[47] Auch in unentgeltlichen Ausgestaltungen der rechtlichen Nutzungsgrundlage kann der Nutzer Risiken im Zusammenhang mit der Produktnutzung tragen, sodass auch das unentgeltliche Nutzen unter Art. 2 Nr. 5 DA-E fällt.[48]

b) *Anspruchsteller verlangt Produkt- oder Dienstdaten, Art. 4 Abs. 1, 2 Nr. 1-3, 7 Abs. 2 DA-E*

Nach Art. 4 Abs. 1 DA-E kann der Nutzer „die bei der Nutzung eines Produktes oder verbundenen Dienstes erzeugten Daten" verlangen. „Daten" sind gemäss Art. 2 Nr. 1 DA-E weit gefasst und umfassen sämtliche digitale Informationen. Ein „Produkt" definiert Art. 2 Nr. 2 DA-E als „einen körperlichen beweglichen Gegenstand, der auch in einem unbeweglichen Gegenstand enthalten sein kann, Daten über seine Nutzung oder Umgebung erlangt, erzeugt oder sammelt und Daten über einen öffentlich zugänglichen elektronischen Kommunikationsdienst übermitteln kann und dessen Hauptfunktion nicht die Speicherung und Verarbeitung von Daten ist".

Speichermedien sind demnach nicht vom Datenzugangsanspruch erfasst.[49] Art. 4 DA-E hätte ansonsten Tür und Tor zu sämtlichen sensiblen Speicherkapazitäten geöffnet. Die Ausnahme für Produkte, deren Hauptfunktion in der Datenverarbeitung liegt, begründet die Kommission damit, dass sie einen menschlichen Beitrag für die Datengenerierung erfordern.[50] Diese Daten möchte sie durch den DA-E nicht adressieren. Damit fallen etwa Computer, Server und mobile Endgeräte nicht unter den DA-E.[51] Übrig bleiben insbesondere *Internet of Things*-Daten, die bei der Nutzung privater Haushaltsgeräte oder industrieller Maschinen entstehen.[52]

Bei einem „verbundenen Dienst" handelt es sich nach Art. 2 Nr. 3 DA-E um „einen digitalen Dienst, einschliesslich Software, der so in ein Produkt integriert oder so mit ihm verbunden ist, dass das Produkt ohne ihn eine seiner Funk-

---

47 Dies zeigt Erwägungsgrund 20 DA-E, der auch auf mehrere Eigentümer oder Vertragsbeteiligte als Nutzer abstellt, so auch Podszun/Pfeifer, 959; Wilken/Rammos, 1242; diese Frage aufwerfend Hennemann/Steinrötter, 1484, Rz 17; Bomhard/Merkle, 170 f., Rz 14.

48 Diese Frage aufwerfend Wilken/Rammos, 1242.

49 Erwägungsgrund 14 DA-E.

50 Erwägungsgrund 14 DA-E.

51 Erwägungsgrund 14 DA-E.

52 Vgl. auch Specht-Riemenschneider (Fn. 17), 814; im Ergebnis auch Wilken/Rammos, 1242.

tionen nicht ausführen könnte". Vermitteln virtuelle Assistenten (Art. 2 Nr. 4 DA-E) Zugang zum Produkt oder verbundenen Dienst, sollen auch Daten dieser Komponente von Art. 4 DA-E erfasst sein (Art. 7 Abs. 2 DA-E).[53]

Der Nutzer kann indes nur solche Daten nach Art. 4 DA-E anfragen, die „bei der Nutzung" erzeugt wurden. Dies ist im Lichte von Erwägungsgrund 17 DA-E, nach dem sowohl absichtlich vom Nutzer aufgezeichnete Daten als auch Daten ohne Nutzerbeteiligung erfasst sein sollen, weit zu verstehen.[54] Somit können auch Daten erfasst sein, die nicht der Nutzer selbst aufzeichnet, sondern andere Personen, die sein Gerät benutzen.[55] Das legt auch der Wortlaut von Art. 4 Abs. 1 DA-E nahe, der von Daten „bei *der* Nutzung" spricht, nicht „bei *seiner* Nutzung". Allerdings umfasst Art. 4 DA-E keine Daten, die das Ergebnis eines rechtmässigen Ableitungsprozesses aus den Produkt- oder Dienstdaten sind.[56] Die Erstellung und Durchführung eines solchen Ableitungsprozesses sieht die Europäische Kommission als schutzwürdig an.[57]

c) *Anspruchsteller kann auf diese Daten nicht ohnehin nach Art. 3 Abs. 1 DA-E zugreifen*

Des Zugangsrechts nach Art. 4 DA-E bedarf der Nutzer nur, wenn er nicht schon nach Art. 3 Abs. 1 DA-E auf die Daten zugreifen kann. Die soeben definierten Produkt- und Dienstdaten müssen dem Nutzer gemäss Art. 3 Abs. 1 DA-E standardmässig direkt zur Verfügung gestellt werden.[58] Der Direktzugang gilt gemäss Art. 3 Abs. 1 DA-E so lange, wie er „relevant und angemessen" ist.[59] Daten, deren Begehren nicht antizipiert werden kann oder Daten, deren nutzertaugliche Darstellung für sämtliche Nutzer ohne Anfrage unangemessen erscheint, fallen damit aus Art. 3 Abs. 1 DA-E heraus. In diesen Fällen kommt Art. 4 Abs. 1 DA-E zum Zuge.

d) *Anspruchsgegner ist tauglicher Dateninhaber, Art. 4 Abs. 1, 2 Nr. 6, 7 Abs. 1 DA-E*

Der Anspruchsgegner muss tauglicher Dateninhaber sein. Dies ist gemäss Art. 2 Nr. 6 DA-E „eine juristische oder natürliche Person, die nach dieser Ver-

---

53 Weitergehend hierzu Erwägungsgrund 22 DA-E.

54 Wilken/Rammos, 1242.

55 Erwägungsgrund 14 DA-E.

56 Erwägungsgrund 14 DA-E.

57 Erwägungsgrund 14 DA-E.

58 Podszun/Pfeifer, 956; Hennemann/Steinrötter, 1483, Rz 11.

59 Dieses systematische Verständnis teilen Specht-Riemenschneider (Fn. 17), 815; Podszun/Pfeifer, 956.

ordnung, nach anwendbarem Unionsrecht oder nach den anwendbaren nationalen Rechtsvorschriften zur Umsetzung des Unionsrechts berechtigt oder verpflichtet bzw. im Falle nicht personenbezogener Daten und durch die Kontrolle über die technische Konzeption des Produktes und damit verbundener Dienste in der Lage ist, bestimmte Daten bereitzustellen".

Diese recht sperrige Legaldefinition wirft Fragen auf. So wird befürchtet, dass auch Arbeitnehmer Dateninhaber sein könnten, da sie faktisch auf Produkt- und Dienstdaten zugreifen können.[60] Hiergegen lassen sich zwei Argumente anführen. Erstens geht Erwägungsgrund 24 DA-E davon aus, dass im Falle personenbezogener Daten der Dateninhaber auch Verantwortlicher i. S. d. Art. 4 Nr. 7 DS-GVO sein sollte. Er muss also über Mittel und Zweck der Verarbeitung personenbezogener Daten zumindest mitentscheiden können[61] und damit diese Daten wesentlich kontrollieren. Diese Kontrolle übt im Verhältnis zwischen Arbeitnehmer und Arbeitgeber grundsätzlich der Arbeitgeber aus.[62] Zweitens stellt der Wortlaut des Art. 2 Nr. 6 DA-E im Falle nicht personenbezogener Daten auf die „durch die Kontrolle über die technische Konzeption des Produktes und damit verbundener Dienste" vermittelte Möglichkeit der Datenbereitstellung ab. Die Zugriffsmöglichkeit muss also auf der Produkt- und Dienstkontrolle beruhen, eine rein faktische Zugriffsmöglichkeit reicht nicht aus.[63] Als Dateninhaber werden daher in der Praxis vorwiegend industrielle Hersteller der Produkte und verbundenen Dienste anzusehen sein.[64] Der Rechtssicherheit halber sollte allerdings die Voraussetzung einer Kontrolle über personenbezogene Daten aus Erwägungsgrund 24 DA-E ausdrücklich in Art. 2 Nr. 6 DA-E aufgenommen werden und neben die Voraussetzung einer rechtlichen Pflicht zur Datenbereitstellung treten.

---

60 Bomhard/Merkle, 169, Rz 6 f.

61 Weiterführend hierzu Paal/Pauly-Ernst, Art. 4 DS-GVO Rz 55; Sydow/Marsch-Raschauer, Art. 4 DS-GVO, Rz 114 ff.

62 Franzen Martin, in: ders./Gallner Inken/Oetker Hartmut (Hrsg.), Kommentar zum europäischen Arbeitsrecht, 4. A., München 2022, Art. 7 DS-GVO, Rz 12a.

63 Dies verdeutlichen englische und französische Fassung des Art. 2 Nr. 6 DA-E: „'data holder' means a legal or natural person who has the right or obligation, in accordance with this Regulation, applicable Union law or national legislation implementing Union law, or in the case of non-personal data and *through control of the technical design of the product and related services, the ability*, to make available certain data"; „„détenteur de données', une personne morale ou une personne physique qui, conformément au présent règlement, aux dispositions législatives applicables de l'Union ou à la législation nationale mettant en œuvre le droit de l'Union, a le droit ou l'obligation ou, dans le cas de données à caractère non personnel et *par le contrôle de la conception du produit et des services liés, a la possibilité*, de rendre disponibles certaines données à caractère personnel" (Hervorhebungen hinzugefügt).

64 I.E. auch Specht-Riemenschneider (Fn. 17), 813.

Da Art. 2 Nr. 6 DA-E unter anderem nur solche Personen als Dateninhaber definiert, die nach dem DA-E zur Datenbereitstellung verpflichtet werden, wird zum Teil ein Zirkelschluss in dieser Definition gesehen.[65] Art. 4 f. DA-E verpflichte ohnehin sämtliche Dateninhaber zur Datenbereitstellung, sodass das Definitionsmerkmal einer ‚rechtlichen Verpflichtung nach dem DA-E' ohne Anwendungsbereich bleibe.[66] Dem scheint die soeben herausgearbeitete Annahme zugrunde zu liegen, dass Art. 2 Nr. 6 DA-E unter Berücksichtigung von Erwägungsgrund 24 DA-E zweierlei voraussetzt: Eine rechtliche Verpflichtung zur Datenbereitstellung und eine faktische Kontrolle über die begehrten Daten. In diesem Lichte liegt indes kein Zirkelschluss vor: Art. 7 Abs. 1 DA-E sieht eine Ausnahme von den Pflichten nach Art. 3 ff. DA-E zugunsten von Daten vor, die aus Produkten oder Diensten stammen, die Kleinst- oder Kleinunternehmen i. S. d. Art. 2 des Anhangs der Empfehlung 2003/361/EG hergestellt bzw. erbracht haben. Art. 14 Abs. 2 DA-E zeichnet Kleinst- und Kleinunternehmen i. S. d. Art. 2 des Anhangs der Empfehlung 2003/361/EG ferner vom Datenzugang der Träger öffentlicher Gewalt nach Art. 14 Abs. 1 DA-E frei. Es gibt also Personen, die Kontrolle über Daten ausüben, aber nicht zur Datenbereitstellung verpflichtet werden und deshalb keine Dateninhaber sind. Das Merkmal der rechtlichen Verpflichtung hat daher in der Definition des Dateninhabers einen eigenen Anwendungsbereich.

e) Geschäftsgeheimnisschutz steht nicht entgegen, Art. 4 Abs. 3 DA-E

Nach Art. 4 Abs. 3 S. 1 DA-E dürfen Geschäftsgeheimnisse nur offengelegt werden, „wenn alle besonderen Massnahmen getroffen worden sind, die erforderlich sind, um die Vertraulichkeit der Geschäftsgeheimnisse, insbesondere gegenüber Dritten, zu wahren". Dazu können Dateninhaber und Nutzer gemäss Art. 4 Abs. 3 S. 2 DA-E Vertraulichkeitsvereinbarungen treffen.

Der Geschäftsgeheimnisschutz ist damit zwar zu berücksichtigen, er kann den Anspruch jedoch nicht unterbinden.[67] Über Art. 4 Abs. 3 S. 2 DA-E erwartet die Praxis daher den Abschluss strenger Non-Disclosure-Agreements.[68] Dies kann zu Streitigkeiten über die zulässige Reichweite dieser Vereinbarungen führen.[69] Das scheint die Europäische Kommission aber in Kauf zu nehmen, um Art. 4 DA-E weitestgehend zur Anwendung zu verhelfen.

---

65 Bomhard/Merkle, 169, Rz 5.

66 Bomhard/Merkle, 169, Rz 5.

67 Specht-Riemenschneider (Fn. 17), 816.

68 Hennemann/Steinrötter, 1484, Rz 18; Wilken/Rammos, 1244; Bomhard/Merkle, 171, Rz 22.

69 Bomhard/Merkle, 171, Rz 22.

f) Personenbezogene Daten: Rechtsgrundlage, Art. 6 u. 9 DS-GVO, Art. 4 Abs. 5 DA-E

Bei personenbezogenen Daten bedarf es für Art. 4 Abs. 1 DA-E einer Rechtsgrundlage nach Art. 6 u. 9 DS-GVO (siehe B.II.1.).

g) Bereitstellung im Umfang des Art. 4 DA-E

Art. 4 Abs. 1 S. 1 DA-E sieht vor, dass die Daten dem Nutzer „unverzüglich, kostenlos und gegebenenfalls kontinuierlich und in Echtzeit zur Verfügung" zu stellen sind. Dies kann als blosses Einsichtsrecht für den Nutzer ausgestaltet werden.[70] Das ergibt sich aus Erwägungsgrund 21 DA-E, der für den Zugang auch die Bereitstellung auf „eigenen lokalen Serverkapazitäten" des Dateninhabers hinreichen lässt.[71]

Die zur Verfügung gestellten Daten darf der Nutzer ferner nicht zur Entwicklung eines Konkurrenzprodukts nutzen, Art. 4 Abs. 4 DA-E. Wann genau eine solche Konstellation vorliegt, wird man im Einzelfall beurteilen müssen. Sollte der Gesetzgeber dieses Verbot im Übrigen auf verbundene Dienste ausweiten wollen, wäre eine Klarstellung in Art. 4 Abs. 4 DA-E angezeigt.[72]

h) Einordnung

Art. 4 DA-E verpflichtet Dateninhaber, Daten bereitzustellen. Dies schränkt ihre unternehmerische Freiheit nach Art. 16 GRCh ein.[73] Eine Einschränkung kann indes nicht aus einem Recht auf Dateneigentum[74] der Dateninhaber abgeleitet werden, da der DA-E ein solches nicht anerkennt, wie sich aus den

---

70 Podszun/Pfeifer, 956; Klink-Straub/Straub, 01076.

71 Überzeugend herausgearbeitet von Specht-Riemenschneider (Fn. 17), 815; Specht-Riemenschneider Louisa, Data Act – Auf dem (Holz-)Weg zu mehr Dateninnovation?, ZRP 2022, 137, 139; Specht-Riemenschneider Louisa, Der Entwurf des Data Act: Ein grosser Wurf in die falsche Richtung?, GRUR 2022, 937, 938.

72 Bomhard/Merkle, 172, Rz 24.

73 Wollenschläger Ferdinand, in: von der Groeben Hans/Schwarze Jürgen/Hatje Armin (Hrsg.), Europäisches Unionsrecht, 7. A., Baden-Baden 2015, Art. 16 GRCh Rz 1 ff.; Ruffert, Matthias, in: ders./Calliess, Christian, EUV/AEUV, 6. A. München 2022, Art. 16 GRCh, Rz 1 ff.

74 Vgl. in der Diskussion gegen ein „Dateneigentum" Hoeren Thomas, Datenbesitz statt Dateneigentum. Erste Ansätze zur Neuausrichtung der Diskussion um die Zuordnung von Daten, MMR 2019, 5; Kühling Jürgen/Sackmann Florian, Irrweg „Dateneigentum". Neue Grosskonzepte als Hemmnis für die Nutzung und Kommerzialisierung von Daten, ZD 2020, 24; dafür Fezer Karl-Heinz, Dateneigentum der Bürger. Ein originäres Immaterialgüterrecht sui generis an verhaltensgenerierten Informationsdaten der Bürger, ZD 2017, 99.

Erwägungsgründen 5 und 6 DA-E ergibt. Als Rechtfertigung für den Eingriff in die unternehmerische Freiheit kann der durch Art. 4 DA-E bezweckte Verbraucherschutz und die Förderung des wirtschaftlichen Datenaustauschs durch einen besseren Datenzugang angeführt werden.[75] Aufgrund der Nicht-Rivalität von Daten können Dateninhaber im Übrigen die Daten weiterhin nutzen, sodass sie in dieser Hinsicht ihre unternehmerische Betätigung fortsetzen können.[76] Art. 4 DA-E begegnet mithin keinen gravierenden grundrechtlichen Bedenken.

Insgesamt hat die Kommission damit einen rechtssicheren Rahmen für eine sektorübergreifende Harmonisierung des Datenzugangsrechts vorgeschlagen. Dies ist zu begrüssen. Damit der DA-E zügig sein Harmonisierungspotenzial entfalten kann, ist eine zeitnahe Anpassung der sektorspezifischen Zugangsvorschriften an Art. 4 DA-E zu empfehlen.[77]

3. Datenzugangsanspruch des Nutzers an Dritte (Art. 5 DA-E)

Auf Geheiss des Nutzers kann gemäss Art. 5 DA-E auch eine Bereitstellung von Daten an Dritte erfolgen. Dritte erhalten damit kein eigenes Datenzugangsrecht. Vielmehr ist ihr Zugang akzessorisch zum Nutzerverlangen.[78] Möchten also etwa Reparaturbetriebe für Kraftfahrzeuge Daten über vernetzte Kraftfahrzeuge erlangen, um wiederkehrende Anfälligkeiten für Ausfälle zu erfassen, müssen sie den Nutzer um eine Weiterleitung dieser Daten bitten. Art. 5 DA-E ist wie folgt aufgebaut.

Anspruch des Nutzers auf Weitergabe von Produkt- und Dienstdaten an Dritte, Art. 5 DA-E

Tatbestand

a) Anspruchsteller ist Nutzer, Art. 5 Abs. 1, 2 Nr. 5 DA-E

b) Anspruchsteller verlangt Produkt- oder Dienstdaten, Art. 5 Abs. 1, 2 Nr. 1-3, 7 Abs. 2 DA-E

c) Anspruchsteller verlangt Datenbereitstellung an zulässigen Dritten, Art. 5 Abs. 2 DA-E

75 DA-E, 16.

76 DA-E, 16.

77 Dieses Ziel ist bereits angelegt in DA-E, 6.

78 Specht-Riemenschneider (Fn. 17), 816; Hennemann/Steinrötter, 1484, Rz 19.

d) Anspruchsgegner ist tauglicher Dateninhaber, Art. 5 Abs. 1, 2 Nr. 6, 7 Abs. 1, DA-E

e) Geschäftsgeheimnisschutz steht nicht entgegen, Art. 5 Abs. 8 DA-E

f) Personenbezogene Daten: Rechtsgrundlage, Art. 6 u. 9 DS-GVO, Art. 5 Abs. 6 u. 9 DA-E

Rechtsfolge

g) Bereitstellungsverhältnis nach Art. 5, 6, 8 ff. DA-E

a) Erläuterung der Tatbestandsmerkmale und der Rechtsfolge

Art. 5 DA-E weist grosse Parallelen zu Art. 4 DA-E auf. Unterschiede zu Art. 4 DA-E ergeben sich beim Datenempfänger (zulässiger Dritter), dem Schutz von Geschäftsgeheimnissen (Art. 5 Abs. 8 DA-E) und der Rechtsfolge (Art. 5, 6, 8 ff. DA-E).

„Dritter" i. S. d. Art. 5 DA-E kann jede juristische oder natürliche Person sein (vgl. Art. 2 Nr. 7 DA-E). Der DA-E zählt beispielhaft Unternehmen, Forschungseinrichtungen und gemeinnützige Organisationen auf.[79] Art. 5 Abs. 2 DA-E schliesst einzig Gatekeeper gemäss Art. 3 DMA (in der verabschiedeten deutschen Fassung des DMA nunmehr „Torwächter") aus. Dies sind Unternehmen, die erheblichen Einfluss auf den Binnenmarkt haben, einen zentralen Plattformdienst bereitstellen, der gewerblichen Nutzern als wichtiges Zugangstor zu Endnutzern dient und die hinsichtlich ihrer Tätigkeiten eine gefestigte und dauerhafte Position innehaben oder absehbar ist, dass sie eine solche Position in naher Zukunft erlangen werden (Art. 3 Abs. 1 DMA). Hierunter fallen Unternehmen wie Alphabet und Amazon.[80] Diesen Unternehmen attestiert die Europäische Kommission ein derart hohes Datensammlungspotenzial, dass sie es für unverhältnismässig hält, sie in den Kreis der Dritten nach Art. 5 DA-E aufzunehmen.[81] Gatekeeper dürfen Nutzer daher nicht zur Geltendmachung von Art. 5 Abs. 1 DA-E auffordern oder geschäftlich anreizen (Art. 5 Abs. 2 lit. b DA-E). Auch nach Art. 4 DA-E vom Nutzer erlangte Daten darf ein Gatekeeper nicht in Empfang nehmen (Art. 5 Abs. 2 lit. a u. c DA-E). Selbst die Konstella-

79 Erwägungsgrund 29 DA-E.

80 Podszun Rupprecht/Bongartz Philipp/Kirk Alexander, Digital Markets Act – Neue Regeln für Fairness in der Plattformökonomie, NJW 2022, 3249, 3250.

81 Erwägungsgrund 36 DA-E; hierin wirtschaftspolitische Erwägungen hineinlesend Wilken/Rammos, 1247 f.

tion, dass der Nutzer aus freien Stücken den Anspruch nach Art. 5 Abs. 1 DA-E zugunsten eines Gatekeepers auslöst, unterbindet Art. 5 Abs. 2 DA-E, indem er Gatekeeper pauschal als unzulässige Dritte einordnet. Gatekeeper können damit in keinem Fall am Datenzugangsanspruch nach Art. 5 DA-E partizipieren.

Für die Offenlegung von Geschäftsgeheimnissen ist nach Art. 5 Abs. 8 DA-E zusätzlich erforderlich, dass die Datenbereitstellung für den zwischen dem Nutzer und dem Dritten vereinbarten Zweck „unbedingt erforderlich" ist. Nutzer und Dritter könnten in der Praxis allerdings einen weiten Zweck der Datennutzung vereinbaren. Daher droht Art. 5 Abs. 8 DA-E nach jetziger Fassung leerzulaufen.[82]

In der Rechtsfolge müssen die Daten grundsätzlich ähnlich zu Art. 4 Abs. 1 DA-E gemäss Art. 5 Abs. 1 DA-E bereitgestellt werden. Darüber hinaus besteht jedoch ein erweitertes Pflichtenprogramm des Dritten nach Art. 6 DA-E, etwa die Zweckbindung der Verarbeitung an dem mit dem Nutzer vereinbarten Zweck (Art. 6 Abs. 1 DA-E). Wie beim Geschäftsgeheimnisschutz besteht allerdings auch hier die Gefahr, dass die Norm mit einer weiten Zweckvereinbarung unterlaufen wird. Überdies darf der Dritte die erhaltenen Daten keinen Gatekeepern zur Verfügung stellen (Art. 6 Abs. 2 lit. d DA-E), was bei der Verwendung von Gatekeeper-Anwendungen erhöhte Compliance-Anforderungen nach sich ziehen wird.[83] Ferner wird das Verhältnis des Dritten zum Dateninhaber durch die Art. 8 ff. DA-E ausgestaltet (siehe C.I.4.).

b) Einordnung

Statt den Datenzugang Dritter von einem Nutzerverlangen abhängig zu machen, könnte im weiteren Verfahren ein eigenes Datenzugangsrecht des Dritten angedacht werden.[84] Dies würde dem von der Kommission ausgemachten Problem eines mangelnden Datenaustauschs zwischen Unternehmen entgegenwirken.[85] Stand jetzt können Unternehmen nach dem Rahmen des DA-E nur dann Daten voneinander beanspruchen, wenn sie das Produkt oder den verbundenen Dienst des jeweils anderen nutzen (Art. 4 DA-E) oder einen Nutzer überzeugen, die Datenbereitstellung zu verlangen (Art. 5 DA-E). Die Entscheidung eines Nutzers, den Anspruch nach Art. 5 Abs. 1 DA-E geltend zu machen, hätte damit eine wesentliche Torwächterfunktion für den Datenaustausch in der Digitalwirtschaft. Dies fusst vor dem Hintergrund der Stärkung der Rechte der (häufig als Verbraucher einzustufenden) Nutzer auf einer legi-

82 Bomhard/Merkle, 171 f., Rz 23.

83 Kritisch Wilken/Rammos, 1243.

84 In diese Richtung auch Podszun/Pfeifer, 959.

85 COM (2020) 66 final, 7 ff.

timen Leitlinie. Dennoch sollte im weiteren Verfahren nicht ausser Acht gelassen werden, dass die Stärkung von Nutzerrechten und der umfangreiche Datenaustausch im Wirtschaftsverkehr in einem Zielkonflikt stehen können, der aufgelöst werden muss.

Ferner ist zu erörtern, ob der Zweckvereinbarung zwischen Nutzer und Dritten Grenzen gesetzt werden müssen, um den Geschäftsgeheimnisschutz in Art. 5 Abs. 8 DA-E und die Zweckbindung in Art. 6 Abs. 1 DA-E nicht leerlaufen zu lassen.[86]

4. Bedingungen verpflichtender Datenweitergaben

a) Anwendungsbereich

Die Art. 8 ff. DA-E finden Anwendung, wenn ein Dateninhaber nach Art. 5 DA-E, anderem Unionsrecht oder auf Unionsrecht beruhenden nationalen Regelungen verpflichtet ist, einem Datenempfänger Daten bereitzustellen (Art. 8 Abs. 1 DA-E). Art. 4 DA-E wird von Art. 8 Abs. 1 DA-E nicht erfasst. Der DA-E sieht Art. 4 DA-E also als lex specialis an. Auch auf freiwillige Vereinbarungen finden Art. 8 ff. DA-E keine Anwendung; auf diese sollen sie jedoch eine Ausstrahlungswirkung entfalten.[87]

In zeitlicher Hinsicht sollen die Art. 8 ff. DA-E lediglich für Datenbereitstellungspflichten gelten, die nach dem Geltungsbeginn des DA-E in Kraft treten (Art. 12 Abs. 3 DA-E). Anders als teilweise angenommen[88] finden Art. 8 ff. DA-E daher insbesondere keine Anwendung auf Art. 15 u. 20 DS-GVO.[89] Sollen aber die Art. 8 ff. DA-E den gewünschten Marktstandard vorgeben, wäre eine Wirkung auch für vor Geltungsbeginn des DA-E normierte Datenbereitstellungspflichten angezeigt. Dies sollte erwogen werden.

b) Ausgestaltung des Rechtsverhältnisses zwischen Dateninhaber und Datenempfänger

Sind die Art. 8 ff. DA-E anwendbar, bildet ein Vertrag die Grundlage des Rechtsverhältnisses zwischen Dateninhaber und Datenempfänger (Art. 8

---

86 Bomhard/Merkle, 171, Rz 17.

87 Erwägungsgrund 38 DA-E.

88 Specht-Riemenschneider (Fn. 17), 821.

89 Erwägungsgrund 38 DA-E.

Abs. 2 S. 1 DA-E). Grundsätzlich soll also die Privatautonomie massgeblich sein.[90] Diese wird von den zwingenden (Art. 12 Abs. 2 DA-E)[91] Vorgaben der Art. 8 ff. DA-E flankiert.

Art. 8 DA-E sieht die wesentlichen Pflichten des Dateninhabers vor. Dieser muss nach Art. 8 Abs. 1 DA-E die Daten „zu fairen, angemessenen und nichtdiskriminierenden Bedingungen und in transparenter Weise" bereitstellen. Er unterliegt dabei einem Gleichbehandlungsgebot, für dessen Einhaltung er die Beweislast trägt (Art. 8 Abs. 3 DA-E). Unterschiedliche Vertragsbedingungen je nach Vertrag sollen aber bei Vorliegen objektiver Gründe möglich sein.[92] Eine exklusive Bereitstellung von Daten darf nur auf Nutzerverlangen erfolgen (Art. 8 Abs. 4 DA-E). Eine Pflicht zur Offenlegung von Geschäftsgeheimnissen muss sich gemäss Art. 8 Abs. 6 DA-E aus der Datenbereitstellungspflicht ergeben, die den Weg in die Art. 8 ff. DA-E bahnt. Dies ist beispielsweise Art. 5 Abs. 8 DA-E, auf den Art. 8 Abs. 6 wohl (statt auf Art. 6 DA-E) verweisen wollte.

Im Gegenzug darf der Dateninhaber nach Art. 11 Abs. 1 DA-E technische Schutzmassnahmen wie intelligente Verträge (Art. 2 Nr. 16 DA-E) einsetzen, um unbefugte Zugänge zu verhindern und die Einhaltung der Art. 5, 6, 9, 10 DA-E und der für die Datenbereitstellung vereinbarten Vertragsbedingungen sicherzustellen.

Dem Datenempfänger obliegt die Pflicht, nach Art. 9 Abs. 1 DA-E eine Gegenleistung zu erbringen.[93] Von Kleinstunternehmen sowie kleinen und mittleren Unternehmen i. S. d. Art. 2 des Anhangs der Empfehlung 2003/361/EG darf der Dateninhaber gemäss Art. 9 Abs. 2 DA-E nur einen Kostenausgleich verlangen. Eine niedrigere Gegenleistungspflicht oder ihren völligen Ausschluss durch leges speciales hält Art. 9 Abs. 3 DA-E offen.

Im Rahmen von Art. 5 DA-E kann es dazu kommen, dass der Datenempfänger für die Bereitstellung von Daten doppelt zur Kasse gebeten wird: *Erstens* vom Nutzer für die Geltendmachung von Art. 5 DA-E, *zweitens* vom Dateninhaber für die Datenbereitstellung nach Art. 9 Abs. 1 DA-E.[94]

Möglicherweise könnte der Datenempfänger aber zumindest der Vergütungspflicht des Art. 9 Abs. 1 DA-E entkommen, indem er den Nutzer incentiviert, Daten nach Art. 4 DA-E einzuholen, um diese dem Datenempfänger anschliessend freiwillig zur Verfügung zu stellen. Dann wären Art. 8 ff. DA-E und damit

---

90 Erwägungsgrund 39 DA-E.

91 Hennemann/Steinrötter, 1485, Rz 24.

92 Erwägungsgrund 41 DA-E.

93 Erwägungsgründe 42 ff. DA-E.

94 Specht-Riemenschneider (Fn. 17), 823; Specht-Riemenschneider (Fn. 71), 140.

auch Art. 9 Abs. 1 DA-E für die zweite Datenübertragung vom Nutzer auf den Datenempfänger unanwendbar.[95] Diesen Pfad hat auch die Kommission gesehen: Nach Art. 5 Abs. 2 lit. c DA-E darf ein Gatekeeper keine Daten erhalten, die ein Nutzer nach Art. 4 Abs. 1 DA-E erlangt hat. Wäre der Weg für Dritte, vom Nutzer nach Art. 4 DA-E erlangte Daten zu erhalten, gesperrt, hätte ein Ausschluss der Gatekeeper vom Kreis der Dritten i. S. d. Art. 5 DA-E gereicht. Dass Art. 5 Abs. 2 lit. c DA-E aber ausdrücklich auch die Empfangnahme der vom Nutzer nach Art. 4 DA-E erlangten Daten untersagt, zeigt im Umkehrschluss, dass Dritten dieser Weg grundsätzlich nicht versperrt ist. Dem Dritten i. S. d. Art. 5 DA-E steht damit die Umgehung zumindest der Vergütungspflicht aus Art. 9 Abs. 1 DA-E offen.

Darüber hinaus bestehen für den Datenempfänger gemäss Art. 11 Abs. 2 DA-E gewisse Verhaltenspflichten im Umgang mit dem Dateninhaber.

Eine handhabbare Anwendung all dieser Pflichten kann die Kommission gemäss Art. 34 DA-E in Mustervertragsbedingungen ausarbeiten. Diesen Bedingungen blickt die Praxis mit Spannung entgegen.[96]

Schliesslich steht bei Meinungsverschiedenheiten über die Einhaltung der Art. 8 u. 9 DA-E ein Streitbeilegungsverfahren nach Art. 10 DA-E zur Verfügung.[97]

5. Missbrauchskontrolle für Datenverträge

Die gemeinsame Datennutzung gestaltet die Missbrauchskontrolle für Datenverträge in Art. 13 DA-E weiter aus. Hierdurch soll verhindert werden, dass ungleiche Verhandlungspositionen beim Zugang zu Daten zulasten von Kleinstunternehmen, kleinen und mittleren Unternehmen i. S. d. Art. 2 des Anhangs der Empfehlung 2003/361/EG ausgenutzt werden.[98] Art. 13 DA-E statuiert damit einen zwingenden (Art. 13 Abs. 8 DA-E) Kontrollmassstab im B2B-Bereich,[99] der parallel zur Kontrolle Allgemeiner Geschäftsbedingungen[100] ausgestaltet ist. Die Norm ist systematisch geschickt in einem eigenen Kapitel IV

---

95 Specht-Riemenschneider (Fn. 17), 822; Bomhard/Merkle, 171, Rz 16.

96 DA-E, 12 f.; siehe auch Wilken/Rammos, 1243.

97 Erwägungsgründe 48 ff. DA-E.

98 DA-E, 6.

99 Witzel Michaela, Der Entwurf des Data Act und seine Vorgaben an die Vertragsgestaltung Missbräuchliche Klauseln - Fairness-Standards - Schwarze und Graue Klauseln, CR 2022, 561, 562, Rz 5.

100 Richtlinie 93/13/EWG des Rates vom 5. April 1993 über missbräuchliche Klauseln in Verbraucherverträgen, ABl L 96 vom 21. April 1993, 29 ff.

neben Kapitel III verortet, damit sie nicht nur auf Verträge für verpflichtende Datenbereitstellungen (Art. 8 Abs. 1 DA-E), sondern auch auf freiwillige Verträge Anwendung findet.

Entfall der Bindungswirkung missbräuchlicher Vertragsklauseln, Art. 13 DA-E

Tatbestand

a) Anwendbarkeit: Keine Festlegung des Hauptgegenstandes oder des zu zahlenden Preises, Art. 13 Abs. 7 DA-E

b) Vertragsklausel in Bezug auf den Datenzugang und die Datennutzung oder die Haftung und Rechtsbehelfe bei Verletzung oder Beendigung datenbezogener Pflichten, Art. 13 Abs. 1 DA-E

c) Vertragsklausel zwischen Unternehmen und Kleinstunternehmen, kleinem oder mittlerem Unternehmen, Art. 13 Abs. 1 DA-E

d) Vertragsklausel durch Unternehmen einseitig auferlegt, Art. 13 Abs. 1, 5 DA-E

e) Vertragsklausel ist missbräuchlich, Art. 13 Abs. 1 DA-E

   aa) Ausnahmslose Missbräuchlichkeit bei Verstoss gegen Art. 13 Abs. 3 DA-E

   bb) Vermutete Missbräuchlichkeit bei Verstoss gegen Art. 13 Abs. 4 DA-E

   cc) Missbräuchlichkeit qua Generalklausel, Art. 13 Abs. 2 DA-E

Rechtsfolge

f) Vertragsklausel ist für Kleinstunternehmen, kleines oder mittleres Unternehmen nicht bindend, Art. 8 Abs. 2 S. 2, 13 Abs. 1 DA-E; übrige Vertragsklauseln bleiben bei Abtrennbarkeit bindend, Art. 13 Abs. 6 DA-E

Hinsichtlich der Reichweite des Art. 13 DA-E stellt die Kommission klar, dass zum Schutz der Vertragsfreiheit nur solche Vertragsbestandteile erfasst sein sollen, die sich auf die Bereitstellung von Daten beziehen.[101]

Die Klausel muss dem Kleinstunternehmen, kleinen oder mittleren Unternehmen i. S. d. Art. 2 des Anhangs der Empfehlung 2003/361/EG nach Art. 13 Abs. 1 DA-E einseitig auferlegt worden sein. Dies wird nach Art. 13 Abs. 5 DA-E vermutet, „wenn sie von einer Vertragspartei eingebracht wird und die andere Vertragspartei ihren Inhalt trotz des Versuchs, hierüber zu verhandeln, nicht beeinflussen kann“. Die Vermutung ist widerleglich, wie Art. 13 Abs. 5 S. 2 DA-E

[101] Erwägungsgründe 52 f. DA-E.

zeigt. Die Widerlegung obliegt der Vertragspartei, die die Klausel eingebracht hat. Da Art. 13 Abs. 5 S. 1 DA-E einen Verhandlungsversuch verlangt, wird sich ein Unternehmen, das eine Vertragsklausel ‚kampflos' hinnimmt, nicht auf Art. 13 DA-E berufen können.[102]

Ferner müssen von Art. 13 Abs. 1 DA-E erfasste Vertragsklauseln der Missbräuchlichkeitsprüfung standhalten. Art. 13 DA-E überprüft Klauseln auf eine absolute (Art. 13 Abs. 3 DA-E), vermutete (Art. 13 Abs. 4 DA-E) und sich aus der Generalklausel ergebende (Art. 13 Abs. 2 DA-E) Unzulässigkeit.[103]

Absolut unzulässig ist gemäss Art. 13 Abs. 3 lit. b DA-E der „Ausschluss der Haftung der Partei, die die Klausel einseitig auferlegt hat, bei einer Verletzung" von Vertragspflichten. Hier wird gefragt, ob dies nur einen Haftungsausschluss für sämtliche Verschuldensformen verbietet, oder bereits den Ausschluss einzelner Verschuldensformen.[104] Der Wortlaut „Ausschluss" ist in systematischer Zusammenschau mit Art. 13 Abs. 3 lit. a DA-E, der von „Ausschluss oder (…) Beschränkung" spricht, als völlige Freizeichnung einer Vertragspartei von der in Bezug genommenen Materie zu verstehen. Diese Bezugsmaterie ist in Art. 13 Abs. 3 lit. b DA-E eine Vertragspflichtverletzung. Folglich ist nur der vollkommene Ausschluss der Haftung für Vertragspflichtverletzungen erfasst. Ein Ausschluss für einzelne Verschuldensformen bei der Vertragspflichtverletzung ist zulässig.

Bei der Generalklausel in Art. 13 Abs. 2 DA-E ist ein restriktiver Massstab anzuwenden. Bloss nachteilhafte Klauseln für eine Partei sollen für eine Missbräuchlichkeit nicht ausreichen.[105]

Insgesamt könnten auch bei Art. 13 DA-E die Musterverträge gemäss Art. 34 DA-E Aufschluss über die Tragweite der Norm geben.[106]

Im Falle eines Verstosses gegen Art. 13 DA-E ist die Klausel für das Kleinstunternehmen, kleine oder mittlere Unternehmen nicht bindend, Art. 8 Abs. 2 S. 2, 13 Abs. 1 DA-E. Nach der Verordnungsbegründung soll dies dazu führen, dass keiner der beiden Parteien die vom Vertrag adressierten Daten nutzen darf.[107] Dies gibt der Rechtstext des DA-E bislang jedoch nicht her.

---

102 Witzel, 563, Rz 10.

103 Dieses systematische Verständnis teilen Specht-Riemenschneider (Fn. 17), 822; Hennemann/Steinrötter, 1485, Rz 25; Witzel, 565, Rz 30.

104 Witzel, 564, Rz 25.

105 Erwägungsgrund 54 DA-E; vgl. Witzel, 564, Rz 19 ff.

106 Erwägungsgrund 55 DA-E.

107 DA-E, 18 f.

II. Datenzugang und Datennutzung im B2G-Bereich

Auch Träger hoheitlicher Gewalt erhalten gemäss Art. 14 DA-E flächendeckenden Zugang zu Daten des Binnenmarkts. Dies soll ihre Entscheidungsgrundlage verbessern.[108] Einsatzfelder wären etwa Daten über die Auslastung von Infrastrukturen, damit ihr Ausbau besser geplant werden kann.[109] Ein solcher Datenzugang wurde von einer Expertengruppe,[110] Politik[111] und Behörden[112] gefordert; in der Wirtschaft[113] stösst er wohl aufgrund zusätzlicher Pflichten auf ein durchwachsenes Echo.

Datenzugang durch Träger hoheitlicher Gewalt, Art. 14 DA-E

Tatbestand

a) Anspruchsteller ist Träger hoheitlicher Gewalt, Art. 14 Abs. 1, Art. 2 Nr. 9 DA-E

b) Anspruchsteller stellt taugliches Verlangen nach Daten, Art. 14 Abs. 1, 17 Abs. 1 u. 2 DA-E

c) Verlangen des Anspruchsstellers bezieht sich nicht auf eine Bereichsausnahme, Art. 16 Abs. 2 S. 1 DA-E

d) Anspruchsgegner ist tauglicher Dateninhaber, Art. 14 Abs. 1 u. 2, 2 Nr. 6 DA-E

e) Für Datennutzung besteht aussergewöhnliche Notwendigkeit, Art. 14 Abs. 1, 15 DA-E

Rechtsfolge

f) Bereitstellung im Umfang der Art. 14 Abs. 1, 17 Abs. 3 u. 4, 18 – 22 DA-E

---

108 Mit den gegenwärtigen Datenzugängen sieht die Europäische Kommission eine angemessene Entscheidungsgrundlage gefährdet, siehe COM (2020) 66 final, 7 ff.

109 Die Bundesregierung, Datenstrategie der Bundesregierung. Eine Innovationsstrategie für gesellschaftlichen Fortschritt und nachhaltiges Wachstum, Berlin 2021, 57.

110 High-Level Expert Group on Business-to-Government Data Sharing, Towards a European strategy on business-to-government data sharing for the public interest. Final report, Luxemburg 2020, 8.

111 Eine europäische Datenstrategie. Entschliessung des Europäischen Parlaments vom 25. März 2021 zum Thema „Eine europäische Datenstrategie", P9_TA(2021)0098, Rz 55.

112 DA-E, 13.

113 DA-E, 13.

1. Erläuterung der Tatbestandsmerkmale und der Rechtsfolge

Damit ein Träger hoheitlicher Gewalt (vgl. Art. 2 Nr. 9 DA-E) Daten erhalten kann, muss sein Datenverlangen den Anforderungen nach Art. 14 Abs. 1, 17 Abs. 1 u. 2 DA-E entsprechen. Art. 17 Abs. 1 DA-E sieht dafür Gestaltungsanforderungen vor, während Art. 17 Abs. 2 DA-E sonstige Rechtmässigkeitsanforderungen normiert. Eine trennscharfe Abgrenzung der beiden Absätze ist der Kommission nicht gelungen. Da der Dateninhaber bei einem Verstoss gegen einen der beiden Absätze aber den Datenzugang verweigern darf (Art. 18 Abs. 2 DA-E), müssen ohnehin sämtliche Voraussetzungen kumulativ erfüllt sein.

Das behördliche Verlangen darf sich nach Art. 14 Abs. 1 DA-E ferner pauschal auf „Daten" (Art. 2 Nr. 1 DA-E) beziehen, nicht nur auf Produkt- oder Dienstdaten wie in den Art. 3 ff. DA-E. Der Anwendungsbereich des Art. 14 DA-E ist damit wesentlich weiter.

Der Träger öffentlicher Gewalt muss für den Datenzugang schliesslich eine aussergewöhnliche Notwendigkeit ins Feld führen. Die Fälle der aussergewöhnlichen Notwendigkeit sind abschliessend (!) in Art. 15 DA-E definiert. Zu ihnen zählen die Bewältigung oder Vorbeugung eines öffentlichen Notstands (Art. 2 Nr. 10 DA-E) oder die Erholung von einem solchen (Art. 15 lit. a u. b DA-E). Daneben kann der Datenzugang für die Erfüllung einer öffentlichen Aufgabe geltend gemacht werden, wenn der Träger öffentlicher Gewalt die dafür erforderlichen Daten nicht erlangen kann und eine entsprechende Änderung der Rechtsordnung zu lange dauern würde (Art. 15 lit. c Nr. 1 DA-E), oder die Erlangung der Daten nach Art. 14 Abs. 1 DA-E den Verwaltungsaufwand der Dateninhaber oder anderer Unternehmen erheblich verringern würde (Art. 15 lit. c Nr. 2 DA-E).

Die Rechtsfolgen des Datenzugangs regeln Art. 14 Abs. 1, 17 Abs. 3 u. 4, 18 – 22 DA-E umfassend. Die Bereitstellung der Daten hat nach Art. 18 Abs. 1 DA-E grundsätzlich unverzüglich zu erfolgen. Bei Nichtverfügbarkeit der Daten oder Rechtsverstössen der Behörde stehen dem Dateninhaber gemäss Art. 18 Abs. 2 u. 3 DA-E ausnahmsweise Ablehnungsrechte zu. Art. 19 f. DA-E statuieren zudem diverse Pflichten des Trägers öffentlicher Gewalt. Insbesondere hat in den Fällen des Art. 15 lit. c DA-E ein Ausgleich für die Datenbereitstellung zu erfolgen;[114] ein solcher ist für Art. 15 lit. a u. b DA-E indes nicht vorgesehen (Art. 20 DA-E).

Die nach Art. 14 Abs. 1 DA-E erlangten Daten können über Art. 17 Abs. 4, 21 Abs. 1, 22 Abs. 1 DA-E weitergegeben werden. Die Verarbeitung der dabei ggf.

---

[114] Auf Rechtsunsicherheiten hinsichtlich der Höhe hindeutend Wilken/Rammos, 1245.

enthaltenen personenbezogenen Daten dürfte aufgrund des Bezugs der Art. 14 ff. DA-E zu öffentlichen Aufgaben nach Art. 6 Abs. 1 lit. e DS-GVO erfolgen.[115] Von einer pauschalen Weiterverarbeitung nach der Open Data-Richtlinie 2019/1024 sind die nach Art. 14 ff. DA-E erlangten Daten allerdings ausgenommen (Art. 17 Abs. 3 DA-E).

2. Einordnung

Grundsätzlich ist zu befürworten, Träger öffentlicher Gewalt im Lichte der zunehmenden Datenfixierung aller Lebensbereiche an Daten partizipieren zu lassen. Bei einem öffentlichen Notstand (Art. 15 lit. a u. b. DA-E) geht es um aussergewöhnliche Situationen (Art. 2 Nr. 10 DA-E), sodass gegenläufige grundrechtliche Positionen regelmässig nachrangig sein dürften. Art. 15 lit. c Nr. 1 DA-E erlaubt aber auch schon bei Schwierigkeiten, Daten mit gegenwärtigen Mitteln zu erlangen, einen Datenzugang. Hier ist im Einzelfall gegenüber widerstreitenden Interessen der Vorrang abzuwägen. Zu beachten ist dabei, dass es nach Art. 20 Abs. 2 DA-E eine Ausgleichspflicht zugunsten des Dateninhabers gibt. Schwierig dürfte es sein, „harte Kriterien" wie eine ausnahmslose Pflicht zur Pseudonymisierung personenbezogener Daten aufzustellen, wie dies teilweise gefordert wird.[116]

III. Verhaltensregeln für zentrale Marktakteure im Digitalwettbewerb

1. Vereinfachter Wechsel zwischen Datenverarbeitungsdiensten

Jenseits der Regelung von Datennutzung und Datenzugang sollen die Art. 23 ff. DA-E den Wechsel zwischen Datenverarbeitungsdiensten (Art. 2 Nr. 12, Erwägungsgrund 71 DA-E), also Cloud- und Edge-Diensten erleichtern. Hier sah die Europäische Kommission das Bedürfnis nach hoheitlichen Vorgaben, weil sich der bislang mit der Verordnung (EU) 2018/1807[117] verfolgte Ansatz der regulier-

115 A. A. EDPB/EDPS, Joint Opinion 2/2022, 20, Rz 74, nach denen die Verarbeitung auf eine Rechtspflicht und damit auf Art. 6 Abs. 1 lit. c DS-GVO zu stützen ist.

116 Vgl. EDPB/EDPS, Joint Opinion 2/2022, 21, Rz 81 f.

117 Verordnung (EU) 2018/1807 des Europäischen Parlaments und des Rates vom 14. November 2018 über einen Rahmen für den freien Verkehr nicht-personenbezogener Daten in der Europäischen Union, ABl L 303 vom 28. November 2018, 59 ff.

ten Selbstregulierung des Anbieterwechsels nicht bewährt hatte.[118] Auf diese Weise möchte sie Lock-In-Effekten auf dem Cloud- und Edge-Markt begegnen und die Anbieterauswahl für private und geschäftliche Nutzer erhöhen.[119]

In diesem Lichte schreibt Art. 23 Abs. 1 DA-E vor, dass Anbieter von Datenverarbeitungsdiensten Hindernisse für den Anbieterwechsel beseitigen müssen. Nach dem Verordnungsentwurf sollen sie dazu unter anderem künftig ein Kündigungsrecht von 30 Tagen in ihre Nutzungsverträge aufnehmen (Art. 23 Abs. 1 S. 2 lit. a DA-E).

Weitere Anforderungen an die Vertragsbeziehung zwischen Diensteanbieter und Nutzer geben Art. 24 u. 25 DA-E vor. Insbesondere sollen Wechselentgelte drei Jahre nach Inkrafttreten des DA-E abgeschafft werden (Art. 25 Abs.1 DA-E). Technische Vorgaben des Wechsels hält Art. 26 DA-E bereit. Die Vorschriften treten neben die bestehenden Schutzvorgaben der Richtlinie (EU) 2019/770[120] und der DS-GVO.[121]

Insgesamt erinnern die Art. 23 ff. DA-E an die Regulierung des Anbieter- und Nummernwechsels im Telekommunikationsrecht.[122] Wie einst den dortigen Vorschriften wird den Art. 23 ff. DA-E ein hohes Potenzial beigemessen, um die in der Praxis vereinbarten Cloud- und Edge-Verträge grundlegend zu modifizieren.[123]

---

118 Erwägungsgrund 70 DA-E.

119 DA-E, 17.

120 Richtlinie (EU) 2019/770 des Europäischen Parlaments und des Rates vom 20. Mai 2019 über bestimmte vertragsrechtliche Aspekte der Bereitstellung digitaler Inhalte und digitaler Dienstleistungen, ABl L 136 vom 22. Mai 2019, 1 ff.

121 Erwägungsgrund 74 DA-E.

122 Art. 30 f. Richtlinie 2002/22/EG des Europäischen Parlaments und des Rates vom 7. März 2002 über den Universaldienst und Nutzerrechte bei elektronischen Kommunikationsnetzen und -diensten (Universaldienstrichtlinie), ABl L 108 vom 24. April 2002, 51 ff.; Art. 106 Richtlinie (EU) 2018/1972 des Europäischen Parlaments und des Rates vom 11. Dezember 2018 über den europäischen Kodex für die elektronische Kommunikation, ABl L 321 vom 17. Dezember 2018, 36 ff.; siehe als Beispiel zur Umsetzung dieser Normen in deutsches Recht Kiparski Gerd, Die TKG-Novelle 2021. Die neuen kundenschützenden Regelungen des TKG-RefE im Überblick, CR 2020, 818, 823 f.; Beine Heinrich, Anbieterwechsel und Umzug nach der TKG-Novelle 2012. Wichtige Neuerungen für Kunden und Wettbewerb MMR 2012, 718; Holznagel Bernd, Das neue TKG: Im Mittelpunkt steht der Verbraucher, NJW 2012, 1622.

123 Wilken/Rammos, 1245; Bomhard/Merkle, 175, Rz 56.

2. Schutzvorkehrungen für nicht personenbezogene Daten im internationalen Umfeld

Mit dem DA-E möchte die Europäische Kommission den Datenschutz in internationalen Kontexten weiter ausbauen. Rechtswidrige Zugriffe drittstaatlicher Organisationen auf in der Union gespeicherte Daten sind ihr ein Dorn im Auge.[124] Aus diesem Grunde weitet Art. 27 DA-E im Wesentlichen die aus Art. 31 DGA bekannten Pflichten zum Schutz nicht personenbezogener Daten im internationalen Umfeld auf Datenverarbeitungsdienste aus. Er bildet damit gemeinsam mit Art. 31 DGA das Gegenstück zu den Art. 44 ff. DS-GVO, die den internationalen Schutz personenbezogener Daten regeln.[125]

Gemäss Art. 27 Abs. 1 DA-E müssen Anbieter von Datenverarbeitungsdiensten angemessene Massnahmen treffen, um eine rechtswidrige internationale Übermittlung von oder Zugriffsgewährung zu in der Union gespeicherten Daten zu verhindern. Die Rechtswidrigkeit kann sich aus unionalem und nationalem Recht ergeben.

Art. 27 Abs. 2 – 5 DA-E normieren darüber hinaus besondere Anforderungen an die Übermittlung und Zugriffsgewährung auf Grund drittstaatlicher Gerichts- und Verwaltungsentscheidungen.

Die drittstaatliche Gerichts- oder Verwaltungsentscheidung darf nach Art. 27 Abs. 2 DA-E nur dann anerkannt oder vollstreckbar werden, wenn die Entscheidung auf einer internationalen Übereinkunft wie etwa einem Rechtshilfeabkommen fusst.

Besteht eine solche Übereinkunft nicht und würde die Übermittlung bzw. Zugriffsgewährung gegen unionales oder nationales Recht verstossen, darf die Übermittlung nur dann erfolgen, wenn die Voraussetzungen des Art. 27 Abs. 3 UAbs. 1 DA-E gewahrt sind. Dieser Absatz verlangt rechtsstaatliche Mindestqualitäten im Drittstaat, dessen Gericht oder Behörde die Daten verlangt. Die Einhaltung der Anforderungen hat der Anbieter des Datenverarbeitungsdienstes selbstständig zu prüfen. Er kann dabei eine Stellungnahme der nach Art. 31 DA-E zuständigen Behörde einholen (Art. 27 Abs. 3 UAbs. 2 DA-E). Zudem kann die Kommission Leitlinien für die Einstufung nach Art. 27 Abs. 3 UAbs. 1 DA-E erlassen (Art. 27 Abs. 3 UAbs. 3 DA-E).

Sind die Voraussetzungen nach Art. 27 Abs. 2 oder 3 DA-E erfüllt, stellt der Anbieter des Datenverarbeitungsdienstes den erforderlichen Mindestdatensatz

---

124 DA-E, 4.

125 EDPB/EDPS, Joint Opinion 2/2022, 24, Rz 94.

zur Verfügung (Art. 27 Abs. 4 DA-E). Mit Ausnahme der Strafverfolgung muss vorab eine Mitteilung an den betroffenen Dateninhaber erfolgen (Art. 27 Abs. 5 DA-E), damit dieser bei Bedarf rechtliche Schritte einleiten kann.

3. Interoperabilität bei der Datenbereitstellung

Schliesslich nimmt sich der DA-E in Kapitel VIII der Interoperabilität an. Darunter versteht Art. 2 Nr. 19 DA-E „die Fähigkeit von zwei oder mehr Datenräumen oder Kommunikationsnetzen, Systemen, Produkten, Anwendungen oder Komponenten, Daten auszutauschen und zu verwenden, um ihre Funktionen auszuführen".[126] In der Datenstrategie hat die Kommission die Errichtung sektorspezifischer Datenräume, z. B. für die Industrie oder Energiewirtschaft, als wichtiges Instrument zur Förderung des Wirtschaftswachstums gesehen.[127] Da viele Anwendungen aber eine sektorübergreifende Datenauswertung benötigen, soll die Interoperabilität auch zwischen den verschiedenen Datenräumen gestärkt werden (Art. 28 DA-E).[128] Im Einklang mit dem erleichterten Anbieterwechsel (siehe C.III.1.) werden auch Datenverarbeitungsdienste künftig Interoperabilitätsstandards unterworfen (Art. 29 DA-E). Ferner sollen für intelligente Verträge (Art. 2 Nr. 16 DA-E), also Mechanismen, die die Einhaltung von Datennutzungsverträgen zwischen Dateninhabern und Datenempfängern überprüfen können, künftig Mindeststandards gelten (Art. 30 DA-E).

Die Art. 28 – 30 DA-E stellen umfassend auf harmonisierte Normen (Art. 28 Abs. 3 u. 4, 29 Abs. 4, 30 Abs. 4 u. 5 DA-E), Durchführungsrechtsakte (Art. 28 Abs. 5, Art. 30 Abs. 6 DA-E), delegierte Rechtsakte (Art. 28 Abs. 2, 29 Abs. 5 DA-E) und Kommissionsleitlinien (Art. 28 Abs. 6 DA-E) ab. Sie sind daher als Anstoss für die Interoperabilität zu sehen, deren praktische Umsetzung aber erst sukzessiv nach Inkrafttreten des DA-E erfolgen kann. Dennoch gehen sie bereits jetzt deutlich über andere Interoperabilitätsstandards hinaus, etwa für für Messenger-Dienste in Art. 61 Abs. 2 UAbs. 1 Richtlinie (EU) 2018/1972.

---

126 Vgl. zur Definition der Interoperabilität im Digitalbereich Kalbhenn Jan Christopher/Freese Benedikt/Flamme Florian, Wirtschaftsverwaltungsrechtliche Interoperabilitätspflichten für Messenger-Dienste und soziale Netzwerke im Lichte des deutschen und europäischen Rechts, DÖV 2022, 805, 807 f.

127 COM (2020) 66 final, 26 f.

128 Podszun/Pfeifer, 958.

IV. Aufsicht über die Einhaltung des DA-E

Mit neuen Vorschriften im Digitalbereich geht stets die Frage einher, welche Behörde ihre Anwendung und Durchsetzung beaufsichtigen soll. Dies regelt für den vorliegenden Entwurf Art. 31 DA-E.

Nach Art. 31 Abs. 1 DA-E bestimmt jeder Mitgliedstaat eine oder mehrere zuständige Behörden für die Anwendung und Durchsetzung des DA-E. Hierfür können neue oder bestehende Behörden eingesetzt werden. Die ausgewählte Behörde soll für die Beaufsichtigung des Wechsels zwischen Datenverarbeitungsdiensten (siehe C.III.1.) eine hinreichende Kompetenz besitzen (Art. 31 Abs. 2 lit. c DA-E). Zudem muss sie frei von Einflussnahmen und Weisungen (Art. 31 Abs. 6 DA-E) sowie mit hinreichenden Mitteln zur Erfüllung ihrer Aufgaben ausgestattet sein (Art. 31 Abs. 8 DA-E). Bei mehreren Aufsichtsbehörden muss eine Koordination erfolgen (Art. 31 Abs. 4 DA-E).

Unberührt bleiben soll allerdings die Zuständigkeit der Datenschutzbehörden nach Art. 55 ff. DS-GVO. Sobald im Rahmen des DA-E personenbezogene Daten betroffen sind, sollen die Datenschützer auch die Aufsicht über die Einhaltung des DA-E übernehmen (Art. 31 Abs. 2 lit. a DA-E).

Art. 31 DA-E überlässt die Wahl der zuständigen Behörde damit dem politischen Diskurs der Mitgliedstaaten. Insofern gleicht er Art. 26 DGA. Auch der DSA sieht ähnliche Bestimmungen vor, enthält allerdings eine äusserst starke Stellung der Europäischen Kommission (vgl. ihre Zuständigkeit für sehr grosse Online-Plattformen, Art. 33 ff. DSA) sowie des nationalen Koordinators für digitale Dienste (vgl. Art. 49 ff. DSA). Art. 31 DA-E ist überdies von den Art. 51 ff. DS-GVO zu unterscheiden, die die Unabhängigkeit der national zuständigen Datenschutzbehörden umfassend absichern. Ferner verfolgen auch die Art. 20 ff. DMA mit ihrer Durchsetzung durch die Europäische Kommission einen anderen Ansatz.

Die verschiedenen Regelungen zeigen, dass die Europäische Union keinen einheitlichen Aufsichtsansatz in ihrer Digitalgesetzgebung verfolgt. Dies birgt das Risiko einer uneinheitlichen und ineffizienten Regulierung durch zahlreiche Behörden. Möchten die Mitgliedstaaten dies vermeiden, sollten sie erwägen, die national zuständigen Behörden möglichst einheitlich zu benennen. Die po-

litische Debatte für den zuständigen digitalen Koordinator nach dem DSA ist bereits in vollem Gange.[129] Dies ist auch für Art. 31 DA-E zu erwarten.[130] Diese Entwicklungen dürfen weiter mit Spannung verfolgt werden.

D. Fazit

Die vorstehende Analyse hat gezeigt, wie gross das Projekt ist, das sich die Europäische Union mit dem DA-E vorgenommen hat. Die Vielzahl an Vorschriften, zu denen der DA-E in Beziehung steht, deutet darauf hin, dass sich das europäisches Datenrecht als neues Rechtsgebiet zu festigen beginnt. In dieses könnte die Union mit dem DA-E künftig eine im Grundsatz stimmige Verordnung einfügen. Bei Verfassen dieses Beitrags im November 2022 befindet sich der Verordnungsentwurf in der ersten Lesung im Rat der Europäischen Union. Ein Verordnungsentwurf kommt dabei niemals aus dem Gesetzgebungsverfahren heraus, wie er in das Verfahren eingeführt wurde. Es bleibt abzuwarten, welche Veränderungen am Entwurf politisch umsetzbar sind. Insgesamt ist aber zu hoffen, dass es der Europäischen Union gelingt, diesen nächsten Schritt in der Umsetzung der europäischen Datenstrategie erfolgreich zu gehen.

---

129 Gerald Spindler spricht insofern von neuer Nahrung für den politischen Diskurs, Spindler Gerald, Der Vorschlag für ein neues Haftungsregime für Internetprovider – der EU-Digital Services Act. Teil 2: Grosse und besonders grosse Plattformen, GRUR 2021, 653, 661.

130 Die europäischen Datenschützer bringen bereits die europäischen und nationalen Datenschutzbehörden in Stellung, EDPB/EDPS, Joint Opinion 2/2022, 24 ff., Rz 97 ff.

EuZ
ZEITSCHRIFT FÜR EUROPARECHT

25. Jahrgang

Herausgeber

Europa Institut an der
Universität Zürich
Hirschengraben 56
8001 Zürich
Schweiz
eiz@eiz.uzh.ch

Institut für deutsches und
europäisches Gesellschafts-
und Wirtschaftsrecht der
Universität Heidelberg
Friedrich-Ebert-Platz 2
69117 Heidelberg
Deutschland

LL.M. Internationales
Wirtschaftsrecht
Universität Zürich
Hirschengraben 56
8001 Zürich

Redaktion
Dr. Tobias Baumgartner, LL.M., Rechtsanwalt (Leitung)
MLaw Sophie Tschalèr
Dr. Wesselina Uebe, Rechtsanwältin

Cover-Foto: dlohner, Pixabay

Erscheinungsweise
EuZ – Zeitschrift für Europarecht erscheint zehnmal jährlich online. Die Leitartikel werden zu Beginn des Folgejahres zusätzlich in Form eines Jahrbuchs als eBook sowie im Wege des print on demand veröffentlicht.

Zitierweise
EuZ, Ausgabe 1/2022, A 13.

ISSN 1423-6931

Kontakt
EIZ Publishing c/o Europa Institut an der Universität Zürich
Dr. Tobias Baumgartner, LL.M., Rechtsanwalt
Hirschengraben 56
8001 Zürich
Schweiz
eiz@eiz.uzh.ch

Version 1.02-20230130

DOI
Bernd Holznagel/Benedikt Freese, EU Data Act – Ein wichtiger Baustein in der Europäischen Datenstrategie, https://doi.org/10.36862/eiz-euz014