Centrum für Europäische Politik
FREIBURG | BERLIN

cepInput

Nr. 3 | 2022 9. Februar 2022

Unternehmen sollen ihre Daten teilen

Der „Data Act“ soll die europäische Datenwirtschaft entscheidend voranbringen. Auch der Staat will von den Daten profitieren. Ein erster Entwurf der Kommission ist inzwischen durchgesickert. Doch die Regeln müssen ausgewogen sein. Weitere Hindernisse müssen beseitigt und Vertrauen geschaffen werden. Sonst droht eines der wichtigsten Datengesetze Europas sein Ziel zu verfehlen.

Anja Hoffmann

Das Erheben, Speichern und Verknüpfen von Daten ist zu einer ökonomischen Ressource geworden. Das wirtschaftliche Potenzial der Datenökonomie wird jedoch nicht ausgeschöpft, da Daten in der EU bislang nur begrenzt ausgetauscht und weiterverwendet werden. Die Kommission will am 23. Februar einen sogenannten Data Act vorschlagen, der den Datenaustausch in der EU erleichtern soll.

Der Data Act ist ein weiteres Puzzlestück der europäischen Datenstrategie und setzt damit den europäischen Ansatz zur Förderung der Datenwirtschaft fort. Er soll vor allem regeln, unter welchen Bedingungen und zu welchem Zweck Daten des Privatsektors an den Staat (Business to Government) weitergereicht und zwischen privaten Unternehmen (Business to Business) ausgetauscht werden können. Dies ist eine schwierige Aufgabe: Nutzungsrechte an Daten müssen angemessen verteilt und vergütet, Geschäftsgeheimnisse geschützt und Missbrauch verhindert werden. Der Data Act darf wichtige Fragen wie die Haftung nicht ausklammern. Zudem müssen weitere Hindernisse abgebaut werden, denen die Akteure der Datenwirtschaft derzeit ausgesetzt sind. Gelingt all dies nicht, droht der Data Act sein Ziel zu verfehlen, zum Beschleuniger der Digitalisierung zu werden.

Das cep hat die wesentlichen Punkte des Data Act auf der Basis des Inception Impact Assessment und der öffentlichen Konsultation der Kommission vorab herausgearbeitet und analysiert. Am 2. Februar 2022 ist ein ausformulierter Entwurf des Data Act an die Öffentlichkeit gelangt. Zu diesem „Leak“ findet sich in den nachfolgenden Kernpunkten eine ergänzende Kommentierung. Es zeigt sich: Die wesentlichen vom cep herausgearbeiteten Aspekte bleiben hochaktuell.

Die wichtigsten Regulierungsziele und kritischen Punkte:

- **Der Data Act will den Staat ermächtigen, Daten von Privatunternehmen für eigene Zwecke im öffentlichen Interesse zu nutzen**. Unter anderem soll in Krisensituationen wie einer Pandemie der Zugriff „schnell und unentgeltlich" ermöglicht werden. Die zulässigen Zwecke im öffentlichen Interesse müssen genau definiert werden, denn eine Datenteilungspflicht stellt einen erheblichen Eingriff in die Grundrechte der Unternehmen dar. Sie muss verhältnismäßig ausgestaltet und auf Situationen beschränkt werden, in denen eine freiwillige Kooperation oder sonstige alternative Beschaffung ausscheidet. Zudem muss ein Missbrauch durch den Staat verhindert und der Schutz von Daten und Geschäftsgeheimnissen auch bei der Weiterverarbeitung sichergestellt werden.

  Dass der Staat nach dem geleakten Entwurf über Krisenfälle hinaus auch dann generell dazu berechtigt werden soll, Daten anzufordern, wenn er ansonsten „rechtliche Pflichten nicht erfüllen" kann, ist als Zweck zu vage. Die Pflicht, „geeignete Maßnahmen" zum Schutz von Geschäftsgeheimnissen zu ergreifen, ist sachgerecht, aber ebenfalls zu unkonkret.

- **Der Data Act will den Austausch von Daten zwischen Unternehmen fördern.** Der Wettbewerb auf digitalen Märkten hängt wesentlich vom Zugang der Unternehmen zu Daten ab. Durch den Austausch von Daten entstehen wirtschaftliche Mehrwerte und datenbasierte Innovationen. Der Datenaustausch zwischen Unternehmen muss aber klar und ausgewogen geregelt werden. Die Vertragsfreiheit muss weitestmöglich erhalten bleiben; freiwillige Regeln und Musterklauseln sind daher vorzugswürdig. Angesichts sehr unterschiedlicher Probleme und Herausforderungen beim Austausch von Daten je nach Markt sollte die EU Datenteilungspflichten vorzugsweise sektorspezifisch regeln. Allgemeine Grundregeln im Data Act ermöglichen die einheitliche Ausübung solcher Pflichten und verhindern Fragmentierung. Mustervertragsklauseln und Regeln zur Unwirksamkeit von Klauseln können den freiwilligen Datenaustausch erleichtern.

  Ausweislich des geleakten Entwurfs sollen Hersteller von vernetzten Objekten wie intelligenten Haushaltsgeräten, Maschinen und Autos verpflichtet werden, privaten und geschäftlichen Nutzern dieser Objekte auf Anfrage die bei der Nutzung des Objekts erzeugten Daten bereitzustellen. Ob der Eingriff in die Vertragsfreiheit der Hersteller durch diese generelle Datenteilungspflicht verhältnismäßig ist, wurde noch nicht abschließend geprüft. Da durch diese Pflicht die Anreize für Hersteller vernetzter Objekte sinken, in die Objekte und die Generierung hochwertiger Daten zu investieren, könnte es aber sachgerecht sein, dass die Kommission diese negativen Effekte zumindest abmildert.

- **Um die Datenwirtschaft zu fördern, muss das Vertrauen in den Datenaustausch gestärkt werden. Ein Missbrauch der Daten muss verhindert werden; zudem darf der Data Act wichtige Fragen wie die Haftung für Datenmängel und andere Pflichtverletzungen nicht ausklammern**.

  Regelungen zur Datenqualität und Haftung sind gerade auch bei Datenteilungspflichten wichtig. An der Nutzung interessierte Dritte sind ebenso wie der Staat auf eine gute Datenqualität angewiesen. Um einen Missbrauch der Daten zu verhindern, regelt der geleakte Entwurf zahlreiche Nutzungsbeschränkungen für Weiterverwender wie das Verbot, die Daten zur Entwicklung von Konkurrenzprodukten zu nutzen. Offen bleibt aber, wie deren Einhaltung kontrolliert und durchgesetzt werden kann.

- **Die EU sollte maßgeblich (auch) den freiwilligen Datenaustausch fördern.** Regelungen und Anreize zum freiwilligen Datenaustausch fehlen mit Ausnahme der Festlegung missbräuchlicher Vertragsklauseln im geleakten Entwurf bislang völlig. Dass die Kommission Musterklauseln für Datenaustauschverträge erarbeiten will, die deren Abschluss erleichtern, ist sachgerecht.
- **Es müssen dringend weitere wirtschaftliche, technische und rechtliche Hindernisse für die Datenwirtschaft beseitigt werden,** damit Unternehmen ihre Daten tatsächlich teilen – z.B. mangelnde Interoperabilität oder die Rechtsunsicherheit, wie Daten DSGVO-konform geteilt werden können.

  Es ist daher sachgerecht, dass die Kommission laut dem geleakten Entwurf die Interoperabilität verbessern und dazu ein eigenes Kapitel im Data Act vorsehen will.
- **Die Kommission muss verhindern, dass der Data Act bestehende Unterschiede in den Verhandlungspositionen von Datengebern und Datennehmern verstärkt und somit – zumindest anfänglich – kontraproduktiv wirkt**. Diese Gefahr könnte drohen, wenn die Erleichterung des Datenaustauschs zunächst vor allem marktstarken Anbietern nutzt, die bereits über die nötigen Kompetenzen und Strukturen für die Nutzung von Daten verfügen, während kleinere Unternehmen faktisch und technisch noch nicht in der Lage sind, vom Datenaustausch zu profitieren.

  Dass Gatekeeper gemäß dem geleakten Entwurf nicht von der Datenteilungspflicht der Hersteller vernetzter Objekte profitieren dürfen, ist daher sachgerecht, vermutlich aber nicht ausreichend.
- **Der Data Act muss rechtssicher mit den anderen EU-Rechtsakten über Daten abgestimmt werden**, insbesondere mit dem Data Governance Act, der DSGVO, dem Digital Markets Act und speziellen Datennutzungsrechten in einschlägigen sektorspezifischen Rechtsvorschriften.
- **Die EU muss das Potenzial der Weiterverwendung von Daten heben, um im globalen Wettbewerb zu bestehen.** Der Data Act und ergänzende sektorspezifische Datennutzungsrechte müssen dafür die Grundlage schaffen. Sie sind entscheidend für den dringend nötigen Aufholprozess der europäischen Datenwirtschaft, der vor allem durch die Nutzbarmachung von Industriedaten gelingen kann. Nur durch die Entwicklung eigener datengetriebener Produkte und Dienstleistungen, die zugleich hohe Datenschutz-, Sicherheits- und Ethik-Standards wahren, kann die EU langfristig die Abhängigkeit von Produkten und Diensten aus Drittstaaten reduzieren und so verhindern, dass europäische Werte durch den Einsatz eingekaufter Technologie untergraben werden.
- Zu möglichen Details dieser und weiterer Regelungspunkte des Data Act wird auf die nachfolgenden Ausführungen verwiesen. Das cep wird die Entwicklungen rund um den Data Act weiter begleiten.

Inhaltsverzeichnis

Abbildungsverzeichnis

1 Einleitung

Gesellschaft und Wirtschaft befinden sich in einem tiefgreifenden Wandel. Digitale Technologien verändern unseren Alltag und führen dazu, dass weltweit immer mehr Daten produziert werden. Große Internetplattformen wie Google, Amazon, Facebook und Co. sammeln und kommerzialisieren Nutzerdaten. Maschinen, Haushaltsgeräte, „Wearables“, Industrieanlagen und Autos werden zunehmend mit Sensoren ausgerüstet und mit dem Internet vernetzt und liefern so ebenfalls Daten. Vernetzte Maschinen der Generation „Industrie 4.0“ und die von ihnen produzierten Güter kommunizieren sowohl untereinander als auch mit anderen Systemen und optimieren stetig ihre Abläufe, bestellen Bauteile oder planen Produktionsabläufe um. Auf diese Weise werden Produktion, Vertrieb, Entwicklung sowie Kunden und Lieferanten immer mehr miteinander vernetzt.[1] Aus solchen Daten können zudem physische Produkte und Systeme virtuell in „digitalen Zwillingen“ nachgebildet werden. Werden diese stetig mit neuen Betriebsdaten gefüttert, können mit Hilfe von Datenanalysen Ausfälle von Maschinen vorhergesagt und Ferndiagnosen ermöglicht werden. Auch lassen sich Veränderungen in der Produktion so virtuell simulieren.[2]

Im Jahr 2018 prognostizierte die Kommission einen Anstieg der weltweit produzierten Daten auf voraussichtlich 175 Zettabyte im Jahr 2025. Um diese Zahl begreiflich zu machen: Ein Zettabyte steht dabei in etwa für so viele Informationen, wie es Sandkörner an allen Stränden der Welt zusammen gibt.[3] Dieser stetig anwachsende Datenberg birgt angesichts verbesserter technischer Möglichkeiten zur Sammlung, Speicherung und Analyse von Daten ein großes wirtschaftliches Potential. Das Sammeln und Auswerten von Daten kann zum einen dazu beitragen, die gesellschaftlichen, klimapolitischen und umweltpolitischen Herausforderungen besser zu bewältigen. Zum anderen kann es Unternehmen helfen, effizienter zu produzieren und bessere Produkte und Dienstleistungen oder komplett neue, datengetriebene Geschäftsmodelle zu entwickeln und sich so Wettbewerbsvorteile zu verschaffen. Daten gelten daher als Quelle für Wachstum und Innovation und als „Lebensader“ der künftigen wirtschaftlichen Entwicklung[4]. Sie sind zu einem wichtigen Wirtschaftsgut geworden. Auch die Entwicklung von Anwendungen der künstlichen Intelligenz (KI) hängt massiv von der Verfügbarkeit von Daten ab. Digitale Daten sind oft nicht-rivalisierende Güter, d.h. sie verbrauchen sich bei ihrer Nutzung nicht und können mehrfach und von mehreren Nutzern verwendet werden, ohne an Wert zu verlieren.[5] Sie sind für die Wettbewerbsfähigkeit europäischer Unternehmen in der Datenwirtschaft der Zukunft – insbesondere mit Blick auf die starke Konkurrenz aus den USA und aus China – und damit für die digitale Souveränität der EU von zentraler Bedeutung.

In der EU werden Daten aber bislang viel zu wenig genutzt, auch weil viele Daten sich in den Händen weniger Unternehmen konzentrieren, die alleinigen Zugriff auf die Daten haben. Die EU will deshalb Daten in der EU besser nutzbar machen, um die Datenwirtschaft anzukurbeln und öffentliche Politiken und Dienstleistungen in der EU zu unterstützen.[6] Hierzu wird die Kommission am 23. Februar 2022[7]

---

1 https://www.wfb-bremen.de/de/page/stories/digitalisierung-industrie40/was-ist-industrie-40-eine-kurze-erklaerung

2 https://www.digital-bw.de/-/unternehmen-aus-baden-wurttemberg-setzen-auf-digitalen-zwilling; https://www.wfb-bremen.de/de/page/stories/digitalisierung-industrie40/was-ist-industrie-40-eine-kurze-erklaerung.

3 D’Cunha, C., European Commission, Vortrag im IIEA Webinar, The European Data Act: Harnessing the Value of Europe’s Data, aufgenommen am 13.12.2021, abrufbar unter https://www.youtube.com/watch?v=oOYGx-ES668.

4 EU-Kommission, Mitteilung [COM(2020) 66] vom 19.02.2020 – Eine europäische Datenstrategie (nachfolgend: „EU-Datenstrategie“], S. 3.

5 Eckhardt, P./Anzini, M. cepAnalyse 6/2021, S. 3.

6 Siehe auch Bertuzzi, L., LEAK: Draft impact assessment sheds some light on upcoming Data Act, 1. Nov. 2021, abrufbar unter https://www.euractiv.com/section/data-protection/news/leak-draft-impact-assessment-sheds-some-light-on-upcoming-data-act.

7 SEC(2021) 2401, S. 2, vgl. https://ec.europa.eu/transparency/documents-register/detail?ref=SEC(2021)2401&lang=en.

ihren lang erwarteten Vorschlag für einen „Data Act“[8] vorlegen, der voraussichtlich als Verordnung erlassen werden soll. Die ursprünglich für das vierte Quartal 2021 geplante[9] Veröffentlichung des Kommissionsvorschlags wurde verschoben, nachdem der Ausschuss für Regulierungskontrolle, ein Gremium, das die Folgenabschätzungen der Kommission für neue Legislativ-Vorschläge prüft[10], den Vorschlag am 27. Oktober 2021 abgelehnt hatte. Grund für diese Ablehnung soll laut Medienberichten[11] gewesen sein, dass der Data Act die Bedingungen für den Datenzugang, die korrespondierende Vergütung für Unternehmen sowie das Verhältnis des Data Act zu anderen EU-Rechtsakten noch nicht ausreichend regelte.

Zur Vorbereitung auf dieses neue, für die Datenwirtschaft wichtige EU-Gesetz stellt der vorliegende cep**Input** die Hintergründe und Ziele des Data Act (Kapitel 2) und seine möglichen Inhalte dar (Kapitel 3). Dabei stützt er sich insbesondere auf das Inception Impact Assessment[12] der Kommission vom 28. Mai 2021 (nachfolgend: „IIA“) sowie die von der Kommission im Frühsommer 2021 durchgeführte Konsultation[13] zum Data Act, die wichtige Anhaltspunkte dafür liefern, auf welche möglichen Regelungen im Data Act sich Unternehmen künftig einstellen müssen.[14] Der Fokus wird dabei auf die geplanten Regeln zur Förderung der Weiterverwendung von Daten des Privatsektors gelegt, die im Anschluss in einem eigenen Kapitel ausführlicher behandelt werden (Kapitel 4). Anschließend werden die Erkenntnisse zusammengefasst (Kapitel 5) und ein vorläufiges Fazit gezogen (Kapitel 6).

2 Was sind die Hintergründe und Ziele des Data Act?

2.1 Die Europäische Datenstrategie

Der Data Act ist ein weiterer wichtiger Baustein der Europäischen Datenstrategie[15], die darauf abzielt, die EU zu einem Vorreiter in der datenbasierten Gesellschaft zu machen.[16] Um dies zu erreichen, will die EU-Kommission einen einheitlichen europäischen Datenraum für personenbezogene und nichtpersonenbezogene sowie öffentliche Daten[17] und Geschäftsdaten schaffen und den Austausch, die Nutzung und die Weiterverwendung von Daten in der EU fördern. Ziel ist, dass mehr öffentliche und private Akteure von Techniken wie Big Data und maschinellem Lernen profitieren können.[18] Gleichzeitig will die Kommission ein vertrauenswürdiges Umfeld für die gemeinsame Nutzung, Verwendung und Weiterverwendung sowie den Austausch von Daten in der EU schaffen und dadurch Innovationen und Wachstum fördern.[19] Im so geschaffenen „Binnenmarkt für Daten“[20] sollen Daten innerhalb der EU frei

---

8 Die Kommission kündigte den Data Act bereits in der Datenstrategie an, vgl. dort (Fn. 4), S. 15.

9 EU-Kommission, Inception Impact Assessment (nachfolgend: “IIA”) vom 28.05.2021, Ref. Ares(2021)3527151, S. 1.

10 https://ec.europa.eu/info/law/law-making-process/regulatory-scrutiny-board_de.

11 Bertuzzi, L., a.a.O. (Fn. 6).

12 IIA, a.a.O. (Fn. 9), S. 2.

13 Europäische Kommission, Public consultation on the Data Act (nachfolgend: „Konsultation“), abrufbar unter https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13045-Data-Act-including-the-review-of-the-Directive-96-9-EC-on-the-legal-protection-of-databases-/public-consultation_en.

14 Am 2. Februar 2022 ist ein Entwurf des Data Act an Teile der Öffentlichkeit gelangt, vgl. https://www.euractiv.de/section/innovation/news/leak-kommissionsvorschlaege-zum-eu-data-act/. Dieser „Leak“ wurde noch auf S. 2 und 3 berücksichtigt. Es zeigt sich: Die im nachfolgenden Haupttext herausgearbeiteten Aspekte bleiben hochaktuell.

15 EU-Datenstrategie, a.a.O. (Fn. 4).

16 https://ec.europa.eu/commission/presscorner/detail/de/ip_20_273. Näher zur EU-Datenstrategie cep**Analysen** Nr. 2020-7 und 2020-8] sowie https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/european-data-strategy_en.

17 Öffentliche Daten (public data) sind Daten, die keinen gültigen Datenschutz, Sicherheits- oder Zugangsbeschränkungen unterliegen, vgl. Marti, E./Marinelli, E./Plaud, S./Quinquilla, A./Massucci, F., Open Data, Open Science & Open Innovation for Smart Specialisation monitoring, S. 9, abrufbar unter https://publications.jrc.ec.europa.eu/repository/handle/JRC119687.

18 IIA, a.a.O. (Fn. 9), S. 1, siehe bereits EU-Kommission, Mitteilung „Aufbau eines gemeinsamen europäischen Datenraums“ vom 25.04.2018, COM(2018) 232, S. 1.

19 cep**Analyse** Nr. 2020-7 zur EU-Datenstrategie – Teil 1, S. 1; EU-Datenstrategie, a.a.O. (Fn. 4), S. 5-7.

20 EU-Datenstrategie, a.a.O. (Fn. 4), S. 5, 7, 13.

und sektorübergreifend zum Nutzen von Unternehmen, Forschern und öffentlichen Verwaltungen fließen können.[21]

Die europäische Datenstrategie ist ebenso wie auch das Weißbuch zur künstlichen Intelligenz[22] Teil der übergeordneten EU-Digitalstrategie.[23] Die EU will damit ihren eigenen, europäischen Weg finden, um den Austausch und die Nutzung von Daten zu erleichtern und gleichzeitig hohe Datenschutz-, Sicherheits- und Ethik-Standards zu wahren.[24] Dies ist wichtig, denn die Datenwirtschaft in der EU hinkt derjenigen in den USA und in China seit Jahren hinterher.[25] In den USA wird die Datenwirtschaft vor allem von dienstleistungs- und datenbasierten Technologieunternehmen wie Google, Amazon, Facebook und Co. vorangetrieben[26], die massenhaft Daten ihrer Nutzer abschöpfen und monetarisieren. Auch in China entstehen immer mehr große Technologieunternehmen, die riesige Datenmengen kontrollieren.[27] Zudem fördern die USA und China gezielt Big-Data-Anwendungen, um einheimischen Unternehmen Wettbewerbsvorteile zu sichern.[28] Treiber der Datenwirtschaft in der EU, wo es an vergleichbar großen Plattformen fehlt, waren dagegen ursprünglich in erster Linie Teile der Fertigungsindustrie.[29]

Die Maßnahmen der EU-Datenstrategie sind auf vier strategische Prioritäten ausgerichtet:

Säule 1: Schaffung eines sektorübergreifenden **Governance-Rahmens** für den Zugang zu und die Nutzung von Daten. Die Kommission will einen europäischen Datenraum schaffen.

Säule 2: Förderung von **Investitionen** in Daten und Dateninfrastrukturen

Säule 3: Stärkung der **Kontrolle des Einzelnen über seine Daten**, Förderung von Investitionen in digitale Kompetenzen und in KMU

Säule 4: Schaffung **gemeinsamer europäischer Datenräume** in verschiedenen strategischen Sektoren und Gesellschaftsbereichen von öffentlichem Interesse. Zwar sind Daten überall von großer Bedeutung; jeder Wirtschaftszweig oder Bereich hat aber seine eigenen Besonderheiten, und nicht alle bewegen sich im gleichen Tempo. Die EU will zunächst in den Sektoren Industrie, Green Deal, Mobilität, Gesundheit, Finanzen, Energie, Agrarwirtschaft, öffentliche Verwaltung und Kompetenzen gemeinsame sektorspezifische Datenräume schaffen.[30]

Der Data Act soll bestehende europäische Maßnahmen im Rahmen der EU-Datenstrategie ergänzen[31] und betrifft insbesondere die Säulen 1 und 3 der europäischen Datenstrategie (vgl. Abbildung 1). Der Europäische Rat hat die Kommission in seinen Schlussfolgerungen vom Oktober 2021 aufgefordert, schnellstmöglich einen umfassenden, innovationsfreundlichen Regelungsrahmen vorzuschlagen, der das Datenpotenzial in Europa ausschöpft und eine bessere Datenübertragbarkeit und einen fairen Zugang zu Daten ermöglicht und Interoperabilität gewährleistet.[32]

---

21 https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/european-data-strategy_en.

22 COM(2020) 65; näher dazu cep**Analyse** Nr. 4/2020 – Weißbuch für künstliche Intelligenz.

23 Mitteilung COM(2020) 76 der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen vom 19.02.2020, Gestaltung der digitalen Zukunft Europas, abrufbar unter https://eur-lex.europa.eu/legal-content/DE/ALL/?uri=COM:2020:67:FIN.

24 EU-Datenstrategie, a.a.O., S. 4.

25 So bereits Dassis, G., Stellungnahme des Europäischen Wirtschafts- und Sozialausschusses zur Mitteilung (EU) COM(2017) 9, 5. Juli 2017, Ziffer 2.10.

26 Dassis, G., a.a.O., Ziffer 2.10.

27 EU-Datenstrategie, a.a.O., S. 4, Dassis, G., a.a.O., Ziffer 2.10.

28 Dassis, G., a.a.O., Ziffer 2.11.

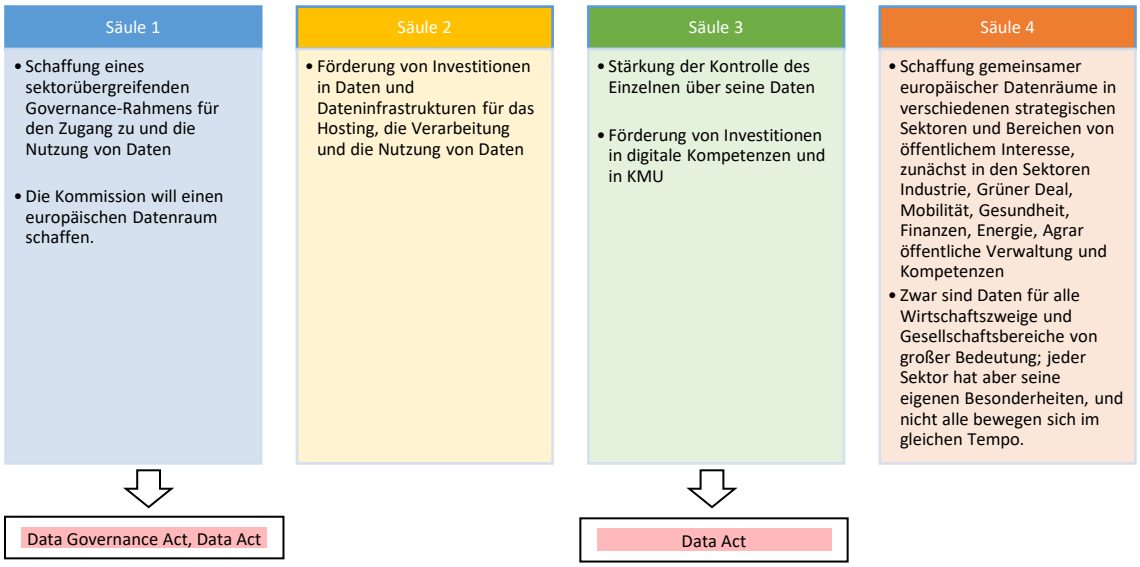
29 Die digitale Transformation der Industrie, Studie im Auftrag des Bundesverbands der Deutschen Industrie, 01.02.2015.

30 EU-Datenstrategie, S. 30ff. Siehe dazu auch cepAnalyse 2020-8 zur EU-Datenstrategie, Teil 2.

31 EU-Datenstrategie, a.a.O., S. 15f.

32 Europäischer Rat, Schlussfolgerung der Tagung vom 21./22. Oktober 2021, EUCO 17/21, Ziffer 8, abrufbar unter https://www.consilium.europa.eu/media/52636/20211022-euco-conclusions-de.pdf.

Abb. 1: Die vier strategischen Prioritäten der EU-Datenstrategie



Quelle: cep auf der Basis von Informationen der EU-Kommission [COM(2020) 66]

2.2 Das Zusammenspiel des Data Act mit bestehenden EU-Rechtsakten

2.2.1 Horizontale EU-Rechtsakte

Bislang hat die EU im Rahmen ihrer Datenstrategie insbesondere folgende horizontale EU-Rechtsakte erlassen bzw. auf den Weg gebracht, die grundsätzlich für alle Wirtschaftssektoren gelten:

- die Richtlinie (EU) Nr. 2019/1024 über offene Daten und die Weiterverwendung von Informationen des öffentlichen Sektors (engl. „public sector information", nachfolgend „**PSI-Richtlinie**"[33], die die Weiterverwendung von Daten fördern soll, die sich im Besitz von Behörden und öffentlichen Unternehmen befinden;[34]
- die vorgeschlagene Verordnung COM(2020) 767 über europäische Daten-Governance (Daten-Governance-Gesetz, nachfolgend: „**Data Governance Act**"[35]. Der Data Governance Act soll zum einen die Weiterverwendung bestimmter, von der PSI-Richtlinie nicht erfasster Daten im Besitz des öffentlichen Sektors sowie freiwillige Datenspenden zu „altruistischen", d.h. gemeinwohldienlichen Zwecken fördern. Vor allem aber führt er neue Rechtsregeln für Datenvermittlungsdienste (Datenintermediäre) ein, das sind neutrale Dienste, die den Austausch oder die gemeinsame Nutzung von Daten ermöglichen oder erleichtern sollen;
- die vorgeschlagene Verordnung COM (2020) 842 über bestreitbare und faire Märkte im digitalen Sektor [Gesetz über digitale Märkte, nachfolgend: **Digital Markets Act** (DMA)][36], die verschiedene

[33] 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.

[34] Zu den Details siehe Van Roosebeke, B./Anzini, M./Eckhardt, P./Pierrat, A., cep**Study** "European Leadership in the Digital Economy, 2020, S. 25ff.

[35] Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates vom 25.11.2020 über europäische Daten-Governance (Daten-Governance-Gesetz), COM(2020) 767, näher dazu cep**Analyse** Nr. 6/2021. Am 10. Dezember 2021 haben sich Rat und Europäisches Parlament im Gesetzgebungsverfahren im sogenannten TRILOG-Verfahren auf einen Kompromisstext zum DGA geeinigt (Ratsdokument 14606/21). Dieser Kompromisstext ist abrufbar unter: https://data.consilium.europa.eu/doc/document/ST-14606-2021-INIT/en/pdf.

[36] Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates vom 15.12.2020 über bestreitbare und faire Märkte im digitalen Sektor (Gesetz über digitale Märkte), COM(2020) 842. Näher zum DMA siehe cep**Input** Nr. 12/2021, cep**Analyse** Nr. 14/2021 und Nr. 15/2021.

Datenkombinierungsverbote und Datenportabilitätspflichten für besonders marktmächtige „Gatekeeper-Plattformen“ vorsieht. Solche Plattformen dürfen personenbezogene Daten aus ihren unterschiedlichen Diensten nicht ohne Einwilligung der Endnutzer kombinieren.[37] Ferner soll der DMA Gatekeeper u.a. dazu verpflichten, Endnutzern die Übertragung der durch die Nutzung ihrer zentralen Plattformdienste erzeugten Daten permanent und in Echtzeit zu ermöglichen und ihnen die hierzu erforderlichen Instrumente (d.h. einen permanenten Echtzeitzugang) bereitzustellen.[38] Schließlich sollen Gatekeeper gewerblichen Nutzern gratis einen permanenten Echtzeitzugang zu Daten gewähren, die von ihnen oder ihren Endnutzern generiert oder bereitgestellt wurden, und ihnen die Nutzung dieser Daten ermöglichen müssen.[39]

Neben der PSI-Richtlinie, dem Data Governance Act und der Digital Markets Act sind die geltenden allgemeinen EU-Vorschriften zum Schutz personenbezogener Daten und der Privatsphäre[40] sowie zum freien Verkehr nicht-personenbezogener Daten von wesentlicher Bedeutung. Die Weiterverwendung von Daten auch unter dem Data Act muss mit diesen Regelungen in Einklang stehen, namentlich mit

- der **Datenschutzgrundverordnung** (EU) 2016/679 (DSGVO)[41], die natürliche Personen bei der Verarbeitung ihrer personenbezogener Daten schützt und den freien Verkehr dieser Daten sicherstellt;
- der Verordnung (EU) 2018/1807 über einen Rahmen für den freien Verkehr nicht-personenbezogener Daten[42] [**Free Flow of Data-Verordnung** (FFD-VO)], und
- der Datenschutzrichtlinie 2002/58/EG für elektronische Kommunikation („**E-Privacy-Richtlinie**“)[43], die den Austausch personenbezogener Daten und anderer Informationen über öffentliche elektronische Kommunikationsdienste und -netze regelt. Ergänzend zur DSGVO sieht die E-Privacy-Richtlinie spezielle Garantien zur Gewährleistung des Rechts auf Privatsphäre vor und schützt die Endnutzer vor Cookies und SPAM. Sie soll durch die vorgeschlagene „E-Privacy-Verordnung“ über Privatsphäre und elektronische Kommunikation ersetzt werden, die sich noch immer im Gesetzgebungsprozess befindet.[44]

---

37 Art. 5 lit. a) des Kommissionsvorschlags zum DMA [COM (2020) 842].

38 Art. 6 Abs. 1 lit. h) des Kommissionsvorschlags zum DMA [COM (2020) 842].

39 Art. 6 Abs. 1 lit. i) des Kommissionsvorschlags zum DMA [COM (2020) 842].

40 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), konsolidierte Fassung abrufbar unter https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A02016R0679-20160504.

41 Weitere relevante Vorschriften sind die Datenschutzrichtlinie (EU)2016/680 für Polizei und Justiz sowie die Verordnung EG Nr. 45/2001, die hier aus Platzgründen nicht näher erwähnt werden. Näher dazu cep**Studie** EU-Datenschutzrecht, S. 23 ff., abrufbar unter https://www.cep.eu/eu-themen/details/cep/eu-datenschutzrecht.html.

42 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, abrufbar unter https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32018R1807.

43 Richtlinie [2002/58/EG] über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation), ABl. L 201 vom 31.07.2002, S. 37ff.; letzte konsolidierte Fassung abrufbar unter https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A02002L0058-20091219.

44 COM(2017) 10, vgl. cep**Analyse** Nr. 16/2017.

- Daneben können auch die EU-**Richtlinie über Geschäftsgeheimnisse**[45], die **EU-Datenbankrichtlinie**[46] sowie die übrigen **EU-Rechtsvorschriften zum Schutz des geistigen Eigentums**[47] ggf. einer Weiterverwendung von Daten entgegenstehen.

Laut Kommission wird der Data Act die bestehenden Datenschutzvorschriften nicht ändern.[48] Vielmehr soll er bestehende Gesetze wie die DSGVO, die E-Privacy-Richtlinie und die Richtlinie über Geschäftsgeheimnisse in vollem Umfang achten.[49]

2.2.2 Vertikale oder sektorspezifische EU-Rechtsakte

Neben den genannten horizontalen Regelungen enthalten zahlreiche bereichsspezifische Rechtsakte auf EU-Ebene relevante Regelungen für die Datenwirtschaft. Das sind beispielsweise

- im Bereich **Umweltpolitik**
  - die *INSPIRE-Richtlinie* 2007/2/EG, die allgemeine Bestimmungen zur Schaffung einer Geodaten-Infrastruktur in Europa für die Zwecke der Umweltpolitik der Europäischen Union (EU) und anderer umweltrelevanter politischer Maßnahmen festlegt und die Mitgliedstaaten verpflichtet, bestimmte Geodatensätze über Netzdienste bereitzustellen;
  - die *Umweltinformationsrichtlinie* 2003/4/EG, die die Mitgliedstaaten verpflichtet, der Öffentlichkeit Zugang zu behördlichen Umweltinformationen zu verschaffen;
  - die *EU-Chemikalienverordnung* (EG) Nr. 1907/2006 (REACH-Verordnung)[50], die u.a. künftige Registranten chemischer Stoffe berechtigt, bestehende Informationen von früheren Registranten anzufordern, um wiederholte Versuche an Wirbeltieren zu vermeiden, und die die Parteien verpflichtet, sich nach besten Kräften um eine Nutzungsvereinbarung bezüglich der Informationen und um eine gerechte Verteilung der Kosten zu bemühen;[51]
- im Bereich **Verkehr** die *EU-Typgenehmigungsverordnung* (EU) 2018/858[52] über die Genehmigung und die Marktüberwachung von Kraftfahrzeugen und Kraftfahrzeuganhängern, die die Hersteller verpflichtet, unabhängigen Wirtschaftsakteuren uneingeschränkten, standardisierten und diskriminierungsfreien Zugang zu On-Board-Diagnose (OBD)-Informationen von Fahrzeugen sowie zu Fahrzeugreparatur- und -wartungsinformationen zu gewähren;

---

45 Richtlinie (EU) 2016/943 des Europäischen Parlaments und des Rates vom 8. Juni 2016 über den Schutz vertraulichen Know-hows und vertraulicher Geschäftsinformationen (Geschäftsgeheimnisse) vor rechtswidrigem Erwerb sowie rechtswidriger Nutzung und Offenlegung, ABl. L 157 vom 15.06.2016, S. 1ff. Näher dazu unten Kap. 3.2.4.

46 Richtlinie 96/9/EG des Europäischen Parlaments und des Rates vom 11. März 1996 über den rechtlichen Schutz von Datenbanken, konsolidierte Fassung abrufbar unter https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:01996L0009-20190606&from=EN. Näher dazu unten Kap. 3.2.3 und 4.3.

47 Dazu gehören etwa das Urheberrecht, das Markenrecht oder das Patentrecht. Die hier möglicherweise relevanten Vorschriften können an dieser Stelle aufgrund ihrer Vielzahl nicht näher dargestellt werden.

48 Summary Report of the public consultation, Ref. ARES(2021)7509117 vom 06.12.2021, abrufbar unter https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13045-Data-Act-including-the-review-of-the-Directive-96-9-EC-on-the-legal-protection-of-databases-/public-consultation_en, S. 1.

49 IIA, S. 4.

50 Verordnung (EG) Nr. 1907/2006 des Europäischen Parlaments und des Rates vom 18. Dezember 2006 zur Registrierung, Bewertung, Zulassung und Beschränkung chemischer Stoffe (REACH), zur Schaffung einer Europäischen Chemikalienagentur, zur Änderung der Richtlinie 1999/45/EG und zur Aufhebung der Verordnung (EWG) Nr. 793/93 des Rates, der Verordnung (EG) Nr. 1488/94 der Kommission, der Richtlinie 76/769/EWG des Rates sowie der Richtlinien 91/155/EWG, 93/67/EWG, 93/105/EG und 2000/21/EG der Kommission, ABl. L 396 vom 30.12.2006, S. 1ff.

51 Art. 27 REACH-Verordnung (a.a.O.).

52 Verordnung (EU) 2018/858 des Europäischen Parlaments und des Rates vom 30. Mai 2018 über die Genehmigung und die Marktüberwachung von Kraftfahrzeugen und Kraftfahrzeuganhängern sowie von Systemen, Bauteilen und selbstständigen technischen Einheiten für diese Fahrzeuge, zur Änderung der Verordnungen (EG) Nr. 715/2007 („Euro-5-6-Verordnung“) und (EG) Nr. 595/2009 („Euro VI-Verordnung“) und zur Aufhebung der Richtlinie 2007/46/EG.

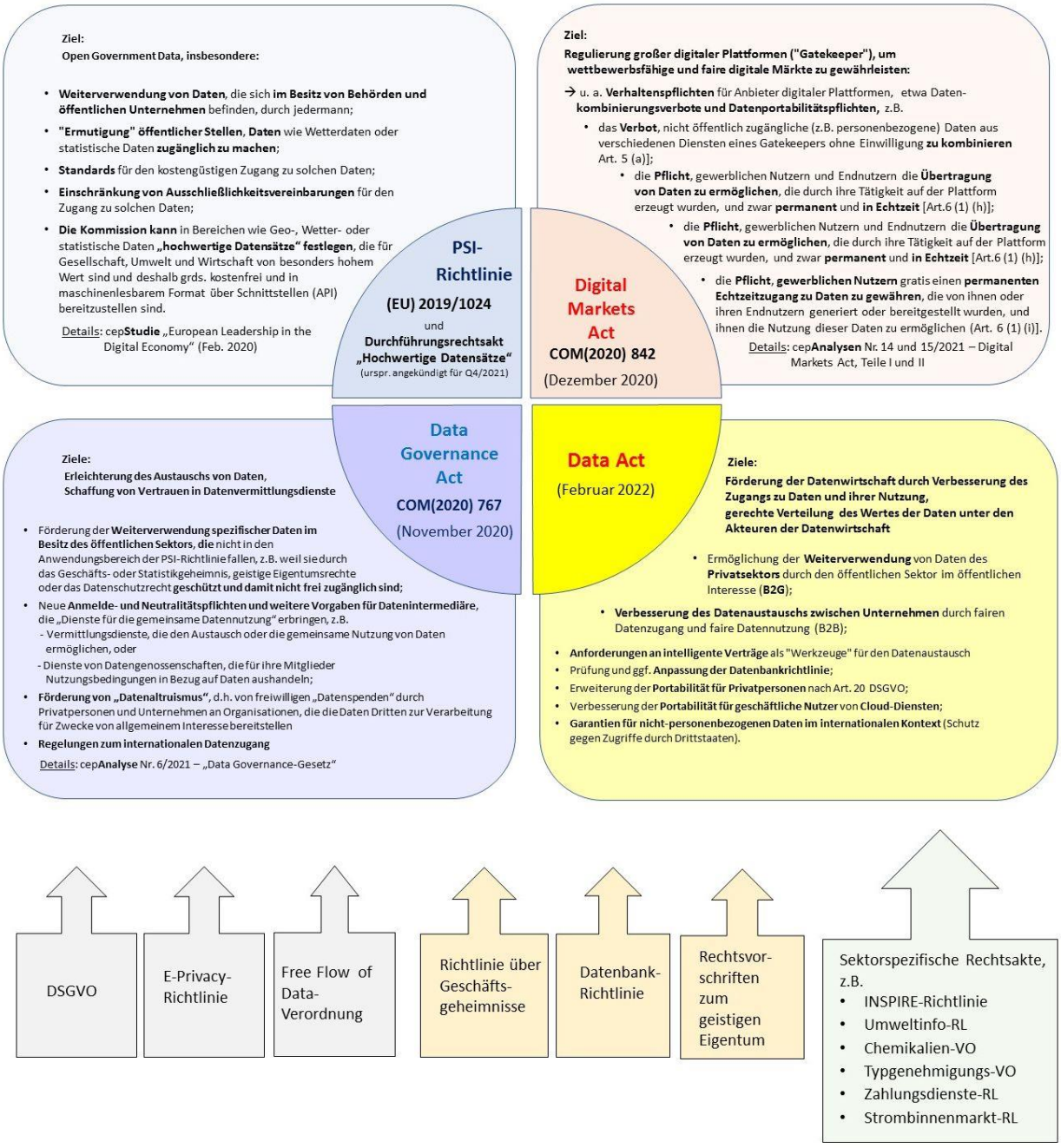
- im Bereich **Finanzen** die zweite EU-*Zahlungsdiensterichtlinie* (EU) 2015/2366[53], nach der Banken Zahlungsdienstleistern auf Wunsch der Kunden Zugang zu deren Bankkontodaten gewähren müssen;
- Im Bereich **Energie** regeln mehrere Richtlinien den Zugang der Verbraucher zu Zähler- und Energieverbrauchsdaten und deren Übertragbarkeit auf transparente, diskriminierungsfreie Weise.[54] So verpflichtet etwa die *Strombinnenmarktrichtlinie* (EU) 2019/944[55] die Mitgliedstaaten, berechtigten Parteien diskriminierungsfreien Zugang zu intelligenten Messdaten (Smart-Metering-Daten) der Endkunden zu verschaffen und Regeln und Verfahren für den Datenaustausch zwischen Elektrizitätsunternehmen (Stromnetzbetreibern) vorzusehen.

[53] Richtlinie (EU) 2015/2366 des Europäischen Parlaments und des Rates vom 25. November 2015 über Zahlungsdienste im Binnenmarkt, zur Änderung der Richtlinien 2002/65/EG, 2009/110/EGund 2013/36/EU und der Verordnung (EU) Nr. 1093/2010 sowie zur Aufhebung der Richtlinie2007/64/EG, konsolidierte Fassung siehe ABl. Nr. L2366 vom 23.12.2015, S. 1ff., näher dazu cepAnalyse Nr. 10/2014.

[54] EU-Datenstrategie, a.a.O. (Fn. 4), S. 36.

[55] Richtlinie (EU) 2019/944 des Europäischen Parlaments und des Rates vom 05. Juni 2019 mit gemeinsamen Vorschriften für den Elektrizitätsbinnenmarkt und zur Änderung der Richtlinie 2012/27/EU.

Abb. 2: Überblick über das Zusammenspiel der relevanten Rechtsakte



Quelle: cep auf der Basis der in der Grafik genannten Dokumente der EU-Kommission sowie des Inception Impact Assessment zum Data Act [Ares(2021)3527151 - 28/05/2021] [56]

2.3 Ziele des Data Act

Übergeordnetes Ziel des Data Act ist es, mehr Daten nutzbar zu machen, um die Datenwirtschaft in der EU zu fördern und öffentliche Politiken und Dienstleistungen zu unterstützen.[56] Während der Data Governance Act mit seinen Regeln für Datenvermittlungsdienste und datenaltruistische Organisationen einen Beitrag dazu leistet, die nötige *Architektur* für die freiwillige Weitergabe und gemeinsame

[56] Siehe auch Bertuzzi, L., a.a.O. (Fn. 6).

Nutzung von Daten zu schaffen, geht es beim Data Act insbesondere darum, den *Zugang* zu Daten und ihre faire gemeinsame Nutzung sicherzustellen. Der Data Act soll den Zugang zu Daten und deren Nutzung fördern und die gerechte Verteilung des Wertes der Daten unter den Akteuren der Datenwirtschaft sicherstellen.[57] Anders als die PSI-Richtlinie und der Data Governance Act, die die Weiterverwendung von Daten im Besitz des öffentlichen Sektors fördern sollen, zielt der Data Act darauf ab, Daten im Besitz der Privatwirtschaft für andere Unternehmen, für private Besitzer vernetzter Geräte und für den öffentlichen Sektor nutzbar zu machen.

Der Data Act soll damit maßgeblich

- den Datenaustausch zwischen Unternehmen und dem öffentlichen Sektor (business to government, **B2G**) einerseits,
- die Portabilität von Daten privater Nutzer (**B2C**) und
- den Datenaustausch zwischen Unternehmen (business to business, **B2B**) andererseits fördern.

3 Was wird der Data Act im Detail regeln?

Was der Data Act im Detail regeln wird, ist noch offen; aus dem Inception Impact Assessment[58] und der von der Kommission durchgeführten Konsultation[59] ergeben sich aber zahlreiche Hinweise. In Kapitel 3.1 listen wir die möglichen Regelungen im Data Act überblicksweise auf. Im Anschluss hieran werden in Kapitel 3.2. die bekannt gewordenen Details zu den einzelnen Politikoptionen des Data Act zusammengefasst. Kapitel 4 befasst sich sodann näher mit ausgewählten Regelungskomplexen.

3.1 Überblick

Der Data Act könnte insbesondere – alternativ oder kumulativ[60] – Folgendes enthalten:

- Regelungen zur Weiterverwendung von Daten des Privatsektors durch den öffentlichen Sektor im öffentlichen Interesse (B2G, näher dazu Kapitel 3.2.1);
- Regelungen zur Verbesserung des „fairen“ Datenaustauschs zwischen Unternehmen (B2B, näher dazu Kapitel 3.2.2);
- Transparenzpflichten zur Klarstellung der Rechte an nicht-personenbezogenen Daten, die aus der beruflichen Nutzung von Gegenständen des Internets der Dinge stammen (Kapitel 3.2.2);
- Regelungen zur Anpassung der EU-Datenbankrichtlinie (Kapitel 3.2.3);
- Aussagen zur Anwendbarkeit der Richtlinie über Geschäftsgeheimnisse auf die Datenwirtschaft (Kapitel 3.2.4);
- Regelungen zur Verbesserung der Portabilität für Privatpersonen nach Art. 20 DSGVO (Kapitel 3.2.5);
- Regelungen zur Verbesserung der Portabilität für geschäftliche Nutzer von Cloud-Diensten (Kapitel 3.2.6);
- Regelungen zur Nutzung intelligenter Verträge als „Werkzeuge“ für den Datenaustausch (Kapitel 3.2.7);
- Regelungen für den internationalen Transfer nicht-personenbezogenen Daten zum Schutz gegen Zugriffe durch Drittstaaten (Kapitel 3.2.8).

---

[57] Summary Report of the public consultation, a.a.O. (Fn. 48), S. 1.
[58] IIA, a.a.O. (Fn. 9), S. 2.
[59] Konsultation, a.a.O. (Fn. 13).
[60] Laut dem IIA, a.a.O. (Fn. 9), S. 5, schließen die genannten Politikoptionen einander nicht aus.

3.2 Mögliche Politikoptionen zur Förderung des Datenaustauschs

3.2.1 Bessere Nutzung privater Unternehmensdaten durch den öffentlichen Sektor im öffentlichen Interesse („B2G“):

3.2.1.1 Hintergrund

Der Zugang zu Daten des privaten Sektors kann den Behörden in der EU wertvolle Erkenntnisse liefern, um zum Beispiel den öffentlichen Verkehr zu verbessern, Städte umweltfreundlicher zu gestalten, Epidemien zu bekämpfen und politische Entscheidungen – z.B. in Bezug auf Plattformen – stärker auf Fakten stützen zu können.[61] Um dies zu ermöglichen, will die Kommission dem öffentlichen Sektor die Weiterverwendung bestimmter Daten – einschließlich Massendaten (Big Data)[62] – erleichtern, die sich in der Hand privater Unternehmen befinden. Im Fokus stehen Daten, die für „innovative Nutzungen“, für die digitale Transformation der Erbringung öffentlicher Dienstleistungen und für eine bessere politische Entscheidungsfindung und Politikgestaltung wertvoll sein können, und an deren Verwendung daher laut Kommission ein öffentliches Interesse besteht.[63]

Trotz ihres potenziellen Nutzens für die Allgemeinheit kann der öffentliche Sektor das Potenzial privater Unternehmensdaten laut Kommission derzeit nicht oder nur eingeschränkt nutzen, z.B. um eigene Datenmodelle zu entwickeln. Ein Grund hierfür sei, dass es an Regeln für einen verlässlichen Transfer von Daten aus der Wirtschaft an öffentliche Stellen („business to government, B2G“) fehle. Die Nutzung privater Daten durch die öffentliche Hand sei in den einzelnen Sektoren und den Mitgliedstaaten uneinheitlich geregelt. Insbesondere in unvorhersehbaren Notfällen wie Naturkatastrophen oder Pandemien, in denen die Beschaffung von Daten besonders schwierig sei, weil regelmäßige Meldepflichten zu belastend und eine marktbasierte Beschaffung zu langsam wäre, würden Daten bislang nur selten verwendet. Zudem hinderten wirtschaftliche Erwägungen die gemeinsame Nutzung solcher Daten, weil diese nicht nur hohe Anfangsinvestitionen erfordere, sondern auch das nachträgliche Risiko von Datenschutzverstößen berge. Dies führe dazu, dass Unternehmen ihre Daten daher nicht frei zur Verfügung stellten, sondern es vorzögen, Datendienste an den öffentlichen Sektor zu vermarkten.[64]

3.2.1.2 Mögliche Regelungen im Data Act

Der Data Act soll daher einen neuen, „flexibleren“ Rechtsrahmen für den Zugang zu Daten des Privatsektors und deren Nutzung durch die öffentliche Hand einführen.[65] Behörden sollen bestimmte Daten privater Unternehmen „im öffentlichen Interesse“ nutzen dürfen, um stärker faktengestützt und evidenzbasiert agieren und damit u.a. effizientere öffentliche Dienstleistungen anbieten und bessere politische Entscheidungen treffen zu können. Die Kommission folgt damit der Empfehlung der von ihr eingesetzten „High Level Expert Group on Business-to-Government Data Sharing“, ein Mindestmaß an Harmonisierung für B2G-Datenaustauschprozesse zu schaffen, um Klarheit und Rechtssicherheit zu gewährleisten.[66]

---

61 Konsultation, a.a.O. (Fn. 13), S. 8; siehe auch EU-Datenstrategie, a.a.O. (Fn. 4), S. 9.

62 Unter Big Data versteht man große Datenmengen, die sehr schnell von einer Vielzahl unterschiedlicher Quellen, z.B. Menschen oder Maschinen mit Sensoren erzeugt werden, vgl. https://digital-strategy.ec.europa.eu/en/policies/big-data.

63 IIA, a.a.O. (Fn. 9), S. 2, 4, 7.

64 IIA, a.a.O. (Fn. 9), S. 2.

65 IIA, a.a.O. (Fn. 9), S. 5.

66 Konsultation, a.a.O. (Fn. 13), S. 8. Bereits die von der Kommission eingesetzte High Level Expert Group on Business-to-Government Data Sharing hatte in ihrem finalen Bericht 2020 der Kommission die Schaffung eines EU-Rechtsrahmens empfohlen, der ein Mindestmaß an Harmonisierung für B2G-Datenaustauschprozesse schafft, vgl. https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=64954, S. 3.

Der Data Act wird daher möglicherweise u.a. Folgendes regeln[67]:

- **die Ziele und die allgemeinen Pflichten für die Beschaffung und Weiterverwendung von Daten des Privatsektors durch die öffentliche Hand im öffentlichen Interesse**,
- möglicherweise „als schärfstes Mittel" auch **eine Pflicht für Unternehmen, öffentlichen Stellen Zugang zu bestimmten Daten zu gewähren und ihnen deren Nutzung zu ermöglichen, bzw. ein korrespondierendes Recht für öffentliche Stellen, im Privatbesitz befindliche Daten für bestimmte, näher definierte Zwecke des öffentlichen Interesses zu nutzen**[68],
- **Transparenzpflichten für öffentliche Stellen, wie sie die Daten weiterverwenden,** und
- **Schutzmaßnahmen für den Datenaustausch.**

Welche genauen Regelungen zum B2G-Data-Sharing sich hinter den genannten Politikoptionen im Einzelnen verbergen könnten, stellen wir in Kapitel 4.1 näher dar.

3.2.2 Besserer Datenaustausch innerhalb des Privatsektors durch fairen Datenzugang und faire Datennutzung – insbesondere bei IoT-Daten („B2B")

3.2.2.1 Hintergrund

Darüber hinaus will die Kommission auch den Datenaustausch und die Weiterverwendung von Daten zwischen privaten Unternehmen (business to business, „B2B") fördern. Um neue Produkte oder Dienstleistungen entwickeln zu können, sind Unternehmen in der digitalen Wirtschaft auf relevante Daten angewiesen. Deshalb will die Kommission insbesondere für Start-ups und KMU[69], die oft noch nicht selbst über die nötigen Daten verfügen, den Zugang zu Daten anderer Unternehmen erleichtern. In der Praxis vereinbaren Unternehmen die Bedingungen für den Zugang zu Daten und für ihre weitere Nutzung untereinander üblicherweise in privaten Verträgen (Datenlizenzverträgen), weil es an gesetzlichen Eigentumsrechten für Daten fehlt.[70] Ist die Verhandlungsposition des Datenlizenzgebers ungleich stärker, kann dies den Austausch der Daten erschweren.

Um den Datenaustausch anzukurbeln, will die Kommission Unternehmen daher den Abschluss fairer Datenaustauschverträge erleichtern. Verträge über den Zugang zu und die gemeinsame Nutzung von Daten sollen für beide Seiten fair sein und im Einklang mit dem Wettbewerbsrecht stehen. Auf diese Weise sollen Datennutzungsrechte in industriellen Wertschöpfungsketten gerecht verteilt werden.

Ungleiche Verhandlungspositionen können unter anderem den Zugang zu gemeinsam erzeugten IoT-Daten aus dem industriellen Umfeld erschweren.[71] Auf diese Daten legt der Data Act einen besonderen Fokus. Konkret geht es dabei um nicht-personenbezogene Daten, die von vernetzten IoT-Objekten erzeugt werden – das sind mit dem Internet der Dinge (Internet of Things, IoT) verbundene intelligente Objekte wie Industrieroboter, Werkzeugmaschinen mit Sensoren, Baumaschinen oder intelligente landwirtschaftliche Maschinen. Obwohl mehrere Akteure „gemeinsam" zur Erzeugung dieser Daten beitragen (z.B. der Hersteller des IoT-Geräts, der Nutzer des Geräts oder dessen Kunde), werden die Daten faktisch oft allein vom Hersteller des IoT-Geräts kontrolliert. Dieser hat es in der Hand, den

[67] IIA, a.a.O. (Fn. 9), S. 2, 5.
[68] IIA, a.a.O. (Fn. 9), S. 5.
[69] IIA, a.a.O. (Fn. 9), S. 2.
[70] EU-Kommission, Datenstrategie, S. 16; EU-Kommission, Leitfaden für die gemeinsame Nutzung von Daten des Privatsektors in der europäischen Datenwirtschaft vom 25.04.2018, SWD 2018(125), S. 5.
[71] EU-Kommission, Datenstrategie, S. 10.

Zugang zu den Daten und ihre Weiterverwendung vertraglich zu erlauben, zu beschränken oder andere durch technische Maßnahmen vom Zugriff auszuschließen.[72]

Die Kommission betont, dass gemeinsam erzeugte („co-generierte“) IoT-Daten eine besondere Art von Daten sind, deren Bedeutung noch exponentiell wachsen wird.[73] Weil IoT-Daten ein bislang ungenutztes Innovationspotenzial für die Entwicklung neuer sekundärer Dienste bergen, die auf solchen Daten beruhen[74], will sie mit dem Data Act maßgeblich den Zugang zu und die Weiterverwendung von Daten fördern, die von vernetzten IoT-Objekten erzeugt werden. Hierzu will sie für Klarheit sorgen, welche Nutzungsrechte an gemeinsam erzeugten, nicht-personenbezogenen IoT-Daten aus dem industriellen bzw. geschäftlichen Umfeld bestehen.[75]

3.2.2.2 Mögliche Regelungen im Data Act

Die Kommission will den Abschluss „fairer“ Datenaustauschverträge erleichtern und könnte deshalb[76]

- **Herstellern von IoT-Objekten zumindest Transparenzpflichten auferlegen,**
- **einen „B2B-Fairness-Test“ für Verträge über den Datenzugang einführen,**
- **Mustervertragsklauseln für B2B-Datenaustauschverträge empfehlen,**
- **Datenzugangs- und nutzungsrechte für nicht-personenbezogene Daten festlegen, und**
- **harmonisierte Grundregeln als Basis für die Ausübung sektorspezifischer Datenzugangs- und Nutzungsrechte festlegen.**

Welche genauen Regelungen zum B2B-Data-Sharing sich hinter den genannten Politikoptionen im Einzelnen verbergen könnten, stellen wir unten in Kapitel 4.2 näher dar.

3.2.3 Mögliche Anpassung der EU-Datenbankrichtlinie

3.2.3.1 Hintergrund

Datenbanken unterliegen nach der Richtlinie 96/9/EG über den rechtlichen Schutz von Datenbanken (Datenbankrichtlinie)[77] einem besonderen Schutz, der ggf. der Weiterverwendung von in der Datenbank enthaltenen Daten entgegenstehen könnte. Datenbanken sind Sammlungen von Daten, die systematisch oder methodisch angeordnet und einzeln zugänglich sind, z.B. mit elektronischen Mitteln.[78] Nach der Richtlinie können Datenbanken auf zwei verschiedene Arten geschützt sein: erstens durch das Urheberrecht, wenn die Struktur der Datenbank, einschließlich der Auswahl oder Anordnung des Inhalts, originell ist und deshalb eine eigene geistige Schöpfung darstellt – dies ist eher selten der Fall. Zweitens können Datenbanken, auch wenn sie die genannte Schöpfungshöhe nicht aufweisen, unter den Schutz des sogenannten "Sui-generis"-Rechts fallen – das ist ein spezielles, vom Urheberrecht unabhängiges geistiges Eigentumsrecht. Dieser Schutz entsteht automatisch, wenn die finanziellen oder fachlichen Investitionen für die Beschaffung, Überprüfung und Darstellung der Daten – also für ihre Klassifizierung bzw. Zusammenstellung – wesentlich waren. Der Hersteller einer solchen öffentlich

---

72 Van Roosebeke, B./Anzini, M./Eckhardt, P./Pierrat, A., cep**Study** a.a.O. (Fn. 34), S. 31, 60f.
73 IIA, a.a.O. (Fn. 9), S. 2.
74 IIA, a.a.O. (Fn. 9), S. 2.
75 EU-Datenstrategie, a.a.O. (Fn. 4), S. 30, Konsultation, a.a.O. (Fn. 13), S. 19.
76 IIA, a.a.O. (Fn. 9), S. 5.
77 Richtlinie 96/9/EG des Europäischen Parlaments und des Rates vom 11. März 1996 über den rechtlichen Schutz von Datenbanken, kons. Fassung abrufbar unter https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:01996L0009-20190606&from=EN.
78 Art. 1 Datenbankrichtlinie 96/9/EG (a.a.O.).

zugänglichen Datenbank kann Benutzern die Entnahme oder Weiterverwendung wesentlicher Teile des Inhalts seiner Datenbank untersagen. Ausnahmen von diesem Recht sieht die Richtlinie etwa für die wissenschaftliche Forschung vor. Dagegen dürfen unwesentliche Teile des Inhalts von allen rechtmäßigen Benutzern zu beliebigen Zwecken weiterverwendet werden. Die Kommission hat die Datenbankrichtlinie im Jahr 2018 bewertet und festgestellt, dass Rechtsunsicherheit dahingehend besteht, wie die Richtlinie auf die aktuelle Datenwirtschaft anzuwenden ist. Dies ist insbesondere darauf zurückzuführen, dass unklar ist, inwieweit maschinell erzeugte Daten und insbesondere Daten, die von mit Sensoren ausgestatteten und mit dem Internet der Dinge (IoT) verbundenen Objekten erzeugt werden, unter das das Sui-Generis-Recht fallen.

3.2.3.2 Mögliche Regelungen

Die Kommission überprüft daher derzeit die Datenbankrichtlinie und will diese ggf. anpassen, um den Zugang zu Daten und deren Nutzung im Rahmen der Datenwirtschaft zu erleichtern. Insbesondere erwägt sie[79],

- **den Anwendungsbereich des Sui-Generis-Rechts zu klären, um Rechtssicherheit in Bezug auf maschinell erzeugte Daten zu schaffen;**
- **sicherzustellen, dass die Rechte unter der Richtlinie den Datenzugang – insbesondere zu maschinell erzeugten Daten – nicht behindern;**
- **spezifische Zugangsrechte festzulegen, um den Handel mit und den Zugang zu Datenbanken zu erleichtern;**
- **die Datenbankrichtlinie auch im Übrigen zu modernisieren, etwa ihre Ausnahmen an die neuen EU-Urheberrechtsinstrumente anzupassen.**

Wie die Kommission die Datenbankrichtlinie im Einzelnen anpassen will, ist noch offen. So könnte sie etwa den Geltungsbereich des Sui-Generis-Rechts einschränken und maschinell erzeugte Daten ausdrücklich von dieser Form des Datenbankschutzes ausschließen, um den Zugang zu diesen Daten zu erleichtern und „Lock-in"-Situationen zu vermeiden.[80] Nicht ausgeschlossen erscheint jedoch, dass die Kommission IoT-Daten auch ausdrücklich in den Geltungsbereich der Richtlinie einbeziehen könnte. In diesem Fall könnte sie ggf. spezifische Zugangsrechte zu den Daten vorsehen, um es Unternehmen zu verbieten, den Zugang zu und die Entnahme von Daten durch vertragliche und technische Maßnahmen zu verhindern.[81] Unklar ist, ob der Data Act selbst Vorschläge zu einer Anpassung der Richtlinie enthalten wird oder ob die Kommission hierzu eine separate Änderungsrichtlinie vorschlagen wird.[82]

---

[79] IIA, a.a.O. (Fn. 9), S. 5f.

[80] Bertuzzi, L., a.a.O. (Fn. 6).

[81] Dies könnte sich aus den im Rahmen der Konsultation gestellten Fragen ergeben. Darin suchte die Kommission u.a. zu klären, ob die Befragten eher eine Einschränkung des Geltungsbereichs des Sui-Generis-Rechts befürworten, um einen möglicherweise hinderlichen Datenbankschutz für maschinell erzeugte Daten auszuschließen, oder maschinell erzeugte Daten ausdrücklich in den Geltungsbereich der Richtlinie einbeziehen und damit einen Datenbankschutz von Maschinendaten schaffen wollen. Ferner fragte die Kommission in ihrer Konsultation u.a. auch ab, ob spezifische Zugangsrechte geschaffen werden sollten und wie sie am besten zu verwirklichen seien, etwa durch Schaffung einer neuen Ausnahme, durch Einführung von Zwangslizenzen für den Datenzugang oder durch Schaffung eines allgemeinen Zugangsrechts, vgl. Konsultation, a.a.O. (Fn. 13), S. 34f.

[82] Dafür, dass die Änderung der Richtlinie parallel zum Data Act erfolgen wird, spricht der von der Kommission verwendete Wortlaut "in the context of" the Data Act, vgl. Summary Report of the public consultation, a.a.O. (Fn. 48), S. 1.

3.2.4 Prüfung der Richtlinie über Geschäftsgeheimnisse

3.2.4.1 Hintergrund

Auch die Unsicherheit über den Umgang mit Geschäftsgeheimnissen, die sich in oder hinter geschäftlichen Daten des Privatsektors verbergen, erschwert die Weiterverwendung dieser Daten. Die EU-Richtlinie über Geschäftsgeheimnisse[83] verpflichtet die Mitgliedstaaten, sensible geschäftliche Informationen vor unrechtmäßigem Erwerb, Nutzung und Offenlegung zu schützen. Auch sie bildet damit einen rechtlichen Rahmen für geistige Eigentumsrechte an solchen Informationen. Geschäftsgeheimnisse sind – vereinfacht dargestellt – Daten, die nicht allgemein bekannt oder zugänglich und daher geheim sind, einen kommerziellen Wert haben und deshalb von ihrem Inhaber geheim gehalten werden.[84] Um die Bereitschaft zu erhöhen, geschäftliche Daten zu teilen, benötigen Unternehmen Klarheit, wie sie sensible Daten und Geschäftsgeheimnisse auch im Fall der Weiterverwendung der Daten durch Dritte wirksam schützen können. In ihrer Datenstrategie hat die Kommission deshalb Präzisierungen angekündigt, wie die Richtlinie über Geschäftsgeheimnisse im Rahmen der Datenwirtschaft anzuwenden ist.[85] Sodann hat sie im Impact Inception Impact Assessment mitgeteilt, dass sie aktuell die Anwendbarkeit der Richtlinie im Zusammenhang mit der Datenwirtschaft prüfe und „zu einem späteren Zeitpunkt“ klarstellende Leitlinien dazu herausgeben wolle.[86]

3.2.4.2 Mögliche Regelungen

Aus den Ankündigungen der Kommission wird nicht deutlich, inwieweit bereits der Data Act selbst gewisse Präzisierungen zur Anwendung der Richtlinie über Geschäftsgeheimnisse im Rahmen der Datenwirtschaft enthalten wird, etwa, ob und wann die Weitergabe von Geschäftsdaten ggf. als „rechtmäßiger“ Erwerb solcher Daten zu qualifizieren ist, der zu einer Ausnahme vom Geheimnisschutz führen kann. Vermutlich wird die Kommission diese Klarstellungen gesonderten Leitlinien vorbehalten. Auf eine nähere Auseinandersetzung mit der Problematik wird daher vorliegend verzichtet.

3.2.5 Verbesserung der Portabilität personenbezogener Daten nach Art. 20 DSGVO

3.2.5.1 Hintergrund

Auch Privatpersonen erzeugen bei der Nutzung digitaler Online-Dienste oder bei der Nutzung von IoT-Geräten wie intelligenten Haushaltsgeräten oder Wearables[87] immer größere Datenmengen. Dabei handelt es sich regelmäßig um personenbezogene Daten, die durch die Datenschutzgrundverordnung (DSGVO) geschützt werden.[88] Auf Daten, die in den IoT-Geräten (Endgeräten) gespeichert sind, kann nach der E-Privacy-Verordnung zudem nur unter besonderen Voraussetzungen zugegriffen werden. Die Hersteller solcher Geräte oder die Anbieter solcher Dienste haben daher oft de facto die alleinige Kontrolle über die bei der Nutzung dieser Geräte oder Dienste erzeugten Daten.[89] Dies kann zu einer Abhängigkeit von bestimmten Anbietern (sogenannten „Lock-in“-Effekten) führen.[90]

---

[83] Richtlinie (EU) 2016/943 des Europäischen Parlaments und des Rates vom 8. Juni 2016 über den Schutz vertraulichen Know-hows und vertraulicher Geschäftsinformationen (Geschäftsgeheimnisse) vor rechtswidrigem Erwerb sowie rechtswidriger Nutzung und Offenlegung, ABl. L 157 vom 15.6.2016, S. 1ff.

[84] Art. 2 Nr. 1 der Richtlinie (EU) 2016/943 über Geschäftsgeheimnisse (a.a.O).

[85] Siehe auch Datenstrategie, S. 16.

[86] IIA, a.a.O. (Fn. 9)., S. 3. Unklar ist, wann dieser spätere Zeitpunkt sein könnte. Die Kommission merkt in ihrer Konsultation lediglich an, dass die Richtlinie nicht vor 2026 zur Bewertung anstehe (s. dort S. 36).

[87] Beispiele für Wearables sind Fitness- und Wellness-Tracker, die am Handgelenk oder als Brustgurt getragen werden und Vitalwerte des Körpers messen und aufzeichnen.

[88] Konsultation, a.a.O. (Fn. 13), S. 28.

[89] D’Cunha, C., a.a.O. (Fn. 3).

[90] EU-Datenstrategie, a.a.O. (Fn. 4), S. 12.

Die Kommission will daher auch die Portabilität (Übertragbarkeit) der von Privatpersonen erzeugten Daten verbessern. Portabilität bedeutet, dass Privatpersonen die Möglichkeit haben sollen, personenbezogene Daten, die sie einem Anbieter zur Verfügung gestellt haben, zu erhalten und in das System eines anderen Anbieters zu übertragen oder vom Anbieter direkt dorthin übertragen zu lassen. Betroffene sollen so die Kontrolle über ihre personenbezogenen Daten zurückerhalten[91] und leichter zu anderen Anbietern, z.B. Internet-Dienstleistern, wechseln können, wodurch zugleich der Wettbewerb gestärkt werden soll. Konkret geht es insbesondere darum, ob private Nutzer von IoT-Geräten oder Diensten in der Lage sein sollen, die bei der Nutzung generierten Daten anderen Anbietern zur Verfügung zu stellen.

Ein allgemeines Recht auf Datenübertragbarkeit für Privatpersonen besteht bereits und ist in Art. 20 DSGVO geregelt. Danach sind private Nutzer berechtigt, von dem für die Datenverarbeitung Verantwortlichen, also beispielsweise von ihrem Internet-Dienstleister, eine Kopie der von ihnen bereitgestellten Daten in einem „gängigen und maschinenlesbaren Format“ zu erhalten. „Bereitgestellt“ werden beispielsweise Namen und Anschriften, die der Betroffene bei der Online-Registrierung angegeben oder Fotos, Texte oder Kommentare, die er in einem sozialen Netzwerk in sein Profil hochgeladen oder öffentlich geteilt hat.[92] Der Nutzer hat jedoch nur dann ein Recht auf direkte Übermittlung der Daten vom alten an den neuen Anbieter, „soweit dies technisch machbar ist“. Art. 20 schreibt den Verantwortlichen dagegen nicht vor, dass sie die nötigen technischen Spezifikationen vorsehen müssen, die eine solche Übertragung erleichtern könnten. Auch hatte der Gesetzgeber wohl eher die einmalige Portierung der Daten im Auge. Jedenfalls verpflichtet Art. 20 die Verantwortlichen nicht, eine kontinuierliche Übertragbarkeit der Daten oder deren Übertragbarkeit in Echtzeit zu ermöglichen und die hierzu nötige technische Infrastruktur – z.B. technische Schnittstellen – einzurichten.[93] Art. 20 bietet Nutzern daher derzeit keine umfassende Grundlage, die Portierung von Daten zu verlangen, die von IoT-Objekten erzeugt werden. Dies erschwert laut Kommission das Angebot von Diensten, die einen Datenfluss in Echtzeit erfordern, z. B. die Reparatur oder die vorausschauende Wartung eines Haushaltsgeräts, und führt so zu Lock-in-Situationen für betroffene Nutzer. Zudem wird die Entwicklung neuer innovativer Dienste behindert, die auf dem Zugang zu solchen Daten beruhen und an denen die Nutzer ggf. interessiert wären.[94] Allerdings sollen künftig besonders marktmächtige Plattformen („Gatekeeper“) nach dem DMA verpflichtet werden, Endnutzern die Portabilität der durch die Nutzung ihrer zentralen Plattformdienste erzeugten Daten permanent und in Echtzeit zu ermöglichen.[95] Für Nicht-Gatekeeper bliebe es dagegen bei Art. 20 DSGVO, deren Regelungen die Kommission noch nicht für ausreichend hält.[96] Nachbesserungsbedarf bestehe insbesondere bei der Portabilität von Daten, die bei der Nutzung von Sprachassistenten durch Verbraucher generiert würden.[97]

---

91 Gola, Datenschutzgrundverordnung, Kommentar, 2. Aufl. 2018, Art. 20 Rn. 3.

92 Gola, Datenschutzgrundverordnung, Kommentar, 2. Aufl. 2018, Art. 20 Rn. 16. Die Art. 29 Datenschutzgruppe, deren Leitlinien vom Europäischen Datenschutzausschuss übernommen wurden, hat den Begriff der vom Betroffenen „bereitgestellten“ Daten Art. 20 allerdings weit ausgelegt und versteht darunter nicht nur aktiv bereitgestellte Daten, sondern auch Daten, die aus der Beobachtung der Tätigkeiten des Nutzers resultieren und von diesem ggf. auch unbewusst durch die Nutzung eines Dienstes oder Geräts bereitgestellt werden (z.B. Suchverlauf, Verkehrsdaten und Standortdaten, ebenso andere Rohdaten wie die von einem Trackinggerät aufgezeichnete Herzfrequenz, vgl. Art 29-Datenschutzgruppe, Leitlinien zum Recht auf Datenübertragbarkeit, WP 242 Rev. 01 vom 13.12.2016, überarbeitet am 05.04.17, S. 11f. Diese weite Auslegung wird in der Literatur kritisiert, vgl. Gola, a.a.O., Rn. 15.

93 Konsultation, a.a.O. (Fn. 13), S. 28.

94 IIA, a.a.O. (Fn. 9), S. 3.

95 Art. 6 Abs. 1 lit. h) des Kommissionsvorschlags COM (2020) 842 (siehe bereits oben Kapitel 2.2.1).

96 D’Cunha, C., a.a.O. (Fn. 3).

97 D’Cunha, C., a.a.O. (Fn. 3) unter Bezugnahme auf den vorläufigen Bericht der Kommission zur sektoralen Untersuchung zum Internet der Dinge für Verbraucher vom 9.6.2021, SWD(2021) 144 (dort S. 86).

3.2.5.2 Mögliche Regelungen im Data Act

Die Kommission will deshalb das Portabilitätsrecht gemäß Art. 20 DSGVO ergänzen, um privaten Nutzern zu helfen, ihr Recht auf Portabilität auch tatsächlich in Anspruch zu nehmen und die Daten Unternehmen bereitzustellen, die ihnen Dienste in Bezug auf ihr intelligentes Gerät anbieten. Dies soll es auch anderen Anbietern als den Herstellern der Geräte ermöglichen, Dienste anzubieten, die vom Zugang zu den von diesem Gerät erzeugten Daten abhängen[98] und Verbraucher etwa in die Lage versetzen, ihr Gerät von einem günstigeren Anbieter reparieren zu lassen. Der Data Act könnte damit Herstellern von IoT-Objekten möglicherweise ihr De-Facto-Privileg nehmen, über die Nutzung der von den IoT-Geräten erzeugten Daten exklusiv zu bestimmen.[99] Auch in der Konsultation zum Data Act hat sich die Mehrheit der Antwortgeber dafür ausgesprochen, dass nicht die Hersteller einseitig, sondern die Eigentümer bzw. Nutzer eines IoT-Objekts berechtigt sein sollten, über die Nutzung der von diesen Objekten generierten Daten zu bestimmen. Als größte Hindernisse für die effektive Ausübung des Portabilitätsrechts wurden die mangelnde Interoperabilität der Daten, unklare Regeln für die vom Portabilitätsrecht erfassten Datentypen und fehlende Identifizierungsmethoden für die zur Portabilität berechtigten Personen angegeben.[100]

Der Data Act könnte daher – über bereits bestehende speziellere Regelungen hinaus[101] – auch die allgemeinen Portabilitätspflichten erweitern. Insbesondere könnte er[102]

- **allgemeine technische Spezifikationen für die Portierung von personenbezogenen Daten vorschreiben**, etwa
- **Verantwortliche verpflichten, technische Schnittstellen für die Portierung einzurichten, und**
- **Unternehmen, die intelligente Haushaltsgeräte, Wearables und Haushaltsassistenten verkaufen, dazu verpflichten, eine Echtzeitübertragbarkeit der Daten ermöglichen, die diese Geräte während ihrer Nutzung erfassen,**
- **eine Pflicht zur kontinuierlichen Bereitstellung von Daten regeln**[103],
- **klarere Regeln enthalten, welche Datentypen vom Portabilitätsrecht erfasst werden,**
- **klarere Regeln für die Haftung bei Missbrauch der portierten Daten vorsehen.**

3.2.5.3 Vorläufige Einschätzung

Dass die Kommission die Lock-in-Effekte in Bezug auf IoT-Daten beseitigen und so den Wettbewerb auf nachgelagerten Märkten ankurbeln will, ist grundsätzlich sinnvoll. Wie die Maßnahmen zur Verbesserung der Portabilität für Privatpersonen zu bewerten sind, wird aber von der konkreten Ausgestaltung der Maßnahmen abhängen. Die Kommission sollte insbesondere sicherstellen, dass die Portabilitätspflichten verhältnismäßig bleiben und eine durch die verbesserte Portabilität erleichterte Teilung

98 IIA, a.a.O. (Fn. 9), S. 5, 6.
99 IIA, a.a.O. (Fn. 9), S. 7.
100 Summary Report on the Public Consultation, a.a.O. (Fn. 48), S. 4f.
101 So etwa die Strombinnenmarktrichtlinie (s.o. Kap. 2.2.2) und der vorgeschlagene Digital Markets Act (s.o. Kap. 2.2.1), die entsprechende Datenteilungsrechte vorsehen.
102 IIA, a.a.O. (Fn. 9), S. 6, 5, Konsultation, a.a.O. (Fn. 13), S. 28f. In diesem Zusammenhang fragte die Kommission in ihrer Konsultation ferner nach, ob fehlende Interoperabilität, Unklarheit über die vom Portabilitätsrecht erfassten Daten oder Probleme bei der Identifizierung oder Authentifizierung des berechtigten Antragstellers die Ausübung des Rechts beeinträchtigen, so dass auch insoweit Politikoptionen zur Beseitigung dieser Hindernisse in Betracht kommen.
103 In diesem Zusammenhang hat die Kommission ihrer Konsultation auch die Frage gestellt, ob intelligente Verträge ein wirksames Instrument zur technischen Umsetzung der Portierung sein könnten, vor allem dann, wenn die Übermittlung nicht nur einmalig ist, sondern ein kontinuierlicher Datenaustausch angestrebt wird, vgl. Konsultation, a.a.O. (Fn. 13), S. 18.

der Daten die Hersteller nicht übermäßig von Investitionen in IoT-Objekte bzw. in die Datenerzeugung und/oder -erfassung durch solche Objekte abschreckt. Außerdem sollte der Data Act den Grundsatz der Technologieneutralität wahren – also grundsätzlich keine bestimmte Technologie bevorzugen – und Innovationsanreize beibehalten. Zudem sollte die Kommission klarstellen, inwieweit die DSGVO durch die „ergänzenden" Regelungen im Data Act geändert wird.

Weil Datenportabilität nach der DSGVO eine Einwilligung der betroffenen Person voraussetzt[104], ist es wichtig, dafür zu sorgen, dass Nutzer ihre Einwilligungen in die Portierung unkompliziert und wirksam erteilen können. Hierzu könnten sogenannte PIMS (Personal Information Management Systeme) – das sind Systeme, die Nutzer in die Lage versetzen, ihre personenbezogenen Daten zentral zu verwalten und z.B. Einwilligungen zu erteilen oder zu widerrufen – einen wichtigen Beitrag leisten.[105] Die EU sollte daher PIMS – die als Datenintermediäre künftig unter den Data Governance Act fallen – weiter fördern.

3.2.6 Verbesserung der Portabilität für geschäftliche Nutzer von Cloud-Diensten

3.2.6.1 Hintergrund

Ferner will die Kommission wettbewerbsfähigere und offenere europäische Märkte für Cloud-Dienste schaffen.[106] Weil Unternehmen bei der Datenverarbeitung zunehmend auf Cloud-Dienste angewiesen sind, will sie geschäftlichen Nutzern von Cloud-Computing-Diensten (nachfolgend: „Cloud-Diensten") einen einfacheren Wechsel des Cloud-Diensteanbieters (nachfolgend: „Cloud-Anbieter") ermöglichen und hierzu auch die Daten- und Anwendungsportabilität zwischen Cloud-Diensten in der gesamten Datenwirtschaft verbessern.[107] Um die Bindung an einen bestimmten Cloud-Anbieter zu verhindern, müssen die Nutzer ihre Daten und Anwendungen problemlos zwischen verschiedenen Anbietern von Cloud-Diensten übertragen oder ihre Daten ohne vertragliche, technische oder wirtschaftliche Hindernisse in ihre eigenen IT-Systeme zurückübertragen können (Datenportabilität).[108] Bei nicht-personenbezogenen Daten gewährt die Free Flow of Data-Verordnung[109], die den freien Verkehr solcher Daten in der EU regelt, geschäftlichen Nutzern anders als die DSGVO[110] keinen gesetzlichen Anspruch auf Datenportabilität. Stattdessen zielt sie darauf ab, die Selbstregulierung von Cloud-Anbietern durch Verhaltensregeln zu fördern.[111] Auf Basis dieser Verordnung haben Cloud-Anbieter und Nutzer im Rahmen der von der Kommission geförderten Arbeitsgruppe für Cloud-Switching/Porting-Daten (SWIPO)[112] – Verhaltenskodizes erarbeitet, die u.a. vorvertragliche Transparenzpflichten vorsehen, um die Portabilität zu erleichtern.[113] Die Kommission hält diese Kodizes jedoch möglicherweise nicht (mehr) für ausreichend. Denn die Kodizes enthielten zum einen keine hinreichenden Regeln zu wichtigen Punkten wie den nötigen technischen Anforderungen, den Kosten und dem Zeitrahmen für den Cloud-Wechsel. Zum anderen beschränkten sie sich auf die Portabilität von Daten, ohne zugleich die

---

[104] Art. 20 Abs. 1 lit. a) DSGVO.

[105] Vgl. Krämer, J./Senellart, P./de Streel, A., Making Data Portability more effective for the Digital Economy - Economic Implications and Regulatory challenges, Juni 2020, S. 11, 66, 83, abrufbar unter https://cerre.eu/wp-content/uploads/2020/07/cerre_making_data_portability_more_effective_for_the_digital_economy_june2020.pdf.

[106] IIA, a.a.O. (Fn. 9), S. 3.

[107] Konsultation, a.a.O. (Fn. 13), S. 24, IIA, a.a.O. (Fn. 9), S. 5.

[108] IIA, a.a.O. (Fn. 9), S. 3, Konsultation, a.a.O. (Fn. 13), S. 24.

[109] Siehe oben Fn. 42.

[110] Zur Portabilität unter der DSGVO siehe oben Kapitel 3.2.5.

[111] Art. 6 Abs. 1 FFD-VO (EU) 2018/1807 (Fn. 42). Näher dazu cep**Analyse** Nr. 33/2017.

[112] https://swipo.eu/. Die Arbeitsgruppe hat weitere Untergruppen für Infrastructure-as-a-Service (IaaS) und für Software-as-a-Service (SaaS) Cloud-Dienste, vgl. Van Roosebeke, B./Anzini, M./Eckhardt, P./Pierrat, A., cep**Study** a.a.O. (Fn. 34), S. 29.

[113] Die SWIPO Codes erfassen die Portierung in IaaS- und SaaS-spezifischen Kontexten (IaaS, d. h. Infrastructure as a Service; SaaS, d. h. Software as a Service).

Portabilität von Anwendungen in eine andere Cloud zu ermöglichen, um sie dort auszuführen.[114] Die Ineffektivität der SWIPO-Regeln könnte allerdings auch darauf beruhen, dass die Kodizes außerhalb der IT-Branche noch immer weitgehend unbekannt sind.[115]

3.2.6.2 Mögliche Regelungen im Data Act

Die Kommission untersucht derzeit noch näher, ob die Selbstregulierung die Portabilität im B2B-Bereich hinreichend verbessert hat; andernfalls will sie andere politische Maßnahmen ergreifen, um vertragliche, technische und/oder wirtschaftliche Hindernisse für die Portabilität zwischen Cloud-Diensten zu beseitigen und so die Position der gewerblichen Cloud-Nutzer zu stärken.[116] In der Konsultation haben sich die Befragten sehr gespalten zur Notwendigkeit eines verbindlichen Portabilitätsrechts geäußert. Von den Befürwortern eines solchen Rechts bevorzugt etwa die Hälfte dessen Regelung in Form eines allgemeinen Grundsatzes, während sich knapp ein Drittel wünscht, dass der Data Act die Bedingungen des Portabilitätsrechts genauer regeln solle.[117]

Je nach Ausgang ihrer Untersuchung könnte die Kommission insbesondere[118]

- **ein verbindliches Recht auf die Portabilität von Cloud-Diensten einführen bzw. Anbieter von Cloud-Diensten verpflichten, die Übertragbarkeit von Daten und Anwendungen zu ermöglichen**.

Um dies zu erreichen, könnte sie etwa

- die Einhaltung der Grundsätze der SWIPO-Verhaltensregeln verbindlich vorschreiben bzw**. Standardvertragsklauseln bereitstellen**, die auf der Grundlage bestehender Verhaltenskodizes der Branche entwickelt wurden und die Anforderungen der Kodizes in Vertragsklauseln umsetzen;[119]
- **allgemeine rechtliche Anforderungen** für alle Anbieter von Cloud-Diensten auf dem europäischen Markt regeln, z.B. eine Vorschrift in den Data Act aufnehmen, die das Recht des Cloud-Nutzers, seine Daten in einem strukturierten, weit verbreiteten und maschinenlesbaren Format auf einen anderen Anbieter oder eigene Server zu übertragen, allgemein gesetzlich verankert[120], oder
- **spezifischere Anforderungen vertraglicher, technischer, kommerzieller oder wirtschaftlicher Natur für Cloud-Diensteanbieter festlegen**, z.B. [121]
  - die Pflicht, Daten auf Antrag der Nutzer kostenlos oder gegen eine angemessene Vergütung in einem strukturierten, weit verbreiteten und maschinenlesbaren Format zu übertragen,
  - Fristen, innerhalb derer die Übertragung abgeschlossen sein muss, sowie
  - eine Pflicht, Garantien vorzusehen, um die Fortführung des Geschäftsbetriebs während des Portierungsprozesses zu ermöglichen.

Zur technischen Infrastruktur:

Die Kommission will im Data Act laut Medienberichten über einen geleakten Entwurf des Impact Assessments zwar gewisse Mindestfunktionalitäten, aber keine technischen Merkmale oder

[114] IIA, a.a.O. (Fn. 9), S. 3
[115] Summary Report on the Public Consultation, a.a.O., S. 5.
[116] IIA, a.a.O. (Fn. 9), S. 5, s. auch Konsultation, a.a.O. (Fn. 13), S. 24.
[117] Summary Report on the Public Consultation, a.a.O. (Fn. 48), S. 5.
[118] IIA, a.a.O. (Fn. 9), S. 3.
[119] Vgl. die Fragen auf S. 24 der Konsultation, a.a.O. (Fn. 13).
[120] IIA, a.a.O. (Fn. 9), S. 6, Konsultation, a.a.O. (Fn. 13), S. 26.
[121] IIA, a.a.O. (Fn. 9), S. 6, Konsultation, a.a.O. (Fn. 13), S. 26.

Standards für die gemeinsame Datennutzung vorschreiben.[122] **Vielmehr sollen die für die Portierung erforderlichen Standard-APIs, offenen Standards und zulässigen Datenformate im Wege von Durchführungsrechtsakten[123] oder sogenannten delegierten Rechtsakten[124] zum Data Act näher spezifiziert werden.** Dies würde es ermöglichen, spezifische Wechselstandards in unterschiedlichen Bereichen vorzuschreiben. So könnte der Data Act die Kommission ermächtigen, die von Normungsgremien oder der Industrie ausgearbeiteten Anforderungen an die Dateninteroperabilität sektorspezifisch für bestimmte gemeinsame europäische Datenräume zu genehmigen, ohne diese jedoch verbindlich vorzuschreiben.[125]

Die Konsultation zum Data Act ergab, dass etwa die Hälfte der Antwortgeber die Entwicklung von Standard-APIs, offenen Standards und interoperablen Datenformaten, Zeitrahmen und anderen technischen Elementen grundsätzlich befürwortet.[126]

Da die Rechtslage im Bereich Cloud Computing derzeit aufgrund verschiedener Vorschriften und Selbstregulierungsinitiativen unübersichtlich ist, will die Kommission demnächst ein EU-„Regelwerk" für Cloud-Dienste vorschlagen – laut dem Inception Impact Assessment zum Data Act im 2. Quartal 2022. Dieses Regelwerk soll alle bindenden und nicht-bindenden Regelungen, Richtlinien und Normen für Cloud-Dienste auf dem europäischen Markt zusammenfassen und dadurch Anbietern, Nutzern und Aufsichtsbehörden einen besseren Überblick geben. Das künftige Regelwerk soll deshalb auch auf die im Data Act festgelegten Regelungen zum Cloud Computing verweisen.[127]

3.2.6.3 Vorläufige Einschätzung

Der Wechsel des Cloud-Anbieters wird geschäftlichen Nutzern durch unterschiedliche vertragliche, technische und wirtschaftliche Barrieren wie z.B. fehlende Interoperabilität oder hohe Kosten erschwert. Nachdem sich in der Konsultation zum Data Act eine klare Mehrheit der Antwortenden für ein gesetzliches Recht auf Portabilität ausgesprochen hat,[128] ist anzunehmen, dass die Kommission im Data Act zumindest ein allgemeines Portabilitätsrecht für geschäftliche Nutzer von Cloud-Diensten vorsehen wird. Ein Grund dafür, warum die Kommission die Cloud-Portabilität nicht im künftigen EU-Regelwerk zum Cloud Computing, sondern im Data Act regeln will, dürfte sein, dass dieses Regelwerk voraussichtlich kein Gesetzesakt, sondern eine geordnete Sammlung bestehender Regeln sein wird.

Bei der Bewertung der Maßnahmen zur Verbesserung der Portabilität für geschäftliche Cloud-Nutzer, die von der konkreten Ausgestaltung der Maßnahmen abhängt, werden insbesondere folgende Erwägungen zu berücksichtigen sein:

- Inwieweit lassen sich bestehende Lock-in-Effekte durch die Einführung von Portabilitätspflichten für Cloud-Anbieter voraussichtlich effektiv beheben? Portabilitätspflichten helfen etwa allein nicht weiter, wenn die fehlende Portabilität technische Ursachen hat, etwa wenn es an der Interoperabilität von Daten und Diensten fehlt.

---

[122] "(…) by setting up minimum levels of functionality via a standardization framework", vgl. Bertuzzi, L., a.a.O. (Fn. 6).
[123] IIA, a.a.O. (Fn. 9), S. 6.
[124] Bertuzzi, a.a.O. (Fn. 6).
[125] So offenbar das geleakte Impact Assessment, vgl. Bertuzzi, a.a.O. (Fn. 6).
[126] Summary Report on the Public Consultation, a.a.O. (Fn. 48), S. 5f.
[127] IIA, a.a.O. (Fn. 9), S. 6.
[128] 52% der Antwortgeber sind für ein solches Recht, 19% dagegen; 46% der Antwortgeber bevorzugen dabei allgemeine („high-level")-Regeln, während 29 % spezifischere Regeln fordern, vgl. Summary report on the public consultation, a.a.O. (Fn. 48), S. 5. Demgegenüber hatten sich in der Konsultation zur Datenstrategie noch knapp 1/3 der Antwortgeber für die Selbstregulierung als beste Praxis ausgesprochen, während knapp ¼ der Antwortgeber dies verneinten. Auch dort gab allerdings fast die Hälfte der Antwortgeber an, selbst von Problemen beim Funktionieren des Cloud-Markts wie der Bindung an einen bestimmten Anbieter betroffen gewesen zu sein, vgl. Konsultation zum Data Act, a.a.O., S. 24.

- Inwieweit sind geschäftliche Nutzer von Cloud-Diensten insoweit überhaupt schutzbedürftig? Solange ausreichender Wettbewerb zwischen Cloud-Anbietern besteht, steht es diesen Nutzern grundsätzlich frei, einen Cloud-Anbieter zu wählen, der ihnen Portabilität zusichert.
- Sind die Pflichten für Cloud-Anbieter verhältnismäßig, oder sollten zunächst mildere Mittel wie z.B. Informationspflichten und/oder eine bessere Bekanntmachung oder Erweiterung der freiwilligen SWIPO-Codes in Betracht gezogen werden?
- Sind die geplanten Regelungen ausreichend technologieneutral und behalten Innovationsanreize bei? Soweit die Kommission die Interoperabilität als Voraussetzung der Portabilität verbessern will, ist zu beachten, dass die fehlende Interoperabilität auch direkte Folge der Entwicklung eines innovativen Dienstes sein kann.[129]
- Soweit die Kommission – ggf. in Durchführungs- oder delegierten Rechtsakten – Schnittstellen, Standards und Datenformate näher spezifizieren und dabei auch auf den künftigen Normungsprozess einwirken will, sollte sie ihre Prioritäten eng mit den relevanten Anbietern abstimmen, um die Marktrelevanz der Normen sicherzustellen.

3.2.7 Smart Contracts als Hilfsmittel für die Weiterverwendung von Daten

3.2.7.1 Hintergrund

Smart Contracts („Intelligente Verträge“) sind keine Verträge im rechtlichen Sinn[130], sondern Computerprogramme, die Übermittlungen von Daten oder Werten nach bestimmten vorgegebenen Parametern automatisch ausführen.[131] Smart Contracts können etwa Datentransfers und Datenpooling automatisieren, Zahlungen für Datentransfers auslösen und die Umsetzung von Bedingungen gewährleisten, an die ein Datentransfer geknüpft ist.[132] Sie basieren auf Distributed Ledger Technologien wie Blockchain[133] und könnten möglicherweise als Hilfsmittel eingesetzt werden, die das Teilen von Unternehmensdaten im B2B-Bereich und im B2G-Bereich ebenso wie die Portierung personenbezogener Daten erheblich erleichtern. Sind die festgelegten Bedingungen erfüllt, veranlasst ein Algorithmus automatisch eine Transaktion, die anschließend validiert und in einem Block gespeichert wird.[134] Deshalb können Smart Contracts den Zugang zu und die Nutzung von gemeinsam erzeugter IoT-Daten ggf. auch dann technisch umsetzen, wenn auf solche Daten nicht einmalig, sondern kontinuierlich zugegriffen werden soll.[135] Gleichzeitig bieten Smart Contracts Sicherheit, da mit Hilfe dieser Verträge ggf. auch Nutzungsbeschränkungen in Bezug auf die Daten automatisiert durchgesetzt werden können. Nach Auffassung der Kommission können Smart Contracts daher in den Bereichen Industrie 4.0, intelligente Mobilität und intelligente Energie eine wichtige Rolle spielen.[136]

Derzeit gibt es allerdings keine harmonisierten Normen für Smart Contracts, was laut Kommission die grenzüberschreitende oder sektorübergreifende Nutzung solcher Programme erschwert.[137]

---

[129] Eckhardt, P./Baran, A., cep**Analyse** 16/2015, S. 3.
[130] Bundesamt für Sicherheit in der Informationstechnik (BSI), Blockchain sicher gestalten, Stand März 2019, S. 28, 59, abrufbar unter https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Krypto/Blockchain_Analyse.pdf?__blob=publicationFile&v=3.
[131] Eine einheitliche Definition von „Smart Contracts“ in der EU gibt es bislang nicht.
[132] Konsultation, a.a.O. (Fn. 13), S. 17.
[133] https://weissenberg-group.de/was-sind-smart-contracts/.
[134] https://weissenberg-group.de/was-sind-smart-contracts/.
[135] Siehe die entsprechenden Fragestellungen auf S. 17 der Konsultation, a.a.O. (Fn. 13).
[136] Konsultation, a.a.O. (Fn. 13), S. 17.
[137] IIA, a.a.O. (Fn. 9), S. 3.

3.2.7.2 Mögliche Regelungen im Data Act

Die Kommission erwägt daher,

- die europäischen Normungsorganisationen zu beauftragen, freiwillige **technische Normen für intelligente Verträge auszuarbeiten,** und – parallel dazu – **im Data Act**
- **grundlegende rechtliche Anforderungen an intelligente Verträge bzw. deren Interoperabilität festzulegen,** evtl. z.B. Mindestanforderungen an die Cybersicherheit[138],
- die Möglichkeit vorzusehen, **die aus dem genannten Auftrag resultierenden europäischen Normen als harmonisierte Normen zu veröffentlichen.**[139]

Die Kommission will so das Risiko einer Marktfragmentierung bei den technischen Normen für intelligente Verträge reduzieren, die Interoperabilität intelligenter Verträge verbessern und so technische Unterstützung für die Schaffung von Datenräumen leisten.[140]

3.2.7.3 Vorläufige Einschätzung

In der Konsultation zum Data Act haben eine große Mehrheit der antwortenden Interessenträger, insbesondere auch Unternehmen und Unternehmensverbände und Behörden zugestimmt, dass intelligente Verträge die gemeinsame wirtschaftliche Nutzung und kontinuierliche Übertragung insbesondere von IoT-Daten, aber auch die Umsetzung der Datenportabilität gegenüber Einzelpersonen erleichtern könnten.[141] Es ist daher zu erwarten, dass die Kommission die angekündigten Maßnahmen ergreifen wird, um das Potenzial dieser Verträge auszuschöpfen.

Wenn EU-Vorschriften harmonisierte Normen als Mittel zur Konkretisierung der in diesen Vorschriften geregelten wesentlichen Anforderungen an Produkte vorsehen, kann die Kommission den europäischen Normungsorganisationen nach Art. 10 Abs. 1 und 2 der EU-Normungsverordnung (EU) 1025/2012 einen Auftrag zur Erarbeitung einer harmonisierten Norm erteilen.[142] Gemäß Art. 1 Nr. 1 lit. c dieser Verordnung ist eine „harmonisierte Norm“ eine europäische Norm, die auf der Grundlage eines Auftrags der Kommission zur Durchführung von Harmonisierungsrechtsvorschriften der Union angenommen wurde.

Gemeinsame Normen für Smart Contracts führen zwar nicht zwingend zu Interoperabilität, solange die Einhaltung dieser Normen nicht rechtsverbindlich ist, dürften aber die Möglichkeiten verbessern, Interoperabilität herzustellen, und so die Nutzung von Smart Contracts erleichtern. In jedem Fall sollte der Data Act auch in Bezug auf Smart Contracts den Grundsatz der Technologieneutralität wahren, um die Entwicklung anderer innovativer Formen von Smart Contracts nicht zu gefährden.

---

[138] Siehe die entsprechende Fragestellung auf S. 19 der Konsultation, a.a.O. (Fn. 13).
[139] Zu allen diesen Punkten siehe IIA, a.a.O. (Fn. 9), S. 3, 6.
[140] IIA, a.a.O. (Fn. 9), S. 3, 6.
[141] Summary Report on the Public Consultation a.a.O. (Fn. 48), S. 4.
[142] Dingemann, K./ Kottmann, M., Rechtsgutachten zum europäischen System der harmonisierten Normenerstellt im Auftrag des Bundesministeriums für Wirtschaft und Energie (BMWi), August 2020, S. 10.

3.2.8 Schutzvorkehrungen für nicht-personenbezogenen Daten gegen Zugriffe durch Drittstaaten

3.2.8.1 Hintergrund

Schließlich will die Kommission auch *nicht-personenbezogene* Daten besser gegen unautorisierte Zugriffe schützen, insbesondere gegen Zugriffe durch Drittstaaten.[143] Diese Gefahr besteht insbesondere dann, wenn ein Cloud-Anbieter, in dessen Cloud die Daten gespeichert werden, dem Recht eines Drittstaats und damit auch möglichen Zugriffen nationaler Behörden des Drittstaats unterliegt.[144] Dies kann der Fall sein, wenn die Cloud, in der die Daten gespeichert werden, in den USA gehostet wird. Aber auch wenn Daten in der EU gespeichert werden, können Cloud-Anbieter in manchen Fällen zur Offenlegung von Daten gegenüber Behörden von Drittstaaten verpflichtet sein.[145]

Übermittlungen *personenbezogener* Daten in Drittstaaten sind nach der DSGVO grundsätzlich verboten, sofern sie nicht durch eine spezielle Rechtsgrundlage in deren Kapitel V. erlaubt werden. Fordert ein Gericht oder eine Behörde eines Drittstaates bestimmte personenbezogene Daten an, darf deren Offenlegung nur erfolgen, wenn die Anfrage auf eine in Kraft befindliche internationale Übereinkunft wie etwa ein Rechtshilfeabkommen gestützt wird, die die Datenübermittlung auf Basis gerichtlicher oder behördlicher Entscheidung abdeckt.[146]

Demgegenüber unterwirft das geltende EU-Recht die Übermittlung *nicht-personenbezogener* Daten in Drittländer bislang keinen spezifischen Regeln oder Anforderungen. Zwar sieht der vorgeschlagene Data Governance Act[147] nunmehr bestimmte Informationspflichten und andere Regelungen vor, um Zugriffe auf bestimmte nicht-personenbezogenen Daten durch Drittlandsbehörden oder Datentransfers in Drittländer zu verhindern, wenn solche Zugriffe oder Transfers mit dem EU-Recht oder dem Recht eines Mitgliedstaats im Widerspruch stehen. Damit soll dem möglichen Diebstahl geistigen Eigentums sowie der Industriespionage vorgebeugt werden.[148] Einige dieser Regelungen ähneln den Vorschriften der DSGVO zum internationalen Transfer personenbezogener Daten. Der Data Governance Act soll jedoch nicht für Anbieter von Cloud-Computing-Diensten gelten, sondern nur für öffentliche Stellen, Datenvermittlungsdienste, datenaltruistische Organisationen[149] und Personen, die nach dem Data Governance Act zur Weiterverwendung von Daten berechtigt sind.

Anbieter von Cloud-Computing-Diensten sind daher nach EU-Recht bislang nicht gesetzlich verpflichtet, dem Schutz geistigen Eigentums und von Geschäftsgeheimnissen gemäß EU-Recht Vorrang vor rechtlichen Verpflichtungen nach Drittstaatsrecht einzuräumen.[150] Aus Sicht der Kommission besteht allerdings insoweit eine vergleichbare Gefährdungslage. Denn auch Cloud-Anbieter können in einen

---

[143] IIA, a.a.O. (Fn. 9), S. 2, 3f., 6. Drittstaaten sind alle Staaten, die nicht der EU oder dem EWR angehören. Der EWR umfasst neben allen EU-Mitgliedsstaaten auch die Staaten Island, Liechtenstein und Norwegen der Europäischen Freihandelsassoziation (EFTA).

[144] Konsultation, a.a.O. (Fn. 13), S. 39.

[145] So verpflichtet etwa der US-amerikanische CLOUD Act (US Clarifying Lawful Overseas Use of Data Act) Anbieter elektronischer Kommunikations- und Cloud-Dienste unter bestimmten Bedingungen zur Offenlegung von Kommunikationsdaten, die außerhalb der Vereinigten Staaten, aber unter ihrer Kontrolle gespeichert werden. Näher dazu Hoffmann, A., Unzulässigkeit der Datenübermittlung in die USA, cep**Studie** vom 26.01.2021, S. 43, abrufbar unter https://www.cep.eu/eu-themen/details/cep/unzulaessigkeit-der-datenuebermittlung-in-die-usa-cepstudie.html.

[146] Art. 48 DSGVO, siehe auch Gola, P., DSGVO, Kommentar, 2. Aufl. 2018, Art. 48 Rn. 2ff. Häufig wird etwa in bi- oder multilateralen internationalen Abkommen geregelt, unter welchen Bedingungen und Garantien Zugriffsersuchen für grenzüberschreitende strafrechtliche Ermittlungen zulässig sind, vgl. Konsultation, a.a.O. (Fn. 13), S. 39.

[147] Siehe oben Kap. 2.2.1 (S. 8).

[148] Erwägungsgrund 15 des Data Governance Acts in der Fassung des Trilogkompromisses vom 10.12.2021, abrufbar unter https://data.consilium.europa.eu/doc/document/ST-14606-2021-INIT/en/pdf.

[149] Datenaltruistische Organisationen sammeln gemeinnützig Daten, welche die Privatpersonen oder Unternehmen freiwillig für gemeinwohldienliche Zwecke zur Verfügung stellen, vgl. Art. 2 Abs. 10 des Data Governance Acts, a.a.O.

[150] Konsultation, a.a.O. (Fn. 13), S. 39.

Konflikt geraten, wenn sie einerseits nach Drittlandsrecht Behörden Zugang zu den Daten gewähren und andererseits nach EU-Recht Geschäftsgeheimnisse schützen müssen. Wirtschaftlich sensible Daten von EU-Unternehmen können deshalb auch in diesen Fällen gefährdet sein.[151] Entsprechend halten drei Viertel der Befragten, die in der Konsultation zum Data Act die Fragen zum internationalen Datentransfer beantworteten, den möglichen Zugriff durch ausländische Behörden für ein relevantes oder sogar hohes Risiko und sehen darin zugleich eine Gefahr für ihre Geschäftsgeheimnisse.[152]

3.2.8.2 Mögliche Regelungen im Data Act

Um Geschäftsgeheimnisse und geistiges Eigentum besser gegen staatliche Zugriffe aus Drittstaaten zu schützen und das Vertrauen in die Nutzung von Cloud-Diensten zu stärken, könnte die Kommission im Data Act daher insbesondere folgende Pflichten für Cloud-Anbieter verankern:[153]

- die **Pflicht, Nutzer über** jedes **behördliche Zugangsersuchen** aus Drittstaaten **zu informieren**, soweit dies nach dem ausländischen Recht zulässig ist;
- die **Pflicht,** die **Kommission über** alle **Gesetze mit extraterritorialer Wirkung zu informieren**, denen sie unterliegen, damit die Kommission diese auf einem EU-Transparenz-Portal veröffentlichen kann;
- zusätzlich dazu ggf. die **Pflicht, angemessene rechtliche, technische und organisatorische Maßnahmen zu ergreifen**, um behördliche Zugriffe auf in ihrer Cloud gehostete nicht-personenbezogene Daten von in der EU ansässigen Unternehmen zu verhindern, die gegen EU-Recht oder das Recht eines EU-Mitgliedstaats verstoßen.[154] Solche Maßnahmen sollen aber dann nicht erforderlich sein, wenn ein internationales Abkommen den Zugriff erlaubt oder das betreffende Drittland einen vergleichbaren rechtlichen Schutz und Rechtsbehelfsmöglichkeiten bietet wie die EU-Vorschriften über den internationalen Zugang zu elektronischen Beweismitteln.[155] Diese Option würde laut Kommission die im Vorschlag für das Data-Governance-Gesetz enthaltenen Bestimmungen zu diesem Thema auf Anbieter von Cloud-Computing-Diensten ausweiten.[156]

Die Kommission könnte also im Data Act entweder reine Informationspflichten oder aber auch darüberhinausgehende Pflichten regeln wie die Pflicht, angemessene Schutzmaßnahmen gegen Zugriffe auf die Daten und damit auf Geschäftsgeheimnisse zu ergreifen, die mit EU- oder mitgliedstaatlichem Recht im Widerspruch stehen. Eine vergleichbare Pflicht sieht auch der Data Governance Act für die von ihm erfassten öffentlichen Stellen, Weiterverwender, Datenintermediäre und datenaltruistischen Organisationen vor.[157] Dieser regelt ferner, dass gerichtliche oder behördliche

[151] Konsultation, a.a.O. (Fn. 13), S. 39, die darauf hinweist, dass Drittländer den Zugang zu Daten etwa für Strafverfolgungs- und andere Zwecke ggf. in weitergehendem Umfang erlauben, in weiteren Anwendungsbereichen oder unter abweichenden Grundrechtsgarantien.

[152] Summary Report on the Public Consultation a.a.O. (Fn. 48), S. 6.

[153] IIA, a.a.O. (Fn. 9), S. 6.

[154] IIA, a.a.O. (Fn. 9), S. 6, ebenso offenbar das geleakte Impact Assessment der Kommission, vgl. Bertuzzi, a.a.O. (Fn. 6).

[155] IIA, a.a.O. (Fn. 9), S. 6. Laut Kommission stehen die avisierten Verpflichtungen für Cloud-Anbieter mit dem vorgeschlagenen Data Governance Act, der vorgeschlagenen EU-Gesetzgebung für internationalen Zugriff auf elektronische Beweismittel sowie den internationalen Verpflichtungen der Kommission im Rahmen der WTO und bilateraler Handelsabkommen, u. a. in den Bereichen Dienstleistungen, Investitionen und Rechte des geistigen Eigentums, im Einklang. Die Kommission will mit den neuen Regeln in dem bestehenden Spannungsfeld allen Seiten gerecht werden: sie will Cloud-Anbietern helfen, mit widersprüchlichen Regeln umzugehen, Geschäftsgeheimnisse und geistiges Eigentum schützen und zugleich die nach WTO-Recht und bilateraler Handelsabkommen bestehenden Pflichten wahren, s. IIA, a.a.O. (Fn. 9), S. 5, 6.

[156] Die Kommission spricht im IIA, a.a.O. (Fn. 9), S. 6, von einer Ausdehnung der im Data Governance Act vorgesehenen Vorschriften auf Cloud-Dienste.

[157] Art. 30 Abs. 1 des DGA in der Fassung des Trilogkompromisses, a.a.O. (Fn. 148).

Entscheidungen eines Drittstaats, die die Offenlegung von Daten anordnen, nach dem Data Governance Act nur anerkannt oder vollstreckbar werden dürfen, wenn sie von einer internationalen Übereinkunft – z.B. einem Rechtshilfeabkommen – gedeckt sind.[158] Fehlt es an einem solchen Abkommen, sollen Offenlegungsanordnungen nur befolgt werden dürfen, wenn (1) das Drittlandsrecht vorschreibt, dass die Entscheidung begründet, verhältnismäßig und spezifisch sein muss – d.h. eine ausreichende Verbindung zu einem bestimmten Verdächtigen oder Verstoß aufweist, also keine Sammlung von Massendaten erlaubt, (2) der Adressat die Entscheidung im Drittland gerichtlich anfechten kann und (3) das dortige Gericht befugt ist, die in der EU geschützten rechtlichen Interessen des Dateninhabers gebührend zu berücksichtigen.[159] Auch wenn die Offenlegung zulässig ist, dürfen nur so viele Daten wie nötig übermittelt werden (Datenminimierung). In jedem Fall muss der Adressat eines gerichtlichen oder behördlichen Offenlegungsersuchens dem Dateninhaber vorab über das Ersuchen informieren, sofern dadurch nicht Strafverfolgungsmaßnahmen vereitelt würden.[160] Es ist anzunehmen, dass die Kommission diese Regelungen des Data Governance Acts in den Data Act übernehmen und so auf Cloud-Anbieter erstrecken wird.

Der Data Governance Act ermächtigt die Kommission ferner, Standardklauseln für Verträge öffentlicher Stellen mit Weiterverwendern festzulegen, die geheimhaltungsbedürftige Daten des öffentlichen Sektors[161] in Drittländer übermitteln wollen. Zudem soll die Kommission unter bestimmten Bedingungen auch Angemessenheitsbeschlüsse in Bezug auf Drittländer erlassen dürfen, in denen ein vergleichbares Schutzniveau im Hinblick auf geistiges Eigentum und von Geschäftsgeheimnissen herrscht wie in der EU, und in die geheimhaltungsbedürftige nicht-personenbezogene Daten im Besitz des öffentlichen Sektors daher ohne weitere Vorkehrungen übermittelt werden dürfen.[162] Auch soll die Kommission für die Übermittlung bestimmter hochsensibler Daten des öffentlichen Sektors wie z.B. Gesundheitsdaten strengere Bedingungen festlegen dürfen.[163] Die Kommission erwähnt diese Regelungen in den bisher veröffentlichten Dokumenten zum Data Act nicht; es sind daher noch keine Anhaltspunkte dafür erkennbar, dass die Kommission ähnliche Regelungen für den Data Act plant.

3.2.8.3 Vorläufige Einschätzung

Auch die internationale Übermittlung nicht-personenbezogener Daten bewegt sich in einem komplexen Spannungsfeld: Cloud-Anbieter müssen Geschäftsgeheimnisse und das grundrechtlich geschützte geistige Eigentum ihrer Geschäftskunden in der EU (Art. 17 Abs. 2 GRCh) schützen, unterliegen aber ggf. nach dem Drittlandsrecht dem widersprechenden Offenlegungspflichten. Zugleich müssen die nach WTO-Recht und bilateralen Handelsabkommen bestehenden Pflichten gewahrt werden.

Informationspflichten bei Zugriffsersuchen können helfen, rechtswidrige Datenzugriffe ggf. zu verhindern, allerdings nur, wenn das Drittlandsrecht diese Information nicht verbietet. Auch eine Pflicht für Cloud-Provider, angemessene technische Maßnahmen zu ergreifen, um vertrauliche nicht-personenbezogene Daten gegen Zugriffe zu schützen – etwa Daten oder Unternehmensrichtlinien zu verschlüsseln[164] –, kann grundsätzlich das Vertrauen in die Nutzung von Cloud-Diensten und die Bereitstellung von Daten fördern. Fraglich ist aber, ob eine Verschlüsselung der Daten ausreicht, um behördliche

[158] Art. 30 Abs. 2 des DGA in der Fassung des Trilogkompromisses, a.a.O. (Fn. 148).
[159] Art. 30 Abs. 3 des DGA in der Fassung des Trilogkompromisses, a.a.O. (Fn. 148).
[160] Art. 30 Abs. 5 des DGA in der Fassung des Trilogkompromisses, a.a.O. (Fn. 148).
[161] Konkret geht es dabei um Daten, die durch das Geschäfts- oder Statistikgeheimnis, geistige Eigentumsrechte oder das Datenschutzrecht geschützt und damit nicht frei zugänglich sind, vgl. Art. 3 Abs. 1 des DGA in der Fassung des Trilogkompromisses, a.a.O. (Fn. 148).
[162] Siehe Art. 5 Abs. 10a, 10b des DGA in der Fassung des Trilogkompromisses, a.a.O. (Fn. 148).
[163] Siehe Art. 5 Abs. 11 sowie Erwägungsgrund 19 des DGA in der Fassung des Trilogkompromisses, a.a.O. (Fn. 148).
[164] Vgl. Erwägungsgrund 18a des DGA in der Fassung des Trilogkompromisses, a.a.O. (Fn. 148).

Zugriffe effektiv zu verhindern, wenn der Cloud-Provider Zugriff auf die Klardaten im unverschlüsselten Zustand hat bzw. benötigt, um diese zu verarbeiten. Unterliegt der Cloud-Provider selbst den Gesetzen des Drittlands, könnte er ggf. auch verpflichtet sein, einen in seinem Besitz befindlichen Schlüssel herauszugeben.[165]

Auch wenn nicht-personenbezogene Daten voraussichtlich weniger strengen Transferanforderungen unterworfen werden als personenbezogene Daten nach der DSGVO, sollte die Kommission verhindern, dass die Regelungen zur Übermittlung nicht-personenbezogener Daten in Drittstaaten zu spiegelbildlichen Problemen wie bei personenbezogenen Daten und zu Rechtsunsicherheit führen.[166] Die Kommission sollte deshalb eine internationale Lösung anstreben. Es ist sinnvoll, dass die EU die Befolgung von Offenlegungsersuchen auch in Bezug auf heikle nicht-personenbezogene Daten in Drittstaaten grundsätzlich an gültige internationale Übereinkommen und Rechtshilfeabkommen knüpft. Die EU sollte daher in solchen Abkommen möglichst auch Bedingungen und Garantien für die Übermittlung von bzw. den Zugriff auf nicht-personenbezogene Daten regeln und dabei dem Schutz von Geschäftsgeheimnissen und geistigem Eigentum Rechnung tragen.

In jedem Fall ist es wichtig, dass die Regelungen in DSGVO, Data Governance Act, Data Act und künftige separat geregelte strengere Bedingungen für hochsensible Daten gut aufeinander abgestimmt werden, sodass keine Rechtsunsicherheit entsteht, wann welche Arten nicht-personenbezogener Daten aktiv oder zur Befolgung behördlicher Offenlegungsersuchen in Drittländer übermittelt werden dürfen.

Gewisse Unsicherheiten werden jedoch auch dann verbleiben, etwa die Frage, ob im Ausland sitzende Muttergesellschaften von Cloud-Anbietern in der EU vertrauliche Geschäftsdaten abziehen könnten.

4 Mögliche Regelungen des Data Act zur Weiterverwendung von Unternehmensdaten – eine detailliertere Betrachtung

Weil die in Kapitel 3 skizzierten Vorschläge der Kommission, den Zugang zu privaten Unternehmensdaten zu verbessern, den Kern des Data Act ausmachen und mögliche Datenteilungspflichten für Unternehmen zudem i.d.R. eine besondere Brisanz aufweisen, geht dieser cep**Input** auf drei ausgewählte Regelungsbereiche des Data Act nachfolgend ausführlicher ein. Dabei wird in Kapitel 4.1 zunächst die Weiterverwendung der Daten durch den öffentlichen Sektor und in Kapitel 4.2 die Weiterverwendung durch andere Unternehmen behandelt. Kapitel 4.3 befasst sich schließlich näher mit der möglichen Anpassung der Datenbankrichtlinie.

4.1 Bessere Nutzung privater Unternehmensdaten durch den öffentlichen Sektor im öffentlichen Interesse („B2G“)

Wie in Kapitel 3.2.1. angesprochen, will die Kommission die Weiterverwendung bestimmter Daten in der Hand privater Unternehmen durch den öffentlichen Sektor fördern. Behörden sollen bestimmte Unternehmensdaten „im öffentlichen Interesse“ nutzen dürfen, etwa, um stärker faktengestützt

[165] Aus diesem Grund bietet die Verschlüsselung personenbezogener Daten, die in eine in den USA gehostete Cloud transferiert werden, um sie dort zu verarbeiten, derzeit aus Sicht der Datenschutzaufsichtsbehörden dann keinen ausreichenden Schutz gegen staatliche Zugriffe, wenn der in den USA ansässige Cloud-Provider Zugriff auf die Klardaten im unverschlüsselten Zustand hat bzw. benötigt, um diese auftragsgemäß zu verarbeiten. Näher hierzu Hoffmann, A., Unzulässigkeit der Datenübermittlung in die USA, cepStudie Januar 2021, S. 24ff. (27).

[166] Die Transferproblematik personenbezogener Daten in Drittstaaten mit nicht vergleichbarem Datenschutzniveau ist nach wie vor ungelöst, insoweit besteht weiterhin eine große Rechtsunsicherheit. Näher hierzu Hoffmann, A., Unzulässigkeit der Datenübermittlung in die USA, cepStudie Januar 2021.

agieren und damit u.a. effizientere öffentliche Dienstleistungen anbieten und bessere politische Entscheidungen treffen zu können.

Wie oben bereits dargelegt, soll der Data Act hierzu u.a. Folgendes regeln:[167]

- die Ziele und die allgemeinen Pflichten für die Weiterverwendung von Daten des Privatsektors durch die öffentliche Hand im öffentlichen Interesse,
- möglicherweise „als schärfstes Mittel" auch eine Pflicht für Unternehmen, öffentlichen Stellen Zugang zu bestimmten Daten zu gewähren und ihnen deren Nutzung zu ermöglichen, bzw. ein korrespondierendes Recht für öffentliche Stellen, im Privatbesitz befindliche Daten für bestimmte, näher definierte Zwecke des öffentlichen Interesses zu nutzen[168],
- Transparenzpflichten für öffentliche Stellen, wie sie die Daten weiterverwenden, und
- Schutzmaßnahmen für den Datenaustausch.

Die Kommission hatte angekündigt, dass sie prüfen wolle, auf welche Rechtsgrundlage im geltenden Recht – einschließlich der Datenschutzgrundverordnung – die Weiterverwendung von Unternehmensdaten durch den öffentlichen Sektor gestützt werden kann bzw. muss.[169]

4.1.1 Welche Zwecke sollen eine Pflicht zur B2G-Datenteilung rechtfertigen?

Die Kommission könnte Unternehmen zur Teilung von Daten „für bestimmte Verwendungszwecke, an denen ein eindeutiges öffentliches Interesse besteht", verpflichten. [170]

Laut Kommission liegt die Datennutzung dann im „öffentlichem Interesse", wenn sie

- einen allgemeinen Nutzen für die Gesellschaft als Ganzes hat, und deshalb
- auf EU-Ebene oder in den Mitgliedstaaten anerkannt ist.[171]

Ein allgemeiner Nutzen und damit ein öffentliches Interesse besteht aus Sicht der Kommission offenbar beispielsweise an der Datennutzung zu folgenden Zwecken:[172]

- Notfall- und Krisenmanagement bei außergewöhnlichen Umständen, auch bei Naturkatastrophen, sowie Prävention und Resilienz;
- Verbesserung öffentlicher Dienstleistungen, z.B. von Bildungsdiensten;
- Umweltschutz;
- Förderung der öffentlichen Gesundheit;
- Förderung einer sozial integrativen Gesellschaft;
- Ermöglichung einer besser faktengestützten politische Entscheidungsfindung;
- die Erstellung amtlicher Statistiken.

Der Data Act wird laut Medienberichten[173], die sich auf einen Leak des noch unveröffentlichten Impact Assessments zum Data Act beziehen, daher voraussichtlich eine Liste von auf EU-Ebene definierten Zwecken enthalten, bei denen eine Pflicht zur B2G-Datenteilung besteht. Darüber hinaus sollen die Mitgliedstaaten ggf. die Möglichkeit erhalten, auf der Grundlage einer Analyse des öffentlichen

[167] IIA, a.a.O. (Fn. 9), S. 2, 5.
[168] IIA, a.a.O. (Fn. 9), S. 5.
[169] IIA, a.a.O. (Fn. 9)., S. 5.
[170] In ihrer Konsultation fragte die Kommission, an welchen Daten ein „klares" öffentliches Interesse besteht, vgl. Konsultation, a.a.O. (Fn. 13), S. 9, 11.
[171] Konsultation, a.a.O. (Fn. 13), S. 8
[172] Dies ergibt sich daraus, dass die Kommission diese Beispiele in der Konsultation als „key examples" Konsultation, a.a.O. (Fn. 13), S. 9, 11, so teilweise auch Bertuzzi., L., a.a.O. (Fn. 6).
[173] Bertuzzi, L., a.a.O. (Fn. 6).

Bedarfs weitere *nationale Zwecke* in die Liste aufzunehmen. Die Zwecke sollen sich auf „die dringendsten sozialen Bedürfnisse beschränken, für die es keine anderen Möglichkeiten des Datenzugriffs gibt".

4.1.2 Für welche Daten soll es möglicherweise eine Datenteilungspflicht geben?

Die Kommission will dem öffentlichen Sektor spontan („ad hoc") oder regelmäßig Zugang zu Daten ermöglichen, die wegen ihres Umfangs nicht Gegenstand von Meldepflichten sein können (z.B. Big Data), deren bessere Nutzung aber dennoch für bestimmte Zwecke sinnvoll sein könnte.

Konkret ins Auge fasst die Kommission dabei beispielsweise möglicherweise u.a. folgende Daten:[174]

- Mobilitätsdaten von Telekommunikationsbetreibern oder Schadendaten von Versicherungsunternehmen (für das Notfall- und Krisenmanagement);
- Preisdaten von Supermärkten (für amtliche Statistiken);
- Emissionsdaten von Produktionsbetrieben (für den Umweltschutz);
- Kraftstoffverbrauchsdaten von Verkehrsbetrieben (für die öffentliche Gesundheit);
- Beschäftigungsdaten von Unternehmen (für eine sozial integrative Gesellschaft).

4.1.3 Welche Konditionen sollen bei einer Datenbereitstellungspflicht gelten?

Soweit Datenbereitstellungspflichten gesetzlich geregelt werden, soll ein verpflichtender Zugang laut der EU-Datenstrategie nur „unter fairen, zumutbaren, angemessenen und nichtdiskriminierenden Bedingungen" erfolgen.[175] Unklar ist bislang noch, inwieweit die EU im Data Act konkrete Konditionen für die Bereitstellung der Daten regeln und möglicherweise sogar verpflichtend vorgeben wird. Wie die öffentliche Konsultation zeigt, könnte der Data Act Vorgaben zur Vergütung enthalten, etwa, ob die Daten dem öffentlichen Sektor kostenlos, zu einem Vorzugspreis, zum Marktpreis, oder je nach Zweck unterschiedlich zur Verfügung zu stellen sind.[176] Laut Medienberichten sollen Unternehmen die Daten dem Staat offenbar zu niedrigeren als den üblichen Preisen bereitstellen, d.h. der Staat soll eine Vorzugsbehandlung genießen. Daten, die die öffentliche Hand für Notfälle anfordert, sollen sogar kostenlos bereitgestellt werden müssen.[177]

4.1.4 Werden die Daten bei der Weiterverwendung geschützt?

Insbesondere wenn Datensätze personenbezogene Daten oder vertrauliche betriebliche Informationen enthalten oder an den Daten Rechte Dritter – z.B. geistige Eigentumsrechte – bestehen, stellt sich die Frage, wie der Schutz dieser Daten, Geschäftsgeheimnisse und Rechte bei der gemeinsamen Nutzung bzw. Weiterverwendung der Daten sichergestellt werden kann. Die Kommission will im Data Act „angemessene" Schutzvorkehrungen vorsehen, um die Grundrechte der Betroffenen zu schützen und die Interessen des Unternehmens zu respektieren, das die Daten bereitstellt. Beispielsweise sollen die an den öffentlichen Sektor zu übermittelnden Daten durch technische Lösungen auf ein Mindestmaß beschränkt werden. Soweit eine solche Datenminimierung nicht möglich ist, soll der Data Act geeignete Schutzmaßnahmen bzw. „angemessene Garantien" bieten.[178] Welche Schutzvorkehrungen die

[174] Siehe die von der Kommission in der Konsultation erwähnten Daten, vgl. Konsultation (Fn. 13), S. 8.
[175] EU-Datenstrategie, a.a.O. (Fn. 4), S. 16.
[176] Die Kommission hat die Stakeholder in ihrer Konsultation zu dieser Frage befragt, vgl. dort (Fn. 13), S. 11. Laut der High Level Expert Group könnten bei der Beschaffung privater Daten für Zwecke des öffentlichen Interesses ggf. Vorzugsbedingungen gelten, https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=64954, S. 3.
[177] Bertuzzi, L., a.a.O. (Fn. 6).
[178] IIA, a.a.O. (Fn. 9), S. 5; Konsultation, a.a.O. (Fn. 13), S. 12; Bertuzzi, L., a.a.O. (Fn. 6).

Kommission für den B2G-Datenaustausch konkret vorschreiben wird, ist aber noch offen.[179] In Frage kommen laut Kommission u.a.[180]

- Datensicherheitsmaßnahmen einschließlich von Maßnahmen zum Schutz wirtschaftlich sensibler Informationen,
- besondere Anforderungen an die Verhältnismäßigkeit und Angemessenheit des Ersuchens, die Daten zu teilen,
- Transparenzpflichten, z.B. Berichtspflichten der öffentlichen Stelle, wie sie die Daten verwendet hat,
- eine Beschränkung der Nutzungsdauer, d.h. des Zeitraums, innerhalb dessen eine öffentliche Stelle bestimmte Datensätze verwenden oder speichern darf, bevor sie sie vernichten muss.

4.1.5 Erleichterung des Austauschs durch Datenintermediäre

Der B2G-Datenaustausch soll zudem durch sogenannte Datenintermediäre erleichtert werden. Hierzu sollen die Mitgliedstaaten nationale Koordinierungsstrukturen bzw. Vermittlungsstellen einrichten, die die Nachfrage bündeln, den Datenaustausch professionalisieren, registrieren und erleichtern und öffentliche Stellen, die an bestimmten Daten interessiert sind, mit Dateninhabern des Privatsektors zusammenbringen.[181] Zu den Aufgaben der Datenintermediäre könnte es auch gehören, Vereinbarungen über die Nutzungsbedingungen für solche Daten, einschließlich der Vergütung, zu erleichtern, und ggf. einen Streitbeilegungsmechanismus bereitzuhalten.[182]

4.1.6 „Anreize“ für die gemeinsame Nutzung von Daten

Ferner überlegt die Kommission, Anreize zu schaffen, die Unternehmen veranlassen könnten, dem öffentlichen Sektor Daten zur Weiterverwendung im öffentlichen Interesse bereitzustellen. In Betracht zieht sie dabei gemäß der öffentlichen Konsultation[183] sowohl

- finanzielle Anreize für die datengebenden Unternehmen wie
  - Grenzkosten für die Weitergabe oder für die Verbreitung, ggf. zuzüglich einer angemessenen Investitionsrendite (ROI),
  - eine Vergütung in Höhe des Marktpreises oder
  - Steuervergünstigungen, als auch
- nicht-monetäre Anreize für die datengebenden Unternehmen wie
  - mehr Know-how und Innovation durch gemeinsame Entwicklung mit öffentlichen Einrichtungen,
  - eine gesteigerte Reputation, etwa durch Programme zur öffentlichen Anerkennung der sozialen Verantwortung von Unternehmen oder
  - eine Investition öffentlicher Mittel, um die Entwicklung vertrauenswürdiger technischer Instrumente für den B2G-Datenaustausch zu fördern.

[179] Im IIA, a.a.O. (Fn. 9) gab die Kommission an, dass sie noch prüfen wolle, welche Datenminimierungsmaßnahmen oder Schutzvorkehrungen nötig sind, um personenbezogene Daten und Geschäftsgeheimnisse zu schützen (dort S. 5).
[180] Konsultation, a.a.O. (Fn. 13), S. 12.
[181] IIA, a.a.O. (Fn. 9), S. 5, siehe auch Bertuzzi, L., a.a.O. (Fn. 6).
[182] IIA, a.a.O. (Fn. 9), S. 5.
[183] Konsultation, a.a.O. (Fn. 13), S. 12.

4.1.7 Vorläufige Einschätzung

Auch wenn es auf die konkrete Ausgestaltung der Regelungen im Data Act zur Datenteilung im B2G-Bereich ankommt, lässt sich zu den geplanten Regeln vorab Folgendes anmerken:

- Bei der Regulierung der Weiterverwendung von Daten des Privatsektors durch die öffentliche Hand müssen EU und Mitgliedstaaten das öffentliche Interesse an der Weiternutzung der Daten mit den damit kollidierenden Grundrechten der Beteiligten in einen angemessenen Ausgleich bringen. Dazu gehören neben etwaigen geistigen Eigentumsrechten an den Daten [Art. 17 Abs. 2 der EU-Grundrechtecharta (GRCh)[184]] die unternehmerische Freiheit der Dateninhaber (Art. 16 GRCh) – einschließlich ihres Interesses am Schutz ihrer Geschäftsgeheimnisse – sowie die Grundrechte Dritter, z.B. deren Rechte auf Privatsphäre (Art. 7 GRCh) und Datenschutz (Art. 8 GRCh).
- Die EU sollte primär die freiwillige Bereitstellung von Daten an staatliche Stellen fördern. Datenteilungspflichten für private Unternehmen stellen einen erheblichen Eingriff in deren Grundrechte dar. Solche Pflichten müssen aufgrund des Bestimmtheitsgrundsatzes nicht nur hinreichend klar und genau geregelt werden, sondern auch verhältnismäßig ausgestaltet, d.h. geeignet und erforderlich sein und in einem angemessenen Verhältnis zum verfolgten Ziel stehen. Datenteilungspflichten müssen daher auf Ausnahmesituationen beschränkt werden, in denen eine freiwillige Kooperation oder sonstige alternative Beschaffung als milderes Mittel ausscheidet.
- Der Data Act muss die öffentlichen Interessen bzw. die diesen dienenden Zwecke für die Weiternutzung der Daten so genau wie möglich definieren[185] und klar vorgeben, nach welchen Kriterien die Mitgliedstaaten weitere öffentliche Interessen bzw. Zwecke festlegen dürfen.[186]
- Bei der verhältnismäßigen Ausgestaltung der Pflichten sind u.a. der Grad des öffentlichen Interesses[187] und die Schwere des Eingriffs[188] zu berücksichtigen. Je aufwändiger und riskanter die Datenteilungspflicht für die Unternehmen ist, umso gewichtiger muss das öffentliche Interesse an der staatlichen Nutzung dieser Daten sein. Je stärker die Nutzung der Daten Gemeinwohlinteressen dient und je gewichtiger diese Interessen sind, desto eher erscheint umgekehrt eine Datenteilungspflicht gerechtfertigt.[189] So lässt sich eine solche Pflicht zur unmittelbaren Bekämpfung einer Pandemie leichter rechtfertigen als zur lediglich geringfügigen Verbesserung einer öffentlichen Dienstleistung. Zudem sollte der Kreis der Verpflichteten (d.h. welche Unternehmen welcher Branche oder Größe Daten liefern müssen) sowie der Umfang der bereitzustellenden Daten möglichst eng begrenzt werden. Schließlich sollten Unternehmen die Datenteilung verweigern können, wenn ihr Interesse daran im Einzelfall das öffentliche Interesse erheblich überwiegt.

---

[184] Charta der Grundrechte, Abl. C 326 vom 26.10.2012, S. 391ff.

[185] Siehe auch Dutch Non-Paper on the Data Act, S. 3f., abrufbar unter https://www.permanentrepresentations.nl/permanent-representations/pr-eu-brussels/documents/publications/2021/10/1/non-paper-on-the-data-act.

[186] Laut Bertuzzi, L., a.a.O. (Fn. 6), gibt es beim Konzept des öffentlichen Interesses im Data Act offensichtlich noch Schwierigkeiten.

[187] Der Grad des öffentlichen Interesses kann sich unterscheiden. Siehe dazu etwa EU-Datenstrategie, a.a.O. (Fn. 4), S. 25, wonach der Grad des öffentlichen Interesses im Gesundheitswesen höher und in der Fertigung geringer sein kann.

[188] Jarass, Charta der Grundrechte der EU, 4. Aufl. 2021, Art. 52 Rn. 42.

[189] Ähnlich – allerdings bezogen auf Datenzugangsrechte für Wissenschaft und Forschung – Specht-Riemenschneider, L., Studie zur Regulierung eines privilegierten Zugangs zu Daten für Wissenschaft und Forschung durch die regulatorische Verankerung von Forschungsklauseln in den Sektoren Gesundheit, Online-Wirtschaft, Energie und Mobilität im Auftrag des Bundesministeriums für Bildung und Forschung, S. 143, abrufbar unter https://www.jura.uni-bonn.de/fileadmin/Fachbereich_Rechtswissenschaft/Einrichtungen/Lehrstuehle/Specht/Dateien/2021-08-25-LSR.pdf.

- Unternehmen, die dem öffentlichen Sektor Daten bereitstellen, sollten hierfür grundsätzlich adäquat entlohnt werden, um entstandene Kosten für die Generierung oder Aufbereitung von Daten adäquat zu kompensieren. Vorzugskonditionen für den Staat bedürfen einer speziellen Rechtfertigung. Inwieweit angemessene Preisregelungen horizontal ex ante festgelegt werden können, ist allerdings fraglich. Welcher Preis „fair" wäre, ist schwierig zu beurteilen, weil sich für viele Daten noch keine „Marktpreise" herausgebildet haben und ihr wirtschaftlicher Wert daher unklar ist. In der öffentlichen Konsultation der Kommission gaben 55% der Antwortgeber an, dass die Höhe der Entschädigung für ein Unternehmen, das Daten mit öffentlichen Stellen teilt, vom konkreten Anwendungsfall abhängen sollte.[190]
- Unternehmen werden sich eher dann freiwillig auf eine Kooperation mit der öffentlichen Hand einlassen, wenn dadurch auch für sie ein Mehrwert entsteht (win-win-Situation). Sonstige Anreize, die etwa die Reputation eines datengebenden Unternehmens verbessern, können helfen, sollten Unternehmen aber nicht zum Teilen von Daten drängen.
- Interessierte öffentliche und private Akteure müssen einander finden. Es ist daher sachgerecht, dass die Kommission den B2G-Datenaustausch mit Hilfe sogenannter Datenintermediäre erleichtern will.
- Es muss sichergestellt werden, dass Unternehmen nicht länger aus Angst vor der Verletzung von Geschäftsgeheimnissen, geistigen Eigentumsrechten, Datenschutzvorschriften und mangelnder Cybersicherheit vor einer freiwilligen Weitergabe ihrer Daten zurückschrecken. Daher ist es sachgerecht, dass die Kommission den öffentlichen Stellen Pflichten auferlegen will, personenbezogene Daten, Geschäftsgeheimnisse und geistige Eigentumsrechte an den Daten bei der Weiterverarbeitung angemessen zu schützen.
- Um einen Missbrauch der bereitgestellten Daten auszuschließen, sollten öffentliche Stellen zudem verpflichtet werden, die Daten nur streng zweckgebunden[191], d.h. ausschließlich zur Förderung des Gemeinwohls zu verwenden. Transparenzpflichten können helfen, das Vertrauen der Datengeber in die rechtmäßige Nutzung der Daten zu stärken. Die Weitergabe der Daten an Dritte, z.B. an Personen, derer sich die öffentliche Stelle zur Erfüllung ihrer Aufgaben bedient, sollte vergleichbar strengen Bedingungen unterworfen werden.
- Der Staat ist für die Erfüllung seiner Aufgaben auf richtige und verwertbare Daten angewiesen; umgekehrt haben Unternehmen ein Interesse daran, dass ihnen durch die staatliche Nutzung ihrer Daten kein Schaden entsteht. Um Vertrauen zu schaffen, sollte der Data Act nicht nur einen Streitbeilegungsmechanismus, sondern auch angemessene Haftungsregelungen vorsehen bzw. sicherstellen, dass etwaige vertragliche Regeln zur Haftung – etwa für Schäden aufgrund mangelnder Datenqualität oder durch Pflichtverletzungen des Staates – nach dem Recht der Mitgliedstaaten auch durchgesetzt werden können. Hierzu schweigt das Inception Impact Assessment jedoch.
- Um eine flexiblere Regulierung zu ermöglichen, könnte es ggf. auch im B2G-Bereich sinnvoll sein, Datenteilungspflichten sektorspezifisch zu regeln und im Data Act grundlegende allgemeine Regeln festzulegen, die durch speziellere sektorspezifische Regeln konkretisiert werden können.[192]

[190] Summary report of the public consultation, a.a.O., S. 3. 23% der Antwortgeber sprachen sich für Kostenfreiheit, 8 % für eine Vergütung in Höhe des Marktpreises und 7 Prozent für einen Vorzugspreis aus.
[191] Ebenso Specht-Riemenschneider, L., a.a.O. (Fn. 189), S. 143, zu Datenzugangsrechten für Wissenschaft und Forschung.
[192] Dies plant die Kommission offenbar für den B2B-Bereich, siehe dazu unten Kapitel 4.2.4 und 4.2.5.

- Die Kommission sollte sich allerdings zunächst darauf fokussieren sicherzustellen, dass der öffentliche Sektor fachlich und technisch überhaupt in der Lage ist, das Potenzial bereitgestellter Unternehmensdaten auszuschöpfen.
- Zusätzlich müssen rechtliche Barrieren beseitigt werden, etwa bestehende Rechtsunsicherheiten im Zusammenhang mit der DSGVO, die Anwendung findet, wenn Datensätze personenbezogene Daten enthalten. Geklärt werden muss, wie Daten DSGVO-konform weitergenutzt werden können, u.a.
  - ab wann Daten als anonymisiert[193] gelten und die Anwendbarkeit der Datenschutzgrundverordnung daher ausgeschlossen ist[194]; hier sollte die EU schnellstmöglich eine Lösung anstreben, etwa durch Unterstützung der Entwicklung von Standards, bei deren Einhaltung ein hinreichender Anonymisierungsgrad vermutet wird,
  - ob und wenn ja, ab wann die gemeinsame Nutzung von Daten zu einer gemeinsamen Verantwortlichkeit[195] für die Daten und die Einhaltung der DSGVO-Pflichten führt, und
  - auf welche Rechtsgrundlage in der DSGVO die Weiternutzung von Daten gestützt werden kann. Ob die Kommission insoweit hilfreiche Hinweise geben wird, bleibt abzuwarten.

4.2 B2B: Besserer Austausch von Daten zwischen Unternehmen: fairer Datenzugang und faire Nutzung

Wie in Kapitel 3.2.2. angesprochen, will die Kommission mit dem Data Act auch den Abschluss von Datenaustauschverträgen zwischen privaten Unternehmen (B2B) erleichtern und damit insbesondere die Weiterverwendung von Daten fördern, die von vernetzten IoT-Objekten erzeugt werden.

Wie oben dargestellt, könnte die Kommission insbesondere

- Herstellern von IoT-Objekten Transparenzpflichten auferlegen (siehe sogleich Kap. 4.2.1);
- einen „B2B-Fairness-Test“ für Verträge über den Datenzugang einführen (Kap. 4.2.2);
- Mustervertragsklauseln für B2B-Datenaustauschverträge empfehlen (Kap. 4.2.3);
- Datenzugangs- und -nutzungsrechte für nicht-personenbezogene Daten festlegen (Kap. 4.2.4);
- harmonisierte Grundregeln als Basis für sektorspezifische Datennutzungsrechte festlegen (Kap. 4.2.5).

4.2.1 Transparenzpflichten für Hersteller von IoT-Objekten

Um die Weiterverwendung von IoT-Daten zu fördern, könnte sich die Kommission zunächst auf Regelungen beschränken, die für mehr Klarheit darüber sorgen, welche Nutzungsrechte an gemeinsam erzeugten, nicht-personenbezogenen IoT-Daten aus dem industriellen bzw. geschäftlichen Umfeld überhaupt bestehen.[196] Hierzu könnte sie Herstellern von vernetzten IoT-Objekten bestimmte Transparenzpflichten auferlegen, welche Zugangs- und Nutzungsrechte sie gewerblichen Nutzern dieser Objekte zu bzw. an den von den Objekten erzeugten nicht-personenbezogenen Daten gewähren.[197]

---

[193] Laut Erwägungsgrund 26 findet die DSGVO auf anonymisierte Daten keine Anwendung.

[194] Gründe für die aktuell bestehende Rechtsunsicherheit in Bezug auf die Anonymisierung sind u.a. unklare Regelungen in der DSGVO und fehlende technische Standards, vgl. BDI, Praxisleitfaden Anonymisierung personenbezogener Daten, Stand Oktober 2020, S. 6, abrufbar unter https://bdi.eu/publikation/news/anonymisierung-personenbezogener-daten/.

[195] Art. 26 DSGVO.

[196] EU-Datenstrategie, a.a.O. (Fn. 4), S. 30, Konsultation, a.a.O. (Fn. 13), S. 19.

[197] IIA, a.a.O. (Fn. 9), S. 5.

Bereits in ihrer Mitteilung zum Aufbau eines gemeinsamen Datenraums hatte die Kommission die Schaffung fairer Märkte für IoT-Objekte und für auf maschinengenerierten Daten beruhende Produkte und Dienstleistungen als Ziel ausgerufen und dazu „zentrale Grundsätze“ für Verträge angekündigt. Insbesondere solle „aus den einschlägigen Verträgen“ auf transparente Weise ersichtlich sein, wer Zugang zu den durch das Produkt oder die Dienstleistung erzeugten Daten hat, um welche Art von Daten es sich handelt und wie detailliert sie sind, und zu welchem Zweck diese Daten verwendet werden.[198]

Damit könnte die Kommission möglicherweise anstreben, Herstellern von IoT-Objekten vergleichbare Transparenzpflichten aufzuerlegen, wie sie gemäß Art. 9 der Plattform-to-Business (P2B)-Verordnung (EU) 2019/1150[199] für Betreiber von Online-Plattformen gelten. Diese Plattformbetreiber müssen in ihren AGB erläutern, ob und wie sie ihren gewerblichen Nutzern (Händlern) technisch bzw. vertraglich Zugang zu personenbezogenen und nicht-personenbezogenen Daten gewähren, die die Händler oder deren Kunden – d.h. Verbraucher, die vom Händler Waren oder Dienstleistungen erwerben – dem Betreiber bereitgestellt haben, oder die bei der Nutzung der Plattform erzeugt werden. Dabei müssen die Plattformbetreiber auch angeben, zu welchen Datenkategorien und unter welchen Bedingungen die Händler und/oder sie selbst Zugang zu den Daten haben.

Sollte die Kommission die Transparenzpflicht zudem auch auf die Nutzungsrechte an den Daten erstrecken wollen, könnten dies bedeuten, dass Hersteller in ihren AGB u.a. zusätzlich erklären müssen,

- ob, inwieweit und unter welchen Bedingungen sie gewerblichen Nutzern technischen und vertraglichen Zugang zu Daten gewähren, die diese Nutzer oder deren Kunden im Zusammenhang mit der Nutzung des IoT-Objekts bereitstellen, oder die bei dessen Nutzung erzeugt werden;
- wie bzw. unter welchen Bedingungen gewerbliche Nutzer die Daten weiterverwenden oder unterlizenzieren dürfen;
- welche Beschränkungen es ggf. für den Zugang zu Daten oder für deren Weiterverwendung gibt;
- ob der Hersteller selbst Zugang zu den Daten hat und sie nutzen oder an Dritte weitergeben darf und wie der gewerbliche Nutzer der Weitergabe widersprechen kann.[200]

4.2.2 Ein „B2B-Fairness-Test“ für Datenaustauschverträge

Möglicherweise wird die Kommission aber über bloße Transparenzpflichten hinausgehen und einen „B2B-Fairness-Test“ für alle Datenaustauschverträge im B2B-Bereich einführen. Ein solcher „Test“ soll verhindern, dass ein Dateninhaber mit einer stärkeren Verhandlungsposition anderen Unternehmen, die von ihm kontrollierten Daten nutzen wollen oder darauf angewiesen sind, einseitig unfaire Bedingungen für den Zugang zu Daten oder für deren Nutzung auferlegt.[201]

Der „Fairness-Test“ würde laut Kommission nur unfaire Bedingungen aus Datenaustauschverträgen „ausfiltern“. Die Vertragspartei, der eine unfaire Klausel einseitig[202] auferlegt wird, soll an diese Klausel

---

[198] Siehe dazu die von der EU-Kommission zur gemeinsamen Datennutzung in B2B-Bereich festgelegten Grundsätze, vgl. EU-Kommission, Mitteilung „Aufbau eines gemeinsamen europäischen Datenraums“ vom 25.04.2018, COM(2018) 232, S. 12; EU-Kommission, Leitfaden für die gemeinsame Nutzung von Daten des Privatsektors in der europäischen Datenwirtschaft vom 25.04.2018, SWD 2018(125), S. 3.

[199] Verordnung EU) 2019/1150 des Europäischen Parlaments und des Rates vom 20. Juni 2019 zur Förderung von Fairness und Transparenz für gewerbliche Nutzer von Online-Vermittlungsdiensten, Abl. L 186 vom 11.07.2019, S. 57ff.

[200] Dazu müsste in den Verträgen wohl auch geregelt werden, welche Daten vom IoT-Objekt überhaupt erhoben werden. Die Kommission fragte in ihrer Konsultation u.a. auch ab, ob das Recht auf Information, welche Daten von dem IoT-Objekt erhoben werden, in den Kauf- oder Mietverträgen gut geregelt sei (vgl. Konsultation (Fn. 13), S. 20.

[201] IIA, a.a.O. (Fn. 9), S. 5, Konsultation, a.a.O. (Fn. 13), S. 13.

[202] Siehe Bertuzzi, a.a.O. (Fn. 6): *„Der Vorschlag würde auch eine vertragliche Fairnessprüfung für B2B-Vereinbarungen einführen, die sich auf Vertragsbedingungen beschränken würde, die von einer Partei einseitig auferlegt wurden.“*

dann nicht gebunden sein. Alle anderen Bedingungen sollen von den Parteien weiterhin frei vereinbart werden können. Ihre Vertragsfreiheit würde damit nur teilweise eingeschränkt. [203]

Wie aber könnte ein solcher „Fairness-Test" konkret aussehen? Als Vorbild für den „Fairness-Test" verweist die Kommission[204] auf die Zahlungsverzugsrichtlinie[205] und die Richtlinie über unlautere Geschäftspraktiken in der Lebensmittelversorgungskette (UTP-Richtlinie).[206] Art. 7 Abs 1 Zahlungsverzugsrichtlinie bestimmt, dass Vertragsklauseln oder Praktiken, die etwa im Hinblick auf den Zahlungstermin, die Zahlungsfrist oder den Verzugszinssatz für den Gläubiger grob nachteilig sind, nicht angewendet werden dürfen oder einen Schadensersatzanspruch für diesen begründen. Art. 3 UTP-Richtlinie legt eine Mindestliste verbotener unlauterer Handelspraktiken in Beziehungen zwischen Käufern und Lieferanten in der Agrar- und Lebensmittelversorgungskette fest.

Entsprechend könnte die Kommission entweder eine Liste verbotener Handelspraktiken in Datenaustauschverträgen festlegen. Sie könnte auch wie in der Zahlungsverzugsrichtlinie definieren, welche bestimmten Vertragsklauseln immer als grob nachteilig gelten sollen (Blacklist) oder bei welchen Klauseln widerlegbar vermutet werden soll, dass sie für den Datenlizenznehmer – evtl. auch den Lizenzgeber – grob nachteilig sind (Greylist).[207] Für die übrigen Vertragsklauseln würde dann ggf. wie bei der Zahlungsverzugsrichtlinie auf die Umstände des Einzelfalls, die Handelspraxis und darauf abgestellt, ob es einen „objektiven Grund" für eine Abweichung von üblichen Regeln und Praktiken gibt.

Solche Beschränkungen unfairer Klauseln oder Praktiken könnten entweder

- nur für Verträge über bestimmte Daten vorgeschrieben werden, z.B. für nicht-personenbezogene Daten, die von gewerblich genutzten vernetzten IoT-Objekten erzeugt werden, oder
- für eine Vielzahl von Verträgen über die gemeinsame Datennutzung gelten.[208]

4.2.3 Mustervertragsklauseln für B2B-Datenaustauschverträge

Zusätzlich zum „Fairness-Test" will die Kommission ggf. ergänzende Mustervertragsklauseln für Datenaustauschverträge vorschlagen.[209] Dabei könnte es sich entweder um Musterklauseln speziell für Verträge über den Austausch nicht-personenbezogener Daten handeln, die von gewerblich genutzten vernetzten IoT-Objekten erzeugt werden, oder um Klauseln für eine größere Bandbreite von Datennutzungsverträgen.[210] Die Mustervertragsklauseln sollen Unternehmen, denen es an Erfahrung mangelt, eine praktische Hilfestellung geben, wie ein Datenaustauschvertrag auf Grundlage fairer Bedingungen gestaltet werden kann.[211] Die Nutzung dieser Klauseln soll jedoch freiwillig sein.[212]

[203] Konsultation, a.a.O. (Fn. 13), S. 13.
[204] Konsultation, a.a.O. (Fn. 13), S. 13.
[205] Richtlinie 2011/7/EU des Europäischen Parlaments und des Rates vom 16. Februar 2011 zur Bekämpfung von Zahlungsverzug im Geschäftsverkehr, EU-Amtsblatt L 48 vom 23.02.2011, S. 1ff.
[206] Richtlinie (EU) 2019/633 des Europäischen Parlaments und des Rates vom 17. April 2019 über unlautere Handelspraktiken in den Geschäftsbeziehungen zwischen Unternehmen in der Agrar- und Lebensmittelversorgungskette, EU-Amtsblatt L 111 vom 25.04.2019, S. 59ff.
[207] Vgl. Art. 7 Abs. 2, 3 der Zahlungsverzugsrichtlinie, a.a.O.
[208] IIA, a.a.O. (Fn. 9), S. 5. Konsultation, a.a.O. (Fn. 13), S. 13.
[209] IIA, a.a.O. (Fn. 9), S. 5.
[210] IIA, a.a.O. (Fn. 9), S. 5. Konsultation, a.a.O. (Fn. 13), S. 13.
[211] Konsultation, a.a.O. (Fn. 13), S. 13.
[212] Konsultation, a.a.O. (Fn. 13), S. 13.

4.2.4 Festlegung von Datenzugangs- und nutzungsrechten für nicht-personenbezogene Daten

Möglicherweise will die Kommission aber zumindest teilweise über freiwillige vertragliche Musterklauseln hinausgehen und auch im B2B-Bereich zwingende konkrete Datenzugangs- und -nutzungsrechte zu und von nicht-personenbezogenen Daten festlegen.[213] Unternehmen würden damit über die geplanten Rechte gegenüber Gatekeepern[214] und die in bestehenden sektorspezifischen Vorschriften geregelten Rechte[215] hinaus weitere verbindliche Rechte auf Datenzugang und Datennutzung erhalten. Auch solche Rechte könnten entweder

- nur für den Zugang zu oder die Nutzung von bestimmten Daten eingeführt werden, z.B. für Daten, die von gewerblich genutzten vernetzten IoT-Objekten erzeugt werden, oder
- für eine Vielzahl von Verträgen über die gemeinsame Datennutzung vorgesehen werden.[216]

Vermutlich wird die Kommission unmittelbar im Data Act selbst aber keine konkreten Zugangs- und Nutzungsrechte festlegen, wie es der Wortlaut des Inception Impact Assessments zunächst nahezulegen scheint.[217] Die Formulierungen in der Konsultation[218], in der Datenstrategie[219] sowie vereinzelte Medienberichte[220] sprechen eher dafür, dass sich der Data Act darauf beschränken wird, allgemeine Bedingungen für den Datenzugang und die Datennutzung zu regeln.[221] Die Festlegung neuer, konkreter Datenzugangs- und Nutzungsrechte bliebe dann den einschlägigen sektorspezifischen Rechtsvorschriften vorbehalten.

Datenzugangs- und -nutzungsrechte stellen eine Ausnahme vom allgemeinen Grundsatz der EU-Datenstrategie dar, die primär den *freiwilligen* Datenaustausch erleichtern will.[222] Entsprechend sieht die EU-Datenstrategie vor, dass verbindliche Pflichten für Unternehmen, Zugang zu relevanten Daten zu gewähren, stets sektorspezifisch und nur dann vorgeschrieben werden sollen, wenn besondere Umstände dies erfordern. Abgesehen von besonderen sektorspezifischen Ausnahmen[223] liegen solche Umstände laut Kommission nur vor, wenn im jeweiligen Sektor ein Marktversagen festgestellt wird bzw. vorhersehbar ist, das durch das Wettbewerbsrecht allein nicht behoben werden kann.[224] Der Umfang etwaiger Datenzugangsrechte sollte laut Kommission den berechtigten Interessen des Dateninhabers Rechnung tragen.[225] Zudem sollen Unternehmen nicht verpflichtet sein, wirtschaftlich sensible Daten, die Absprachen auf dem Markt erleichtern könnten, Geschäftsgeheimnisse und andere Daten von großer strategischer Bedeutung für den Wettbewerb und rechtlich – etwa durch geistige Eigentumsrechte – geschützte Daten erstrecken, zu teilen.[226]

---

[213] IIA, a.a.O. (Fn. 9), S. 5. Konsultation, a.a.O. (Fn. 13), S. 13.
[214] Art. 6 Abs. 1 lit. h, I DMA.
[215] Siehe oben Kapitel 2.2.2
[216] IIA, a.a.O. (Fn. 9), S. 5.
[217] IIA, a.a.O. (Fn. 9), S. 5 „Laying down data access and use rights".
[218] Siehe Konsultation, a.a.O. (Fn. 13), S. 13 "horizontal access modalities would regulate (…) how data access rights should be exercised while the possible creation of sectoral data access rights would be left to future sectoral legislation (…)".
[219] EU-Datenstrategie, a.a.O. (Fn. 4), S. 16.
[220] Bertuzzi, a.a.O. (Fn. 6).
[221] Siehe dazu sogleich Kapitel 4.2.5.
[222] EU-Datenstrategie, a.a.O. (Fn. 4), S. 16.
[223] Siehe oben Kapitel 2.2.2.
[224] EU-Datenstrategie, a.a.O. (Fn. 4), S. 16.
[225] EU-Datenstrategie, a.a.O. (Fn. 4), S. 16.
[226] Konsultation, a.a.O. (Fn. 13), S. 13.

4.2.5 Harmonisierte Grundregeln für sektorspezifische Datenzugangs- und Nutzungsrechte

Wie bestehende und künftige Datenzugangs- und -nutzungsrechte in Bezug auf nicht-personenbezogene Daten in der Praxis ausgeübt werden sollen, will die Kommission durch allgemeine, EU-weit einheitliche Grundregeln im Data Act steuern. Wie in Kapitel 2.2.2 ausgeführt, sieht das EU-Recht auch im B2B-Bereich bereits verschiedene sektorspezifische Datenzugriffs- und/oder Nutzungsrechte vor. Neue Datenzugangs- und Nutzungsrechte sollen – wie im vorstehenden Kapitel dargelegt – künftig ebenfalls grundsätzlich in sektorspezifischen Rechtsakten geregelt werden.[227] Diese sektorspezifischen Rechte will die Kommission nun mit allgemein geltenden, harmonisierter Grundregeln umspannen, um sicherzustellen, dass der Datenzugang auf der Basis fairer, angemessener, verhältnismäßiger, transparenter und nichtdiskriminierender Bedingungen[228] erfolgt. Hierzu will sie im Data Act „horizontale Modalitäten“ festlegen, die konkretisieren, wie – z.B. zu welchen Konditionen – die Parteien den Datenzugang im Einzelnen vereinbaren müssen.[229] Diese Regelungen sollen die Grundlage für die Ausübung sektorspezifischer Datenzugangs- und Nutzungsrechte bilden, die in separaten Vorschriften geregelt sind oder werden. Auch bei sektorspezifischen Nutzungsrechten schließen die beteiligten Unternehmen in der Regel einen Vertrag, der die Ausübung dieses Rechts regelt. Dabei müssen sie dann künftig die allgemeinen Regeln des Data Act beachten.

Der Data Act wird Dateninhaber und Zugangsberechtigte daher voraussichtlich verpflichten, für Datenzugänge Verträge mit fairen, angemessenen, verhältnismäßigen, transparenten und nichtdiskriminierenden Bedingungen auszuhandeln. Diese Bedingungen können allerdings nach Ansicht der Kommission für unterschiedliche Szenarien durchaus variieren. Um den Besonderheiten spezifischer Märkte Rechnung zu tragen, sollen die allgemeinen Modalitäten in den einschlägigen sektorspezifischen Rechtsakten ggf. weiter spezifiziert werden.[230] Solche spezielleren Regeln wären dann von den Parteien dann ggf. vorrangig oder zusätzlich zu beachten.

Zusammengefasst ist das Zusammenspiel von Data Act und sektorspezifischem Recht offenbar wie folgt geplant:

- Sektorspezifische Rechtsakte regeln das „Ob“, d.h. die Frage, ob bzw. für wen unter welchen Voraussetzungen überhaupt ein Zugangsrecht besteht.
- Der Data Act regelt das „Wie“, d.h. die Frage, wie das Recht auf Datenzugang ausgeübt werden soll, d.h. wie die Parteien den Zugang zu Daten vereinbaren bzw. unter welchen Bedingungen dieser erfolgen muss.
- Sieht der sektorspezifische Rechtsakt speziellere Modalitäten vor, sind diese ggf. vorrangig oder zusätzlich zu beachten.

Die Kommission ist der Auffassung, dass allgemeine Grundregeln zu einem verstärkten Datenaustausch zwischen Unternehmen – auch von gemeinsam generierten IoT-Daten – beitragen könnten.[231] Durch die Vorgabe solcher Grundsätze will die Kommission das Interesse der datengesteuerten Unternehmen am Datenzugang einerseits und dasjenige der Dateninhaber am Erhalt einer adäquaten Rendite für ihre Investitionen andererseits in Einklang bringen und eine Win-Win-Situation für beide Seiten

[227] IIA, a.a.O. (Fn. 9), S. 5, Konsultation, a.a.O. (Fn. 13), S. 13.
[228] IIA, a.a.O. (Fn. 9), S. 5.
[229] IIA, a.a.O. (Fn. 9), S. 5.
[230] IIA, a.a.O. (Fn. 9), S. 5, Konsultation, a.a.O. (Fn. 13), S. 13. So will die Kommission z.B. die Regeln für bordeigene Daten („in-vehicle“-Daten) im Zuge der Überarbeitung der EU-Typgenehmigungsverordnung überprüfen, vgl. IIA, a.a.O. (Fn. 9)., S. 5.
[231] Konsultation, a.a.O. (Fn. 13), S. 16.

schaffen. Für die Fälle, in denen die Parteien nicht in der Lage sind, eine Einigung zu erzielen, soll ein horizontaler Streitbeilegungsmechanismus eingeführt werden und eine Lösung ermöglichen.[232]

Möglicherweise wird die Kommission in den Data Act auch ergänzende Regelungen einfügen, die sicherstellen sollen, dass die bereitgestellten Daten sicher und nicht missbräuchlich genutzt und dabei vertrauliche Geschäftsdaten geschützt werden.[233]

4.2.6 Haftungsregeln

Unklar ist, ob die Kommission in den Data Act auch Haftungsregeln im Zusammenhang mit der gemeinsamen Nutzung von Daten einführen wird. In der Datenstrategie hatte sie angekündigt, im Data Act ggf. die Regeln für die verantwortungsvolle Nutzung von Daten (z. B. die rechtliche Haftung) „präzisieren“ zu wollen.[234] Im IIA und in der Konsultation finden sich hierzu keine näheren Hinweise.

4.2.7 Vorläufige Einschätzung

Dass die Kommission Hindernisse für die Weiterverwendung von Daten im B2B-Bereich abbauen will, um die Datenwirtschaft in der EU zu fördern, ist grundsätzlich sachgerecht. Denn es bestehen gewisse Anhaltspunkte dafür, dass der bestehende regulatorische Rahmen einschließlich des Kartellrechts nicht ausreicht, um für einen ausreichenden Wettbewerb in der Datenwirtschaft zu sorgen und zukünftige Innovationen im Interesse der Gesellschaft zu ermöglichen.[235] Die Vorschläge der Kommission sind allerdings noch zu wenig konkret und zudem – je nach gewählter Option – in ihrer Eingriffswirkung sehr unterschiedlich, so dass an dieser Stelle auf eine Analyse aller einzelnen Optionen verzichtet wird. Bei der Regulierung sollte die EU aber folgende Erwägungen berücksichtigen:

- Datengenerierungsprozesse sind häufig komplex und dadurch gekennzeichnet, dass mehrere Akteure mit individuellen Interessen miteinander interagieren und dabei in unterschiedlichen Rollen zur Erzeugung von Daten beitragen.[236] Bei der Regulierung von Datenaustauschverträgen und Zugangsrechten müssen grundrechtlich die Rechtspositionen des Dateninhabers (Datengeber), die Interessen derjenigen, die Zugang zu den Daten begehren (Datennehmer)[237] und die Grundrechte betroffener Dritter berücksichtigt und in einen angemessenen Ausgleich gebracht werden. [238]
- Die Regelungen des Data Act greifen insbesondere in die grundrechtlich geschützten Rechte der Datengeber auf Schutz ihrer unternehmerischen Freiheit (Art. 16 GRCh) und ihres geistigen

[232] IIA, a.a.O. (Fn. 9), S. 5, siehe auch Bertuzzi, a.a.O. (Fn. 6).
[233] Darauf deuten die Formulierungen im IIA, a.a.O. (Fn. 9), S. 1, 2 hin.
[234] EU-Datenstrategie, a.a.O. (Fn. 4), S. 16.
[235] Ausführlich dazu Bertschek, I./Bonin, H./Kühling, J./Thüsing, G./Wenzel, T., Entwicklung eines Konzepts zur Datenallmende, Forschungsbericht Nr. 581, Expertise im Auftrag des deutschen Bundesministeriums für Arbeit und Soziales, Juli 2021, S. 26, 85 (insbesondere zu den kartellrechtlichen Hürden auf EU-Ebene S. 59ff,) abrufbar unter https://ftp.zew.de/pub/zew-docs/gutachten/Kurzexpertise-Entwicklung-Konzept-zur-Datenallmende_2021.pdf.
[236] Vgl. Gutachten der Datenethikkommission der deutschen Bundesregierung, Oktober 2019, S. 85, abrufbar unter https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/it-digitalpolitik/gutachten-datenethik-kommission.pdf;jsessionid=2032194AE8CDE254DACD6FE603B6F9FB.1_cid295?__blob=publicationFile&v=6.
[237] Dies kann der Nutzer eines IoT-Objekts sein, der seine Maschine reparieren (lassen), ein Zulieferer, der seine Qualität kontrollieren und verbessern, oder ein unbeteiligter Dritter, der mit Hilfe der Daten neue Produkte oder Dienstleistungen generieren will, vgl. Gutachten der Datenethikkommission, a.a.O. (Fn. 236), S. 91.
[238] Vgl., allerdings bezogen auf Datenzugangsrechte für Wissenschaft und Forschung, Specht-Riemenschneider, L., a.a.O. (Fn. 189), S. 5, 21. Zu den kollidierenden Grundrechten s. auch Bertschek/Bonin/Kühling/Thüsing/Wenzel, a.a.O. (Fn. 235), S. 62, die auch die hier weniger relevante Berufsfreiheit (Art. 15 GRCh) erwähnen.

Eigentums (Art. 17 Abs. 2 GRCh) ein. Betroffene Dritte haben insbesondere ein Recht auf Schutz ihrer Privatsphäre und ihrer personenbezogenen Daten (Art. 7, 8 GRCh).[239]

- Die Freiheit des geistigen Eigentums umfasst u.a. einen etwaigen urheberrechtlichen Datenbankschutz und das „Sui Generis"-Recht des Datengebers.[240] Die unternehmerische Freiheit schützt jegliche Art und Weise des Betriebs[241] und umfasst insbesondere das Recht eines Unternehmens, frei über seine wirtschaftlichen, technischen und finanziellen Ressourcen zu verfügen.[242] Zudem schützt sie die für die unternehmerische Tätigkeit bedeutsamen Geschäfts- und Betriebsgeheimnisse.[243] Daneben stellt der Schutz von Geschäftsgeheimnissen einen allgemeinen Grundsatz des Unionsrechts dar.[244] Art. 16 GrCh stützt sich auch auf Artikel 119 Abs. 1 und 3 AEUV[245], der den freien Wettbewerb anerkennt und als objektiv-rechtliches Prinzip der EU hervorhebt.[246] Noch ungeklärt ist, ob Art. 16 auch eine subjektiv-rechtliche Schutzdimension im Sinne eines Rechts für potenzielle Datennehmer hat, an einem unverfälschten Wettbewerb teilzunehmen.[247] Der Europäische Gerichtshof (EuGH) hat die Wettbewerbsfreiheit allerdings bislang noch nicht als subjektives Recht anerkannt.[248]
- Die inhaltliche Regulierung von Datenaustauschverträgen greift in die Vertragsfreiheit der beteiligten Unternehmen ein, weil diese bestimmte Bedingungen nicht mehr frei vereinbaren dürfen. Die Vertragsfreiheit ist ein zentraler Bestandteil des Grundrechts auf unternehmerische Freiheit.[249] Sie umfasst u.a. die Freiheit, den Vertragspartner zu wählen[250], Verträge inhaltlich auszugestalten[251] und Preise und sonstige Konditionen zu vereinbaren.[252] Es muss grundsätzlich den Unternehmen überlassen bleiben, mit wem sie unter welchen Bedingungen und zu welchem Preis ihre Daten teilen wollen. Daher sollte die Kommission beim Data Act wie

[239] Siehe auch Specht-Riemenschneider, L., a.a.O. (Fn. 189), S. 5.
[240] Specht-Riemenschneider, L., a.a.O. (Fn. 189), S. 5.
[241] EuGH, Urteil vom 18.09.1986, C-116/82, ECLI:EU:C:1986:322, Rn. 27 – Kommission/Deutschland, Jarass, Charta der Grundrechte der EU, 4. Auflage 2021, Art. 16 Rn. 10.
[242] EuGH, Urteil vom 27. März 2014, C-314/12, ECLI:EU:C:2014:192, Rn. 49 – UPC Telekabel Wien; Bertschek/Bonin/Kühling/Thüsing/Wenzel, a.a.O. (Fn. 235), S. 62, Jarass, a.a.O. (Fn. 241). Nicht durch Art. 17 geschützt wird allerdings das berechtigte Vertrauen auf die Beibehaltung einer bestehenden Situation, die durch Entscheidungen der Gemeinschaftsorgane im Rahmen ihres Ermessens verändert werden kann, vgl. EuGH, Urteil vom 5. 10. 1994, C-280/93, ECLI:EU:C:1994:367, Deutschland/Rat der EU; Jarass, a.a.O. (Fn. 241), Art. 17 Rn. 13 (zum Marktanteil eines Unternehmens).
[243] EuGH, Urteil vom 23.09.2004, C-435/02, ECLI:EU:C:2004:552, Rn. 49 – Springer, Jarass, a.a.O. (Fn. 241), Rn. 10, so wohl auch Specht-Riemenschneider, a.a.O. (Fn. 189), S. 5, 21.
[244] EuGH, Urteil vom 14. 2. 2008, C-450/06, ECLI:EU:C:2008:91, Rn. 49 – Varec SA/Belgien, EuGH, Urteil vom 29.03.2012, C-1/11 (Interseroh Scrap), ECLI:EU:C:2012:194, Rn. 44 – Interseroh Scrap, Jarass, a.a.O. (Fn. 254), Rn. 16, Bertschek/Bonin/Kühling/Thüsing/Wenzel, a.a.O. (Fn. 235), S. 64.
[245] Vertrag über die Arbeitsweise der Europäischen Union, ABl. C-326 vom 06.10.2012, S. 47ff.
[246] Vgl. die Erläuterungen zur Charta der Grundrechte (2007/C 303/02), ABl. C 303 vom 14.12.2007, S. 17ff., abrufbar unter https://eur-lex.europa.eu/legal-content/de/ALL/?uri=CELEX%3A32007X1214%2801%29, sowie Bertschek/Bonin/Kühling/Thüsing/Wenzel, a.a.O. (Fn. 235), S. 63.
[247] Dafür sprechen sich Bertschek/Bonin/Kühling/Thüsing/Wenzel, a.a.O. (Fn. 235), S. 63 m.w.N. aus.
[248] Bernsdorf, N., in Meyer/Hölscheidt, Charta der Grundrechte der Europäischen Union, 5. Auflage 2019, Rn. 15, Bertschek/Bonin/Kühling/Thüsing/Wenzel, a.a.O. (Fn. 235), S. 63 m.w.N. (dort Fn 110).
[249] EuGH, Urteil vom 22. Januar 2013, C-283/11, ECLI:EU:C:2013:28, Rn. 42 – Sky Österreich; EuGH, Urteil vom 18.07.2013, Rs. C-426/11, ECLI:EU:C2013:521, Rn. 32 – Alemo-Herron.
[250] EuGH, Urteil vom 05.10.1999, C-240/97, ECLI:EU:C:1999:479, Rn. 99 – Spanien/Kommission (bezogen auf das Recht, geschlossene Verträge zu ändern). Siehe auch Bertschek/Bonin/Kühling/Thüsing/Wenzel, a.a.O. (Fn. 235), S. 63.
[251] EuGH, Urteil vom C-426/11 ECLI:EU:C2013:521, Rn. 33f. – Alemo-Herron; siehe auch Bertschek/Bonin/Kühling/Thüsing/Wenzel, a.a.O. (Fn. 235), S. 63.
[252] Bertschek/Bonin/Kühling/Thüsing/Wenzel, a.a.O. (Fn. 235), S. 63.

von ihr angekündigt[253] die Vertragsfreiheit als Leitprinzip beachten. Freiwillige Regeln und Musterklauseln sind grundsätzlich vorzugswürdig.[254]

- Die genannten Grundrechte gelten jedoch nicht schrankenlos. Eingriffe in diese Rechte durch den Data Act können daher nach Art. 52 Abs.1 GRCh gerechtfertigt sein, wenn sie legitimen Zielen wie der Förderung des Gemeinwohls oder dem Schutz der Rechte anderer dienen.[255] Als legitimer öffentlicher Zweck für die Regelungen des Data Act kommt vor allem die Förderung von Wettbewerb und Innovation in Betracht.[256] Die Regelungen müssen aber verhältnismäßig, also zur Erreichung dieses Ziels geeignet, erforderlich und angemessen sein, was die Kommission genau darlegen muss.[257]
- Um die Vorschriften des Data Act verhältnismäßig auszugestalten, ist eine sorgfältige Abwägung der widerstreitenden Ziele, Rechte und Interessen der Datengeber, der potenziellen Datennehmer, betroffener Dritter und der Allgemeinheit erforderlich. Dabei sollte auch berücksichtigt werden, in welchem Umfang der Datennehmer zur Datengenerierung beigetragen hat, welches Gewicht die Interessen der Allgemeinheit und die einzelnen widerstreitenden Individualinteressen haben und wie die Macht zwischen dem Datengeber und dem potenziellen Datennehmer verteilt ist.[258] Diese Faktoren stehen in einer Wechselwirkung zueinander, so dass z.B. ein besonders hohes Allgemeininteresse an der Verbesserung des Datenzugangs einen besonders geringen Beitrag zur Datengenerierung ausgleichen kann.[259] Kompensationsmöglichkeiten[260] wie Vergütungen oder Schutzmaßnahmen gegen die Preisgabe von Geschäftsgeheimnissen können die Effekte des Eingriffs ggf. abmildern.
- Welche Regeln verhältnismäßig sind, hängt dabei von der Bewertung der ökonomischen Aspekte der einzelnen Regelungen und letztlich von deren Wertschöpfungs- und Innovationsbilanz ab.[261] In ökonomischer Hinsicht dürften u.a. folgende Aspekte zu berücksichtigen sein:
  - FÜR gesetzliche Regeln zur Erleichterung der Datenteilung könnte sprechen, dass das Teilen von Daten große Bedeutung für die Sicherstellung eines fairen und effizienten Wettbewerbs haben kann.[262] Erstens kann eine verbesserte Datenteilung ggf. einer Monopolisierung in datenbasierten Märkten vorbeugen[263] oder eine bereits bestehende Monopolmacht eindämmen, indem solche Märkte wieder dem Wettbewerb unterworfen werden.[264] So kann die verbesserte Nutzbarmachung möglicherweise eine Stärkung des Wettbewerbs bewirken, weil andere Anbieter dadurch leichter in Konkurrenz zu

[253] D'Cunha, C., a.a.O. (Fn. 3).
[254] EuGH, Urteil vom 18.07.2013, ECLI:EU:C2013:521, Rs. C-426/11 (Alemo-Herron).
[255] Jarass, a.a.O. (Fn. 241), Rn. 23
[256] So Bertschek/Bonin/Kühling/Thüsing/Wenzel, a.a.O. (Fn. 235), S. 72, für die Regulierung von Datenzugangsrechten zur Schaffung einer „Datenallmende".
[257] Allerdings räumt der EuGH dem EU-Gesetzgeber für komplexe wirtschaftliche Sachverhalte, bei denen er komplizierte Beurteilungen vornehmen muss, traditionell einen weiten Ermessenspielraum ein, vgl. EuGH, Urteil vom 10. Dezember 2002, C-491/01, EU:C:2002:741, Rn. 123 – British American Tobacco [Investments] und Imperial Tobacco, Jarass, a.a.O. (Fn. 241), Art. 16 Rn. 29, Bertschek/Bonin/Kühling/Thüsing/Wenzel, a.a.O. (Fn. 235), S. 164, zur „Datenallmende".
[258] Gutachten der Datenethikkommission der deutschen Bundesregierung, a.a.O. (Fn. 236), S. 17, 86.
[259] Gutachten der Datenethikkommission der deutschen Bundesregierung, a.a.O. (Fn. 236), S. 86.
[260] Ähnlich Specht-Riemenschneider, a.a.O. (Fn. 189), S. 22 zum Zugang zu Daten für Wissenschaft und Forschung.
[261] Ähnlich Bertschek/Bonin/Kühling/Thüsing/Wenzel, a.a.O. (Fn. 235), S. 14, 78, nach denen die rechtliche Bewertung einer „Datenallmende" stark von der Bewertung der ökonomischen Aspekte der Eingriffe abhängt.
[262] Ebenso Gutachten der Datenethikkommission der deutschen Bundesregierung, a.a.O. (Fn. 236), S. 82, 91.
[263] Bertschek/Bonin/Kühling/Thüsing/Wenzel, a.a.O. (Fn. 235), S. 13, 16 für das Instrument einer „Datenallmende".
[264] Prüfer, J., Die Datenteilungspflicht – Innovation und fairer Wettbewerb auf datengetriebenen Märkten, 2020, S. 12, abrufbar unter http://library.fes.de/pdf-files/fes/15990.pdf.

etablierten Unternehmen treten können. Dies könnte ggf. zu niedrigeren Verbraucherpreisen und somit zu Wohlfahrtssteigerungen führen.[265] Zweitens könnte eine verbesserte Datenteilung u.U. datengetriebene Innovationen erleichtern und auch auf diese Weise eine wohlfahrtssteigernde Wirkung entfalten.[266]

- GEGEN gesetzliche Regeln zur Erleichterung der Datenteilung lässt sich anführen, dass auch die Konzentration von Daten in einer Hand zu effizienten Geschäftsmodellen und Innovation führen kann.[267] Diese Erwägung liegt auch dem Schutz von Geschäftsgeheimnissen und geistigen Eigentums zugrunde.[268] Zudem können Datenteilungspflichten auch negative Effekte haben. Sie könnten evtl. Anreize für die Erhebung, Aufbereitung und den Schutz von zu teilenden Daten schwächen und damit Wohlfahrtseinbußen verursachen.[269] Relevant in diesem Zusammenhang könnte ein Urteil sein, in dem der EuGH anerkannt hat, dass es negative Auswirkungen auf die Schaffung neuer Werke haben kann, wenn die Vergütung des Herstellers trotz risikoreicher Investitionen in die Herstellung von Erzeugnissen nicht mehr angemessen gewährleistet werden kann.[270] Zudem kann die Sicherstellung des freien Wettbewerbs möglicherweise zugleich für und gegen erweiterte Datenzugangsrechte in die Waagschale geworfen werden.[271]
- Je tiefer der Eingriff in die unternehmerische Freiheit oder die Eigentumsfreiheit zu werten ist, desto stärker müssen die ökonomischen Rechtfertigungsgründe sein.[272] Diese Bilanz kann von Markt zu Markt unterschiedlich ausfallen, da sich die spezifischen Gegebenheiten auf einzelnen datenbasierten Märkten unterscheiden.[273] Daher muss – bezogen auf den konkret betroffenen Markt – u.a. geprüft werden, in welchem Umfang durch den verbesserten Datenzugriff der Wettbewerb verbessert, Innovationen beflügelt und Anreize für Investitionen in die Erhebung oder Aufbereitung von Daten gehemmt werden könnten.

- Angesichts dieser Unterschiede auf den einzelnen Märkten erscheint es sachgerecht, dass die Kommission etwaige Datenzugriffs- und Nutzungsrechte sektorspezifisch regeln will. Die parallel dazu geplante Festlegung horizontaler Grundregeln für die Ausübung solcher Rechte im Data Act kann deren EU-weit einheitliche Ausübung und die sektorübergreifende gemeinsame Datennutzung erleichtern. Mustervertragsklauseln sowie ein „Fairness-Test“ können zudem helfen, ungleiche Verhandlungspositionen einander anzunähern und so den freiwilligen Datenaustausch fördern. Mustervertragsklauseln können zudem die Kosten für den Abschluss von Datennutzungsvereinbarungen senken. Die Schwierigkeit liegt allerdings darin, dass die Regeln des Data Act für eine Vielzahl von Wirtschaftssektoren und damit für sehr unterschiedliche Bereiche und Geschäftsmodelle der Datenwirtschaft mit stark divergierenden Interessen

[265] Bertschek/Bonin/Kühling/Thüsing/Wenzel, a.a.O. (Fn. 235), S. 38 in Bezug auf Offenlegungspflichten.
[266] Bertschek/Bonin/Kühling/Thüsing/Wenzel, a.a.O. (Fn. 235), S. 13, 16, für das Instrument einer „Datenallmende“.
[267] Bertschek/Bonin/Kühling/Thüsing/Wenzel, a.a.O. (Fn. 235), S. 38, in Bezug auf die „Datenallmende“.
[268] Ähnlich Bertschek/Bonin/Kühling/Thüsing/Wenzel, a.a.O. (Fn. 235), S. 38.
[269] Bertschek/Bonin/Kühling/Thüsing/Wenzel, a.a.O. (Fn. 235), S. 13, 27, 78 zur Datenallmende.
[270] EuGH, Urteil vom 28.04.1998, C-200/96, ECLI:EU:C:1998:172, Rn. 24 – Metronome Musik (zur freien Berufsausübung). In diesem Urteil hat der EuGH im Rahmen der Prüfung der Verhältnismäßigkeit eines ausschließlichen Rechts für den Hersteller von Tonträgern den Schutz hoher und risikoreicher Investitionen dieser Hersteller als schützenswertes Interesse erachtet, zumal Tonträger von Produktpiraten besonders leicht vervielfältigt werden könnten. Zur Relevanz dieses Urteils auch Bertschek/Bonin/Kühling/Thüsing/Wenzel, a.a.O. (Fn. 235), S. 75.
[271] So Bertschek/Bonin/Kühling/Thüsing/Wenzel, a.a.O. (Fn. 235), S. 64.
[272] Bertschek/Bonin/Kühling/Thüsing/Wenzel, a.a.O. (Fn. 235), S. 79.
[273] Bertschek/Bonin/Kühling/Thüsing/Wenzel, a.a.O. (Fn. 235), S. 14, 78.

der einzelnen Akteure gelten sollen. Die Kommission muss deshalb sicherstellen, dass die Vorschriften des Data Act für alle betroffenen Marktteilnehmer „passen" und zudem sektorspezifischen Rechtsvorschriften nicht widersprechen. Ob es der Kommission gelingen wird, „faire" Bedingungen für Datenaustauschverträge bzw. verbotene grob nachteilige Klauseln auf allgemeiner Ebene und ex ante hinreichend präzise zu regeln, bleibt abzuwarten. Auch hier könnten ggf. zumindest ergänzende sektorspezifische Regeln bzw. Mustervertragsklauseln sachgerecht sein.

- Ferner ist zu beachten, dass der Handel mit Daten und die Entstehung nachgelagerter Datenmärkte aktuell durch eine Vielzahl von Hindernissen rechtlicher, wirtschaftlicher und technischer Art gehemmt wird.[274] Nicht alle dieser Hemmnisse lassen sich durch Regulierung beseitigen.[275] Zu den wichtigsten *rechtlichen Hindernissen* gehören laut einer Studie des Instituts der deutschen Wirtschaft im Auftrag des BDI[276] Sorgen vor einem unautorisierten Zugriff Dritter auf die Daten, ferner datenschutzrechtliche Grauzonen, Unklarheiten bezüglich der Nutzungsrechte an den Daten sowie die fehlende Möglichkeit einer rechtssicheren Anonymisierung personenbezogener Daten.[277] Die Sorge, mit der Weitergabe von Daten einen Kontrollverlust zu erleiden und Geschäftsgeheimnisse preiszugeben, überwiegt bei den Unternehmen noch gegenüber der Aussicht auf mögliche Vorteile durch die wirtschaftliche Nutzung oder Vermarktung der im Unternehmen gewonnene Daten.[278] Dies könnte daran liegen, dass Unternehmen sich des potenziellen Nutzens eines Datenaustauschs noch zu wenig bewusst sind[279] – hierin liegt neben den Kosten zur Ermöglichung des Datenaustauschs ein weiteres, *wirtschaftliches Hindernis*. Die Möglichkeit, im Unternehmen gewonnene Daten wirtschaftlich zu nutzen oder zu vermarkten, ist vielen Unternehmen entweder noch zu wenig bekannt oder erscheint ihnen nicht lukrativ.[280] Letzteres wiederum könnte damit zusammenhängen, dass viele Unternehmen offenbar keine klare Vorstellung von einem „angemessenen" Wert von Daten haben.[281] Aber auch *technische Hindernisse*, insbesondere die mangelnde Interoperabilität von Datensätzen und Informationssystemen, inkompatible Standards oder unterschiedliche Systeme der Datenspeicherung, stellen ein Problem dar.[282]
- Angesichts der Vielzahl bestehender Hindernisse ist generell zu hinterfragen, inwieweit Datenteilungs- und sonstige Pflichten geregelt werden sollten, bevor nicht zunächst oder zumindest gleichzeitig auch zumindest die wichtigsten übrigen rechtlichen, technischen und wirtschaftlichen Hemmnisse beseitigt werden. Solche Pflichten sind wenig zielführend, solange es an Rechtssicherheit, Vertrauen, Bereitschaft und der nötigen Interoperabilität fehlt. Andernfalls

[274] Näher dazu Van Roosebeke, B./Anzini, M./Eckhardt, P./Pierrat, A., cep**Study** a.a.O. (Fn. 34), S. 36ff.
[275] Van Roosebeke, B./Anzini, M./Eckhardt, P./Pierrat, A., cep**Study**, a.a.O. (Fn. 34), S. III.
[276] Röhl, K.-H./Bolwin, L./Hüttl, P., Datenwirtschaft in Deutschland – Wo stehen die Unternehmen in der Datennutzung und was sind ihre größten Hemmnisse?, Studie des Instituts der deutschen Wirtschaft (iw) im Auftrag des BDI, 24.02.2021, S. 4, 40f., abrufbar unter https://www.iwkoeln.de/studien/klaus-heiner-roehl-lennart-bolwin-wo-stehen-die-unternehmen-in-der-datennutzung-und-was-sind-ihre-groessten-hemmnisse.html.
[277] Näher hierzu siehe bereits oben die Ausführungen zur Datenteilung im B2G-Bereich (Kapitel 4.1.7).
[278] Röhl, K.-H./Bolwin, L./Hüttl, P., a.a.O. (Fn. 276), S. 46.
[279] Laut Röhl, K.-H./Bolwin, L./Hüttl, P., a.a.O. (Fn. 276), S. 40 f. trifft dies auf ¾ der deutschen Unternehmen zu.
[280] Laut Röhl, K.-H./Bolwin, L./Hüttl, P., a.a.O. (Fn. 276), S. 41, nannten 77,1 % der befragten deutschen Unternehmen den unklaren Nutzen des Datenaustauschs als limitierenden Faktor für die Datennutzung.
[281] Dies gaben 63% der befragten Unternehmen an, vgl. Röhl, K.-H./Bolwin, L./Hüttl, P., a.a.O. (Fn. 276), S. 40, 41.
[282] Van Roosebeke, B./Anzini, M./Eckhardt, P./Pierrat, A., cep**Study**, a.a.O. (Fn. 34), S. 36f., siehe dazu auch Röhl, K.-H./Bolwin, L./Hüttl, P., a.a.O. (Fn. 276), S. 41, laut der die Unternehmen insbesondere auch fehlende Möglichkeiten zur technischen Absicherung der Daten als Hindernis angaben.

besteht die Gefahr, dass der Data Act nicht die gewünschte Wirkung entfaltet, was u.U. auch Probleme hinsichtlich der Verhältnismäßigkeit aufwerfen könnte.

- Einige dieser Hindernisse will die Kommission mit dem Data Act angehen: So will sie etwa die Unklarheiten bezüglich der Nutzungsrechte an Daten beseitigen. Zudem könnten Transparenzpflichten, welche Daten durch IoT-Objekte erhoben werden und wer sie wie nutzen darf, den Unternehmen helfen, den Wert der Daten besser zu beurteilen. Ob das Problem, Daten einen angemessenen Wert beizumessen, dadurch gelöst werden kann, ist aber fraglich. Da es offensichtlich auf dem Markt noch keine klaren Vorstellungen über einen „angemessenen" Wert von Daten gibt, wird die mögliche Regulierung einer „fairen" Vergütung für die Bereitstellung von Daten durch die EU – insbesondere dann, wenn ex ante und in horizontalen Regelungen – besonders kritisch zu prüfen sein.
- Über diese vertraglichen Probleme hinaus müssen auch die technischen und wirtschaftlichen Barrieren beseitigt werden. Die Kommission sollte sich daher – wo nötig – auch (weiter) für die Verbesserung der Interoperabilität und die Erarbeitung von Normen in enger Abstimmung mit den relevanten Wirtschaftsakteuren einsetzen. Ferner sollte sie Maßnahmen unterstützen, die den Unternehmen den potenziellen wirtschaftlichen Nutzen der freiwilligen Datennutzung und -vermarktung zu verdeutlichen, ihr Bewusstsein stärken und damit deren Bereitschaft zum Datenaustausch erhöhen.
- Ferner muss sichergestellt werden, dass Unternehmen nicht länger aus Angst vor der Verletzung von Geschäftsgeheimnissen, geistigen Eigentumsrechten, des Wettbewerbsrechts[283] oder von Datenschutzvorschriften oder aus Angst vor Cybersicherheitsrisiken vor einer freiwilligen Weitergabe ihrer Daten zurückschrecken. Sie sollten insbesondere darauf vertrauen können, dass Daten und Geschäftsgeheimnisse auch bei der Weiterverarbeitung angemessen geschützt bleiben.
- Daher wird es maßgeblich darauf ankommen, ob es gelingt, das Vertrauen in den Datenaustausch zu stärken. Ausgewogene rechtliche Regelungen und eine effektive Durchsetzung vertraglicher Pflichten dürften insoweit aber nur ein Baustein sein. Ein praktikabler Streitbeilegungsmechanismus kann dazu ein wichtiger Beitrag sein. Der Data Act darf aber auch andere wichtige Punkte wie die Frage der Gewährleistung und Haftung für unrichtige oder nicht repräsentative Daten (Datenmängel) oder bei der Verletzung vertraglicher Pflichten aus Datenaustauschverträgen nicht ausklammern. Es muss sichergestellt werden, dass etwaige vertragliche Ansprüche wegen Pflichtverletzung nach dem Recht der Mitgliedstaaten auch durchgesetzt werden können. Daneben ist es wichtig, praktikable und risikoarme Möglichkeiten des Datenaustausch und sichere Speichermöglichkeiten zu etablieren, die sicherstellen, dass es bei der Weiterverwendung nicht zu unautorisierten Zugriffen auf die Daten kommt. Einen enormen Beitrag hierzu könnte das vernetzte Dateninfrastrukturprojekt Gaia-X leisten.[284] Dieses soll etwa als neutrale Plattform für den Datenaustausch fungieren können, wenn ein Hersteller bestimmte Betriebsdaten von der Maschine eines Drittanbieters benötigt, um seine Produktion sicherer und effizienter zu gestalten.[285] So soll etwa einer der zahlreichen Anwendungsfälle, die unter Gaia-X entstehen sollen, im Bereich Mobilität eine Plattform für den

[283] Hilfreich könnte ggf. eine kartellrechtliche Klarstellung sein, wann ein Teilen von Daten als wettbewerbs- bzw. kartellrechtswidrige Kooperation gewertet werden kann.
[284] Näher zu Gaia-X siehe etwa Van Roosebeke, B./Anzini, M./Eckhardt, P./Pierrat, A., cep**Study**, a.a.O. (Fn. 34), S. 114ff.
[285] https://www.ahd.de/gaia-x-was-die-europaeische-megacloud-leisten-soll/.

vertrauenswürdigen Austausch von branchenspezifischen Daten und KI-Modellen schaffen, um die Digitalisierung der mittelständisch geprägten Kfz-Werkstattbranche voranzutreiben.[286]

- Schließlich müssen bestehende Rechtsunsicherheiten im Zusammenhang mit der DSGVO[287] beseitigt werden, die Anwendung findet, wenn Datensätze personenbezogene Daten enthalten. Dies ist häufig der Fall, da es sich bei der Mehrzahl der Datensätzen um gemischte Datensätze handelt.[288] Eine bloße Regelung, dass die DSGVO Vorrang hat, wäre hierzu allerdings wenig hilfreich. Geklärt werden muss u.a.
  - ab wann Daten als anonymisiert[289] gelten und die Anwendbarkeit der DSGVO daher ausgeschlossen ist[290]; hier sollte die EU schnellstmöglich eine Lösung anstreben, etwa durch Unterstützung der Entwicklung von Standards, bei deren Einhaltung ein hinreichender Anonymisierungsgrad vermutet wird,
  - ob und wenn ja, ab wann die gemeinsame Nutzung von Daten zu einer gemeinsamen Verantwortlichkeit[291] für die Daten und die Einhaltung der DSGVO-Pflichten führt, und
  - auf welche Rechtsgrundlage die Weiterverwendung von Daten gestützt werden kann. Dies ist problematisch, da die DSGVO eine zweckändernde Weiterverarbeitung nur unter engen Bedingungen erlaubt und die Einholung von Einwilligungen oft unpraktikabel ist. Ob die angekündigten Hinweise der Kommission zur Rechtsgrundlage hilfreich sein werden, ist zweifelhaft. Um eine rechtssichere gemeinsame Datennutzung zu ermöglichen, dürfte eine Erweiterung der gesetzlicher Erlaubnistatbestände und damit letztlich eine Änderung der DSGVO erforderlich sein.[292]
- Insgesamt betrachtet muss die Kommission verhindern, dass der Data Act bestehende Unterschiede in den Verhandlungspositionen von Datengebern und -nehmern durch die Hintertür verstärkt und somit – zumindest anfänglich – kontraproduktiv wirkt. Diese Gefahr könnte drohen, wenn die Erleichterung des Datenaustauschs zunächst vor allem marktstarken Anbietern nutzt, die bereits über die nötigen Kompetenzen und Strukturen für die Nutzung von Daten verfügen, verfügen, während kleinere Unternehmen insbesondere angesichts bestehender rechtlicher, wirtschaftlicher und technischer Hindernisse noch nicht in der Lage sind, vom Datenaustausch zu profitieren.
- Um zusätzliche Rechtsunsicherheit zu vermeiden, muss die Kommission den Data Act mit anderen Rechtsvorschriften über Daten – insbesondere mit dem Data Governance Act, den Digital Markets Act, der DSGVO und den einschlägigen sektorspezifischen Rechtsvorschriften, die

[286] https://www.bundesnetzagentur.de/DE/Allgemeines/DieBundesnetzagentur/Insight/Texte/Blog1_Digitalisierung_Gaia-X.html.

[287] Datenschutzrechtliche Unklarheiten gehören zu den am meisten genannten Hindernissen, siehe weiter oben in diesem Abschnitt.

[288] Leitlinien zur Verordnung über einen Rahmen für den freien Verkehr nicht-personenbezogener Daten in der Europäischen Union, Mitteilung COM(2019) 250, S. 4, abrufbar unter https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:52019DC0250&from=DE.

[289] Laut Erwägungsgrund 26 findet die DSGVO auf anonymisierte Daten keine Anwendung.

[290] Gründe für die aktuell bestehende Rechtsunsicherheit in Bezug auf die Anonymisierung sind u.a. unklare Regelungen in der DSGVO und fehlende technische Standards, vgl. BDI, Praxisleitfaden Anonymisierung personenbezogener Daten, Stand Oktober 2020, S. 6, abrufbar unter https://bdi.eu/publikation/news/anonymisierung-personenbezogener-daten/.

[291] Art. 26 DSGVO.

[292] Ebenso, wenn auch bezogen auf den Data Governance Act, Veil, W., Data Governance Act II: Datenmittler, CR-online.de Blog vom 11.10.2021, abrufbar unter https://www.cr-online.de/blog/2021/10/11/in-der-datenschutzrechtlichen-todes-zone-der-data-governance-act-teil-ii/.

Datennutzungsrechte regeln – genau abstimmen und die Anwendungsbereiche dieser Rechtsakte klar abgrenzen.

- Auch die deutsche Bundesregierung hat in ihrem Koalitionsvertrag ein Datengesetz angekündigt.[293] Sofern ein derartiger paralleler Regulierungsansatz tatsächlich für sachgerecht gehalten wird, sollte Deutschland die europäische Gesetzgebung im Auge behalten und – soweit möglich – auf einen deutschen Sonderweg verzichten. Wird der EU Data Act als Verordnung erlassen, was zu erwarten ist, wird er in seinem Anwendungsbereich das deutsche Gesetz verdrängen, soweit er keine Öffnungsklauseln für die Mitgliedstaaten vorsieht.

4.3 Mögliche Anpassung der Datenbankrichtlinie

Wie in Kapitel 3.2.3 angesprochen, überprüft die Kommission derzeit die Datenbankrichtlinie und will diese ggf. anpassen, um den Zugang zu Daten und deren Nutzung im Rahmen der Datenwirtschaft zu erleichtern. Insbesondere will sie die Anwendbarkeit des Sui-Generis-Rechts auf maschinengenerierte Daten klarstellen und so Rechtssicherheit schaffen.

4.3.1 Rechtlicher Hintergrund im Detail

Zwar ist der Anwendungsbereich des Sui-Generis-Rechts derzeit eng gefasst[294], so dass übermäßige Sui-Generis-Rechte an IoT-Datenbanken die Datenwirtschaft auf den ersten Blick nicht wesentlich zu beschränken drohen. Der EuGH legt den Begriff der „wesentlichen Investitionen“ sehr eng aus und bejaht ein Sui-Generis-Schutzrecht nur dann, wenn die Investitionen gerade in die Beschaffung (Sammlung) von Daten und nicht lediglich in deren Erzeugung getätigt werden.[295] Dabei versteht der Gerichtshof unter „Beschaffung“ die *Ermittlung* bereits *vorhandener* Elemente und deren *Zusammenstellung* in einer Datenbank.[296] Aus dieser EuGH-Rechtsprechung wird weithin abgeleitet, dass sogenannte „Spinoff-Datenbanken“ aus Daten, die in einem Unternehmen notwendigerweise als Nebenprodukt anfallen, nicht schutzfähig sind, weil die maßgeblichen Investitionen in die Erzeugung sensor- oder maschinengenerierter Daten (nicht aber in deren Beschaffung) getätigt würden.[297] Unklar sei auch, ob überhaupt eine *Investition* vorliege, wenn Industriedaten quasi als Beiprodukt anfallen, was gerade bei Industrie 4.0-Sachverhalten typisch ist.[298] Datenbanken, die aus erzeugten und nicht aus beschafften

---

[293] Koalitionsvertrag 2021 – 2025 zwischen der Sozialdemokratischen Partei Deutschlands (SPD), BÜNDNIS 90 / DIE GRÜNEN und den Freien Demokraten (FDP), Mehr Fortschritt wagen – Bündnis für Freiheit, Gerechtigkeit und Nachhaltigkeit, S. 17, https://www.bundesregierung.de/resource/blob/974430/1990812/04221173eef9a6720059cc353d759a2b/2021-12-10-koav2021-data.pdf?download=1: *„Für alle, die an der Entstehung von Daten mitgewirkt haben, stärken wir den standardisierten und maschinenlesbaren Zugang zu selbsterzeugten Daten. Mit einem Datengesetz schaffen wir für diese Maßnahmen die notwendigen rechtlichen Grundlagen*:“

[294] Europäische Kommission, Evaluation of Directive 96/9/EC on the legal protection of databases, 25.04.2018 [SWD(2018) 146], S. 24.

[295] Siehe u.a. EuGH, Urteil vom 9. November 2004, British Horseracing Board, C-203/02, ECLI:EU:C:2004:128, Rn. 31. Europäische Kommission, Zusammenfassung der Bewertung der Richtlinie 96/9/EG über den rechtlichen Schutz von Datenbanken vom 25.04.2018, SWD(2018) 147, S. 3. Europäische Kommission, Evaluation of Directive 96/9/EC, a.a.O. (Fn. 294), S. 15, 19, 24. Industriedaten können daher zumindest in der Zwischenphase zwischen ihrer Erzeugung und späteren Sammlung (Aufnahme in eine Datenbank) ungeschützt sein, vgl. Wiebe, A., Protection of industrial data – a new property right for the digital economy?, GRUR Int. 2016, 877 (879).

[296] Das Schutzrecht sui generis solle einen Anreiz für die Erstellung von Datenbanken aus vorhandenen Informationen und nicht für die Erzeugung von Daten geben, die später in einer Datenbank zusammengestellt werden können (vgl. EuGH, British Horseracing Board, a.a.O., Rn. 31). Siehe auch Europäische Kommission, Evaluation of Directive 96/9/EC, a.a.O. (Fn. 294), S. 24. Bei der Frage, ob wesentliche Investitionen in die Erstellung der Datenbank getätigt wurden, dürfen deshalb nur Mittel berücksichtigt werden, die in die Ermittlung bereits vorhandener Elemente und deren Zusammenstellung in einer Datenbank geflossen sind. Investitionen in die Erzeugung von Daten sind dagegen nicht berücksichtigungsfähig.

[297] Europäische Kommission, Evaluation of Directive 96/9/EC, a.a.O. (Fn. 294), S. 35, 36 m.w.N.

[298] Zech: „Industrie 4.0“ – Rechtsrahmen für eine Datenwirtschaft im digitalen Binnenmarkt, GRUR 2015, S. 1151 (1058).

Daten bestehen, seien damit nicht schutzfähig.[299] Auch die nationale Rechtsprechung ist dem EuGH weitgehend gefolgt.[300] Es ist aber fraglich, ob diese Rechtsprechung vollends zum Ausschluss von maschinen- und sensorgenerierter Daten vom Sui-Generis-Recht führt:

Erstens ist die Unterscheidung zwischen Investitionen in die Beschaffung und in die Erzeugung von Daten im Einzelnen schwierig und sorgt für Rechtsunsicherheit. Unklar ist insbesondere, ob die *Aufzeichnung* bereits vorhandener Daten als Beschaffung zu werten und damit schutzfähig sein kann.[301] Dann könnten von Sensoren gemessene und aufgezeichnete Daten wie Temperatur, Geschwindigkeit oder Luftfeuchtigkeit als Datenbank Sui-Generis-Schutz beanspruchen, vorausgesetzt, dass dafür erhebliche Investitionen getätigt wurden. Der deutsche Bundesgerichtshof[302] hat den Sui-Generis-Schutz im Jahr 2010 in Bezug auf Daten über die Autobahnnutzung, die über stationäre Terminals und mobile Geräte zum Zweck der Mautberechnung ermittelt wurden, teilweise bejaht. Denn die erfassten Daten seien bereits vorhanden gewesen und damit nicht erzeugt, sondern gesammelt und geordnet worden, z.B. das KFZ-Kennzeichen, Datum der Fahrt und die Streckenlänge.[303]

Zweitens können neben der Beschaffung auch wesentliche Investitionen in die *Überprüfung* oder *Darstellung* des Inhalts einer Datenbank zum Entstehen des Sui-Generis-Schutzes führen.[304] Der BGH hat daher auch die Kosten für ein Rechenzentrum für relevant erachtet, soweit dessen Tätigkeit auch die Aufbereitung und Zusammenstellung der gesammelten Mautdaten umfasste.[305] Daher stellt sich die weitere Frage, ob ein Schutz zu bejahen ist (oder sein sollte?), wenn eine große Datenflut im Unternehmen durch Verarbeitung, Strukturierung und Optimierung nutzbar gemacht wird, etwa im Rahmen einer Big Data-Analyse von maschinell erzeugten IoT-Daten, oder durch die kostenintensive Verifizierung, Strukturierung oder Aktualisierung von Datenbankinhalten.[306] Ebenso ist unklar, wie es sich auswirkt, wenn mit Sensoren ausgestattete, vernetzte IoT-Objekte (z.B. Industrieroboter) Daten nicht nur automatisiert erheben, sondern die Daten auch bereits systematisch kategorisieren.[307]

In der von der Kommission durchgeführten Konsultation zum Data Act hat sich denn auch die Mehrheit der Befragten für eine Überarbeitung des Sui-Generis-Rechts ausgesprochen. Als größte Schwierigkeit im Zusammenhang mit dem Zugang und der Nutzung von Daten wurde die mangelnde Klarheit über die Anwendung dieses Rechts insbesondere auf maschinell erzeugte Daten genannt.[308]

4.3.2 Vorläufige Einschätzung

- Es ist wichtig, dass die Kommission Rechtsklarheit schafft, ob und wenn ja, wann Unternehmen für automatisch aufgezeichnete Sensorwerte und sonstige Maschinendaten Sui-Generis-Schutz nach der Datenbankrichtlinie beanspruchen können.

[299] Europäische Kommission, Evaluation of Directive 96/9/EC, a.a.O. (Fn. 294), S. 36 m.w.N.
[300] Europäische Kommission, Evaluation of Directive 96/9/EC, a.a.O. (Fn. 294), S. 16 m.w.N.
[301] Europäische Kommission, Evaluation of Directive 96/9/EC, a.a.O. (Fn. 294), S. 25 m.w.N.
[302] BGH, Urteil vom 25.03.2010, Az. I ZR 47/08 „Autobahnmaut“, Rn. 16 ff.
[303] Dagegen hat der BGH den Schutz verneint, soweit die Daten erst errechnet und somit erzeugt wurden, was bei der zu zahlenden Maut der Fall war.
[304] Art. 7 Abs. 1 Datenbank-Richtlinie 96/9/EG.
[305] BGH, Urteil vom 25.03.2010, Az. I ZR 47/08 „Autobahnmaut“, Rn. 20 f.
[306] Dafür Sagstetter, T., Neue Regeln für Big Data & Co.?, S. 18ff., abrufbar unter https://epub.ub.uni-muenchen.de/60564/1/Sagstetter_Digitaler_Strukturwandel_und_Privatrecht.pdf.
[307] Ebenso zu Recht Europäische Kommission, Evaluation of Directive 96/9/EC (a.a.O.), S. 15.
[308] Summary Report of the public consultation, a.a.O. (Fn. 48), S. 5.

- Die Kommission muss zudem sicherstellen, dass die Datenbankrichtlinie die Balance zwischen dem etwaigen Schutz des Datenbankerstellers bzw. des „Inhabers“ von Datensätzen einerseits und den Interessen anderer an der Nutzung dieser Datensätze andererseits wahrt.
- Ist der Schutz zu eng, kann es an Anreizen für Investitionen in die Erstellung von Datenbanken fehlen, andererseits könnte ein zu weitgehender Sui-Generis-Schutz für IoT-Daten zu einem Hemmschuh für datenbasierte Innovationen werden. Zwar können unwesentliche Teile einer Datenbank vom rechtmäßigen Nutzer ohne Genehmigung verwendet werden; lückenhafte Datensätze sind für datenanalytische Zwecke jedoch von geringerem Wert.[309]

[309] Europäische Kommission, Evaluation of Directive 96/9/EC, a.a.O. (Fn. 294), S. 24.

5 Zusammenfassung der wichtigsten Punkte

Während die unter der EU-Datenstrategie bisher erlassenen Rechtsakte maßgeblich darauf abzielen, im Besitz öffentlicher Stellen befindliche Daten leichter zugänglich zu machen, will die EU mit dem Data Act nun auch die Weiterverwendung von Daten privater Unternehmen fördern und hierzu sowohl anderen Unternehmen als auch öffentlichen Stellen den Zugang zu solchen Daten, insbesondere zu gemeinsam erzeugten, nicht-personenbezogenen IoT-Daten erleichtern. Ferner will sie die Datenbankrichtlinie anpassen, die Portabilität von personenbezogenen Daten und Cloud-Diensten verbessern, Regeln für intelligente Verträge festlegen und Daten gegen Zugriffe aus Drittstaaten schützen.

5.1 Zu den Regelungen für den Datenaustausch im B2G-Bereich

Zur Förderung der **Weiterverwendung von Unternehmensdaten** durch den **öffentlichen Sektor** (**B2G**) könnte der Data Act u.a.

- die **Ziele** der Nutzung solcher Daten sowie **allgemeine Pflichten der Parteien** und einen Streitbeilegungsmechanismus festlegen,
- **Unternehmen verpflichten, öffentlichen Stellen die Weiterverwendung bestimmter Unternehmensdaten zu ermöglichen,** wenn hieran ein **klares öffentliches Interesse besteht**,
- **Vorgaben zur Vergütung** oder zumindest **allgemeine Bedingungen** regeln, **zu denen Unternehmen in diesem Fall Daten bereitstellen müssen**,
- **öffentliche Stellen** bei der Weiternutzung u.a. **verpflichten, Maßnahmen zum Schutz von Daten und Geschäftsgeheimnissen zu ergreifen**,
- **Transparenzpflichten für öffentliche Stellen regeln**, wie sie die Daten weiterverwenden,
- **finanzielle oder andere Anreize** vorsehen, um Unternehmen freiwillig zum Teilen ihrer Daten mit öffentlichen Stellen zu bewegen,
- einen **Streitbeilegungsmechanismus** vorsehen.

Vorläufige Einschätzung:

- Bei der Regulierung der Weiterverwendung von Daten des Privatsektors durch die öffentliche Hand muss die EU das öffentliche Interesse an der Weiternutzung der Daten mit den damit kollidierenden Grundrechten der Beteiligten in einen angemessenen Ausgleich bringen, u.a. mit den geistigen Eigentumsrechten und der unternehmerischen Freiheit der Dateninhaber und den Rechten Dritter auf Privatsphäre und Datenschutz.
- Die EU sollte primär die freiwillige Bereitstellung von Daten an staatliche Stellen fördern. Datenteilungspflichten für private Unternehmen stellen einen erheblichen Eingriff in deren Grundrechte dar. Solche Pflichten müssen verhältnismäßig ausgestaltet und auf Ausnahmesituationen beschränkt werden, in denen eine freiwillige Kooperation oder sonstige alternative Beschaffung als milderes Mittel ausscheidet. Unternehmen sollten die Datenteilung verweigern können, wenn ihr Interesse daran im Einzelfall das öffentliche Interesse erheblich überwiegt.
- Der Data Act muss die öffentlichen Interessen bzw. die diesen dienenden Zwecke für die Weiternutzung der Daten so genau wie möglich definieren und klar vorgeben, nach welchen Kriterien die Mitgliedstaaten weitere öffentliche Interessen bzw. Zwecke festlegen dürfen.
- Unternehmen sollten für die Bereitstellung von Daten an den Staat grundsätzlich adäquat entlohnt werden. Ob adäquate Preise horizontal ex ante festgelegt werden können, ist aber fraglich.

- Interessierte öffentliche und private Akteure müssen einander finden. Es ist daher sachgerecht, dass die Kommission den B2G-Datenaustausch mit Hilfe von Datenintermediären erleichtern will.
- Die Kommission sollte Sorge tragen, dass der öffentliche Sektor fachlich und technisch überhaupt in der Lage ist, das Potenzial bereitgestellter Unternehmensdaten auszuschöpfen.
- Damit Unternehmen nicht länger aus Angst vor der Verletzung von Geschäftsgeheimnissen, geistigen Eigentumsrechten, Datenschutzvorschriften und mangelnder Cybersicherheit vor einer freiwilligen Weitergabe ihrer Daten zurückschrecken, ist es sachgerecht, dass die Kommission die öffentlichen Stellen verpflichten will, die Daten bei der Weiterverarbeitung angemessen zu schützen.
- Um einen Missbrauch der bereitgestellten Daten zu verhindern, sollten öffentliche Stellen zu Transparenz verpflichtet werden und die Unternehmensdaten nur streng zweckgebunden verwenden dürfen. Eine Weitergabe an Dritte sollte vergleichbar strengen Bedingungen unterworfen werden.

5.2 Zu den Regelungen für den Datenaustausch im B2B-Bereich:

Um **Unternehmen den Abschluss von Datenaustauschverträgen zu erleichtern** (B2B) und damit insbesondere die **Weiterverwendung von Daten zu fördern, die von vernetzten IoT-Objekten erzeugt werden**, könnte der Data Act

- **Herstellern von IoT-Objekten Transparenzpflichten bezüglich der Nutzungsrechte an nicht-personenbezogenen Daten auferlegen, die von diesen Objekten erzeugt werden**
  - ➔ dies könnte dazu führen, dass die Hersteller z.B. in ihren AGB erklären müssen, ob und unter welchen Bedingungen sie gewerblichen Nutzern von IoT-Objekten Nutzungsrechte in Bezug auf nicht-personenbezogene Daten gewähren, die von den Objekten erzeugt werden, und wie der Hersteller selbst diese Daten nutzen darf; oder
- **einen „Fairness-Test“ für Datenaustauschverträge zwischen Unternehmen einführen**, um zu verhindern, dass Datengeber mit starker Verhandlungsmacht Unternehmen, die diese Daten benötigen, einseitig unfaire Bedingungen auferlegen;
  - ➔ dieser „Test“ könnte darin bestehen, dass die Kommission speziell für IoT-Daten oder allgemein für Verträge über die gemeinsame Datennutzung
    - eine Liste verbotener Handelspraktiken in Datenaustauschverträgen festlegt, oder
    - konkrete Vertragsklauseln auflistet, die in Datenaustauschverträgen immer als grob nachteilig gelten sollen (Blacklist) und/oder bei denen widerlegbar vermutet werden soll, dass sie für den Datenlizenznehmer – evtl. auch den Lizenzgeber – grob nachteilig sind (Greylist), während sonstige Klauseln anhand der Umstände des Einzelfalls zu prüfen wären;
- **freiwillig nutzbare Mustervertragsklauseln für B2B-Datenaustauschverträge empfehlen;**
  - ➔ hierbei könnte die Kommission entweder spezielle Klauseln für den Austausch von IoT-Daten oder allgemeine Klauseln für alle Verträge über die gemeinsame Datennutzung vorschlagen;

- **allgemein geltende Grundregeln für den Zugang zu und die Nutzung von nicht-personenbezogenen Daten festlegen**, z.B. einen Streitbeilegungsmechanismus vorsehen;
  - ➔ diese Regeln sollen die Grundlage für die Ausübung von Datenzugangs- und -nutzungsrechten bilden, die in sektorspezifischen Vorschriften geregelt werden sollen oder bereits geregelt sind.

Vorläufige Einschätzung:

- Die Regelungen des Data Act greifen vor allem in die grundrechtlich geschützten Rechte der Datengeber auf Schutz ihrer unternehmerischen Freiheit und ihres geistigen Eigentums ein. Betroffene Dritte haben zudem u.a. ein Recht auf Schutz ihrer Privatsphäre und ihrer personenbezogenen Daten.
- Die inhaltliche Regulierung von Datenaustauschverträgen greift in die Vertragsfreiheit der beteiligten Unternehmen ein. Es ist sachgerecht, dass die Kommission beim Data Act die Vertragsfreiheit als Leitprinzip beachten will. Freiwillige Regeln und Musterklauseln sind grundsätzlich vorzugswürdig.
- Eingriffe in die genannten Grundrechte durch den Data Act können gerechtfertigt sein, wenn sie legitimen Zielen wie der Förderung des Gemeinwohls oder dem Schutz der Rechte anderer dienen. Als legitimer öffentlicher Zweck kommt vor allem die Förderung von Wettbewerb und Innovation in Betracht. Die Regelungen müssen aber verhältnismäßig, also zur Erreichung dieses Ziels geeignet, erforderlich und angemessen sein.
- Hierfür bedarf es einer sorgfältige Abwägung der widerstreitenden Ziele, Rechte und Interessen der Datengeber, der potenziellen Datennehmer, betroffener Dritter und der Allgemeinheit. Dabei ist auch zu berücksichtigen, in welchem Umfang der Datennehmer zur Datengenerierung beigetragen hat, welches Gewicht die Interessen der Allgemeinheit und kollidierende Individualinteressen haben und wie die Macht zwischen Datengeber und Datennehmer verteilt ist. Vergütungen oder Maßnahmen zum Schutz von Daten und Geschäftsgeheimnissen können die Effekte des Eingriffs abmildern.
- Welche Regeln verhältnismäßig sind, hängt von der Bewertung der ökonomischen Aspekte der einzelnen Regelungen und letztlich von deren Wertschöpfungs- und Innovationsbilanz ab. Einerseits kann eine verbesserte Datenteilung ggf. einer Monopolisierung in datenbasierten Märkten vorbeugen und zugleich datengetriebene Innovationen erleichtern. Andererseits können Datenteilungspflichten evtl. die Anreize für Investitionen in die Erhebung, Aufbereitung und den Schutz von zu teilenden Daten schwächen. Diese Bilanz kann von Markt zu Markt unterschiedlich ausfallen.
- Es ist daher sachgerecht, dass die Kommission etwaige Datenzugriffs- und Nutzungsrechte sektorspezifisch regeln will. Allgemeine Grundregeln im Data Act ermöglichen die EU-weit einheitliche Ausübung solcher Pflichten. Auch Mustervertragsklauseln und ein „Fairness-Test“, d.h. Regeln zur Unwirksamkeit von Klauseln, können den freiwilligen Datenaustausch erleichtern. Die Kommission muss aber sicherstellen, dass die Vorschriften des Data Act für alle betroffenen Marktteilnehmer „passen“.
- Transparenzpflichten, welche Daten IoT-Objekte erheben und wer sie wie nutzen darf, können helfen, den Wert der Daten besser zu beurteilen. Ob das Problem, Daten einen angemessenen Wert beizumessen, so gelöst werden kann, ist fraglich. Da es auf dem Markt noch keine klaren

Vorstellungen über einen „angemessenen“ Wert von Daten gibt, muss eine mögliche Regulierung einer „fairen“ Vergütung für die Bereitstellung von Daten durch die EU – insbesondere dann, wenn ex ante und in horizontalen Regelungen – besonders kritisch geprüft werden.

- Der Handel mit Daten und die Entstehung nachgelagerter Datenmärkte wird durch eine Vielzahl von Hindernissen rechtlicher Art (z.B. Rechtsunsicherheit), wirtschaftlicher Art (z.B. fehlendes Bewusstsein über Potenziale des Datenaustauschs) und technischer Art (z.B. mangelnde Interoperabilität) gehemmt. Auch diese Hemmnisse müssen beseitigt werden, was nicht stets durch Regulierung möglich ist. Ansonsten besteht die Gefahr, dass der Data Act nicht die gewünschte Wirkung entfalten kann.
- Es muss sichergestellt werden, dass Unternehmen nicht länger aus Angst vor der Preisgabe von Geschäftsgeheimnissen, geistigen Eigentumsrechten, des Wettbewerbsrechts und von Datenschutzvorschriften sowie vor Cybersicherheitsrisiken vor einer freiwilligen Weitergabe ihrer Daten zurückschrecken. Sie sollten insbesondere sondern darauf vertrauen können, dass die Daten auch bei der Weiterverarbeitung angemessen geschützt bleiben. Zudem müssen praktikable und risikoarme Möglichkeiten des Datenaustauschs in der EU etabliert und Projekte wie Gaia-X gefördert werden.
- Die Kommission muss verhindern, dass der Data Act bestehende Unterschiede verstärkt und somit – zumindest anfänglich – kontraproduktiv wirkt. Diese Gefahr könnte drohen, wenn die Erleichterung des Datenaustauschs zunächst vor allem marktstarken Anbietern nutzt, die bereits über die nötigen Kompetenzen und Strukturen verfügen, während kleinere Unternehmen faktisch und technisch noch nicht in der Lage sind, vom Datenaustausch zu profitieren.
- Deutschland sollte mit dem im Koalitionsvertrag angekündigten „Datengesetz“ möglichst auf einen Sonderweg verzichten. Der Data Act wird dieses Gesetz in seinem Anwendungsbereich verdrängen.

5.3 Zusätzliche Aspekte, die für beide Bereiche (B2G und B2B) gelten

- Aktuelle Rechtsunsicherheiten, wie Daten DSGVO-konform geteilt werden können, hindern den Datenaustausch ebenfalls und müssen beseitigt werden. Geklärt werden muss u.a.
  - ab wann Daten als anonymisiert gelten und die Anwendbarkeit der DSGVO daher ausgeschlossen ist; insoweit könnte die EU ggf. die Entwicklung von Standards unterstützen, bei deren Einhaltung ein hinreichender Anonymisierungsgrad vermutet wird,
  - ob und wenn ja, ab wann die gemeinsame Nutzung von Daten zu einer gemeinsamen Verantwortlichkeit für die Daten und die Einhaltung der DSGVO-Pflichten führt, und
  - auf welche Rechtsgrundlage die Weiterverwendung von Daten gestützt werden kann.
- Um das nötige Vertrauen zu schaffen, kann ein praktikabler Streitbeilegungsmechanismus ein wichtiger Beitrag sein. Der Data Act darf aber auch andere wichtige Fragen wie die Haftung für Datenmängel und andere Pflichtverletzungen nicht ausklammern.
- Um zusätzliche Rechtsunsicherheit zu vermeiden, muss die Kommission den Data Act mit anderen Rechtsvorschriften über Daten genau abstimmen, insbesondere mit dem Data Governance Act, den Digital Markets Act, der DSGVO und den einschlägigen sektorspezifischen Rechtsvorschriften, die Datennutzungsrechte regeln, und die Anwendungsbereiche dieser Rechtsakte klar abgrenzen.

5.4 Zu den übrigen Regelungen

Darüber hinaus könnte die Kommission im Data Act insbesondere

- **die Datenbankrichtlinie anpassen, um** die Nutzung von Daten zu erleichtern, insbesondere, **den Anwendungsbereich des Sui-Generis-Schutzrechts auf maschinell erzeugte Daten zu klären** und ggf. **Zugangsrechte** zur Datenbank festzulegen;
- zusammen mit dem Data Act oder später **klarstellende Leitlinien zur Anwendung der Richtlinie über Geschäftsgeheimnisse auf die Datenwirtschaft** veröffentlichen;
- die **Portabilitätspflichten für personenbezogene Daten nach Art. 20 DSGVO erweitern** und insbesondere **Hersteller intelligenter Geräte dazu verpflichten, privaten Nutzern eine kontinuierliche Echtzeitübertragung vom Gerät erzeugter Daten an andere Anbieter zu ermöglichen;**
- die **Portabilität von Cloud-Diensten für geschäftliche Nutzer verbessern** und ggf. **ein Portabilitätsrecht** für diese Nutzer einführen sowie Schnittstellen, Standards und Datenformate festlegen;
- **grundlegende rechtliche Anforderungen an „Smart Contracts"** und an deren **Interoperabilität** regeln und die **Entwicklung technischer Normen beauftragen;**
- **Cloud-Anbieter verpflichten, nicht-personenbezogene Daten** durch angemessene Schutzmaßnahmen **besser gegen Zugriffe aus Drittstaaten zu schützen und** Zugangsersuchen offenzulegen.

Vorläufige Einschätzung:

- Die Kommission muss Rechtsklarheit schaffen, ob und wann Unternehmen für maschinell erzeugte Daten Schutz nach der Datenbankrichtlinie beanspruchen können. Zudem muss sie sicherstellen, dass die Richtlinie die Balance zwischen dem etwaigen Schutz des Datenbankerstellers und den Interessen potentieller Nutzer der Datensätze wahrt. Sie sollte sowohl Anreize für Investitionen in die Erstellung von Datenbanken aufrechterhalten als auch datenbasierte Innovationen ermöglichen.
- Die Kommission sollte sicherstellen, dass die Portabilitätspflichten nach Art. 20 DSGVO verhältnismäßig bleiben und die erleichterte Teilung der Daten die Hersteller nicht übermäßig von Investitionen in IoT-Objekte bzw. in die Datenerzeugung durch solche Objekte abschreckt. Zudem muss sie klarstellen, inwieweit die DSGVO durch die „ergänzenden" Regelungen im Data Act geändert wird.
- Vor der Einführung eines Portabilitätsrechts für Cloud-Anbieter sollte die Kommission prüfen, ob nicht weiterhin „mildere Mittel" wie Informationspflichten oder eine bessere Bekanntmachung oder Ergänzung der Selbstregulierung vorzugswürdig sind. Zudem sollte sie sicherstellen, dass der Data Act technologieneutral ist, Innovationsanreize beibehält und künftige Normen marktrelevant sind.
- Gemeinsame Normen für Smart Contracts können die Interoperabilität verbessern und so die Nutzung von Smart Contracts erleichtern.
- Die Kommission sollte verhindern, dass neue Regelungen zum Transfer nicht-personenbezogener Daten in Drittstaaten zu spiegelbildlichen Problemen und Rechtsunsicherheit führen, wie sie derzeit bei personenbezogenen Daten besteht. Sie sollte deshalb eine internationale Lösung anstreben.

6 Vorläufiges Fazit

Für die EU ist es von enormer Wichtigkeit, das Potenzial der Weiterverwendung bzw. gemeinsamen Nutzung von Daten zu heben, um neue innovative Waren oder Dienstleistungen zu entwickeln und im globalen Wettbewerb zu bestehen. Auch die Entwicklung von Anwendungen der künstlichen Intelligenz (KI) hängt massiv von der Verfügbarkeit von Daten ab. Die EU hat sich vorgenommen, ihren eigenen, europäischen Weg zu finden, um die Datenwirtschaft zu fördern und gleichzeitig hohe Datenschutz-, Sicherheits- und Ethik-Standards zu wahren. Ein Data Act mit klaren und ausgewogenen Regelungen kann hierfür ein weiterer wichtiger Baustein sein; das Gesetz und darauf aufbauende spezielle Datennutzungsrechte, die die EU vermutlich in separaten Vorschriften festlegen wird, sind daher von entscheidender Bedeutung. Die EU steht damit jedoch vor einer schwierigen Aufgabe: zum einen muss sie bei der Regulierung eine Vielzahl gegenläufiger Interessen auf unterschiedlichen Märkten in Ausgleich bringen. Zum anderen hindern noch immer zahlreiche weitere Faktoren die Datenwirtschaft – allem voran Rechtsunsicherheit im Hinblick auf die DSGVO-konforme Weiterverwendung von Daten, die Angst vor einem unzureichendem Schutz wirtschaftlich sensibler Daten und vor einer möglichen Haftung, ein noch unzureichendes Bewusstsein über die Potenziale der Datennutzung sowie technische Herausforderungen wie eine mangelnde Interoperabilität. Diese Hindernisse müssen dringend ebenfalls beseitigt werden, damit der Data Act tatsächlich zu einem Motor für die Datenwirtschaft werden kann. Da die gemeinsame Datennutzung auch künftig maßgeblich auf der Basis von Verträgen erfolgen dürfte, muss zudem sichergestellt werden, dass diese vertraglichen Vereinbarungen ebenso wie die im Data Act geregelten Pflichten auch EU-weit durchgesetzt werden können. Darüber hinaus müssen auch die weiteren Säulen der EU-Datenstrategie zügig weiter umgesetzt werden. Nur dann kann die EU ihre Chance auf eine führende Rolle in der Datenwirtschaft der Zukunft wahren.

Zwar fehlt es in der EU an vergleichbar großen Online-Plattformen wie in China und in den USA. Erste Treiber der Datenwirtschaft waren in Europa vielmehr in erster Linie Teile der Fertigungsindustrie.[310] Aber genau hier kann und will die EU ansetzen: Die Kommission geht davon aus, dass ein Großteil der Daten künftig aus industriellen und beruflichen Anwendungen, aus Bereichen von öffentlichem Interesse oder aus Alltagsanwendungen des Internets der Dinge stammen wird, also aus Bereichen, in denen die EU stark ist.[311] Es klingt nachvollziehbar und vielversprechend, dass die EU am besten dort ihren eigenen Weg gehen kann, wo sie traditionell erfolgreich ist. Neue innovative Lösungen und die verbesserte Kooperation viele kleiner Unternehmen im Rahmen der Datenwirtschaft können die Wettbewerbsfähigkeit der EU stärken und so u.U. das Fehlen datengetriebener Plattformriesen kompensieren. Bessere und schnellere faktengestützte, evidenzbasierte politische Entscheidungen können zudem das Vertrauen in die Politik stärken. Nur wenn Europa eigene zukunftsträchtige Lösungen entwickelt, kann es seine Werte langfristig „by design“ in datengetriebene Produkte und Dienstleistungen integrieren, die Abhängigkeit von Produkten und Diensten aus Drittstaaten reduzieren und so verhindern, dass europäische Werte durch den Einsatz eingekaufter Technologie untergraben werden.

Das cep wird den Kommissionsvorschlag weiter begleiten.

[310] Die digitale Transformation der Industrie, Studie im Auftrag des Bundesverbands der Deutschen Industrie, 01.02.2015.
[311] EU-Datenstrategie, a.a.O. (Fn. 4), S. 3f.

Centrum für Europäische Politik
FREIBURG | BERLIN

Autorin:

Dr. Anja Hoffmann, Fachbereich für Binnenmarkt und Wettbewerb
hoffmann@cep.eu

Centrum für Europäische Politik FREIBURG | BERLIN
Kaiser-Joseph-Straße 266 | D-79098 Freiburg
Schiffbauerdamm 40 Raum 4315 | D-10117 Berlin
Tel. + 49 761 38693-0