Kölner Forschungsstelle
für Medienrecht
Technology
Arts Sciences
TH Köln

TH Köln · Gustav-Heinemann-Ufer 54 · 50968 Köln
Deutscher Bundestag
Ausschuss für Digitales
Platz der Republik 1
11011 Berlin

Prof. Dr. Rolf Schwartmann
Leiter der Kölner Forschungsstelle für Medienrecht
+49 221-8275-3446
medienrecht@th-koeln.de
www.medienrecht.th-koeln.de
Claudiusstraße 1
50678 Köln

Technische Hochschule Köln

Postanschrift:
Gustav-Heinemann-Ufer 54
50968 Köln

Sitz des Präsidiums:
Claudiusstraße 1
50678 Köln

www.th-koeln.de

Kölner Forschungsstelle für Medienrecht

Leitung:
Prof. Dr. Rolf Schwartmann

Beirat:
Achim Berg
Dr. Peter Charissé
Prof. Dr. Dieter Dörr
Dr. Florian Drücke
Christian DuMont Schütte
Claus Grewenig
Dr. h.c. Marit Hansen
Markus Hartmann
Matthias Hornschuh
Prof. Dr. Dr. h.c. Joachim Metzner
Dr. Tobias Schmid
Prof. Dr. Stefan Sporn

Stellungnahme

im Rahmen der öffentlichen Anhörung
des Ausschusses für Digitales
des Deutschen Bundestags

zum Thema

Innovative Datenpolitik: Potenziale und Herausforderungen

Berlin, 26. Juni 2024

vorgelegt von

Professor Dr. Rolf Schwartmann
Leiter der Kölner Forschungsstelle für Medienrecht,
Vorsitzender der Gesellschaft für Datenschutz und Datensicherheit (GDD) e.V.

unter Mitwirkung von

Kristin Benedikt, Richterin am VG Regensburg, Mitglied des Vorstandes der GDD
Moritz Köhler, Kölner Forschungsstelle für Medienrecht
Sonja Kurth, Kölner Forschungsstelle für Medienrecht
Steve Ritter, Mitglied des Vorstandes der GDD

Inhaltsverzeichnis

Fragen des Digitalausschusses vom 7.6.2024

1) Mit dem Data Act und dem Data Governance Act (und weitern Rechtsakten) wurde ein wegweisender europäischer Datenraum geschaffen. Welche Spielräume hat der deutsche Gesetzgeber bei der Umsetzung der Vorgaben, die er für eine innovative Datenpolitik nutzen sollte und welche Maßnahmen sehen Sie bei der Umsetzung - etwa in der Bündelung der Aufsicht für die digitalpolitischen Dossiers – als besonders wichtig an?

2) Für eine innovative Datenpolitik bedarf es einer innovativen, modernen aber auch sicheren und vertrauenswürdigen Infrastruktur. Was sind zentrale Elemente dieser Infrastruktur, wie muss diese ausgestaltet sein, um eine innovative Datenpolitik zu ermöglichen und wie weit sind wir beim Aufbau einer solchen Infrastruktur und welche Bedeutung kommt hier einer souveränen europäischen Cloudinfrastruktur zu?

3) Oft wird Datenschutz als Hemmnis für innovative Datenpolitik vorgeschoben oder werden Datenpolitik und Datenschutz gegeneinander in Stellung gebracht. Wie sehen Sie die Rolle des Datenschutzes für eine innovative Datenpolitik, welche Instrumente wie beispielsweise Datentreuhänder können welchen Beitrag leisten, um Datenschutz und innovative Datenpolitik zusammenzudenken und sehen Sie es auch als Wettbewerbsvorteil an, innovative Datenpolitik unter Wahrung des Datenschutzes made in EU sicherzustellen?

4) Welche Elemente fehlen in Deutschland auf dem Weg zu innovativer Datenpolitik, wie können weitere Anreize für das Teilen von Daten in wechselseitigem Interesse weiter ausgebaut werden und welche Bedeutung – Stichwort Open Data, Datenlabore und Transparenzgesetz – kommen dem Staat und der öffentlichen Verwaltung zu und werden diese dieser gerecht?

5) Haben Forschung, Zivilgesellschaft und öffentliche Stellen ausreichend Datenzugang zu den Daten sehr großer Online-Plattformen (VLOPs) und anderen datenhaltenden Unternehmen, um gemeinwohlorientierte Fragestellungen zu Themen wie beispielsweise Klimaschutz, sozialer Gerechtigkeit oder effizienter Verwaltung zu bearbeiten bzw. gibt es weitere Ansatzpunkte im nationalen und EU-Recht, um einen solchen Datenzugang zu gewährleisten und welchen Regelungsbedarf sehen Sie insoweit für die Zukunft?

6) Welchen Effekt haben neue Formate der Datenpolitik wie das von BMWK und BMI vorangetriebene Dateninstitut für eine innovative Datenpolitik und braucht es weitere Maßnahmen, um eine breite Nutzung von Daten für das Wohl der Gesellschaft zu ermöglichen?

7) Welche Form der Zusammenarbeit ist auf internationaler Ebene notwendig, um eine innovative Datenpolitik proaktiv und menschenzentriert voranzutreiben und Bedeutung kommt dabei dem sogenannten „globalen Süden“ zu?

8) Welche Möglichkeiten gibt es, mithilfe von datenbasierten Anwendungen der Klimakrise zu begegnen und datenpolitischen Maßnahmen sind notwendig, um das Potential für eine nachhaltige Digitalisierung sowie für einen innovativen Klimaschutz voll auszuschöpfen?

9) Wie beurteilen Sie das Zusammenwirken der zahlreichen Dateninitiativen (z.B. Daten-institut, MISSION KI, Gaia-X Hub, Förderprojekte, Datenraumvereine, Data Spaces Support Center, Gaia-X etc.) auf deutscher und europäischer Ebene im Hinblick auf Ihre Kohärenz und Zielerfüllung? Wie bewerten Sie ihr Einzahlen auf die Erfüllung von Compliance-Pflichten durch die Wirtschaft, das Ausnutzen von unternehmerischen Effizienzreserven und der Schaffung von Schlüsselinnovationen in Europa, die das Potential haben, ganz neue Märkte zu schaffen?

10) Die Bundesregierung hat im Jahr 2023 eine überarbeitete Datenstrategie veröffentlicht (https://www.bundesregierung.de/breg-de/themen/digitalisierung/datenstrategie-2023-

2216620). Wie beurteilen Sie diese in ihrer Machart und Zielsetzung und in ihrer bisherigen Umsetzung?

11) Wie sollte, vorangestellt die Zielparameter einer verbesserten Datenverfügbarkeit- und Nutzbarkeit, eine grundlegende Neuordnung der Datenschutzaufsicht in Deutschland aussehen, wo genau sollte eine Reform der DSGVO ansetzen und welche möglichen Restriktionen sehen Sie hierbei?

12) Wie kann die Umsetzung von Data Act und AI Act, gerade was die Ermöglichung von KI angeht, durch Standardisierungsarbeiten, Codes of Conducts und Codes of Practices erleichtert werden, insbesondere mit Bedeutung von Transparenz und Kontrolle über Daten?

13) Welche Maßnahmen sind aus Ihrer Sicht prioritär, um eine starke Datenökonomie und ein innovatives Daten-Ökosystem mit Rechen- und Datenzentren in Deutschland und Europa aufzubauen und die Ansiedlung von Daten-getriebenen Unternehmen zu erleichtern?

14) Wie müssten ideale Leitlinien für die rechtssichere Anonymisierung von Daten im Rahmen der DSGVO und des Data Acts aus Ihrer Sicht ausgestaltet sein? Wie wird die Anonymisierung in anderen EU-Mitgliedsstaaten gehandhabt, und welche Maßnahmen sind erforderlich, damit Deutschland in diesem Bereich endlich Fortschritte erzielt?

15) Inwiefern sind die Zweifel an der Rechtssicherheit des Data Protection Agreements zwischen den USA und der EU, das auf zwei vorhergehend aufgehobene Agreements nach dem Schrems I- und Schrems II-Urteil des EuGH folgte, berechtigt und außerdem eine

16) Wie können Innovationen sowohl im Bereich digitaler Dienste als auch im Bereich Regulierung für mehr Datenschutz und Einhaltung der Grundrechte sorgen und welche guten Beispiele kennen Sie dafür?

17) Was kann und sollte Ihrer Auffassung nach der Staat tun, damit die Datenbestände, über die er selbst auf Bundes-, Landes- und kommunaler Ebene verfügt, nicht weiterhin unberührt in Silos schlummern, sondern von der Gesellschaft insgesamt besser genutzt werden können, etwa zum Bürokratieabbau, zu mehr Sicherheit und Komfort beim Nutzen staatlicher Leistungen? Wäre vor diesem Hintergrund das Zusammenlegen einzelner Datenbanken zu einem großen Register ein vernünftiger Weg, und falls ja, wie ließe sich dieser verfassungsfest im Sinne des Föderalismus beschreiten?

18) Die großen Digitalkonzerne zeigen es: Maschinenlesbare Daten haben einen Wert, mit ihrer Monetarisierung werden die zahlreichen Dienste, die unseren Alltag prägen, finanziert. Sollten Ihrer Auffassung nach digitale Daten, die die Menschen alltäglich erzeugen und die gleichsam als Blut der Gesellschaft zirkulieren, auch offiziell einen Wert und damit einen Preis bekommen, und wenn ja, wie ließe sich eine solche Datenökonomie im Wortsinn aufbauen und regulieren? Wie ließe sich die griffige Formel vom „Eigentum an den eigenen Daten“ real umsetzen?

Zuweisung von Fragen und Antworten

Frage	Gliederungspunkt
1	B) I. Gestaltungsspielräume für Innovation und Abbau von Hemmnissen
2	B) III. Datensicherheit
3	B) II. 1. Anonymisierung und Personenbezug B) II.3. Datentreuhänder und PIMS
4	B) I. 1. c) Data Governance Act B) II. Anreize für die Datenwirtschaft in einem wettbewerbsfähigen Datenökosystem
5	B) II. 6. c) Zugang zu den Daten sehr großer Unternehmen bei Gemeinwohlorientierung
6	B) II. 5. c) Dateninstitut des BMI und des BMWK
7	B) II. 5. Initiativen zur Förderung der Datenwirtschaft in Europa und in Deutschland
8	B) II. 6. a) Sektor Klima: Daten als Hilfsmittel im Umgang mit der Klimakrise
9	B) II. 5. Initiativen zur Förderung der Datenwirtschaft in Europa und in Deutschland
10	A) II. Datenstrategie der Bundesregierung
11	B) I. 2. Aufsichtsstrukturen
12	B) II. 1. Anonymisierung und Personenbezug B) II. 2. Musterverträge für Datenteilung
13	B) II. Anreize für die Datenwirtschaft in einem wettbewerbsfähigen Datenökosystem
14	B) II. 1. Anonymisierung und Personenbezug
15	B) II. 4. Wirtschaft binden und Standards in Europa bündeln
16	B) I. 2. Aufsichtsstrukturen B) II. 1. Anonymisierung und Personenbezug
17	B) II. 6. c) Zugänglichmachung und Nutzung staatlicher Daten an die Bevölkerung
18	B) IV. Alternative Modelle einer Datenökonomie

Vorbemerkung

Die Anhörung vor dem Digitalausschuss zu Anforderungen und Potentialen innovativer Datenpolitik steht im Zeichen eines Paradigmenwechsels. Sie trägt der veränderten regulatorischen Wirklichkeit Rechnung, in der das Datenrecht sich von einem primären Datenschutzrecht zum Datenwirtschaftsrecht entwickelt. Die in diesem Kontext gestellten Fragen bewegen sich im Kern eines rechtlich und wirtschaftspolitisch relevanten Bereichs der Digitalpolitik. Sie soll in der Europäischen Union und ihren Mitgliedstaaten ein Datenökosystem etablieren, das menschenzentriert ist, indem es ökonomische Notwendigkeiten auf einer rechtlich und ethisch verlässlichen Basis mit Persönlichkeits- und sonstigen Rechten in einen fairen und rechtssicheren Ausgleich bringt. So sollen die Union und ihre Mitgliedstaaten weltweit wettbewerbsfähig sein, bleiben oder werden können.

Die in diesem Kontext aus den Reihen des Deutschen Bundestages gestellten Fragen treffen den Kern dieses Bereiches. Sie sind komplex und erfassen größtenteils miteinander verwobene Fragestellungen. Sie sind so innovativ, vielschichtig und herausfordernd wie der Gegenstand der Anhörung. Deshalb wurde bei der Beantwortung der Fragen ein **methodischer Weg** gewählt, der das Thema der Anhörung in einen Kontext setzt und auf die aufgeworfenen Fragen in diesem Kontext eingeht, ohne sich an deren Reihenfolge zu halten. Teilweise werden Fragen auch an unterschiedlichen Punkten adressiert. Zur Verortung der Antworten auf die konkret gestellten Fragen kann die **vorstehende Übersicht** herangezogen werden.

In dieser Stellungnahme wird aus Gründen der sprachlichen Klarheit häufig das generische Maskulinum verwendet, ohne dass damit eine darüberhinausgehende Wertung verbunden ist.

A) Einleitung

Die Anhörung vor dem Digitalausschuss zu den Potenzialen und den Herausforderungen innovativer Datenpolitik steht im Zeichen eines Paradigmenwechsels im Datenrecht: Neben das Datenschutzrecht tritt nunmehr ebenbürtig das Datenwirtschaftsrecht.

I. Datenstrategie der EU

Die europäische Datenstrategie soll die EU in eine Führungsposition in der datengestützten Gesellschaft bringen. Daten sollen branchenübergreifend zum Wohl von Wirtschaft, Wissenschaft und Staat weitergegeben werden können. Die zentralen Rechtsakte dafür sind der **Data Governance** Act (DGA) und der **Data Act** (DA). Nach ersterem bekommen öffentliche Stellen die Möglichkeit, Daten zur Weiterverwendung bereitzustellen. Letzterer adressiert die Wirtschaft. Daten, die sich aktuell in den Händen von großen Plattformen befinden, sollen auch für kleine und mittelständische Unternehmen wirtschaftlich nutzbar gemacht werden. Auf diese Weise will der Gesetzgeber Anreize für innovative Geschäftsideen an der richtigen Stelle schaffen. Zudem sollen Nutzer ihre Daten teilen können. Für die „Dateninhaber" in der Wirtschaft wird eine nutzergetriebene Pflicht zur Datenteilung etabliert, die sich nach Maßgabe der DS-GVO vollziehen muss.

Ergänzend erlegt der **Digital Markets Act** (DMA) den „Gatekeepern", welche die Digitalwirtschaft auch innerhalb der EU dominieren, Pflichten auf, um fairen Wettbewerb im Binnenmarkt herzustellen. Nutzer sollen mehr Datensouveränität erhalten. Der **Digital Services Act** (DSA) wiederum beansprucht nicht weniger, als die Demokratie zu sichern. Er verpflichtet die großen Online-Plattformen insbesondere dazu, Hass, Fakenews und Kriminalität im Netz zu bekämpfen. Die Konzerne müssen Verfahren etablieren, die Risiken ihres Geschäftsmodells mindern.[1]

Besondere Bedeutung misst die EU auch der **Verordnung zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz (Gesetz über künstliche Intelligenz, kurz: KI-VO)** bei, die Europa zum weltweiten Trendsetter einer wirtschaftlich führenden und fairen Nutzung dieser Schlüsseltechnologie machen soll.[2] Die KI-VO soll im Juli im Amtsblatt der Europäischen Union veröffentlicht werden und 20 Tage danach in Kraft treten. Generative KI im Sinne der am 1. August 2024 in Kraft tretenden KI-Verordnung (KI-VO) hat das Potential, die europäische Wirtschaft zu revolutionieren. Die Menschen in Europa sind ebenso wie die Wirtschaft auf Fortschritt und einen verlässlichen Rahmen für Innovation angewiesen. Fortschrittsoptimismus ist selbst dann alternativlos, wenn die Technik sich dahin entwickelt, dass man sich vor ihr in Acht nehmen muss. Das ist bei generativer KI der Fall, denn es geht insofern um autonome und deshalb unbeherrschbare Technik, als sie sich auch ohne menschliches Zutun verändern kann. Wenn das Risiko wegen der Autonomie eines Werkzeugs nicht mehr allein vom Menschen ausgeht, sondern auch vom Werkzeug, dann muss das Recht damit umgehen. Die KI-VO wählt eine Lösung mit zwei Kernelementen. Sie steckt zunächst einen gesetzlichen Rahmen für die Entwicklung und den Betrieb künstlicher Intelligenz ab und ordnet Nutzungen in Risikoklassen ein, etwa so wie es die Datenethikkommission der Bundesregierung 2019 vorgeschlagen hatte[3]. Sodann löst die KI-VO das Problem der Sicherung der menschlichen Verantwortung bei maschineller Hilfe, indem sie den Menschen in die Pflicht nimmt, wenn es darum geht, die autonome Technik selbstbestimmt zu stoppen. Jenseits der Grenzen dieses Rechtsrahmens zum Schutz der Menschen und ihrer Rechte herrscht Freiheit zum Einsatz von KI, soweit nicht

[1] *Schwartmann* F.A.Z. v. 27.6.2022, 18.

[2] Dazu Schwartmann/Keber/Zenner (Hrsg.), KI-Verordnung, 2. Teil 1. Kap., im Erscheinen; *Schwarmann/Keber/Darda* F.A.Z. v. 17.6.2024, 19; *Schwartmann/Köhler* RDV 2024, 27 ff.

[3] Gutachten der Datenethikkommission v. 23.10.2019, S. 173-182.

das von der KI-VO unberührte und unabhängig davon geltende sonstige Recht – etwa das Datenschutz- oder Urheberrecht – Grenzen setzt. Gerade die KI-VO muss beweisen, ob sie sich zum Goldstandard der verantwortungsvollen Ermöglichung eines Fortschritts entwickelt, der die Menschenrechte und die demokratischen und rechtsstaatlichen Errungenschaften Europas stärkt. Sie will vertrauenswürdige KI ohne schädliche Auswirkungen in der Union fördern und entsprechende Innovationen unterstützen. Offene Fragen lauten, wo die Grenzen des autonom agierenden KI-Arztes verlaufen und wie weit der Rat des Kollegen Chatbot gehen darf, wenn es um Personalentscheidungen im Betrieb oder die Benotung von Schülern geht und ob Bots am Ende gar Tipps für faire Gerichtsurteile geben dürfen.[4]

Die von der EU vorgestellte **europäischen Datenstrategie**[5] enthält nicht nur den Grundstein für den Data Act und den Data Governance Act, sondern auch Überlegungen zu sog. **europäischen Datenräumen (European Data Spaces)**. Diese sollen dazu dienen, Unternehmen und den öffentlichen Sektor in die Lage zu versetzen, vermehrt Daten zu nutzen, damit diese bessere Entscheidungen treffen können und daraus resultierend eine Chance für soziales und wirtschaftliches Wohlergehen entstehen kann.[6] Deshalb ist das Ziel der Kommission die Schaffung eines einheitlichen europäischen Datenraums, also eines Binnenmarkts für Daten, in dem sowohl personenbezogene als auch nicht-personenbezogene Daten sicher sind und in dem Unternehmen leicht Zugang zu hochwertigen industriellen Daten erhalten. Hierdurch soll das Wachstum und die Wertschöpfung in Bezug auf Daten steigen.[7] Insoweit erinnert die Idee von einem Binnenmarkt für Daten an die Grundfreiheiten, wie z. B. die Warenverkehrsfreiheit, die Arbeitnehmerfreizügigkeit, die Niederlassungs- und Dienstleistungsfreiheit. Der Datenbinnenmarkt soll allerdings nicht auf Ebene des Primärrechts angesiedelt, sondern für einzelne Sektoren in jeweils vorgesehenen Rechtsakten verwirklicht werden. 2020 hat sich die Kommission vorgenommen, neun europäische Datenräume und eine europäische Cloud zu schaffen.[8] Mittlerweile sind 14 europäische Datenräume zumindest geplant, die die Sektoren „Landwirtschaft, Kulturelles Erbe, Energiewirtschaft, Finanzen, Grüner Deal, Intelligente Städte und Gemeinden, Gesundheit, Sprache, Herstellung, Medien, Mobilität, Öffentliche Verwaltung, Forschung und Innovation, Fähigkeiten und Tourismus“ umfassen.[9] In allen diesen Sektoren soll ein eigener Regulierungsvorschlag, zumeist in Form einer Verordnung (Art. 288 Abs. 2 AEUV), auf den Weg gebracht werden.[10] Aufgrund der COVID-19-Pandemie wurde der Sektor

[4] *Schwartmann/Keber/Darda* F.A.Z. v. 17.6.2024, 19.

[5] *Europäische Kommission* Mitteilung der Kommission an das Europäische Parlament, den Rat, den europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen – Eine europäische Datenstrategie vom 19. Februar 2020, COM(2020) 66 final.

[6] *Europäische Kommission* Mitteilung der Kommission an das Europäische Parlament, den Rat, den europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen – Eine europäische Datenstrategie vom 19. Februar 2020, COM(2020) 66 final, S. 5.

[7] *Europäische Kommission* Mitteilung der Kommission an das Europäische Parlament, den Rat, den europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen – Eine europäische Datenstrategie vom 19. Februar 2020, COM(2020) 66 final, S. 5.

[8] *Europäische Kommission* Mitteilung der Kommission an das Europäische Parlament, den Rat, den europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen – Eine europäische Datenstrategie vom 19. Februar 2020, COM(2020) 66 final, S. 26.

[9] *Europäische Kommission* Gemeinsame europäische Datenräume, abrufbar unter https://digital-strategy.ec.europa.eu/de/policies/data-spaces (Stand: 24.4.2024).

[10] Heinze/*Raji* Daten, Plattformen und KI als Dreiklang unserer Zeit, DSRITB 2022, 187, 188; zudem *Raji* ZD 2023, 3.

„Gesundheit“ priorisiert[11] und infolgedessen ein Vorschlag für eine „Verordnung über den europäischen Raum für Gesundheitsdaten“ (European Health Data Space, EHDS) unterbreitet.[12]

Der Vorschlag zur Verordnung zum **European Health Data Space (EHDS)** wurde am 3.5.2022 von der Kommission veröffentlicht.[13] Eine Einigung zwischen dem Europäischen Parlament und dem Rat konnte am 15.3.2024 gefunden werden.[14] Ziel des EHDS ist es, einen gemeinsamen Raum zu schaffen, in dem erstens natürliche Personen ihre elektronischen Gesundheitsdaten leicht kontrollieren können (**Primärnutzung elektronischer Gesundheitsdaten**, Art. 2 Abs. 2 Buchst. d) EHDS-E).[15] Zweitens soll es Akteuren aus Forschung und Innovation sowie politischen Entscheidungsträgern ermöglicht werden, elektronische Gesundheitsdaten auf vertrauenswürdige und sichere Weise unter Wahrung der Privatsphäre zu nutzen (**Sekundärnutzung elektronischer Gesundheitsdaten**, Art. 2 Abs. 2 Buchst. e) EHDS-E)[16].[17] Der EHDS soll „den **diskriminierungsfreien Zugang zu Gesundheitsdaten** und das **Training von KI-Algorithmen** mithilfe dieser Datensätze erleichtern […]“.[18] Zu erwähnen ist, dass der deutsche Gesetzgeber mit dem Gesundheitsdatennutzungsgesetz (GDNG),[19] welches am 26.03.2024 in Kraft getreten ist, auf den kommenden EHDS reagiert. Das GDNG will die grenzüberschreitende Datenverfügbarkeit fördern und erste Schritte zur Vorbereitung des deutschen Gesundheitswesens auf eine europäische Anbindung an den EHDS vornehmen.[20] Letztlich bietet die verbreitete Nutzung von KI-Systemen die Chance, das Gesundheitssystem zu verbessern. Werden Daten strukturiert in den EHDS eingebracht, können Datensilos aufgebrochen und der Zugriff auf notwendige Daten für die Forschung ermöglicht werden. Dadurch können neue Anwendungen im Gesundheitssektor entstehen, die Effizienzsteigerungen hervorrufen.[21]

Die Kommission hat mit der Initiative „**GreenData4All**“ einen neuen Legislativvorschlag vorgestellt, der Teil der europäischen Datenstrategie sein soll. Geplant ist eine Richtlinie (keine Verordnung), die auf die **INSPIRE-Richtline**[22] aufbaut und die dort enthaltenen Vorschriften aktualisiert und weiterentwickelt.[23] Dabei kommt die Kommission zu dem Schluss, dass die Vorschriften der INSPIRE-Richtlinie für die gemeinsame Nutzung von umweltbezogenen

[11] Vgl. ErwG 1 ff. EHDS-E; *Commission* Staff working Document on Common European Data Spaces v. 23. Februar 2023, SWD(2022) 45 final, S. 1; Heinze/*Raji* Daten, Plattformen und KI als Dreiklang unserer Zeit, DSRITB 2022, 187, 188; zudem *Raji* ZD 2023, 3.

[12] *Europäische Kommission* Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über den europäischen Raum für Gesundheitsdaten v. 03. Mai 2022, COM(2022) 197 final.

[13] Dazu überblicksartig *Dierks* PharmR 2023, 369, 370 f.

[14] Hier allerdings der Verweis auf die Abänderungen des Europäischen Parlaments zur vorgeschlagenen Verordnung für einen europäischen Raum für Gesundheitsdaten v. 15.4.2024, A9-0395/2023 Änderungsantrag 558, abrufbar unter https://www.europarl.europa.eu/doceo/document/A-9-2023-0395-AM-558-558_DE.pdf (Stand: 24.04.2024). Die folgenden Erwägungen beziehen sich auf diesen Text.

[15] Dazu u. a. *Denga* EuZW 2023, 25, 29.

[16] Dazu ebenfalls *Denga* EuZW 2023, 25, 29.

[17] *Europäische Kommission* Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über den europäischen Raum für Gesundheitsdaten v. 03. Mai 2022, COM(2022) 197 final, S. 1.

[18] ErwG 68 S. 3 KI-VO.

[19] Gesundheitsdatennutzungsgesetz vom 22. März 2024 (BGBl. 2024 I Nr. 102).

[20] BT-Drucks. 20/9046, S. 2

[21] Dazu *Schwartmann/Wasilewski* in Schwartmann/Keber/Zenner (Hrsg.), KI-Verordnung, 2. Teil 3. Kap. Rn. 100, im Erscheinen.

[22] Richtlinie 2007/2/EG des Europäischen Parlaments und des Rates vom 14. März 2007 zur Schaffung einer Geodateninfrastruktur in der Europäischen Gemeinschaft (INSPIRE).

[23] *Europäische Kommission* Aufforderung zur Stellungnahme zu einer Folgenabschätzung, Ref. Ares(2024)1442613 - 26/02/2024, S. 1, abrufbar unter https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13170-GreenData4All-aktualisierte-Vorschriften-uber-umweltbezogene-Geodaten-und-den-Zugang-zu-Umweltinformationen_de (Stand: 24.4.2024).

Geodaten tendenziell zu präskriptiv seien, die INSPIRE-Daten für die Entwicklung und Umsetzung der Umweltpolitik (Folgenabschätzung, Überwachung und Berichterstattung, Evaluierung) nur von begrenztem Nutzen seien und deshalb nicht die sich rasch verändernden Nutzerbedürfnisse oder die Art und Weise, wie und zu welchem Zweck Daten verwendet werden von der INSPIRE-Richtlinie abgedeckt würden.[24] Deshalb sind die Ziele der Initiative eine **effizientere und zukunftssichere Bereitstellung und Zugänglichkeit von Umweltdaten zur gemeinsamen Nutzung**, die Berücksichtigung von Erfordernissen der Entwicklung und Umsetzung der Umweltpolitik, die Ermöglichung einer datengestützten Umweltüberwachung und -berichterstattung, sowie die Verbesserung der Qualität der Erkenntnisse über den Zustand der Umwelt und Förderung der grünen Datenwirtschaft.[25] Damit sollen Vorteile für Unternehmen und die öffentliche Verwaltung entlang der Datenwertschöpfungskette geschaffen werden, sodass die Weiterverwendung von Umweltdaten gefördert wird und der wirtschaftliche Wert von Daten des öffentlichen Sektors steigt.[26] Insoweit verfolgt die „GreenData4All"-Initiative das gleiche Ziel wie der EHDS: Mit der Schaffung von Datenräumen können hochwertige Daten akquiriert werden, auf die viele Akteure zugreifen dürfen, sodass tendenziell bessere KI-Systeme entwickelt und trainiert werden können.[27]

1. DS-GVO als Teil einer Datenwirtschaftsordnung

Die DS-GVO ist, sofern es um Datenwirtschaft unter Verarbeitung **personenbezogener Daten** geht, im gesamten Datenwirtschaftsrecht zu berücksichtigen. Sie ist allerdings mehr als „nur" eine Datenschutzverordnung, sie ist der – wenn man so will, historische - Kern der „Wirtschaftsverfassung des Datenbinnenmarktes".[28] Art. 1 DS-GVO schützt nicht nur natürliche Personen bei der Verarbeitung personenbezogener Daten, er schützt ausdrücklich auch den „freien Verkehr solcher Daten im Binnenmarkt". Dieser darf aus Gründen des Datenschutzes in der EU weder eingeschränkt noch verboten werden. Erwägungsgrund 4 der DS-GVO erhebt den Dienst des Datenschutzes, um wirtschaftliche Freiheiten für alle Rechtsanwender zu ermöglichen, zur Auslegungsmaxime. Dieser eindeutige Wille der DS-GVO wird oft nicht gesehen und oft zu wenig beachtet.[29] Zugleich liefert die DS-GVO als Ausgleichsordnung die Rechtsgrundlagen für legitime Datenverarbeitungen. Dies sind die Verfolgung interessengerecht abgewogener Zwecke, Verträge über die Datenweitergabe und die freiwillige und informierte Einwilligung unter Wahrung von Transparenz, Betroffenenrechten und Datensicherheitsanforderungen.

Der deutsche Gesetzgeber hat hier einen Spielraum, dem aber eher enge Grenzen gesetzt sind. Deshalb müssen alle Datenschutzinterpreten – vom EuGH, über die nationalen Gerichte bis hin zu den Aufsichtsbehörden – diese Ambivalenz der DS-GVO[30] im Blick behalten, die den vielfältigen Bedürfnissen der Betroffenen, Unternehmen und Behörden dient. Sie ist die Grundlage allen florierenden Datenwirtschaftsrechts zum Wohl der Menschheit.

---

[24] *Europäische Kommission* Aufforderung zur Stellungnahme zu einer Folgenabschätzung, Ref. Ares(2024)1442613 - 26/02/2024, S. 2.

[25] *Europäische Kommission* Aufforderung zur Stellungnahme zu einer Folgenabschätzung, Ref. Ares(2024)1442613 - 26/02/2024, S. 3.

[26] *Europäische Kommission* Aufforderung zur Stellungnahme zu einer Folgenabschätzung, Ref. Ares(2024)1442613 - 26/02/2024, S. 4.

[27] Zum Ganzen *Schwartmann/Wasilewski* in Schwartmann/Keber/Zenner (Hrsg.), KI-Verordnung, 2. Teil 3. Kap. Rn. 94-101, im Erscheinen.

[28] *Kühling/Paal/Schwartmann* F.A.Z. v. 20.10.2022, 6; *Benedikt* RDV 2022, 258 ff.

[29] *Brink/Oetjen/Schwartmann/Voss* F.A.Z. v. 18.7.2022, 18.

[30] *Kühling/Paal/Schwartmann* F.A.Z. v. 20.10.2022, 6.

2. Vom Datenschutzrecht zum Datenwirtschaftsrecht

Die im Bürgerlichen Gesetzbuch umgesetzte Richtlinie für Digitale Inhalte hat den Ausbau zum Wirtschaftsrecht im Kaufrecht unter dem Motto „Zahlen mit Daten“ [31] begonnen. Die Rechtsprechung des Europäischen Gerichtshofs zu Meta aus dem Jahr 2023 hat das Geschäftsmodell „Pay or Consent“ bestätigt.[32] Hiernach müssen Nutzer die freie Wahl haben, ihre Einwilligung verweigern zu können, ohne auf den Online-Dienst vollständig verzichten zu müssen. Gleichwohl können Unternehmen ihren Online-Dienst gegebenenfalls gegen ein angemessenes Entgelt anbieten.[33] Nutzern steht es somit frei, entweder für die Inanspruchnahme eines Dienstes ein Entgelt zu leisten oder ihre personenbezogenen Daten bereitzustellen. Das nachfolgende Datenwirtschaftsrecht, insbesondere in Gestalt des Data Act, setzt diesen Rechtsrahmen für das Datenwirtschaftsrecht konsequent fort. Es setzt auf eine umfassende Datenverarbeitung und -weitergabe anonymer, aber auch personenbezogener Daten unter Wahrung der Standards der DS-GVO. Auf Basis des Datenrechts soll und kann im Binnenmarkt mit personenbezogenen Daten gearbeitet, geforscht und gewirtschaftet werden. Die DS-GVO bietet grundsätzlich einen geeigneten Rahmen für moderne Ansätze. Bei sachgerechter Anwendung ermöglicht sie für eine Vielzahl auch künftiger Fälle angemessene Lösungen. Sie folgt vor allem dem richtigen Grundgedanken, die Parole der DS-GVO lautet: „Privacy Sells“. Ihre Mission besteht darin, den Datenschutz und die Verwendung von Daten im Einklang mit den praktischen und wirtschaftlichen Erfordernissen zu ermöglichen. Nur sehr wenige Datenverarbeitungen sind so risikoreich, dass man sie tabuisieren muss und die Weitergabe und Nutzung dieser sensiblen Daten selbst durch Einsatz von Verschlüsselungs- und Pseudonymisierungstechnik nicht rechtfertigen kann.[34]

Von der rechtssicheren Nutzbarkeit von Daten wird das ökonomische Schicksal der EU in der Digitalisierung im Wettbewerb der Wirtschaftssysteme abhängen. Datenregulierung, die den Gedanken von „Privacy Sells“ erhalten will, muss klug und weitsichtig agieren. Der Datenbinnenmarkt muss auf angemessene Weise ermöglicht werden, ohne hierbei die Privatsphäre auszuverkaufen. Das Fruchten der Datenstrategie verlangt ein Umdenken. Zunächst bedarf das Selbstverständnis der Aufsicht als Sachwalter des Datenschutzes im Dienst von Bürger und Wirtschaft dringend der Korrektur. Es geht darum zu ermöglichen und nicht darum zu verhindern. Der EU-Gesetzgeber legt die Pflicht zur Datenweitergabe im Data Act fest. An diesem Willen muss sich die Anwendung der DS-GVO messen lassen. Um den Anwendungsbereich der Regulierung nicht auszuhöhlen, muss sich das Verständnis der DS-GVO also zukunftsgerichtet auch an diesen Regulierungszielen und Regulierungsinhalten orientieren. Diese müssen sich umgekehrt an den Möglichkeiten der DS-GVO messen lassen. Es geht um Wechselwirkung im Bereich der Verarbeitung personenbezogener Daten. Damit alle Akteure wissen, wann ein angemessenes Verhältnis zwischen Datenschutz und Datenwirtschaft zu finden ist, muss darüber hinaus eine rechtssichere Abgrenzung zwischen personenbezogenen und anonymisierten Daten ermöglicht werden.

II. Datenstrategie der Bundesregierung

Die 2023 überarbeitete Datenstrategie der Bundesregierung[35] verfolgt einen ganzheitlichen Ansatz, um Datennutzung und -zugang zu verbessern. Erste Maßnahmen, wie z.B.

---

[31] *Schwartmann/Reif/Burkhardt* in Schwartmann/Jaspers/Eckhardt (Hrsg.), HK TTDSG, § 25 Rn. 54f; *Kessen/Reif/Burkhardt* RDV 2022, 64 ff.

[32] EuGH Urt. v. 4. 7. 2023 – C-252/21, ECLI:EU:C:2023:537; Zu „Pay or Consent“ *Benedikt/Pfau* RDV 2024, 20 ff.

[33] Vgl. EuGH Urt. v. 4.7.2023 – C-252/21, ECLI:EU:C:2023:537 Rn. 150.

[34] *Schwartmann* F.A.Z. v. 27.6.2022, 18; *Brink/Oetjen/Schwartmann/Voss* F.A.Z. v. 18.7.2022, 18.

[35] Fortschritt durch Datennutzung – Strategie der Bundesregierung für mehr und bessere Daten für neue, effektive und zukunftsweisende Datennutzung, August 2023, im Folgenden kurz: Datenstrategie der Bundesregierung

Pilotprojekte und Förderprogramme wurden bereits initiiert.[36] Große Chancen liegen in der zeitnahen Umsetzung weiterer Maßnahmen wie der Förderung von Datenkompetenz, der internationalen Zusammenarbeit, insbesondere bei Standardisierungsverfahren (Anonymisierung) und der Unterstützung durch Vertragsmuster und Best Practice.[37]

Auffällig ist jedoch, dass sich die Strategie stark auf die Datennutzung und -bereitstellung durch staatliche Stellen konzentriert. Während der Erstellung eines Datenatlasses für die Bundesverwaltung oder dem Zugang der öffentlichen Hand auf Daten aus der Privatwirtschaft zu gemeinwohlorientierten Zwecken viel Aufmerksamkeit geschenkt wird,[38] bleiben Betrachtungen zur Förderung der Datenwirtschaft vergleichsweise oberflächlich und unkonkret.

Zwar erkennt die Datenstrategie Daten als Wirtschaftsfaktor an und will ein wettbewerbliches System auf Datenmärkten gewährleisten.[39] Trotzdem lässt die Strategie ein deutliches Bekenntnis zu genaueren Maßnahmen der Förderung von Digitalmärkten vermissen. Ein „Fahrplan", wie mit mächtigen Tech-Konzernen, die über einen Großteil an Daten verfügen, umgegangen werden soll oder wie bestehende Datensilos aufgebrochen werden könnten, fehlt. Es geht nach wie vor eher darum, dass Unternehmen, Zivilgesellschaft und Wissenschaft Daten freiwillig zur Verfügung stellen sollten,[40] als darum, Daten in einer neuen Form des Wirtschaftens als gewinnbringende Ressourcen zu begreifen.

Insgesamt wird der Fokus weiterhin eher auf das Datenschutzrecht und die DS-GVO als auf das Datenwirtschaftsrecht gelegt. In Zukunft sollte die Bundesregierung in der Datenstrategie ihr Augenmerk deutlicher auf die Datenwirtschaftsordnung richten. Dabei kann das Dateninstitut von BMI und BMWK wichtige Weichen stellen.

B) Fragenbezogene Themenblöcke

Im Folgenden werden die übrigen Fragen des bereitgestellten Katalogs beantwortet. Bei der Beantwortung haben sich **vier Themenblöcke** herausgestellt, denen die Fragen schließlich zugeordnet wurden: Nach einer Betrachtung der Gestaltungsspielräume des deutschen Gesetzgebers (I.) werden daher im Folgenden die Anreize für die Schaffung einer konkurrenzfähigen Datenwirtschaft untersucht (II.). Im Anschluss wird der Frage nachgegangen, wie eine sichere Infrastruktur eine innovative Datenpolitik befördern kann (III.), bevor schließlich die Umsetzungsprobleme einer Betrachtung von Daten als Wirtschaftsgut thematisiert werden (IV.).

I. Gestaltungsspielräume für Innovation und Abbau von Hemmnissen

Der politische Gestaltungsspielraum wird auf nationaler Ebene durch die europäische Gesetzgebung beschränkt. Wo europäische Datenrechtsakte vollharmonisierenden Charakter aufweisen, verbleibt kein Raum für eine individuell-nationale Datenpolitik und ein entsprechendes Datenrecht. Im Folgenden wird dargestellt, inwiefern dem nationalen Gesetzgeber die Möglichkeit zum Erlass eigener Regelungen verbleibt (1.) und wie er durch eine vorausschauende Strukturierung der Aufsicht in den Grenzen des Unions- sowie des Verfassungsrechts eine innovative Datenpolitik ermöglichen kann (2.).

2023, abrufbar unter https://bmdv.bund.de/SharedDocs/DE/Anlage/K/nationale-datenstrategie.pdf?__blob=publicationFile (Stand: 24.06.2024).

[36] Beispielhaft seien die Mobilithek des BMDV oder das Gaia-X Hub Germany genannt.

[37] Vgl. dazu Datenstrategie der Bundesregierung 2023, S. 18.

[38] Vgl. Datenstrategie der Bundesregierung 2023 S. 11 f.

[39] Vgl. Datenstrategie der Bundesregierung 2023, S. 24.

[40] Vgl. Datenstrategie der Bundesregierung 2023, S. 34.

1. Nationale Regelungsspielräume

Regelungsspielräume verbleiben dem nationalen Gesetzgeber zunächst außerhalb des Anwendungsbereichs des vollharmonisierten Unionsrechts. Sofern eine Regelungsmaterie hingegen dem Anwendungsbereich des vollharmonisierten Unionsrechts unterfällt, sind nationale Gesetze grundsätzlich nur im Bereich ausdrücklicher Öffnungsklauseln und Umsetzungsoptionen oder -pflichten möglich. Da für die europäische Digitalstrategie im Bereich der Datenwirtschaft mit dem DA und dem DGA zuvorderst zwei vollharmonisierende Rechtsakte von Bedeutung sind,[41] kann die Reichweite nationaler Regelungsspielräume im Anwendungsbereich nicht vollharmonisierender Richtlinien hier dahinstehen. Einleitend werden in der gebotenen, da als bekannt vorausgesetzten Kürze die nationalen Regelungsspielräume unter der DS-GVO erläutert.

a) DS-GVO

Faktisch macht die DS-GVO als Hybrid zwischen Verordnung und Richtlinie im Unterschied zu DA, DGA und KI-VO intensiv von Öffnungsklauseln Gebrauch,[42] indem sie etwa das Datenschutzrecht der öffentlichen Stellen den nationalen Gesetzgebern zuweist und für das Arbeitsrecht eine Öffnungsoption vorsieht, die in Deutschland mit § 26 BDSG genutzt wurde. Das angekündigte Beschäftigtendatenschutzgesetz soll diese Lücke noch konkreter füllen. Der EuGH unterstreicht diese Sonderstellung. Er hat entschieden, dass sich das Pendant zu § 26 BDSG im Hessischen Datenschutzrecht unter Verstoß gegen das Wiederholungsverbot zu eng an den Wortlaut Art. 88 DS-GVO anlehnt und deshalb gegen Europarecht verstößt.[43]

b) Data Act

Der DA sieht im Gegensatz zur DS-GVO grundsätzlich keine Öffnungsklauseln zugunsten der nationalen Gesetzgeber vor.[44] Möglich ist allein, dass der nationale Gesetzgeber die Gegenleistung des Datenempfängers im Rahmen der Datenweitergabe nach Art. 5 Abs. 1 S. 1 DA ausschließt oder anderweitig festlegt, Art. 9 Abs. 6 DA. Das wäre etwa denkbar, wenn die Transaktionskosten für die Datenweitergabe so hoch sind, dass sie für potenzielle Datenempfänger ein Hindernis darstellen.[45] Hiervon abgesehen verbleibt dem nationalen Gesetzgeber kein nennenswerter Spielraum zur Umsetzung einer innovativen Datenpolitik im Anwendungsbereich des DA. Er kann spezifische Vorschriften für das Zertifizierungsverfahren von Streitbeilegungsstellen erlassen, ErwG 52 DA, hat Sanktionen für Verstöße gegen den DA festzulegen, Art. 40 Abs. 1 DA, und Sachverständige zu benennen, vgl. Art. 45 Abs. 4 DA. Auch außerhalb des Anwendungsbereichs des DA verbleibt kein Raum für die Umsetzung politischer Maßnahmen zur Förderung der Datenwirtschaft.[46]

c) Data Governance Act

Mit dem DGA sollen Projekte wie die finnische Behörde für den Zugang zu Gesundheits- und Sozialdaten (Findata) oder der französische Health Data Hub gefördert werden.[47] Einen Datenzugangsanspruch statuiert der Rechtsakt allerdings nicht, Art. 1 Abs. 2 DGA. Somit können die Mitgliedstaaten selbst entscheiden, ob die Daten öffentlicher Stellen zur

[41] Vgl hierzu ErwG 4 DA, ErwG 3 S. 1 DGA.
[42] Dazu *Schwartmann/Jacquemain* in Schwartmann/Jaspers/Thüsing/Kugelmann (Hrsg.), HK DS-GVO/BDSG, Art. 6 Rn. 195 ff.
[43] EuGH Urt. v. 30.3.2023 – C-34/21, ECLI:EU:C:2023:270 Rn. 90.
[44] *Schmidt-Wudy* in Wolff/Brink/v. Ungern-Sternberg (Hrsg.), DatenschutzR, DA, Art. 23 Rn. 9; *Beinke/Daute* RDi 2024, 69 (72 Rn. 16).
[45] Vgl. ErwG 50 DA; zu Transaktionskosten als Hindernis der Datenwirtschaft *Metzger/Schweitz/Wagner* ZfPW 2023, 227 (235 f.).
[46] Vgl. die geringfügigen Bereichsausnahmen in Art. 1 Abs. 6 UAbs. 2 DA.
[47] *Schreiber/Schoel* LTZ 2024, 3 (4).

Weiterverwendung bereitgestellt werden oder nicht.[48] Eine Pflicht zur Bereitstellung von Daten durch öffentliche Stellen könnte durch ein allgemeines Transparenzgesetz begründet werden, das auf Bundesebene im Koalitionsvertrag angekündigt,[49] bisher aber nicht umgesetzt wurde. Ein solches Vorhaben wäre für die Verwaltung zwar zunächst mit einigem Umsetzungsaufwand verbunden, könnte bestehende Datenbestände in Deutschland aber für die Wirtschaft nutzbar machen und darüber hinaus die Akzeptanz einer wachsenden Datenwirtschaft in der Bevölkerung stärken.[50] Mit den Art. 3 bis 9 DGA wäre den Behörden zudem bereits ein detailliertes Pflichtenprogramm an die Hand gegeben, das die Bedingungen eines rechtssicheren Zugangs konkretisiert. Als zuständige Stelle für die Koordinierung und Umsetzung des Zugangs zu öffentlichen Daten könnte das in der Entstehung befindliche **Dateninstitut** dienen, dessen vorgesehene Aufgaben[51] sich weitläufig mit den Aufgaben der nach Art. 7 Abs. 1 S. 1 DGA vorgesehenen Stellen überschneiden.

Neben der Weiterverwendung bestimmter Kategorien geschützter Daten im Besitz öffentlicher Stellen hat der DGA auch den **Datenaltruismus** als wichtiges Element der Errichtung eines europäischen Binnenmarktes ausgemacht, vgl. ErwG 45 S. 1 DGA.[52] Unter Datenaltruismus versteht der Rechtsakt gem. Art. 2 Nr. 16 DGA „die freiwillige gemeinsame Nutzung von Daten auf der Grundlage der Einwilligung betroffener Personen zur Verarbeitung der sie betreffenden personenbezogenen Daten oder einer Erlaubnis anderer Dateninhaber zur Nutzung ihrer nicht personenbezogenen Daten, ohne hierfür ein Entgelt zu fordern oder zu erhalten, das über eine Entschädigung für die ihnen durch die Bereitstellung ihrer Daten entstandenen Kosten hinausgeht, für Ziele von allgemeinem Interesse gemäß dem nationalen Recht, wie die Gesundheitsversorgung, die Bekämpfung des Klimawandels, die Verbesserung der Mobilität, die einfachere Entwicklung, Erstellung und Verbreitung amtlicher Statistiken, die Verbesserung der Erbringung öffentlicher Dienstleistungen, die staatliche Entscheidungsfindung oder die wissenschaftliche Forschung im allgemeinen Interesse“. Zur Förderung von Datenaltruismus können die Mitgliedstaaten gem. Art. 16 Abs. 1 S. 1 eigene organisatorische oder technische Regelungen oder beides festlegen. Im DGA werden insofern ausdrücklich nationale Strategien genannte, die betroffene Personen dabei unterstützen sollen, sie betreffende personenbezogene Daten im Besitz öffentlicher Stellen freiwillig für den Datenaltruismus zur Verfügung zu stellen. Diese Möglichkeit sollte auf nationaler Ebene ausgeschöpft werden, um die Datenwirtschaft zu fördern.

2. Aufsichtsstrukturen

Neben den angesprochenen Regelungsspielräumen kann der deutsche Gesetzgeber auch durch die Strukturierung der Aufsicht Akzente zugunsten einer innovativen Datenpolitik setzen. Dabei hat er jedoch abermals die Grenzen zu beachten, die sich aus dem Unionsrecht für seinen Handlungsspielraum ergeben. Allgemein können sich insofern Probleme aus unterschiedlichen Strukturvorgaben für verschiedene Behörden ergeben. So hat die

[48] *Schreiber/Schoel* LTZ 2024, 3 (4).
[49] Koalitionsvertrag 2021-2025, S. 9.
[50] Hierzu auch unten II. 6.
[51] Konzept zum Aufbau des Dateninstituts, S. 3-6, abrufbar unter https://www.bmi.bund.de/SharedDocs/downloads/DE/veroeffentlichungen/themen/it-digitalpolitik/dateninstitut/konzeptpapier_dateninstitut.pdf;jsessionid=297A472988697F0703DA382487CE0733.live862?__blob=publicationFile&v=6 (Stand: 25.6.2024). Zum Dateninstitut allgemein unten II. 5. c).
[52] Hierzu auch *Schwartmann/Benedikt* RDV 2022, 59 ff.

vorgeschriebene einfache Unabhängigkeit der Marktüberwachungsbehörden nach der KI-VO eine andere Qualität als die völlige Unabhängigkeit der Datenschutzaufsichtsbehörden.[53]

a) DS-GVO

Die in **Frage 11** adressierte Neuordnung der Aufsichtsstruktur waren Gegenstand einer eigenen Anhörung zur Novelle des BDSG vor dem Innenausschuss vom 24.6.2024.[54] Aus diesem Grund beschränken sich die Ausführungen hier, auf zwei ausgewählte Aspekte der Neuausrichtung der nationalen Aufsichtsstruktur in Deutschland.

Den Datenschutzaufsichtsbehörden ist in der DS-GVO die Aufgabe anvertraut, für die datenverarbeitende Wirtschaft und den Staat klare Leitlinien zu fixieren. Es geht darum, Digitalisierung trotz und mit Datenschutz zu ermöglichen. Die Aufsicht muss – bildlich gesprochen – zunächst und vor allem die Rolle eines Spurassistenten einnehmen und soll nur dann, wenn es nicht anders geht, als bloßer Bremsklotz agieren. Dazu bedarf es neben klaren inhaltlichen Vorgaben, auch deren Durchsetzung durch eine Datenschutzaufsicht, die als Exekutive sachnah, wirksam und mit Augenmaß für einen fairen Ausgleich zwischen Datenschutz und wirtschaftlichen Freiheiten eintritt. Betrachtet man die Realität, so werden die Datenschutzaufsichtsbehörden jedenfalls in Deutschland dieser Rolle schon deshalb oft nicht gerecht, weil es an einheitlichen Entscheidungen fehlt.[55] Das liegt daran, dass die Behörden sich bundesstaatlich verteilt finden und ihr Zusammenwirken orchestrieren müssen. In der aktuellen Novelle des Bundesdatenschutzgesetzes (BDSG) steht die institutionelle Verfestigung des derzeit nur losen Zusammenschlusses der 17 Datenschutzaufsichtsbehörden der Länder und der des Bundes im Zentrum. Schaut man auf die Aufsichtspraxis, dann erkennt man ein intensives Bemühen darum, gleichsam von innen heraus für Einheitlichkeit und Geschlossenheit zu sorgen. Es gibt nicht mehr nur unterschiedliche Orientierungshilfen und Positionspapiere, sondern die Datenschutzkonferenz konsolidiert sich. Das ist eine richtige und wichtige Entwicklung.[56]

Um aus diesen jeweils unabhängigen Behörden einen homogen, rechtsklar und angemessen einheitlich agierenden Verbund zu machen, müssen aber die Gesetzgeber in Bund und Ländern aktiv werden und dabei verfassungsrechtliche Problem der Kooperation von Bund und Ländern bewältigen. Es geht um die Frage nach der Zulässigkeit der Mischverwaltung zwischen Bund und Ländern[57], die Möglichkeit einen Schwerpunkt für die Aufsicht über die Wirtschaft bei der/dem BfDI zu setzen und die verbleibenden Befugnisse der Aufsichtsbehörden der Länder auf den behördlichen Datenschutz zu beschränken. Soll dabei Einheitlichkeit und Entschlusskraft durch Konzentration der Macht auf eine zentrale Stelle bewirkt werden, muss man sich mit den Gefahren einer übermächtigen Superbehörde BfDI auseinandersetzen. Eine andere Lösung könnte einen Staatsvertrag der Länder vorsehen. Letzterer Ansatz müsste aber die Mitwirkung der/des BfDI angemessen lösen. Für eine vermittelnde Lösung hat sich die Gesellschaft für Datenschutz und Datensicherheit (GDD) e.V. ausgesprochen. Danach soll ein effizient arbeitendes, rechtlich institutionalisiertes Gremium nach dem Vorbild des EDSA

---

[53] Hierzu *Schwartmann/Hansen/Keber* in Schwartmann/Keber/Zenner (Hrsg.), KI-Verordnung, 3. Teil 1. Kap. Rn. 24, im Erscheinen.

[54] Dazu https://www.bundestag.de/ausschuesse/a04_inneres/anhoerungen/1008504-1008504 (Stand: 25.6.2024).

[55] *Benedikt/Kranig/Schwartmann* F.A.Z. v. 12.12.2022, 18.

[56] *Grzeszick/Schwartmann* F.A.Z. v. 4.4.2024, 6 und *Grzeszick/Schwartmann* NVwZ 2024, 401 ff.

[57] *Richter/Spiecker gen. Döhmann*, Rechtliche Möglichkeiten zur Stärkung und Institutionalisierung der Kooperation der Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK 2.0), abrufbar unter https://www.datenschutzkonferenz-online.de/media/weitere_dokumente/Richter_Spiecker_Gutachten_DSK_2-0.pdf (Stand: 25.6.2024).

geschaffen werden, das Rechtsauffassungen in angemessener Frist mehrheitlich und verbindlich beschließen darf.[58]

Der aktuell diskutierte Entwurf des BDSG ist hier bestenfalls halbherzig. Das alles führt nicht dazu, dass Datenschutzaufsichtsbehörden ihre Rolle wahrnehmen können, die darin besteht, kluge, klare und angemessene Regeln für die Datenverarbeitung zu fixieren.

Eine Modifikation der Struktur der Datenschutzaufsicht wird in Deutschland aktuell wegen einer verfassungsrechtlich fragwürdigen Entscheidung des EuGH aus dem Jahr 2024 für die Datenschutzaufsicht über den Bundestag und die Landesparlamente gefordert.[59] In Rede steht insbesondere die Errichtung von unabhängigen und spezifischen Aufsichtsbehörden zum Parlamentsdatenschutz[60].

b) Data Act

Der DA sieht vor, dass die Datenschutzaufsichtsbehörden auch bezüglich des Schutzes personenbezogener Daten im Rahmen des grundsätzlich datenwirtschaftlich orientierten Rechtsakts zuständig sind, Art. 37 Abs. 3 UAbs. 1 S. 1 DA. Diese Aufgabenzuweisung mag zunächst verwundern, berührt der DA doch gem. Art. 1 Abs. 5 S. 1 DA gerade nicht das Unionsrecht über den Schutz personenbezogener Daten, namentlich also insbesondere die DS-GVO. Dennoch werden bei der Datenweitergabe datenschutzrechtliche Aspekte relevant, wenn etwa personenbezogene Daten Dritter weitergegeben werden sollen, vgl. Art. 4 Abs. 12, Art. 5 Abs. 7 DA. Ergänzt werden die Vorschriften der DS-GVO zudem gem. Art. 1 Abs. 5 S. 2 DA hinsichtlich des Auskunftsrechts sowie des Rechts auf Datenübertragbarkeit der betroffenen Personen, vgl. auch Art. 5 Abs. 8 DA.[61] Für diese Bereiche sind weiterhin die Datenschutzaufsichtsbehörden zuständig. Sie haben konsequenterweise im Rahmen ihrer Zuständigkeit auch die Befugnis, den Personenbezug der Daten zu prüfen.[62] Neben dieser Spezialzuweisung aufsichtsrechtlicher Befugnisse an die Datenschutzaufsichtsbehörden sollen bei besonderen sektoralen Angelegenheiten des Datenzugangs und der Datennutzung die Zuständigkeiten der sektoralen Behörden gewahrt bleiben.

Abgesehen von diesen speziellen Zuweisungen sind die Mitgliedstaaten bei der Benennung der Behörden, welche die Durchsetzung des DA überwachen sollen, grundsätzlich frei, vgl. Art. 37 Abs. 1 S. 1 DA. Werden mehrere Behörden für zuständig erklärt, ist daneben ein Datenkoordinator zu benennen, der die Zusammenarbeit zwischen den zuständigen Behörden erleichtern und die im DA adressierten Stellen bei der Umsetzung der Vorgaben des Rechtsakts unterstützen soll. Der Datenkoordinator soll „aus der Mitte“ der zuständigen Behörden benannt werden. Der Wortlaut spricht dafür, dass es sich bei dem Koordinator daher nicht um eine eigenständige Behörde handeln soll.[63] Bei der Benennung ist aber darauf zu achten, dass nur eine nach Art. 37 Abs. 1 S. 1 DA benannte Behörde zugleich Datenkoordinator sein darf. Sofern also beispielsweise die Landesdatenschutzbeauftragten mit der Durchsetzung des DA betraut

[58] GDD-Stellungnahme zum Referentenentwurf des BMI für ein Erstes Gesetz zur Änderung des Bundesdatenschutzgesetzes, S. 3, abrufbar unter https://www.gdd.de/wp-content/uploads/2023/09/Stellungnahme-zum-BDSG-E-2023.pdf (Stand: 25.6.2024).

[59] *Grzeszick/Schwartmann* F.A.Z. v. 4.4.2024, 6 und *Grzeszick/Schwartmann* NVwZ 2024, 401 ff.

[60] *Grzeszick/Schwartmann* F.A.Z. v. 4.4.2024, 6 und *Grzeszick/Schwartmann* NVwZ 2024, 401 ff.

[61] Vgl. zum Verhältnis zwischen Data Act und DS-GVO am Beispiel der Datenportabilität die Synopse bei *Schwartmann/Wasilewski* RDV 2024, 76 ff; allgemein zum Zusammenspiel von Data Act und DS-GVO *Paal/Cornelius/Seeland* RDV 2024, 5 ff.

[62] Zur Organisation der Datenschutzaufsichtsbehörden bei der Erfüllung dieser Aufgaben *Remke* MMR 2024, 117.

[63] *Roth-Isigkeit* in Wolff/Brink/v. Ungern-Sternberg (Hrsg.), BeckOK DatenschutzR, DA, Art. 37 Rn. 5.

werden, könnten BfDI und Dateninstitut nur als Datenkoordinator fungieren, wenn sie ebenfalls als zuständige Stellen benannt werden.[64]

c) Data Governance Act

Nach dem DGA müssen die Mitgliedstaaten eine oder mehrere zuständige Behörden für Datenvermittlungsdienste sowie für die Registrierung datenaltruistischer Organisationen benennen, Art. 13 Abs. 1 S. 1 DGA, Art. 23 Abs. 1 UAbs. 1 DGA.

Sie sind dabei grundsätzlich freier als im Rahmen der Benennung nach dem DA: Der DGA sieht keine speziellen Aufgabenzuweisungen hinsichtlich der Aufsichtsstruktur vor. Er legt lediglich fest, dass die Zuständigkeiten der Fachbehörden, insbesondere der Datenschutzaufsichtsbehörden, gem. Art. 13 Abs. 3 S. 1 DGA bei der Wahrnehmung der Aufgaben im Zusammenhang mit dem Anmeldeverfahren für Datenvermittlungsdienste unberührt bleiben. Das bedeutet nicht, dass diese Behörde zwangsläufig als Gegenspieler der nach dem DGA zuständigen Behörde eigenständig bleiben müssen. Vielmehr können auch sie die Aufgaben im Rahmen des Art. 13 Abs. 1 DGA übernehmen.[65]

d) KI-VO

Künstliche Intelligenz (KI) ist eine Technologie, die erheblich von einer konkurrenzfähigen Datenwirtschaft profitiert und ihrerseits entscheidender Faktor allgemeinwirtschaftlichen Wachtsums ist. Daher sollen an dieser Stelle auch die aufsichtsrechtlichen Strukturen nach der KI-VO beleuchtet werden.

Die KI-VO sieht einige Spezialzuweisungen im Bereich der Aufsicht über KI-Systeme vor. Die Marktaufsicht über KI-Systeme, die mit einem nach dem EU-Produktsicherheitsrecht regulierten Produkt in Verbindung stehen, soll von der Behörde übernommen werden, die auch für die Überwachung des Produkts zuständig ist. Hochrisiko-KI-Systeme, die von Finanzinstituten in Verkehr gebracht, in Betrieb genommen oder eingesetzt werden, sollen zudem grundsätzlich der jeweiligen Finanzaufsicht unterstehen. In Deutschland ist in diesen Fällen also grundsätzlich die BaFin für die Marktüberwachung zuständig. Schließlich sollen die Datenschutzaufsichtsbehörden für die Aufsicht über bestimmte Hochrisiko-KI-Systeme zuständig sein. Dies betrifft die Bereiche der Strafverfolgung, der Migration, des Asyls und der Grenzkontrolle sowie der Rechtspflege und der demokratischen Prozesse.[66]

Außerhalb dieser speziellen Zuweisungen können die Mitgliedstaaten auch im Anwendungsbereich der KI-VO sowohl die notifizierenden als auch die Marktüberwachungsbehörden grundsätzlich frei benennen, Art. 70 Abs. 1 S. 1 KI-VO.

e) Politischer Wille als Grundlage der Zuweisung

In den Grenzen des dargestellten Rahmens unterstellt das Unionsrecht die Strukturierung der Aufsicht im Bereich der Datenwirtschaft damit dem politischen Willen der Mitgliedstaaten. Die Zuweisung der Zuständigkeiten auf nationaler Ebene ist naturgemäß Gegenstand umfassender Diskussionen. Hierzu sei lediglich exemplarisch auf die Öffentliche Anhörung des Digitalausschusses am 15.5.2024 zur nationalen Aufsicht im Rahmen der KI-VO verwiesen.[67]

---

[64] Vgl. für BfDI *Remke* MMR 2024, 117 (118).

[65] *Richter* in Wolff/Brink/v. Ungern-Sternberg (Hrsg.), BeckOK DatenschutzR, DGA, Art. 13 Rn. 17

[66] Art. 74 Abs. 3-8 KI-VO. Hierzu *Schwartmann/Hansen/Keber* in Schwartmann/Keber/Zenner (Hrsg.), KI-Verordnung. Leitfaden für die Praxis, 3. Teil 1. Kap. Rn. 25, im Erscheinen.

[67] Nationale Aufsicht bei Künstlicher Intelligenz komplex, abrufbar unter https://www.bundestag.de/dokumente/textarchiv/2024/kw20-pa-digitales-ki-1001728 (Stand: 21.6.2024).

Grundsätzlich lässt sich festhalten, dass den Datenschutzaufsichtsbehörden im Anwendungsbereich europäischer Rechtsakte zur Datenwirtschaft spezialgesetzlich die Zuständigkeit für die Überwachung des Schutzes personenbezogener Daten eingeräumt wird. Das deckt sich mit der Aufgabenzuweisung in Art. 51 Abs. 1 DS-GVO, wonach die Datenschutzaufsichtsbehörden die Grundrechte und Grundfreiheiten natürlicher Personen bei der Verarbeitung schützen und den freien Verkehr personenbezogener Daten erleichtern sollen. Ob die Datenschutzaufsichtsbehörden in Folge dieser Aufgabenzuweisung und ihrer Expertise im Bereich der Verarbeitung personenbezogener Daten die Aufsicht über das gesamte Datenrecht übernehmen sollten, lässt sich differenziert beurteilen. Alternativ wäre daran zu denken, einer wirtschaftlich orientierten Behörde die Zuständigkeit im Bereich des Datenwirtschaftsrechts zuzuweisen, ähnlich wie es im Falle der KI-VO für die Bundesnetzagentur diskutiert wird.

Insofern ist festzuhalten, dass mit einer solche Datenwirtschaftsbehörde ein neuer Akteur in die ohnehin zerstückelte Aufsichtsstruktur im Bereich des Datenschutzes eintreten würde. Es stünde zu befürchten, dass sich die für Datenwirtschaft und für Datenschutz zuständigen Behörden insofern gegenseitig blockieren, was bestehende Probleme im Bereich der Datenschutzaufsicht auf den gesamten Bereich der datenverarbeitenden Wirtschaft übertragen würde. Hinzu kommt, dass die Datenschutzaufsichtsbehörden auch im Anwendungsbereich des DA und des DGA zuständig sind, sofern personenbezogene Daten verarbeitet werden. Es wäre damit sogar ein innergesetzlicher Konflikt zwischen den Aufsichtsbehörden zu befürchten.

Allerdings sind bei der Etablierung einer Aufsichtsstruktur die neuen datenrechtlichen Realitäten in den Blick zu nehmen. Das Datenschutzrecht bildet nicht mehr den unumstößlichen Kern des Datenrechts. Bereits die DS-GVO verweist aber in ihrem Art. 1 Abs. 3 auf die Bedeutung des freien Verkehrs personenbezogener Daten. Mit dem DA und dem DGA tritt das Datenwirtschaftsrecht endgültig gleichberechtigt neben das Datenschutzrecht und bildet gemeinsam mit diesem das Datenrecht.[68] Die historisch bedingte Einordnung des Datenschutzrechts als Zentrum jeglicher Datenverarbeitung muss vor diesem Hintergrund neu gedacht werden: Innerhalb des Datenrechts steht das Datenschutzrecht in einem Wechselwirkungsverhältnis zur Datenwirtschaft. Der Datenschutz würde vernachlässigt, wenn er allein aus der Perspektive der Datenwirtschaft gedacht würde. Ebenso wird die Datenwirtschaft vernachlässigt, wenn sie allein aus der Perspektive des Datenschutzes betrachtet wird. Sinnvoll wäre demnach eine Spiegelung des Wechselwirkungsverhältnisses zwischen Datenschutz und Datenwirtschaft in den Aufsichtsstrukturen. Die Datenschutzaufsichtsbehörden betrachten das Datenrecht bisher allerdings verstärkt aus der Perspektive des Grundrechtsschutzes. Die Bedürfnisse der Datenwirtschaft sind demgegenüber unterrepräsentiert.

Im Ergebnis lassen sich damit zwei entscheidende Aspekte für die weitere Strukturierung der datenrechtlichen Aufsicht formulieren: Eine neue Datenwirtschaftsbehörde würde die Zersplitterung der datenrechtlichen Aufsichtsstruktur verstärken und ist deshalb kritisch zu sehen. Sofern Zuständigkeiten im Bereich des Datenwirtschaftsrechts deshalb nachvollziehbarerweise an die Datenschutzaufsichtsbehörden vergeben werden, müssen diese allerdings ihren Blick weiten, indem sie Datenwirtschaft und Datenschutz in ein angemessenes Verhältnis bringen können. Aufgrund der Unabhängigkeit der Datenschutzaufsichtsbehörden ist eine dahingehende Einflussnahme unzulässig. Die Politik kann lediglich Strukturen schaffen, um den ohnehin stark ausgelasteten Behörden ausreichend personelle und finanzielle Mittel zur

[68] *Steinrötter* GRUR 2023, 216; *Steinrötter* FS Taeger, 491; *Steinrötter* RDi 2021, 480; *Specht-Riemenschneider* ZEuP 2023, 638 (639).

Verfügung zu stellen. Diese müssten die zusätzlichen Mittel dann aus eigenem Antrieb nutzen, um einen Ausgleich zwischen Datenwirtschaft und Datenschutz herzustellen. Für die Verarbeitung personenbezogener Daten ergibt sich diese Aufgabe bereits unmittelbar aus dem Gesetz, Art. 51 Abs. 1 DS-GVO.

II. Anreize für die Datenwirtschaft in einem wettbewerbsfähigen Datenökosystem

Mit Blick auf die wachsende Bedeutung der Datenwirtschaft stellt sich die Frage, wie Anreize für die Datenwirtschaft in einem wettbewerbsfähigen Datenökosystem geschaffen werden können.[69] Im Folgenden werden dazu verschiedene Aspekte angesprochen, die von der datenrechtlichen Realität ausgehen. Es wird gefragt, wie mit den gegebenen Zuständen umzugehen ist, um eine starke Datenwirtschaft zu sichern.

1. Anonymisierung und Pseudonymisierung

Datenschutzrecht und Datenwirtschaftsrecht stehen in einem Wechselwirkungsverhältnis. Der Datenschutz darf die Datenwirtschaft nicht ignorieren. Andererseits gilt das Datenschutzrecht aber auch in datenwirtschaftlichen Angelegenheiten. Ausdrücklich ergibt sich dies etwa aus Art. 1 Abs. 5 DA, Art. 1 Abs. 3 DGA und für KI-Systeme als datenverarbeitende Technologie aus Art. 2 Abs. 7 KI-VO.

Im Anwendungsbereich der DS-GVO dürfen Daten deshalb auch in der Datenwirtschaft nur für festgelegte, eindeutige und legitime Zwecke erhoben werden. Werden Zwecke geändert, müssen diese nach Maßgabe der DS-GVO miteinander kompatibel sein. Sind Zwecke einer Verarbeitung personenbezogener Daten im Rahmen einer Erhebung von Daten nicht absehbar, wird es für Datenverarbeiter umso schwieriger, eine Weiterverwendung datenschutzkonform auszugestalten. Neben Anforderungen an die Rechtmäßigkeit und Zweckbindung von Verarbeitungen personenbezogener Daten treten eine Vielzahl von weiteren Anforderungen, sei es die Transparenz, die Datenminimierung oder das Löschen personenbezogener Daten nach ihrer Zweckerreichung.

Die bußgeldbewehrten Vorgaben der DS-GVO können aus Perspektive der Datenmarktes ein wirtschaftliches Hemmnis darstellen.[70] Insbesondere die Rechtfertigung einer Verarbeitung personenbezogener Daten bedeutet für datenschutzrechtlich Verantwortliche eine Herausforderung. Die in der DS-GVO prominent platzierte Lösung der Einwilligung ist aus vielen Gründen für die Datenwirtschaft wenig geeignet.[71] Friktionen zeigen sich unter anderem mit Blick auf neue Technologien: Werden KI-Modelle auf Basis einer Einwilligung mit personenbezogenen Daten trainiert und die Einwilligung im Anschluss widerrufen, stellt sich die Frage, ob und wie die verarbeiteten Daten aus dem Modell zu entfernen sind.[72] Die Datenwirtschaft hat deshalb ein erhebliches Interesse daran, den Anwendungsbereich der DS-GVO zu verlassen, um ihren umfassenden Vorgaben zu entgehen.

---

[69] *Schwartmann* F.A.Z. 27.6.2022, und *Brink/Oetjen/Schwartmann/Voss* F.A.Z. v. 18.7.2022, 18.

[70] „Konflikt zwischen Datenmarkt und Datenschutz“ bei *Engeler* NJW 2022, 3398 (3398 Rn. 1); „Friktionen“ bei *Hennemann/Steinrötter* NJW 2022, 1481.

[71] Hierzu eingehend *Engeler* NJW 2022, 3398 (3402 Rn. 23-3403 Rn. 31); für Datenprimärmärkte zudem *Metzger/Schweitzer/Wagner* ZfPW 2023, 227 (238).

[72] Zum insofern relevanten Personenbezug von KI-Sprachmodellen *Schwartmann/Köhler* in Schwartmann/Benedikt/Reif (Hrsg.), Datenschutz im Internet, Kap. 29 Rn. 7. Die dänische Datenschutzaufsichtsbehörde Datatilsynet geht davon aus, dass ein KI-Sprachmodell nach Abschluss des Trainings keine personenbezogenen Daten enthält, s. *Datatilsynet*, Offentliggørelse af datasæt og AI-model, abrufbar unter https://www.datatilsynet.dk/afgoerelser/afgoerelser/2024/jan/offentliggoerelse-af-datasaet-og-ai-model (Stand: 24.6.2024). Dann liefe ein Widerruf der Einwilligung ins Leere.

a) Personenbezug als Begründung des Datenschutzrechts

Der Anwendungsbereich der DS-GVO ist auf personenbezogene Daten beschränkt, Art. 2 Abs. 1 DS-GVO. Auf Daten ohne Personenbezug ist die DS-GVO damit nicht anwendbar. Für datenschutzrechtliche Vorgaben besteht in diesem Fall auch kein Bedürfnis: Das Datenschutzrecht dient dem Grundrechtsschutz.[73] Sofern von einer Datenverarbeitung aber kein Grundrechtsträger betroffen ist, ist auch kein Grundrechtsschutz erforderlich.

Die Frage des Personenbezugs eines Datums ist damit von enormer Bedeutung. Die DS-GVO versteht unter personenbezogenen Daten zunächst „alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen", wobei eine natürliche Person als identifizierbar angesehen wird, wenn sie „direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann", Art. 4 Nr. 1 DS-GVO. ErwG 26 S. 3 DS-GVO stellt zudem klar, dass bei der Beurteilung der Identifizierbarkeit einer Person alle Mittel zu berücksichtigen sind, „die von dem Verantwortlichen oder einer anderen Person nach allgemeinem Ermessen wahrscheinlich genutzt werden, um die natürliche Person direkt oder indirekt zu identifizieren".

Damit stellt sich eine entscheidende Frage bei der Bestimmung des Personenbezugs: Ist hinsichtlich der Möglichkeit zur Identifizierung im Kern auf die Kenntnisse und Mittel des Verantwortlichen abzustellen (relatives Begriffsverständnis) oder genügt es für die Annahme des Personenbezugs bereits, wenn ein Dritter die natürliche Person identifizieren kann (absolutes Begriffsverständnis).[74] Zu dieser Frage hat der EuGH in zwei wegweisenden Entscheidungen Stellung genommen und damit das Merkmal des Personenbezugs im Kontext der DS-GVO konkretisiert:

In der Rechtssache Breyer hat der EuGH entschieden, dass für die Annahme eines Personenbezugs nicht alle zur Identifizierung der betreffenden Person erforderlichen Informationen in den Händen einer einzigen Person liegen müssen.[75] Es genügt allerdings nicht, wenn irgendjemand über Informationen verfügt, die zur Identifizierung einer natürlichen Person beitragen können.[76] Entscheidend ist, ob der Verantwortliche über Mittel verfügt, die er vernünftigerweise einsetzen könnte, um die betreffende Person zu bestimmen.[77] Ein Personenbezug ist abzulehnen, wenn die Identifizierung mit eigenen Mitteln oder mit Hilfe eines Dritten gesetzlich verboten oder praktisch nicht durchführbar ist, weil sie einen unverhältnismäßigen Aufwand an Zeit, Kosten und Arbeitskraft erfordern würde.[78] Die praktische Durchführbarkeit der Zuordnung stand auch im Zentrum der Entscheidung in der Rechtssache Gesamtverband Autoteile-Handel e. V. gegen den Lkw-Hersteller Scania.[79] Der EuGH entschied in diesem Verfahren u.a. darüber, ob die Fahrzeug-Identifikationsnummer für den Fahrzeughersteller und andere Wirtschaftsakteure ein personenbezogenes Datum ist. Die Frage, ob der Verantwortliche oder ein Dritter bei vernünftiger Betrachtungsweise über Mittel verfügen, die eine Zuordnung

[73] Vgl. insoweit nur ErwG 1 S. 1 und ErwG 26 S. 1 DS-GVO.

[74] *Klar/Kühling* in Kühling/Buchner (Hrsg.), Ds-GVO/BDSG, Art. 4 Rn. 25-30; *Karg* in Simitis/Hornung/Spiecker gen. Döhmann (Hrsg.), Datenschutzrecht, DS-GVO, Art. 4 Rn. 58.

[75] EuGH Urt. v. 19.10.2016 – C-582/14, ECLI:EU:C:2016:779 Rn. 43 – Breyer; in den Kontext setzend *Schwartmann/Mühlenbeck* RDV 2022, 264 ff.

[76] EuGH, Schussanträge vom 12. Mai 2016, ECLI:EU:C:2016:339 Rn. 68 – Breyer.

[77] Vgl. EuGH Urt. v. 19.10.2016 – C-582/14, ECLI:EU:C:2016:779 Rn. 48 – Breyer.

[78] EuGH Urt. v. 19.10.2016 – C-582/14, ECLI:EU:C:2016:779 Rn. 46 – Breyer.

[79] EuGH Urt. v. 9.11.2023 – C-319/22, ECLI:EU:C:2023:837.

ermöglichen und somit ein Personenbezug gegeben ist, ist stets eine Einzelfallbetrachtung.[80] Aus ErwG 26 S. 4 DS-GVO ergibt sich, dass insofern alle objektiven Faktoren, wie die Kosten der Identifizierung und der dafür erforderliche Zeitaufwand, herangezogen werden sollen. Welche Beziehungen zwischen dem Verantwortlichen und einem Dritten bestehen müssen, um einen Personenbezug anzunehmen, ließ der EuGH bisher offen. Er wird aber in absehbarer Zeit Stellung beziehen müssen: Das EuG hatte im April 2023 eine Entscheidung des Europäischen Datenschutzbeauftragten (EDSB) für nichtig erklärt, weil dieser von einem absoluten Begriffsverständnis ausgegangen war.[81] Gegen die Entscheidung hat der EDSB Rechtsmittel eingelegt, über die vom EuGH entschieden werden muss.

Bereits jetzt steht allerdings fest, dass die Feststellung des Personenbezugs von der praktischen Durchführbarkeit der Identifizierung abhängt und damit eine wertenden Betrachtung der vernünftigerweise einsetzbaren Mittel beim Verantwortlichen und bei Dritten erfordert.[82] Die daraus resultierende rechtliche Unsicherheit führte in der Vergangenheit dazu, dass Wirtschaftsakteure aufgrund risikoaverser Überlegungen im Zweifelsfall von einem Personenbezug ausgingen. Die neuen Datenakte verlangen allerdings nunmehr eine trennscharfe Abgrenzung.[83] Ebenso wird Rechtssicherheit im Bereich datenverarbeitender Technologien wichtiger, da etwa beim Training eines KI-Modells große Mengen an Daten verarbeitet werden. Wenn für all diese Daten vorsorglich von einem Personenbezug ausgegangen wird, bedeutet die dann erforderliche Einhaltung der Vorschriften der DS-GVO für die Wirtschaftsakteure eine enorme finanzielle Belastung. Die Wirtschaft benötigt deshalb dringend Konkretisierungen, aus denen eindeutig abgeleitet werden kann, ob ein relevantes Datum einen Personenbezug aufweist und die Vorgaben der DS-GVO damit Anwendung finden.

b) Leitfaden und Grundsatzregeln zu Anonymisierung und Pseudonymisierung im Auftrag der Stiftung Datenschutz

Die Stiftung Datenschutz hat deshalb bereits im Jahr 2022 einen Praxisleitfaden über die Anonymisierung[84] und zugleich die Erarbeitung von Grundsatzregeln über die Anonymisierung[85] als Basis für Codes of Conducts in diesem Bereich in Auftrag gegeben. Die Anonymisierung von Daten macht den Rückschluss auf eine Person unmöglich. Der Personenbezug ist damit aufgelöst und die Anwendbarkeit der DS-GVO nach dem Gesagten ausgeschlossen. Das ist dann gewünscht und erforderlich, wenn anonyme Daten den Zweck nach der Verarbeitung erfüllen. Sofern dagegen betroffene Personen etwa zur eigenen Gesundheitsvorsorge den Rückschluss auf ihre Daten erhalten möchten, sieht die DS-GVO deren Pseudonymisierung vor. Sie sorgt dafür, dass Daten durch Verschlüsselung gegen Missbrauch geschützt werden.[86] Diesbezüglich verweist die Studie auf den von der Fokusgruppe Datenschutz des Bundesinnenministeriums

[80] Vgl. Schussanträge vom 4. Mai 2023, ECLI:EU:C:2023:385 Rn. 42 – Gesamtverband Autoteile-Handel eV/Scania CV AB.
[81] EuG Urt. v. 26.4.2023 – T-557/20, ECLI:EU:T:2023:219 Rn. 74.
[82] EuGH Urt. v. 19.10.2016 – C-582/14, ECLI:EU:C:2016:779 Rn. 46 – Breyer; EuGH Urt. v. 9.11.2023 – C-319/22, ECLI:EU:C:2023:837 Rn. 49 – FIN.
[83] Hierzu *Bomhard/Merkle* RDi 2022, 168 (172); *Steinrötter* GRUR 2023, 216 (219).
[84] https://stiftungdatenschutz.org/fileadmin/Redaktion/Dokumente/Anonymisierung_personenbezogener_Daten/SDS_Studie_Praxisleitfaden-Anonymisieren-Web_01.pdf (Stand: 25.6.2024).
[85] https://stiftungdatenschutz.org/fileadmin/Redaktion/Dokumente/Anonymisierung_personenbezogener_Daten/SDS_Studie_Grundsatzregeln_Web_01.pdf (Stand: 25.6.2024).
[86] Zu dieser Studie *Schwartmann/Jaspers/Lepperhoff/Weiß* RDV 2023, 40 ff.

im Rahmen des Digital-Gipfels 2019 erarbeiteten „Entwurf für einen Code of Conduct zum Einsatz DS-GVO konformer Pseudonymisierung“.[87]

Der Wunsch von Verantwortlichen per Anonymisierung den Anwendungsbereich der DS-GVO zu verlassen, um Daten einfacher durch sich oder durch Dritte nutzbar zu machen, ist nachvollziehbar. Umso wichtiger ist es aber, die Grenze des rechtlich zulässigen zunächst was deren Grundregeln anbelangt, sauber zu ziehen. Nur so kann Rechtsklarheit und Rechtssicherheit unter Wahrung der Erfordernisse der DS-GVO geschaffen werden. Der Praxisleitfaden der Stiftung Datenschutz befasst sich mit Hinweisen zur Anonymisierung von personenbezogenen Daten.[88] Er ordnet den Begriff der Anonymisierung und dessen Ausprägungen im bestehenden rechtlichen Kontext ein. Dabei muss eine Abgrenzung von anderen Verarbeitungsvorgängen erfolgen, etwa von der Pseudonymisierung. Nach der begrifflichen Einordnung werden gängige Verfahren und Techniken einer Anonymisierung allgemein beschrieben. Um den Praxisbezug zu wahren schließen sich hieran Einsatzklassen einer Anonymisierung an. Hierbei werden Anwendern Einsatzszenarien und -beispiele aufgezeigt, in denen eine Anonymisierung erfolgen kann. Ein gesondertes Kapitel befasst sich mit dem rechtlichen Umfeld der Anonymisierung und den dabei bestehenden Anforderungen, seien es besondere Prüf-, Dokumentations- oder Transparenzpflichten. Um insbesondere kleinere und mittelständische Unternehmen zu unterstützen, wird ein Vorgehensmodell zur Verfügung gestellt, um den Vorgang der Anonymisierung schrittweise und strukturiert zu vollziehen.

Leitfaden und Grundregeln dienen als allgemeine Orientierungshilfe bei der Anonymisierung personenbezogener Daten. Sie können und sollen nicht dazu dienen, abschließende Vorgaben für ein solches Verfahren zu formulieren.[89]

c) Rechtliche Umsetzung

Eine rechtverbindliche Konkretisierung des Personenbezugs, die klare Vorgaben zu den Anforderungen einer Konkretisierung macht, ist auf nationaler Ebene praktisch nicht umsetzbar. Die Datenschutzaufsichtsbehörden können aufgrund ihrer Unabhängigkeit nicht zu einer Präzisierung angewiesen werden. Darüber hinaus ist der Begriff des Personenbezugs von der vollharmonisierenden Wirkung der DS-GVO umfasst und kann deshalb nicht innerstaatlich ausgefüllt werden.[90] Für die Bundesrepublik verbleibt damit nur die Möglichkeit, im Rat der Europäischen Union auf Klarstellungen hinzuwirken, die sich im Kern nur durch eine Reform der DS-GVO verwirklichen lassen.

Konkret wurde insofern vorgeschlagen, Anonymisierungsstandards festzulegen, deren Beachtung die Anwendung der DS-GVO unabhängig von den Informationsbeschaffungsmöglichkeiten des Datenempfängers ausschließen würde, wobei eine tatsächliche De-Anonymisierung zu sanktionieren wäre.[91] Dieser Vorschlag ähnelt dem US-amerikanischen Modell, wonach Gesundheitsdaten, die dem „de-identification of health information“ (DHI)-Standard

[87] Schwartmann/Weiß (Hrsg.), Entwurf für einen Code of Conduct zum Einsatz DS-GVO konformer Pseudonymisierung, abrufbar unter https://www.de.digital/DIGITAL/Redaktion/DE/Digital-Gipfel/Download/2019/p9-code-of-conduct.pdf?__blob=publicationFile&v=2 (Stand: 25.6.2024).

[88] Zu den Anforderungen an die Pseudonymisierung Schwartmann/Weiß (Hrsg.), Entwurf für einen Code of Conduct zum Einsatz DS-GVO konformer Pseudonymisierung, abrufbar unter https://www.de.digital/DIGITAL/Redaktion/DE/Digital-Gipfel/Download/2019/p9-code-of-conduct.pdf?__blob=publicationFile&v=2 (Stand: 25.6.2024).

[89] Zum Ganzen *Schwartmann/Jaspers/Lepperhoff/Weiß/Mayer* in Stiftung Datenschutz (Hrsg.), Anonymisierung und Pseudonymisierung von Daten (2023), S. 2 f.

[90] Vgl. nur EuGH Urt. v. 9.11.2023 – C-319/22, ECLI:EU:C:2023:837 Rn. 44 – FIN.

[91] *Metzger/Schweitz/Wagner* ZfPW 2023, 227 (235).

entsprechen, keiner datenschutzrechtlichen Regulierung unterliegen. Sofern der Vorschlag eine gesetzliche Festsetzung der Anonymisierungsstandards in Bezug nimmt, ist problematisch, dass sich die technischen Möglichkeiten zur Wiederherstellung des Personenbezugs bei anonymisierten Daten stetig weiterentwickeln. So wurde im Mai 2024 eine Studie veröffentlicht, in der die Fähigkeit von KI-Sprachmodelle zur Re-Identifizierung untersucht wurde.[92] Darin wurde festgestellt, dass die Modelle zwar erhebliche Schwierigkeiten bei der Re-Identifizierung von Daten in Gerichtsentscheidungen haben, anonymisierte Wikipedia-Artikel aber einigermaßen problemlos natürlichen Personen zuordnen können.[93] Bereits die wachsende Verfügbarkeit von KI-Sprachmodellen beeinflusst die Bewertung der vernünftigerweise einsetzbaren Mittel und damit die praktische Durchführbarkeit einer Identifizierung. Das Beispiel zeigt, wie oft gesetzlich festgesetzte Anonymisierungsstandards zu ändern wären.

Abhilfe könnte hier ein Blick in die KI-VO leisten, die hinsichtlich der technischen Weiterentwicklung des Regulierungsgegenstands mit ähnlichen Problemen zu kämpfen hat. Dort wurde die Kommission ermächtigt, einige Regulierungsaspekte, die voraussichtlich einer Entwicklung unterliegen, durch Leitlinien und delegierte Rechtsakte zu konkretisieren und anzupassen, vgl. Art. 96 und Art. 97 KI-VO. Dieses Vorgehen ermöglicht einen flexiblen Umgang mit technischen Entwicklungen, der gerade im Bereich der Anonymisierung dringend erforderlich ist. Allerdings stand die Möglichkeit zum Erlass delegierter Rechtsakte auch im Anwendungsbereich der DS-GVO zur Verfügung und wurde dort nur unzureichend ausgeübt.

Vor diesem Hintergrund müssten Anonymisierungsstandards von einer unabhängigen Stelle bereitgestellt werden, an denen sich die Wirtschaft orientieren kann, um einen Personenbezug der verarbeiteten Daten ausschließen zu können. Zu denken ist in diesem Zusammenhang an das im Aufbau befindliche Dateninstitut.[94] Dessen Konzept sieht bereits vor, dass es sich mit der Anonymisierung von Daten beschäftigen soll.[95] Erforderlich wäre nach dem Gesagten, dass das Dateninstitut unter Berücksichtigung der technischen Entwicklung regelmäßig aktualisierte Leitlinien mit Anonymisierungsstandards zur Verfügung stellt.

2. Musterverträge für Datenteilung

Gem. Art. 41 DA erstellt die Kommission unverbindliche Mustervertragsklauseln für den Datenzugang und die Datennutzung, um die Parteien bei der Ausarbeitung und Aushandlung von Verträgen mit fairen, angemessenen und nichtdiskriminierenden vertraglichen Rechten und Pflichten zu unterstützen. Damit soll Dateninhabern und Datenempfängern vor allem dabei geholfen werden, Bedingungen für eine angemessene Gegenleistung und den Schutz von Geschäftsgeheimnissen zu formulieren. Die Idee der Mustervertragsklauseln wurde an anderer Stelle bereits mit Blick auf die AGB zur Kommunikation in sozialen Netzwerken vorgeschlagen, um das Problem der überbordenden Ausübung des virtuellen Hausrechts einzuhegen.[96] Insofern ist die nunmehr gesetzlich vorgesehene Etablierung von Mustervertragsklauseln erfreulich.

Die Kommission muss die Mustervertragsklauseln vor dem 12.9.2025 erstellen. Sofern sich im Anschluss zeigt, dass wesentliche Aspekte in den Mustervertragsklauseln der Kommission nicht enthalten sind, wäre darüber nachzudenken, ob ein Bundesministerium weitere, über

---

[92] *Nyffenegger/Stürmer/Niklaus* NAACL 2024, 2433-2462.
[93] *Nyffenegger/Stürmer/Niklaus* NAACL 2024, 2433.
[94] Hierzu auch unten 5. c).
[95] Konzept zum Aufbau des Dateninstituts, S. 6, abrufbar unter https://www.bmi.bund.de/SharedDocs/downloads/DE/veroeffentlichungen/themen/it-digitalpolitik/dateninstitut/konzeptpapier_dateninstitut.pdf;jsessionid=25C05211F5D4149D4A55F7001B0D25A5.live862?__blob=publicationFile&v=6 (Stand: 25.6.2024).
[96] *Schwartmann* NJW 2022, 133 (135 Rn. 6 und passim).

Art. 41 DA hinausgehende Muster zur Verfügung stellt, die von der Kommission nicht abgedeckt werden. Sollten die Vertragsklauseln der Kommission dies nicht bereits enthalten, wäre etwa an eine Vorgabe verschiedener Zwecke nach Art. 4 Abs. 14 DA zu denken. Wichtig wäre neben Mustervertragsklauseln auch die Bereitstellung von Musterinformationen zur Erfüllung der Pflichten gem. Art. 3 Abs. 2 und 3 DA.

3. Datentreuhänder und PIMS

Die Datenethikkommission der Bundesregierung hat in Ihrem Abschlussgutachten von 2019 auf die besondere Bedeutung von PIMS (Personal Information Management Systems), insbesondere von Datentreuhand-Modellen, hingewiesen und deren Verwendung empfohlen.[97] PIMS sind Systeme, die eine sichere Speicherung, Verwaltung sowie ein nutzerautonomes Weitergabe personenbezogener Daten ermöglichen.[98] Sinn und Zweck solcher Systeme ist es, natürlichen Personen die Kontrolle über ihre Daten zurückzugeben.[99]

Der deutsche Gesetzgeber hat diesen Gedanken in § 26 TDDDG aufgegriffen und einen Rechtsrahmen für die Anerkennung von Diensten zur Einwilligungsverwaltung geschaffen. Die technischen und rechtlichen Anforderungen eines anerkannten Dienstes zur Einwilligungsverwaltung werden durch die Bundesregierung im Wege einer Rechtsverordnung geregelt, § 26 Abs. 2 TDDDG. Anerkannte Dienste zur Einwilligungsverwaltung stärken das Vertrauen der Nutzer beim Umgang mit ihren Daten und schaffen Anreize für Unternehmen, indem ihnen ein rechtssicheres Verfahren zur Einholung von Einwilligungen bereitgestellt wird. Neben der Verwaltung von Einwilligungen nach § 25 TDDDG und Art. 6 Abs. 1 lit. a) DS-GVO können auch Betroffenenrechte nach der DS-GVO mithilfe der Dienste zur Einwilligungsverwaltung geltend gemacht werden. [100]

Des Weiteren haben PIMS Einzug in den Data Governance Act erhalten: Nach Art. 10 ff. DGA unterliegen Datenvermittlungsdienste und Datengenossenschaften einer Anmeldepflicht (Art. 11 DGA). Die Anbieter solcher Dienste sind an einen Verhaltenskodex gebunden (vgl. Art. 12 DGA). Der EU-Gesetzgeber sieht Datenvermittlungsdienste in einer Schlüsselrolle für die Datenwirtschaft, weil sie den Austausch erheblicher Datenmengen erleichtern können. (Erwgr Nr. 27 des DGA).

PIMS dienen in erster Linie dem Datenschutz der einzelnen Nutzer und verfolgen nicht primär datenwirtschaftliche Ziele. Vielmehr verstehen sich solche Systeme als Wahrzeichen digitaler Selbstbestimmung. Diese Zielrichtung muss einer gesteigerten Datennutzung zu wirtschaftlichen Zwecken aber nicht entgegenstehen: Da PIMS ihrer Konzeption nach darauf ausgerichtet sind, (personenbezogene) Daten an Dritte weiterzugeben und eine erhöhte Datenzirkulation zwangsläufige Folge dessen ist, können sie dazu beitragen, die Datenwirtschaft voranzutreiben. Positiv hervorzuheben ist, dass bei PIMS der Schutz persönlicher Daten im Vordergrund steht und sie so zu einer menschenzentrierten Förderung der Datenwirtschaft beitragen können. PIMS versprechen, das Interesse der Wirtschaft an der Erlangung von Daten und das

---

[97] Gutachten der Datenethikkommission v. 23.10.2019, S. 133.

[98] https://www.edps.europa.eu/data-protection/our-work/subjects/systeme-de-gestion-des-informations-personnelles_de (Stand: 24.06.2024).

[99] *Krämer* Digitale Selbstbestimmung durch Personal Information Management Systems? – Chancen, Hemmnisse und politische Handlungsempfehlungen, Vortrag 4 der Reihe „Zu treuen Händen", Janaur 2022, S. 4; abrufbar unter https://www.verbraucherforschung.nrw/sites/default/files/2022-02/zth-4-kraemer-digitale-selbstbestimmung-durch-personal-information-management-systems.pdf (zuletzt abegerufen am 24.06.2024).

[100] Referentenentwurf der Bundesregierung, Verordnung über Dienste zur Einwilligungsverwaltung nach dem Telekommunikation-Telemedien-Datenschutz-Gesetz, Bearbeitungsstand: 07.03.2024; S. 2.

Bedürfnis nach „digitalen“ Grundrechten (vor allem das Recht auf informationelle Selbstbestimmung) in Einklang zu bringen.[101]

Trotz aller politischen Unterstützung solcher Systeme konnten sie sich bislang nicht im großen Stil auf dem Markt etablieren.[102] Datengenossenschaften, wie sie in Art. 10 DGA genannt werden, stehen gerade noch am Anfang ihrer Entwicklung.[103] Die Europäische Kommission bescheinigt PIMS im Allgemeinen ein „erhebliches Potenzial“ [104] und betont ihren Willen zur Unterstützung dieser Systeme. Eine solche Unterstützung bedarf konkreter wirtschaftlicher und rechtlicher Anreize,[105] z.B. durch die Etablierung gemeinsamer Standards für das Einwilligungsmanagement.[106]

Insgesamt bergen PIMS aufgrund ihrer „Doppelausrichtung“ ein enormes Potenzial für Datenschutz und Datenwirtschaft und können sich auf dem Weg zu mehr Datenwirtschaft als wichtiger Faktor herausstellen. Die Zusammenführung von Daten derselben Person von unterschiedlichen Plattformen kann ungeahnte wirtschaftliche Kräfte entfalten. Durch die Bereitstellung von Nutzerdaten können digitale Ökosysteme geschaffen und (europäische) Datenräume gefüllt werden.[107] Hinsichtlich der Umsetzung sind mehrere Szenarien denkbar: So können Betroffene beispielsweise Daten freiwillig freigeben („Datenaltruismus“) oder die Verwendung von Daten kann im Interesse und mit Zustimmung des Betroffenen zu wirtschaftlichen Zwecken erfolgen.[108]

Solange und soweit PIMS eingesetzt werden, dürfen sie aber nicht ihre ursprüngliche Funktion als „Interessenwalter“[109] des Betroffenen verlieren: Bei Übertragung der eigenen Datenhoheit an dritte Anbieter besteht die Gefahr, dass die ursprünglich angestrebte Selbstbestimmung immer mehr in Richtung Fremdbestimmung „kippt“. Bei personenbezogenen Daten dürfen Grundrechte nicht außer Acht gelassen werden (man denke in diesem Zusammenhang beispielsweise an von Algorithmen ausgehende Diskriminierungen), sodass im Zuge einer Abwägung datenwirtschaftliche Aspekte unter Umständen zurückstehen müssen.

4. Wirtschaft binden und Standards in Europa bündeln

Wettbewerber Europäischer Unternehmen insbesondere aus USA und China beherrschen bislang den europäischen Markt. Sie setzen faktisch die Standards und stellen die Plattformen. Wenn Europas Digitalwirtschaft im internationalen Wettbewerb bestehen soll, dann müssen mehrere Faktoren zusammenwirken. Es kommt bei all dem entscheidend darauf an, dass der Zugang zu Onlineangeboten nach transparenten, neutralen, fairen und offenen Standards ermöglicht wird. Aktuell setzen Apple und Google etwa über ihre Webbrowser und App Stores die Regeln, weil sie den Zugang zum Netz für Milliarden Menschen steuern. Unter dem Deckmantel des Datenschutzes wird das damit legitimiert, dass sich der Wille des Nutzers am besten über den Anbieter des Betriebssystems verwalten ließe. Trifft der souveräne Nutzer jedoch auf monopolartige Anbieterstrukturen, so läuft sein Recht, per Einwilligung die

[101] Vgl. dazu *Schwartmann* F.A.Z. v. 12.9.2022, 18; *Schwartmann/Benedikt* RDV 2021, 248 ff.
[102] Für eine beispielhafte Aufzählung von Initiativen und Start-Ups vgl. *Beyer-Katzenberger* in Wolff/Brink/v. Ungern-Sternberg (Hrsg.), BeckOK DatenschutzR, 48. Edition, Stand: 01.05.2024, DGA, Art. 10 Rn. 4.
[103] *Specht-Riemenschneider* in Specht/Hennemann (Hrsg.), Data Governance Act: DGA, DGA, Art. 10 Rn. 15.
[104] Mitteilung der Kommission v. 19.2.2020, COM(2020) 66 final S. 12.
[105] *Specht-Riemenschneider* in Specht/Hennemann (Hrsg.), Data Governance Act: DGA, DGA, Art. 10 Rn. 15.
[106] *Krämer*, Digitale Selbstbestimmung durch Personal Information Management Systems? – Chancen, Hemmnisse und politische Handlungsempfehlungen, Vortrag 4 der Reihe „Zu treuen Händen“, Januar 2022, S. 14 f.
[107] *Schwartmann/Benedikt* RDV 2022, 59 ff.
[108] Gutachten der Datenethikkommission v. 23.10.2019, S. 135.
[109] Gutachten der Datenethikkommission v. 23.10.2019, S. 135.

Nutzung seiner Daten zu steuern, faktisch leer. Die Souveränität des Nutzers geht dann im Willen der Anbieter der technischen Infrastruktur auf – und wird aufgehoben. Hier braucht es mehr Wettbewerb, notfalls auch durch staatliche Wettbewerbsregulierung und Zerschlagung von verbraucherfeindlichen Monopolen.

Eine besondere Rolle spielt die **Rechtsprechung** des EuGH. Das Gericht hat einen entscheidenden Anteil am Geschick der DS-GVO. Der EuGH begreift die DS-GVO häufig als Verbraucherschutzrecht und verliert dabei deren Ziel, auch das wirtschaftliche Potenzial personenbezogener Daten zu heben, weitgehend aus den Augen. Auf der einen Seite nimmt er weltweit agierende Unternehmen zu Recht in die Pflicht, ihre Angebote dem lokalen Recht anzupassen. Nach dem Marktortprinzip gilt europäisches Recht nun einmal für alle, die hierzulande anbieten. Auf der anderen Seite geht der EuGH zu weit, wenn er etwa die nur abstrakte und hypothetische Möglichkeit des Zugriffs nicht-europäischer Sicherheitsbehörden ohne konkretes und reales Risiko für persönliche Daten von Europäern als Killerkriterium für globalen Datenaustausch begreift.

Ein konkretes Problem entsteht aus der sog. „**Schrems-Rechtsprechung“** zum internationalen Datentransfer. Dessen Kern liegt im Umgang der Praxis mit den bisherigen Entscheidungen des EuGH, in denen dieser die in der DS-GVO angelegte risikoabhängige Betrachtung der Datenverarbeitung beim transatlantischen Datenverkehr faktisch negiert.[110] Ein Inhalt, der den Machtbereich US-amerikanischer Behörden erreicht, darf spitz formuliert nicht übermittelt werden, solange den US-Behörden der Zugriff in den Herrschaftsbereich nicht unmöglich gemacht wird. Diese Anforderung greift unabhängig davon, wie belanglos der Inhalt auch sein mag. Im Ergebnis wird, ohne dass Fälle eines konkreten Zugriffs bekannt geworden sind, der gesamte transatlantische Datenverkehr pauschal für unionsrechtswidrig erklärt. Daran ändern auch Vereinbarungen über einen angemessenen Datenschutz zwischen den USA und der EU nichts, denn diese werden durch den EuGH bislang zuverlässig für europarechtswidrig erklärt. Eine solche Auslegung der DS-GVO macht beispielsweise faktisch jeden Einsatz nichteuropäischer Bürosoftware oder Videokonferenzdienste unzulässig. Das ist für Unternehmen, Behörden und Gerichte nur schwer umsetzbar. Wahlweise führt dies in den digitalen Lockdown oder in das rechtliche Chaos. In der Praxis kann der Ansatz des EuGH also gar nicht sinnvoll greifen.[111] Nach der „Schrems-Rechtsprechung“ des EUGH ist selbst die technische Einbindung eines Schrifttyps, die per Datenverarbeitung aus den USA erfolgt, eine Datenschutzverletzung mit der Folge des Schadensersatzes für Unternehmen und Behörden. Das Verbot der Nutzung außereuropäischer Anbieter, etwa von Konferenzsystemen, schneidet Europa von der „Digitalen Daseinsvorsorge“ und Massenkommunikation zu einem Zeitpunkt ab, zu dem nutzbare europäische Alternativen erst noch im Aufbau sind. Die Verwendung von gebräuchlicher Videokonferenzsoftware etwa kann mit existenzbedrohenden Bußgeldern belegt werden, auch wenn es in der Konferenz nur um Wirtschaftszahlen oder um das Wetter geht. Die Klageindustrie steht mit Unterstützung von Legal Tech in den Startlöchern, um Europas Wirtschaft mit Massenklagen zu überziehen.

Es bestehen Zweifel, ob das Data Privacy Framework einer gerichtlichen Kontrolle durch den EuGH im Rahmen eines Vorabentschiedungsverfahren gem. Art. 267 AEUV standhalten wird. Zwar verpflichteten sich die USA anlässlich der EuGH-Entscheidung im Verfahren Schrems II, die behördlichen Überwachungstätigkeiten auf ein angemessenes, verhältnismäßiges Maß zu beschränken und die Rechtsschutzmöglichkeiten der EU-Bürger zu verbessern.[112] Diese

[110] *Kühling/Paal/Schwartmann* F.A.Z. v. 20.10.2022, 6.
[111] *Kühling/Paal/Schwartmann* F.A.Z. v. 20.10.2022, 6.
[112] *Schwartmann/Burkhardt* ZD 2021, 235 ff.

Reformen sind ein Schritt in die richtige Richtung, könnten aber angesichts der strengen Maßstäbe der beschriebenen Rechtsprechung des EuGH noch kein angemessenes Schutzniveau im Sinne der DS-GVO bieten. Das zeigt sich insbesondere am zweistufigen Rechtsbehelfssystem, welches nach europäischem Verständnis weder die Einlegung eines wirksamen Rechtsbehelfs noch ein faires, öffentliches Verfahren vor einem unabhängigen Gericht gewährleistet.[113] Eine betroffene Person kann nicht selbst an der Verhandlung des Data Protection Review Court (DPRC) teilnehmen. Sie wird stets vertreten durch einen ausgewählten „Datenschutzpflichtverteidiger", dem Special Advocat.[114] Auch steht die Entscheidung des DPRC schon fest, bevor der Fall überhaupt verhandelt wurde. Der Angemessenheitsbeschluss bestimmt, dass der Beschwerdeführer stets die Information erhält, dass entweder kein Rechtsverstoß festgestellt wurde oder dieser – sollte es einen gegeben haben – abgestellt wurde.[115] Die Entscheidung des „Datenschutzgerichts" wird auch nicht begründet. Fraglich ist zudem, ob es sich überhaupt um ein Gericht handelt, das über den Rechtsbehelf entscheidet. Vielmehr handelt es sich um ein gerichtsähnliches Verwaltungsgremium.[116]

5. Initiativen zur Förderung der Datenwirtschaft in Europa und in Deutschland

Die Bedeutung und das Potenzial von Daten für die Wirtschaft darf nicht unterschätzt werden: Daten werden als entscheidender Faktor darüber entscheiden, wie sich das Wirtschaftsleben in der digitalen Ökonomie abspielt. Ihre Verwendung kann beispielsweise dabei helfen, Strom- und Wärmeverbrauch zu optimieren, die Gesundheitsversorgung zu verbessern oder die Kosten für öffentliche Dienstleistungen zu senken.[117] Außerdem kann durch die Verwendung von Daten die Produktivität von Unternehmen erhöht und können Produkte verbessert und individualisiert werden.[118] Die Bundesregierung und die Europäische Kommission sehen in Daten nicht mehr nur eine Gefährdung für Grundrechte und individuelle Interessen, sondern begreifen sie als entscheidenden Faktor in einer sich weiterentwickelnden digitalen Wirtschaft. Die Entscheidung des europäischen Gesetzgebers, Daten nicht nur als Wirtschaftsgut anzusehen, sondern die Datenwirtschaft bewusst zu fördern, wird von zahlreichen Dateninitiativen in die Tat umzusetzen versucht (**Frage 9**).

a) Neue Märkte

In der Digitalwirtschaft entstehen ganz neue Märkte, auf denen Datensätze angeboten und nachgefragt werden, z.B. im Verkehrs-, Gesundheits- oder Energiesektor. Gleichzeitig bleiben aktuell etwas 80% der Industriedaten in Deutschland ungenutzt.[119]

Bislang wurde der Markt für Cloud-Systeme von einigen wenigen (US-amerikanischen) Großkonzernen dominiert, darunter Microsoft Azure, Amazon Web Services, Google Cloud, International Business Machines Corporation (IBM) und Oracle.[120] Folge einer solchen

[113] Vgl. Art. 47 GRCh.

[114] Durchführungsbeschluss (EU) 2023/1795 der Kommission vom 10.7.2023 gemäß der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates über die Angemessenheit des Schutzniveaus für personenbezogene Daten nach dem Datenschutzrahmen EU-USA, ErwG 183, 188.

[115] Durchführungsbeschluss (EU) 2023/1795 der Kommission vom 10.7.2023 gemäß der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates über die Angemessenheit des Schutzniveaus für personenbezogene Daten nach dem Datenschutzrahmen EU-USA, ErwG 183, 192.

[116] *Glocker* ZD 2023, 189 (192).

[117] https://digital-strategy.ec.europa.eu/de/policies/strategy-data (Stand: 20.6.2024).

[118] *König*, in: Borges/Keil, Rechtshandbuch Big Data, 1. Aufl. 2024, § 12 Rn. 5.

[119] Fortschritt durch Datennutzung – Strategie der Bundesregierung für mehr und bessere Daten für neue, effektive und zukunftsweisende Datennutzung, August 2023, S. 5, abrufbar unter https://bmdv.bund.de/SharedDocs/DE/Anlage/K/nationale-datenstrategie.pdf?__blob=publicationFile (Stand: 20.6.2024).

[120] https://www.itpro.com/cloud/public-cloud/357185/what-is-gaia-x-a-guide-to-the-eus-unified-cloud-ecosystem (Stand: 20.6.2024).

Machtkonzentration sind in der Regel Wettbewerbsverzerrungen (z.B. in Form von Gatekeeping), die letztlich auch den Verbrauchern schaden. Wie die Anbieter selbst, sitzen auch die Server, auf denen die Daten gespeichert werden, nicht selten im Ausland: Unter den 15 von Google betriebenen Rechenzentren befinden sich allein acht in den USA und nur vier in Europa.[121] Damit ist nicht nur die Hardware oftmals weit entfernt von der EU. Die geographische Verteilung kann auch juristisch komplexe Fragen im Hinblick auf das anzuwendende Daten(schutz)recht aufwerfen.

So wie eine Handvoll Unternehmen digitale Märkte weltweit beherrschen, befindet sich ein großer Teil aller weltweit vorhandener Daten in der Hand weniger großer Tech-Konzerne.[122] Damit entspricht der europäische Anteil an der weltweiten Datenwirtschaft nicht dem Gewicht, das ihm angesichts der Anzahl in Europa generierter und nutzbarer Daten eigentlich zukommen sollte. Insbesondere in Deutschland und Frankreich besteht die Befürchtung, dass europäische Staaten und Unternehmen Einbußen hinsichtlich der datenbezogenen Souveränität hinnehmen müssen. Deshalb entwickelten sich innerhalb der EU Bestrebungen, die es sich zum Ziel gesetzt haben, die eigene Unabhängigkeit in Digitalfragen nicht zu verlieren.[123]

b) Gaia-X

Ein Beispiel für die zu begrüßende länderübergreifende Zusammenarbeit auf dem Gebiet der Datenpolitik ist Gaia-X. Gaia-X ist eine internationale Initiative, deren Ziel der Aufbau einer europäischen Dateninfrastruktur in Form von Cloud- und Edge-Technologien ist. So soll ein digitales Infrastruktursystem erschaffen werden, das es mit ausländischen Cloud-Computing-Anbietern, die den Markt bislang beherrschen, aufnehmen kann. Gaia-X ist dabei weder selbst Marktteilnehmer, noch betreibt es direkt oder exklusiv einen für den Ordnungsrahmen erforderlichen Dienst.[124] In der praktischen Umsetzung sollen bereits bestehende europäische Cloudsysteme verbunden und dadurch gestärkt werden. Europäischen Unternehmen, die Clouddienste anbieten, soll es ermöglicht werden, mit anderen Anbietern weltweit zu konkurrieren.

Derzeit wird der Austausch von Daten zwischen Organisationen durch intransparente systemspezifische und nicht interoperable Technologien eingeschränkt, die nicht das erforderliche Maß an Vertrauen gewährleisten. Gaia-X ist darauf ausgerichtet, Datenräume („data spaces“) in Form von vertrauenswürdigen Plattformen zu schaffen. So sollen Daten sicher und frei zwischen mehreren Akteuren geteilt und ausgetauscht werden können.[125]

Bestehende Datensilos, in denen „Big Data“ schlummert und die sich im Besitz einiger weniger Großkonzerne befinden, sollen geöffnet werden, damit Big Data innovativ und zum Vorteil der Allgemeinheit eingesetzt werden kann. Daneben sollen neue Datenräume in allen Wirtschafts- und Wissenschaftsbereichen geschaffen werden.

Die europäischen Werte, auf die sich Gaia-X stützt, sind Transparenz, Offenheit und Interoperabilität.[126] Die Initiative will sicherstellen, dass europäische Standards im Hinblick auf den

---

[121] https://www.googlewatchblog.de/2020/04/globale-infrastruktur-hier-googles-rechenzentren/ (Stand: 20.6.2024).

[122] Mitteilung der Kommission v. 19.2.2020, COM(2020) 66 final, S. 3.

[123] https://www.itpro.com/cloud/public-cloud/357185/what-is-gaia-x-a-guide-to-the-eus-unified-cloud-ecosystem (Stand: 20.6.2024).

[124] https://gaia-x.eu/ (Stand: 20.6.2024).

[125] https://gaia-x.eu/ (Stand: 20.6.2024).

[126] https://www.bmbf.de/bmbf/de/forschung/digitale-wirtschaft-und-gesellschaft/gaia-x/gaia-x.html (Stand: 19.6.2024).

Umgang mit Date geachtet werden. Nach Ansicht der Kommission soll bei neuen Möglichkeiten der Datennutzung stets der Mensch im Mittelpunkt stehen.[127]

An der Initiative Gaia-X können sich alle Unternehmen sowie alle Wissenschafts- und Forschungseinrichtungen, die Cloud-Dienste anbieten, beteiligen, soweit sie die Vorgaben der Initiative einhalten. Dazu gehören nicht nur die Befolgung europäischer Gesetze, sondern auch die Achtung europäischer Werte wie Offenheit und Transparenz, Kontrollierbarkeit und Interoperabilität.[128]

c) Dateninstitut des BMI und des BMWK

Auf nationaler Ebene ist derzeit das sog. Dateninstitut im Aufbau begriffen, dessen Gründung im Koalitionsvertrag festgeschrieben wurde.[129] Das Institut unterliegt der Leitung des Bundesinnenministerium und des Bundesministeriums für Wirtschaft und Klima. Das Dateninstitut hat es sich zum Ziel gesetzt, „Probleme im Datenökosystem sektoren- und ebenenübergreifend anzugehen“ und Nachhaltigkeit die Verfügbarkeit und Nutzung von Daten zu verbessern.[130] Bei der Umsetzung setzt das Bundesinnenministerium auf die Erkennung struktureller Hürden im Datenökosystem und die Entwicklung darauf bezogener Lösungsansätze.

Es sollen zunächst „Use Cases“ (d.h. geeignete Projektideen aus Wirtschaft, Wissenschaft, Verwaltung und Zivilgesellschaft) gefunden werden, bei denen Datenzugang, -verfügbarkeit und -standardisierung noch nicht im angestrebten Maße erreicht ist; aus diesen „Use Cases“ heraus sollen dann Probleme ausfindig gemacht und benannt werden, die einer stärkeren Datennutzbarkeit entgegenstehen.[131] Am Ende sollen ein sektorübergreifender Datenaustausch und -auswertung sowie die Entwicklung von Governance-Modellen – immer mit Blick auf gemeinwohlorientierte und nachhaltige Lösungen, stehen; darüber versteht sich das Dateninstitut als Vertreter der Open-Data-Bewegung.[132] Entscheidend wird vor diesem Hintergrund die Bereitstellung von Leitlinien zur Anonymisierung sein, um der Wirtschaft Sicherheit bei der Lösung des Personenbezugs zu bieten.[133]

d) Beurteilung der beispielhaft vorgestellten Initiativen

Die beispielhaft vorgestellten Dateninitiativen (Gaia-X, Dateninstitut) streben den Ausbau einer innovativen, aber zugleich sicheren und wertegeleiteten Datenwirtschaft in Europa an.

Dieses Ziels soll nach der Gaia-X-Initiative auf mehreren Ebenen umgesetzt werden: durch eine aktive Förderung des Aufbaus von Infrastruktur, den Erlass innovationsfördernder Rechtsakte sowie die Bindung der Zurverfügungstellung von Infrastruktur an die Achtung europäischer Werte.

---

[127] Mitteilung der Kommission v. 19.2.2020, COM(2020) 66 final, S. 5.
[128] https://gaia-x.eu/ (Stand: 20.6.2024).
[129] Koalitionsvertrag 2021 – 2025, S. 14.
[130] Kick-Off zur Gründung des Dateninstituts, Pressmitteilung des Bundesministeriums des Inneren und für Heimat v. 10.4.2024, abrufbar unter https://www.bmi.bund.de/SharedDocs/pressemitteilungen/DE/2024/04/kick-off-dateninstitut.html (Stand: 20.6.2024).
[131] Der Weg zu einem Dateninstitut in Deutschland, Zwischenbericht – Erste Empfehlungen der Gründungskommission v. 9.12.2023, S. 3, abrufbar unter https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/it-digitalpolitik/bericht-dateninstitut.pdf?__blob=publicationFile&v=5) (Stand: 20.6.2024).
[132] Der Weg zu einem Dateninstitut in Deutschland, Zwischenbericht – Erste Empfehlungen der Gründungskommission v. 9.12.2023, S. 5 f., abrufbar unter https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/it-digitalpolitik/bericht-dateninstitut.pdf?__blob=publicationFile&v=5) (Stand: 20.6.2024).
[133] S. hierzu bereits 1. c).

Die Dateninitiative des BMI und BMWK wählt einen problembasierten Ansatz, der durch die Analyse von „Use Cases“ Verbesserungspotenziale identifiziert und daran orientiert Lösungsansätze entwickeln möchte.

Die Stärkung von europäischen Unternehmen auf verhältnismäßig neuen Märkten wie dem Markt für Cloud-Dienste ist ein sinnvolles Ziel. Über die Umsetzung lässt sich trefflich streiten: Die Initiative Gaia-X hat das Potenzial, die Kräfte und Ressourcen von auf dem europäischen Markt tätigen Unternehmen (Cloud-Dienste-Anbieter) zu bündeln und so Effizienzreserven zu mobilisieren. Mittelbar könnte es jedoch – im Fall von Gaia-X durch die Bereitstellung von Fördermitteln[134] – zu einem Eingreifen des Staats in den Markt kommen, indem Unternehmen, die sich zu europäischen Werten bekennen, gewisse Vorteile (iSe Zurverfügungstellung von Infrastruktur) erlangen. Der Schritt zu tieferen Eingriffen in Digitalmärke ist dann nicht mehr weit. Dabei drängt sich die Frage auf, ob ein solches Vorgehen zielführend und notwendig ist. In einem System freien Wettbewerbs entscheiden die Kräfte des Wettbewerbs (Qualität und Quantität des Angebots, Anforderungen an die Nachfrage, Entscheidung der Nachfrager etc.) darüber, welche Akteure und Produkte sich durchsetzen. Es wird sich zeigen müssen, ob staatliche Initiativen wie Gaia-X die Marktstellung „neuer“ europäischer Anbieter so weit stärken können, dass die Vorteile dieses Vorgehens letztlich den Verbrauchern zugutekommen. Weiterhin ist fraglich, ob die Unternehmen, die bereits jetzt den Markt beherrschen, ein Interesse daran zeigen, sich an Gaia-X zu beteiligen. Deren Compliance ist nicht selbstverständlich: Ein zwingendes Bekenntnis zu den ungesetzlichen Vorgaben der Initiative (Unterwerfung unter die „europäischen Werten“) könnte sich als unattraktiv für die Unternehmen, die an andere Wettbewerbsbedingungen gewöhnt sind, herausstellen, und noch ist ihre Marktmacht ungebrochen.

Der Staat sollte sich, soweit etwas anderes nicht zwingend geboten ist, grundsätzlich darauf beschränken, einen Ordnungsrahmen in Form gesetzlicher Bestimmungen vorzugeben. Solche gesetzlichen Bestimmungen sollten vor dem Hintergrund des gesamteuropäischen Binnenmarktes[135] in ganz Europa gleich oder zumindest kohärent sein. Richtig ist, dass nach der derzeitigen Marktsituation die Marktmacht in den Händen weniger (US-amerikanischer) Großunternehmen gebündelt ist. Festzustellen ist aber auch, dass sich im System freien Wettbewerbs die Endverbraucher letztlich für die Produkte entscheiden, die sie für am attraktivsten halten. Insoweit drängt sich der Schluss, dass ein Bekenntnis zu europäischen Werten unumgänglich Vorteile für die Verbraucher mit sich bringt, nicht auf. An gesetzliche Vorgaben müssen sich ohnehin alle Unternehmen halten, und bei Verstößen werden Sanktionen angedroht.[136]

Am Ende bleibt die Frage, ob und warum es notwendig ist, Unternehmen durch die Gewährung bestimmter Vorteile zugleich zum Einhalten weitergehender Vorgaben verpflichten zu wollen. Maßnahmen in diesem Sinne können, wie gezeigt, unter Umständen in den freien Wettbewerb eingreifen. Manche Mitgliedstaaten der Europäische Union scheinen die Frage, ob es ihnen ein solches Vorgehen auf Digitalmärkten wert ist, für sich bereits beantwortet zu haben.

Im Augenblick sollte zunächst auf anderen Wegen dafür gesorgt werden, das Bewusstsein der Endverbraucher für datenrechtliche Fragen zu schärfen, damit sich diese am Ende tatsächlich und aus freien Stücken für ein Produkt entscheiden können, das für sie vorteilhaft ist.

[134] Bundesministerium für Wirtschaft und Energie, Förderbekanntmachung, “Innovative und praxisnahe Anwendungen und Datenräume im digitalen Ökosystem GAIA-X“ vom 22.2.2021, BAnz AT 15.03.2021 B1.
[135] Vgl. dazu unten II.
[136] Vgl. z.B. Art. 40 Data Act.

Konkret könnte eine Aufklärung über Vorteile erfolgen, die sich aus der Entscheidung zugunsten europäischer Dienste ergeben, z.B. der einfachere und damit bessere Support durch inländische Unternehmen: Inländische Anbieter sind mit der Rechtslage vertraut, können Technik leichter überprüfen und auch die Sicherheit ist insgesamt höher, wenn Infrastruktur wie Server im Inland liegen.

6. Förderung der Akzeptanz für eine wachsende Datenwirtschaft

Das Wachstum der Datenwirtschaft hängt auch von der Akzeptanz in der Bevölkerung ab. Entsprechend sollten Anwendungsbereiche identifiziert und gefördert werden, in denen eine verbesserte Datenwirtschaft der Bevölkerung merklich zugute kommt.

a) Sektor Klima: Daten als Hilfsmittel im Umgang mit der Klimakrise

Kaum ein Bereich konfrontiert Politik und Gesellschaft mit derart weitreichenden und existenziellen Fragestellungen wie der Klimasektor. Bei all den Chancen, die die umfassende Sammlung, Verwertung und der Austausch von Daten mit sich bringen, ergeben sich auch Möglichkeiten, der Klimakrise zu begegnen (**Frage 8**).

Nach Meinung der Kommission werden Daten zur Umsetzung des Green Deal der EU beitragen.[137] Es gibt eine Reihe von Sektoren, in denen Daten gesammelt werden können, die nach Auswertung unmittelbar oder mittelbar zu klimabezogenen Zwecken verwendet werden können.

Als Beispiel sei zunächst der Verkehrssektor genannt: Die Auswertung von Verkehrsdaten kann dazu beitragen, attraktive Angebote im Individualverkehr (z.B. Apps) zu schaffen, die zu umweltfreundlicheren Möglichkeiten der Fortbewegung motivieren können. Darüber hinaus können Daten herangezogen werden, um die Energieeffizienz zu steigern, z.B. in Lichtmanagement- oder Smart-Heating-Systemen, sowohl im privaten als auch im öffentlichen Raum. In der Landwirtschaft kann Precision Farming dazu beitragen, Ressourcen sparsam und effizient einzusetzen.

Bezogen sich die bislang vorgestellten Maßnahmen auf eine Verringerung von Emissionen bzw. auf ressourcenschonendes Wirtschaften und somit auf die Erreichung von Klimazielen, können Daten auch darüber hinaus eingesetzt werden, um den Folgen des Klimawandels zu begegnen. Ein besonderes Augenmerk liegt hier auf der Prävention. Europa- und weltweit gesammelte Wetterdaten können dazu beitragen, extreme Wetterphänomene wie Hitze, Dürren und Waldbrände, Regenfälle und Überschwemmungen vorauszusagen. Auf diese Daten können z.B. Kommunen zugreifen, um die Bevölkerung zu warnen und andere entsprechende Sicherheitsvorkehrungen zu treffen.

Klima- und Wetterdaten sind wie Daten in kaum einem anderen Sektor dazu geeignet, der Allgemeinheit unmittelbar existenziell wichtige Informationen zu verschaffen. Ein Zugriff auf diese Daten sollte im öffentlichen Interesse besonders leicht möglich sein. Eine Möglichkeit, den Zugang zu Wetterdaten zu erleichtern, könnte im Wege der Rechtssetzung erfolgen. Diesen Gedanken verfolgt der Data Act bereits.[138] Zur vollen Ausschöpfung des Potenzials klimabezogener Daten könnte er in weiteren Rechtsakten aufgegriffen und unter Umständen vertieft werden.

b) Zugang zu den Daten sehr großer Unternehmen bei Gemeinwohlorientierung

Die Nutzung von Daten kann und wird gerade bei der Bewältigung von Krisen eine wichtige Rolle einnehmen, z.B. bei Naturkatastrophen, die sich durch die zielgerichtete Auswertung

[137] Mitteilung der Kommission v. 19.2.2020, COM(2020) 66 final, S. 1.
[138] Vgl. ErwG 64 DA.

von Wetter- und Klimadaten besser voraussagen lassen, oder Gesundheitskrisen, die sich durch die Datenbezug ebenfalls besser bewältigen lassen. Art. 14 Data Act verpflichtet Dateninhaber dazu, ihre Daten bei außergewöhnlicher Notwendigkeit an öffentliche Stellen zur Verfügung zu stellen. Der Data Act selbst nennt als Beispielsfälle solcher außergewöhnlicher Notwendigkeit Naturkatastrophen, Gesundheitskrisen oder Cybersicherheitsvorfälle (Erwägungsgrund Nr. 64 des Data Act). In Krisenfällen ist die Weitergabe wichtiger Daten an öffentliche Stellen also gesichert.

Über eine Verpflichtung zu Bereitstellung in außergewöhnlichen Notlagen sollten die Regelungen im nationalen und EU-Recht indes nicht hinausgehen. Wie physische Einrichtungen, deren Betrieb dem Gemeinwohl dient (z.B. Krankenhäuser, Telekommunikationsinfrastruktur), sind auch Unternehmen, die sich gemeinwohlorientierten Themen wie beispielsweise dem Klimaschutz widmen und die über dementsprechende Datensätze verfügen, im Normalfall vor staatlichem Zugriff zu schützen. Allein die Wahl der Geschäftsausrichtung darf einem Unternehmen nicht zum Nachteil gereichen. Ein Zwang zur allgemeinen Datenbereitstellung sollte nicht erfolgen (**Frage 5**).

c) Zugänglichmachung und Nutzung staatlicher Daten an die Bevölkerung

Von der Freisetzung von Datenbeständen sollten nicht nur Unternehmen profitieren. Die Zurverfügungstellen und der Austausch von Daten haben das Potenzial, mehr Sicherheit für die Bevölkerung zu schaffen und den Alltag zu erleichtern. Insofern sollte es ein Anliegen der Politik sein, Datenbestände an die Bevölkerung „zurückzugeben“ (**Frage 17**).

Denkbar sind zum einen digitale Angebote, die Bürgerinnen und Bürger unmittelbar selbst nutzen können. Hier bietet sich vor allem der Verkehrsbereich (Aufzeigen von ÖPNV, Möglichkeiten der Radnutzung etc.) an.[139]

Beispielhaft kann das Stadtnavi Herrenberg[140] genannt werden. Dabei handelt es sich um einen lokalen Online-Kartendienst, der zum einen individuelle Routen berechnet, in dem aber auch Parkplätze (inkl. der Anzahl verfügbarer Stellplätze) Bahn- und Bushaltestellen, Fahrradabstellplätze, Ladestationen für E-Autos etc. verzeichnet sind. Ein Fokus wird dabei auf klimaschonende Fortbewegung gelegt. Darüber hinaus gibt es auch Angebote, die speziell auf einzelne Verkehrsmittel zugeschnitten sind: Die Kampagne Stadtradeln mit eigener App stellt einen Navigationsdienst für Radfahrerinnen und Radfahrer bereit. Die bei Nutzung der App anfallenden Wegedaten werden der entsprechenden Kommune zur Verfügung gestellt, die nach Auswertung die Radinfrastruktur verbessern kann. Werden solche Dienste nutzerfreundlich konzipiert und einfach zur Verfügung gestellt (vor allem als App zur Nutzung auf dem Smartphone), können sie echte Alternativen zu großen Online-Kartendiensten darstellen. Aufgrund der geographischen Nähe und der potenziell größeren Datenmenge, auf die zugegriffen werden kann, können regionale Angebote sogar besser sein als global angebotene Dienste. Über den Erfolg solcher Angebote wird wohl maßgeblich deren Vermarktung entscheiden.

Nicht nur im Verkehrssektor können sich aus der breiten Nutzbarmachung von Daten Vorteile für die Verbraucher entstehen: Der Bayernatlas[141] ist ein Online-Atlas, der vom Land Bayern zur Verfügung gestellt wird und der kostenlos genutzt werden kann. Er verzeichnet nicht nur öffentliche Einrichtungen wie Schulen („Schulatlas“, der u.a. Schulstandorte, -bezirke und

[139] Eine Reihe von Beispielen finden sich unter https://www.aufruhr-magazin.de/digitalisierte-gesellschaft/so-will-stefaan-verhulst-von-the-data-tank-soziale-probleme-loesen/ (Stand: 25.6.2024).
[140] Abrufbar unter https://herrenberg.stadtnavi.de (Stand: 21.6.2024).
[141] Abrufbar unter https://geoportal.bayern.de/bayernatlas/?topic=ba&lang=de&bgLayer=atkis&catalogNodes=11 (Stand: 21.6.2024).

deren jeweilige Ausstattung anzeigt), öffentliche Hotspots oder Freizeitangebote. Darüber hinaus sind Naturgefahren wie Hochwassergefahrenflächen erfasst. Die so nutzbar gemachten Daten können von Gefährdeten verwendet werden, um sich zu informieren und ggf. Schutzmaßnahmen zu ergreifen.

Die genannten Dienste stehen nur beispielhaft dafür, wie staatliche Stellen ihre Datensätze an die Gesellschaft „zurückgeben" könnten. Schon jetzt haben Kommunen und Unternehmen die Möglichkeit, Datensätze zu Wetter und Klima, Verkehr und Baustellen, ÖPNV, Wasserstraßen und Gewässer in der sog. Mobilithek[142] bereitstellen, die vom Bundesministerium für Verkehr und Digitales betrieben wird. An Ideen zur Nutzbarmachung dieser Datensätze für die Bevölkerung als „Endverbraucher" mangelt es freilich nicht. Bei der Umsetzung solcher Vorhaben bestehen mehrere Optionen: Dienste können direkt von der öffentlichen Verwaltung betrieben werden, wie der Bayernatlas vom bayerischen Landesamt für Digitalisierung, Breitband und Vermessung oder die Kampagne Stadtradeln vom Klimabündnis (ein Netzwerk aus Städten, Gemeinden und Landkreisen). Alternativ besteht die Möglichkeit, die entsprechenden Daten privatwirtschaftlichen Akteuren, bestenfalls mit geographischem Bezug, zur Verfügung zu stellen, die damit eigenständig weitere Dienste entwickeln können. Die Zulässigkeit der Weitergabe orientiert sich unter anderem daran, ob es sich um personenbezogene oder um nicht-personenbezogene Daten handelt.

Eine andere Frage ist diejenige nach der Speicherung großer Datenmengen. Das Zusammenlegen einzelner Datenbanken zu einem großen Register birgt Sicherheitsrisiken: Die Gefahr von Anschlägen auf digitale Infrastruktur, z.B. durch Hackerangriffe, besteht bereits jetzt und wird in Zukunft wohl noch steigen. Bei Personenbezug gespeicherter Daten ist eine Betroffenheit des Rechts auf informationelle Selbstbestimmung (Art. 2 Abs. 1 iVm Art. 1 Abs. 1 GG) nicht ausgeschlossen. Dann kann unter Umständen eine staatliche Sicherungspflicht bestehen, um Grundrechtsverletzungen vorzubeugen.

d) Besonderes ethisches Postulat im Gesundheitsbereich

Politisch und ethisch ist insbesondere die datenschutzkonforme Auswertung von Gesundheitsdaten erwünscht. Die Europäische Union hat sich im Frühjahr 2024 auf eine Verordnung zur Schaffung eines europäischen Raums für Gesundheitsdaten geeinigt[143]. Sie soll Einzelpersonen die Kontrolle über ihre Gesundheitsdaten ermöglichen und zugleich die Nutzung von Gesundheitsdaten für bessere medizinische Versorgung und Forschung eröffnen. Die EU soll das Potenzial von Austausch, Nutzung und Weiterverwendung von Gesundheitsdaten ausschöpfen. Auch die Datenethikkommission der Bundesregierung macht sich hierfür unter 3.5.2 des Abschlussgutachtens stark.

Der Koalitionsvertrag der deutschen Ampelregierung hat das aufgegriffen. Die Fortentwicklung der Digitalisierung des Gesundheitswesens ist vereinbart. Zu Recht, denn spätestens die Pandemiebekämpfung hat uns vor Augen geführt, wie wichtig es ist, einen ausgewogenen Rahmen für die Verarbeitung von Gesundheitsdaten zu schaffen, der die Belange des Gesundheitsschutzes in ein angemessenes Verhältnis zum Schutz der Privatheit setzt.

Praktische Anwendungsfälle gibt es schon. Forscher entwickelten mit Hilfe menschlicher Mathematik und künstlicher Intelligenz unter Berücksichtigung der Bewegungsdaten und der Sterbefälle einen Algorithmus. Damit lässt sich anhand eines sechsminütigen Spaziergangs das Sterberisiko innerhalb der nächsten fünf Jahre vorhersagen. Basis des entwickelten

[142] Abrufbar unter https://mobilithek.info (Stand: 21.6.2024).

[143] Hierzu https://health.ec.europa.eu/ehealth-digital-health-and-care/european-health-data-space_de (Stand: 25.6.2024).

Algorithmus sind Daten von gut 100.000 Menschen aus der „UK Biobank“, die Gesundheitsdaten von Erwachsenen aus dem Vereinigten Königreich. Die Technik macht sich die Aussagekraft typischer Muster zunutze. Parameter ist bei Herz- oder Lungenerkrankungen etwa, ob eine Person beim Spaziergang langsamer wird, wenn sie außer Atem ist und dann in kurzen Abständen wieder schneller. Weil Smartphones bei kurzen Spaziergängen dieselben Bewegungsdaten erfassen wie die im Rahmen der Studie genutzten Bewegungssensoren, planen die Forscher nun eine Studie mit reinen Handydaten. Bei Menschen, die ihre Smartphones mit sich führen, kann man – so die Forscher - wöchentliche oder monatliche Vorhersagen errechnen. Erhöht sich das Gesundheitsrisiko wegen mangelnder Bewegung, kann man gegensteuern. Für Menschen, die so etwas wollen, kann das ein sinnvolles Angebot sein, denn schließlich wird das Gesundheitsrisiko errechnet und nicht nur gefühlt. Die Autoren der Studie über die Handydaten gehen davon aus, dass auch die Gesundheitsinfrastruktur durch groß angelegte Screenings ausgesprochen positiv beeinflusst wird. Man könne mit vielen Daten Gesundheitsrisiken aufzeigen, ohne in das Leben der Bevölkerung einzugreifen. Das dient dem Wohl der Menschheit. Man kann es nicht nur als Ziel der DS-GVO sondern auch als ethische Pflicht begreifen, die damit verbundene Datenverarbeitung im Dienst der Menschheit aktiv und verantwortlich vorzunehmen.

III. Datensicherheit

Ein zentrales Element einer sicheren und vertrauenswürdigen Infrastruktur ist die konsequente Implementierung von Privacy und Security by Design. Datenschutz und Datensicherheit dürfen also nicht erst im Nachhinein implementiert, sondern müssen von vorneherein durch die jeweiligen Betreiber bei der Konzeption der Infrastruktur berücksichtigt werden. Dazu gehört auch die Betrachtung von Supply-Chain-Risiken. Die Betreiber sollten also beim Aufbau auch ihre Zuliefererkette bei Hardware, Software und Dienstleistungen in die Sicherheitsbetrachtung einbeziehen. Wo möglich könnte beim Aufbau etwa auf IT-Produkte zurückgegriffen werden, die nach europäischen Schemata für Cybersicherheitszertifizierungen zertifiziert sind. Wo diese noch nicht existieren, kann unter Umständen auf andere Zertifizierungsverfahren zurückgegriffen.

Neben dem Risiko von Sicherheitslücken und Einfallstoren, sollte – das haben die Lieferengpässe während Corona gezeigt – auch die Ausfallrisiken bei der Lieferung von betriebsnotwendigen Komponenten mitbetrachtet werden. Denn wenn es zu Hardware-Ausfällen kommt und schlicht keine Ersatzteile (etwa im Bereich der Netzwerkkomponenten) lieferbar sind, bedroht das unmittelbar die Leistungsfähigkeit der Infrastruktur. Ein sinnvolles Element einer solchen Infrastruktur dürfte daher eine Multi-Vendor-Strategie sein, die hohe Abhängigkeiten von einzelnen Lieferanten, Produzenten oder Weltregionen vermeidet.

Um Innovation und Modernität nicht zu beschränken sollte jedoch unbedingt vermieden werden, zu enge Vorgaben zu machen. So darf die Frage der europäischen oder deutschen digitalen Souveränität darf nicht mit Forderungen nach ausschließlich in Europa oder Deutschland entwickelten Sonderlösungen beantwortet werden. Um es klar zu sagen: Solche Sonderlösungen können sich natürlich als die besseren Lösungen im Vergleich mit anderen Anbietern erweisen. Dann sollte man sie auch wählen. Um die Potentiale moderner Technik zum Wohle der Gesellschaft nutzen zu können, sollte man sich nicht künstlich andere technische Lösungen versagen, bloß weil sie nicht in Deutschland oder anderen EU-Staaten entwickelt wurde.

Bei der Wahl der Lösungen sollte gleichwohl betrachtet werden, wie groß das Risiko wird, dass andere Staaten tatsächlich ihren Einfluss auf die Anbieter von IT-Produkten oder -Dienstleister ausüben werden, um sich im geopolitischen Wettstreit einen Vorteil zu verschaffen –

die IT also gleichsam als Waffe einzusetzen. Für diese Einschätzung werden die Verantwortlichen sicherlich die Unterstützung durch die zuständigen Behörden brauchen.

Um zukunftsoffen zu sein und Abhängigkeiten von einzelnen Marktteilnehmern zu vermeiden, sollte, da wo dies möglich ist, möglichst auf offene – nicht proprietäre – Standards gesetzt werden. So werden zum einen Lock-in-Effekte vermieden, die Interoperabilität verschiedener Anbieter gefördert und gleichzeitig die Entwicklungsoffenheit gefördert. Wo sie noch nicht existieren, sollten sich Deutschland und die anderen Mitgliedstaaten stärker in der Entwicklung offener und damit auch kontrollierbarer internationaler Standards engagieren.

Entsprechende Bemühungen gibt es bereits etwas mit Gaia-X, wo offene Standards bei Hard- und Software als Grundlage einer europäischen Dateninfrastruktur dienen sollen. Auch wenn die Verabschiedung der Spezifikationen bei Gaia-X selbst nur langsam vorankommt, ist das Ziel richtig. Solche Vorhaben müssen mit dem nötigen Nachdruck betrieben werden. Insbesondere die öffentliche Hand könnte hier mehr leisten, etwa, indem sie selbst als Vorbild agiert und die skizzierten Elemente in der Ausschreibung ihrer eigenen IT einfordert und damit auch den Markt für solche souveränen und sicheren Lösungen mitentwickelt. Die von den Anbietern für die öffentliche Hand entwickelten Lösungen könnten dann auch von kleineren Nutzern für ihre eigene Infrastruktur eingekauft werden.

IV. Alternative Modelle einer Datenökonomie

Die „griffige Formel“, in Frage 18 durch den Pleonasmus vom „Eigentum an den eigenen Daten“ beschrieben, läuft unter Betrachtung der datenrechtlichen Realität leer. Darüber hinaus verspräche eine Umstrukturierung des Datenrechts auf Basis eines property rights an Daten weder einen datenökonomischen Mehrwert noch eine Verbesserung des Schutzniveaus für personenbezogene Daten.

Nach deutschem Zivilrecht ist Eigentum an Daten ausgeschlossen. Das Recht an Daten kann zwar als absolut wirkendes Bündel an Verbots- und Nutzungsrechten beschrieben werden, die eine eigentumsähnliche Struktur aufweisen.[144] Unter Eigentum wird nach dem Konzept des BGB aber das Vollrecht an einer Sache verstanden.[145] Da Sachen gem. § 90 BGB nur körperliche Gegenstände sind, Daten gem. Art. 4 Nr. 1 DS-GVO aber ausschließlich Informationen umfassen, kann Eigentum an Daten nicht begründet werden.[146] Damit kann Eigentum ausschließlich am Datenträger, nicht aber am Datum selbst bestehen.[147]

In der Rechtswissenschaft wird die Gewährung eines Herrschafts- und Verfügungsrechts im Sinne eines property rights in Analogie zum Eigentumsschutz diskutiert.[148] Damit wären Berechtigte mit haftungsrechtlichen Mitteln vor schuldhafter Zerstörung oder Beschädigung der ihnen zustehenden Datensätze geschützt, Daten könnten als Kreditunterlage eingesetzt werden und Gläubiger könnten Daten im Wege der Zwangsvollstreckung verwerten.[149] Sofern die Frage auf die Etablierung eines solchen property rights abzielt, ist dies vornehmlich unter ökonomischen Gesichtspunkten zu diskutieren. Aus ökonomischer Perspektive unzureichend wäre es jedenfalls, Daten lediglich einen Preis zuzuschreiben. Schon die praktische Umsetzbarkeit dieser Maßnahme wirft Fragen auf. Doch auch unabhängig davon wird die analoge

[144] *Metzger/Schweitzer/Wagner* ZfPW 2023, 227 (233); *Wagner* in MüKO BGB, § 823 Rn. 381; *Amstutz* AcP 218 (2018), 438 (528 f., 548).
[145] *Brückner* in MüKo BGB, § 903 Rn. 2.
[146] *Amstutz* AcP 218 (2018), 438 (544); *Metzger/Schweitzer/Wagner* ZfPW 2023, 227 (233).
[147] *Wagner* in MüKO BGB, § 823 Rn. 378-380.
[148] *Wagner* in MüKO BGB, § 823 Rn. 380-382; *Faust*, DJT-Gutachten, A 79.
[149] *Wagner* in MüKO BGB, § 823 Rn. 380.

Anwendung der Vorschriften zum Sacheigentum unter Verweis auf die Nicht-Rivalität, Nicht-Exklusivität und Nicht-Abnutzbarkeit von Daten zu Recht abgelehnt.[150]

Zentrale Probleme der Datenökonomie könnten schließlich auch mit Einführung eines property rights an Daten nicht gelöst werden. Der Forderung liegt insofern eine begrenzte Betrachtung der Ordnungsprinzipien zugrunde, die das Recht bei der Schaffung von Marktordnungen gewährleisten muss. Diese liegen im Privateigentum, der Vertragsfreiheit, dem Wettbewerb und dem funktionsfähigen Währungssystem.[151] Mit der Einführung eines eigentumsähnlichen Rechts an Daten wäre zwar der Grundstein für die erste der vier Säulen gelegt, die Friktionen in der Datenökonomie wären damit aber nicht aufgelöst: Es ließe sich zwar argumentieren, dass Daten durch ihre unmittelbare wirtschaftliche Verwertbarkeit durch das Individuum ein stärkeres Preissignal erhalten würden. Ein aktuelles Beispiel zeigt aber, dass die Entwicklung eines solchen Marktes für Daten nicht ohne Weiteres zu erwarten ist: So wird ein gegen Angabe umfangreicher personenbezogener Daten übereignetes Fan-Trikot gemeinhin als kostenlos wahrgenommen. Persönlichkeitsrechte können zwar mit und ohne Angleichung an das Eigentumsrecht vermögensrechtliche Eigenschaften entwickeln, und dann als Grundlage für Transaktionen in Frage kommen.[152] Solange Güter und Dienstleistungen, die im Austausch gegen Daten erlangt werden, aber als kostenlos wahrgenommen werden, hilft auch die Etablierung eines eigentumsähnlichen Rechts an Daten nicht weiter.

Hieran zeigt sich die besondere Bedeutung der betroffenen Person und ihrer Vertragsfreiheit als Ausgangspunkt der Transaktion. Die Ausübung der Vertragsfreiheit muss tatsächlich und damit in erster Linie informiert möglich sein. Insofern ist vornehmlich anderen Marktstörungen wie Informationsasymmetrien und den Machtlagen auf Datenmärkten entgegenzuwirken.[153] Andernfalls werden der Sogeffekt unentgeltlicher Leistungen und populärer digitaler Dienste in der breiten Gesellschaft die Entstehung eines handelbaren Datenwerts auch weiterhin verhindern.[154] Aus eben diesem Grund ist die gegenwärtig auf zahlreichen Plattformen angewandte Methode des „Pay or Consent“ zumindest bei den derzeit geforderten Preisen allenfalls eine Scheinlösung und es steht zu befürchten, dass auch eine Umsatzbesteuerung am Maßstab des monetären Preises mit dem Ziel, diesen zu senken, wirkungslos bleiben würde.[155]

Solange sich in der breiten Gesellschaft kein handelbarer Datenwert entwickelt hat, hilft die Einführung eines eigentumsähnlichen Rechts an Daten also nicht weiter. Sobald sich aber in der breiten Gesellschaft ein handelbarer Datenwert entwickelt hat, ist die Einführung eines eigentumsähnlichen Rechts an Daten für den Aufbau einer Datenökonomie nicht mehr erforderlich. Diese hat sich dann bereits aus dem Persönlichkeitsrecht entwickelt. Denkbar wäre in diesem Fall lediglich der Ausbau einer Datenökonomie durch Einführung eines eigentumsähnlichen Rechts an Daten.

So griffig die Formel vom „Eigentum an den eigenen Daten“ also sein mag, so wenig kann sie derzeit leisten. Sie ist daher möglicherweise für (rechts-)philosophische Überlegungen von

---

[150] *Arbeitsgruppe „Digitaler Neustart“*, Bericht vom 15. Mai 2017, S. 30; *Zech* CR 2015, 137 (139).
[151] *Eucken*, Grundsätze der Wirtschaftspolitik, S. 254 ff.
[152] *Metzger/Schweitzer/Wagner* ZfPW 2023, 227 (233).
[153] *Metzger/Schweitzer/Wagner* ZfPW 2023, 227 (236).
[154] Hierzu bereits II. 4.
[155] *Metzger/Schweitzer/Wagner* ZfPW 2023, 227 (247); hierzu auch *Bieg* ZD 2022, 487; *Rüscher* MwStR 2018, 419.

Relevanz, beim derzeitigen Entwicklungsstand des Datenmarktes aber für realpolitische Maßnahmen unter Berücksichtigung rechtlicher und ökonomischer Erwägungen ungeeignet.

C) Fazit

Europas Wirtschaft ist zwingend angewiesen auf einen fairen und praktisch umsetzbaren Rechtsrahmen, der nicht zuletzt auch Big-Tech-Unternehmen wirksame Verhaltensregeln auferlegt. Die datengetriebene Wirtschaft in Europa kann im Jahr 2024 nicht mehr eindimensional per Bürgerschutz und Abwehr reguliert werden. Vielmehr muss Daten(schutz)recht als mehrdimensionales Wirtschaftsrecht verstanden werden, das mit der DS-GVO auf die Ermöglichung von Geschäftsmodellen setzt.

Das Datenrecht wird nicht mehr ausschließlich durch die DS-GVO konstituiert. Vielmehr tritt verstärkt das **Datenwirtschaftsrecht** als gleichberechtigter Bestandteil des **Datenrechts** neben das Datenschutzrecht. Datenwirtschaftsrecht und Datenschutzrecht stehen in einem **Wechselwirkungsverhältnis**, sodass jedes der beiden Teilrechtsgebiete bei der Anwendung des jeweils anderen zu berücksichtigen ist. Innovative Datenpolitik verlangt damit die Förderung der Datenwirtschaft unter Berücksichtigung des Datenschutzrechts.

Acht Kernaussagen sind dabei entscheidend:

1. Datenrecht ist Datenschutz- und Datenwirtschaftsrecht
Moderne Daten- und Digitalstrategien müssen die **Wechselwirkung** zwischen Datenschutzrecht und Datenwirtschaftsrecht in ihr Zentrum stellen. Die Datenstrategie der Bundesregierung enthält gute Ansätze hinsichtlich einer vermehrten Nutzung und Teilen von Daten. Sie ist im Gesamten aber noch zu sehr auf datenschutzrechtliche Aspekte fokussiert. Sie sollte im Willen des europäischen Gesetzgebers angepasst werden und den Aspekt des Datenwirtschaftsrechts stärker in den Blick nehmen.

2. Anonymisierung als Ermöglichungswerkzeug
Die **neuen Datenakte der Europäischen Union** und die Funktionsweise neuer datenverarbeitender Technologien wie künstliche Intelligenz machen eine trennscharfe **Abgrenzung** zwischen **personenbezogenen** und **nicht-personenbezogenen** Daten zwingend erforderlich. Die Wirtschaft muss sich darauf verlassen können, dass sie bei Anwendung konkreter **Anonymisierungsstandards** den datenschutzrechtlichen Vorgaben nicht unterliegt. Das macht eine Konkretisierung erforderlich, die angesichts technischer Entwicklungen durch Leitlinien einer unabhängigen Stelle wie dem Dateninstitut erreicht werden könnte.

3. Stabilität schaffende Aufsichtsstrukturen
Das aufgezeigte Verhältnis von Datenschutzrecht und Datenwirtschaftsrecht sollte sich in den **Aufsichtsstrukturen** widerspiegeln, die der nationale Gesetzgeber im Rahmen seines unionsrechtlich eingeräumten Gestaltungsspielraums festlegen darf. Den Datenschutzaufsichtsbehörden sollten Mittel zur Verfügung gestellt werden, um neben dem Grundrechtsschutz auch datenwirtschaftliche Belange in Zusammenarbeit mit dem Dateninstitut berücksichtigen zu können.

4. Hilfe durch Muster
Die **Mustervertragsklauseln** der Kommission zum Data Act, die bis zum 12.9.2025 erstellt werden müssen, sollten durch ein Bundesministerium **ergänzt** werden, sofern sie relevante Aspekte nicht berücksichtigen. Dies betrifft etwa die Vorgabe verschiedener **zulässiger Zwecke für die Weitergabe** nicht-personenbezogener Produktdaten. Darüber

hinaus sollten **Musterinformationen** zur Verfügung gestellt werden, um die Erfüllung der Informationspflichten nach dem Data Act zu unterstützen.

5. PIMS als Anreiz für digitale Ökosysteme

Einen **Anreiz** für mehr Datenwirtschaft können **Personal Information Management Systems** (PIMS) bieten. Sie eröffnen die Chance, **digitale Ökosysteme** zu schaffen und (europäische) Datenräume zu füllen, während gleichzeitig das Recht auf informationelle Selbstbestimmung im Blick behalten wird. Neben den aufgezählten Chancen bergen PIMS auch Risiken, die staatlicherseits einzuhegen sind.

6. Initiativen bündeln

Auf nationaler wie auf internationaler Ebene gibt es zahlreiche Initiativen, die die Datenwirtschaft vorantreiben wollen (z.B. Gaia-X, Dateninstitut). Die auf Digitalmärkten entstandenen Machtverhältnisse begünstigen Gate Keeping und andere Formen der Wettbewerbsverzerrung. Ziel sollte auch auf neu entstehenden und entstandenen Digitalmärkten ein **System freien Wettbewerbs** sein. Dateninitiativen können Märkte durch gezielte Förderung im besten Fall öffnen und die Wettbewerbsverhältnisse stabilisieren. Fördert der Staat Projekte, die die Unterstützung von Unternehmen an das Bekenntnis zu bestimmten (europäischen) Werten knüpfen, entsteht die Gefahr tiefer, ideologisch motivierter Eingriffe in den Markt. Wo es nicht zwingend geboten ist, sollte sich staatliches Handeln darauf beschränken, einen Ordnungsrahmen für ein freies Wirtschaften vorzugeben.

7. Mittel zur Förderung der Akzeptanz für Datenteilung

Es sollten Maßnahmen ergriffen werden, um die **Akzeptanz** der wachsenden **Datenwirtschaft durch die Zivilgesellschaft** zu **steigern**. Daten mit Gemeinwohlbezug sollten staatlichen Stellen und Unternehmen leichter zugänglich gemacht werden. In Krisenfällen sollte eine leicht umsetzbare Pflicht zur Herausgabe entscheidender Daten bestehen. Daten zum Nutzungsverhalten kann sich der Staat bei der Bekämpfung der Klimakrise zu Nutze machen (z.B. Lichtmanagement, Smart-Heating-Systeme). In öffentlichen Sektoren (Mobilität, öffentliche Infrastruktur) bietet sich eine „Rückgabe“ von Daten an die Bevölkerung durch aufbereitete Apps, Webangebote etc. an.

8. Eigenverantwortlich über Daten verfügen können

(Personenbezogene) **Daten haben einen Wert**. Die Gesellschaft muss über diesen ins Bild gesetzt werden. Bürgerinnen und Bürger müssen ihre existierenden Verfügungs- und Verwertungsbefugnisse kennen, um sie auch ökonomisch wirksam ausüben zu können. Dazu sollte bestehenden Marktstörungen wie insbesondere **Informationsasymmetrien** und **Machtkonzentrationen entgegengewirkt** werden. Die Einführung eines eigentumsähnlichen Rechts an Daten ginge unter Berücksichtigung des gegebenen Entwicklungsstands der Datenökonomie fehl.