Schriften zum Katastrophenrecht

Kai von Lewinski | Meinhard Schröder | Tristan Barczak [Hrsg.]

Datenrecht im Ausnahmefall

Nomos

Schriften zum Katastrophenrecht

Herausgegeben von
Prof. Dr. Michael Kloepfer

Band 13

Kai von Lewinski | Meinhard Schröder | Tristan Barczak [Hrsg.]

Datenrecht im Ausnahmefall

Nomos

Die Publikation wurde durch die Universität Passau finanziell unterstützt (Open-Access-Publikationsfonds der Universitätsbibliothek).

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.d-nb.de abrufbar.

1. Auflage 2025

Publiziert von
Nomos Verlagsgesellschaft mbH & Co. KG
Waldseestraße 3–5 | 76530 Baden-Baden
www.nomos.de

Gesamtherstellung:
Nomos Verlagsgesellschaft mbH & Co. KG
Waldseestraße 3–5 | 76530 Baden-Baden

ISBN (Print): 978-3-7560-3038-5
ISBN (ePDF): 978-3-7489-5348-7

DOI: https://doi.org/10.5771/9783748953487

Onlineversion
Nomos eLibrary

Vorwort

Am 28. November 2024 fand an der Universität Passau die Tagung „Datenrecht im Ausnahmefall" statt, die zugleich die Abschlussveranstaltung der „Forschungsstelle für Rechtsfragen der Digitalisierung" (FREDI) war. Tagungszeitpunkt, Tagungsort, Thema sowie Referentinnen und Referenten standen dabei in einer bemerkenswerten Wechselbeziehung, so dass sich die konkrete Gestalt der kleinen Konferenz mehr oder minder von alleine ergab.

Die Forschungsstelle FREDI (https://www.jura.uni-passau.de/forschung/forschungseinrichtungen/fredi) war knapp 10 Jahre von der bayerischen Staatsregierung finanziert worden, um die daten- und digitalbezogene Forschung zu fördern. Hierfür war sie an den datenrechtlichen Lehrstuhl an der Universität Passau angebunden, den von 2017 bis 2018 *Louisa Specht* und von 2020 bis 2023 *Moritz Hennemann* innehatten; in den Zeiten dazwischen und danach war FREDI kommissarisch von *Kai v. Lewinski* geleitet worden. – Damit standen für die Abschlusstagung von FREDI drei Personen schon fest.

An der Juristischen Fakultät der Universität Passau gibt es einen gewissen Fokus auf Fragen des Katastrophenrechts und der Resilienz des Rechts. Hier sind (ohne Anspruch auf Vollständigkeit und in aller gebotenen Bescheidenheit) die drei Herausgeber dieses Tagungsbands zu nennen.

Und als sich dann herausstellte, dass (zum Zeitpunkt der Tagung) die bis dahin vorliegenden Kommentierungen (sowie die ausführlichste Einführungsdarstellung) zu den Art. 14 ff. DA alle aus Passauer Federn stammten, zudem ein wichtiger DA- (und DGA-)Kommentar von *Louisa Specht-Riemenschneider* und *Moritz Hennemann* herausgegeben wird, war das passende Thema für die Tagung klar und eindeutig. Abgerundet wurde es dann nur noch durch den Beitrag von *Harald Erkens*, einen der besten Kenner der Vorsorge- und Sicherstellungsgesetze.

Aufgebaut ist vorliegender Tagungsband (im Detail abweichend von der Reihenfolge der Referenten bei der Tagung) wie folgt: Zunächst werden Vorbilder (*Specht-Riemenschneider/Schneider*) sowie primär- und verfassungsrechtlicher Rahmen (*v. Lewinski*) dargestellt, die Regelung in das größere datenrechtliche Bild eingeordnet (*Hennemann*) und mit einigen plastischen und drastischen Pinselstrichen akzentuiert (*Erkens*). Dies führ-

te dann zu zentralen Fragen des Tatbestands (*Wienroeder*) und des Rechtsschutzes (*Schröder*). Abgeschlossen wurde die Tagung durch eine Diskussion (*Sonnenberg*).

Passau, im Sommer 2025

Kai v. Lewinski *Meinhard Schröder* *Tristan Barczak*

Inhaltsverzeichnis

Abkürzungsverzeichnis

ABI.	Amtsblatt
AEUV	Vertrag über die Arbeitsweise der Europäischen Union
AktG	Aktiengesetz
AO	Abgabenordnung
AöR	Archiv des öffentlichen Rechts
ASG	Arbeitssicherstellungsgesetz
BaFin	Bundesanstalt für Finanzdienstleistungsaufsicht
bayBodSchG	Bayerisches Bodenschutzgesetz
bayLStVG	Gesetz über das Landesstrafrecht und das Verordnungsrecht auf dem Gebiet der öffentlichen Sicherheit und Ordnung
bayPAG	Gesetz über die Aufgaben und Befugnisse der Bayerischen Polizei
BayVBI	Bayerische Verwaltungsblätter
BayVGH	Bayerischer Verwaltungsgerichtshof
BBergG	Bundesberggesetz
BBodSchG	Gesetz zum Schutz vor schädlichen Bodenveränderungen und zur Sanierung von Altlasten
Bd.	Band
BeckRS	Beck-Rechtsprechung
BfDI	Bundesbeauftragte für den Datenschutz und die Informationsfreiheit
BfJ	Bundesamt für Justiz
BGB	Bürgerliches Gesetzbuch
BKAG	Bundeskriminalamtgesetz
BKartA	Bundeskartellamt
BLG	Bundesleistungsgesetz
BMBF	Bundesministerium für Bildung und Forschung
BMG	Bundesmeldegesetz
BNetzA	Bundesnetzagentur
BPolG	Gesetz über die Bundespolizei
BSI	Bundesamt für Sicherheit in der Informationstechnik

BSI-G	Gesetz über das Bundesamt für Sicherheit in der Informationstechnik
BT-Drs.	Bundestags-Drucksache
BVerfG	Bundesverfassungsgericht
BVerfGE	Entscheidungen des Bundesverfassungsgerichts
BVerwG	Bundesverwaltungsgericht
CERRE	Centre on Regulation in Europe
ChemG	Chemikaliengesetz
ChemGiftInfoV	Giftinformationsverordnung
COM	Dokumente der Europäischen Kommission
CR	Computer und Recht
DA	Data Act
DGA	Data Governance Act
DMA	Digital Markets Act
DNG	Gesetz für die Nutzung von Daten des öffentlichen Sektors
DÖV	Die Öffentliche Verwaltung
DRK	Deutsches Rotes Kreuz
DSA	Digital Service Act
DSGVO	Datenschutz-Grundverordnung
DSK	Datenschutzkonferenz
DVBl.	Deutsches Verwaltungsblatt
EDIB	European Data Innovation Board
EDSA	Europäischer Datenschutzausschuss
EGZPO	Gesetz, betreffend die Einführung der Zivilprozeßordnung
Einf.	Einführung
Einl.	Einleitung
EnSiG	Energiesicherungsgesetz
ErdölBevG	Erdölbervorratungsgesetz
ErgLfg.	Ergänzungslieferung
ESVG	Ernährungssicherstellungs- und -vorsorgegesetz
EU	Europäische Union
EuDIR	Zeitschrift für Europäisches Daten- und Informationsrecht
EuGH	Europäischer Gerichtshof

EuR	Europarecht
EUV	Vertrag über die Europäische Union
EuZW	Europäische Zeitschrift für Wirtschaftsrecht
EZB	Europäische Zentralbank
FREDI	Forschungsstelle für Rechtsfragen der Digitalisierung der Universität Passau
GBO	Grundbuchordnung
GeschGehG	Gesetz zum Schutz von Geschäftsgeheimnissen
GewO	Gewerbeordnung
GewStG	Gewerbesteuergesetz
GG	Grundgesetz
GRCh	Charta der Grundrechte der Europäischen Union
GRUR	Gewerblicher Rechtsschutz und Urheberrecht
GRUR-Prax	Gewerblicher Rechtsschutz und Urheberrecht in der Praxis
GRUR-RR	Gewerblicher Rechtsschutz und Urheberrecht Rechtsprechungs-Report
GSZ	Zeitschrift für das Gesamte Sicherheitsrecht
GwG	Gesetz über das Aufspüren von Gewinnen aus schweren Straftaten
hessHundeVO	Hessische Gefahrenabwehrverordnung über das Halten und Führen von Hunden
hmbHundeG	Hamburgisches Gesetz über das Halten und Führen von Hunden
hmbWaG	Hamburgisches Wassergesetz
Hrsg.	Herausgeber
IIC	International Review of Intellectual Property and Competition Law
IKM	Internationales Krisenmanagement
JZ	Juristen Zeitung
Kap.	Kapitel
KKW	Kernkraftwerk
Ls.	Leitsatz
LuftVG	Luftverkehrsgesetz
m.w.N.	mit weiteren Nachweisen
MarkenG	Markengesetz
MMR	Zeitschrift für das Recht der Digitalisierung, Datenwirtschaft und IT

MPIIC	Max-Planck-Institute for Innovation and Competition
NATO	North Atlantik Treaty Organization
NFM	NATO Force Model
NJW	Neue Juristische Wochenschrift
NRF	NATO Response Force
PatG	Patentgesetz
PostG	Postgesetz
RDi	Recht Digital
Rn.	Randnummer
SchRegO	Schiffsregisterordnung
SGB X	Zehntes Buch Sozialgesetzbuch
SortSchG	Sortenschutzgesetz
StPO	Strafprozessordnung
StVG	Straßenverkehrsgesetz
thürTierGefG	Thüringer Tiergefahrengesetz
THW	Technisches Hilfswerk
TKG	Telekommunikationsgesetz
UAbs.	Unterabsatz
UrhG	Urhebergesetz
Urt.	Urteil
VerkLG	Verkehrsleistungsgesetz
VerkSiG	Verkehrssicherstellungsgesetz
Vorbem.	Vorbemerkung
VwGO	Verwaltungsgerichtsordnung
VwVfG	Verwaltungsverfahrensgesetz
WasSiG	Wassersicherstellungsgesetz
WHG	Gesetz zur Ordnung des Wasserhaushalts
WiSiG	Wirtschaftssicherstellungsgesetz
WpHG	Gesetz über den Wertpapierhandel
ZAP	Zeitschrift für die Anwaltspraxis
ZD-Aktuell	Newsdienst ZD-Aktuell
ZEuP	Zeitschrift für Europäisches Privatrecht
ZfDR	Zeitschrift für Digitalisierung und Recht

ZfPW	Zeitschrift für die gesamte Privatrechtswissenschaft
ZGE	Zeitschrift für geistiges Eigentum
ZGI	Zeitschrift für das gesamte Informationsrecht
ZPO	Zivilprozessordnung
ZRP	Zeitschrift für Rechtspolitik

Was Datenwirtschafts- und Datenschutzrecht (nicht) voneinander lernen können

Louisa Specht-Riemenschneider[*] *und Ruben Schneider*[**]

Spätestens seit Geltungserlangung der DSGVO im Jahr 2018 lag der Schwerpunkt der rechtlichen Betrachtung von Daten im Datenschutzrecht. Nur vereinzelte Stimmen[1] betrachteten Daten als zivilrechtliches Wirtschaftsgut. Der Begriff des Datenwirtschaftsrechts entwickelte sich erst mit der europäischen Digitalstrategie, insbesondere mit Data Act (DA) und Data Governance Act (DGA)[2].

* Louisa Specht-Riemenschneider ist Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) und Inhaberin des Lehrstuhls für Bürgerliches Recht, Recht der Datenwirtschaft, des Datenschutzes, der Digitalisierung und der Künstlichen Intelligenz an der Universität Bonn.

** Ruben Schneider ist persönlicher Referent bei der Bundesbeauftragten für den Datenschutz und die Informationssicherheit (BfDI).

1 *Specht*, Konsequenzen der Ökonomisierung informationeller Selbstbestimmung, 2011 m.w.N.

2 *Specht-Riemenschneider*, ZEuP 2023, 638; *Hennemann/Steinrötter*, NJW 2022, 1481; *Steinrötter*, RDi 2021, 480; *Jakl*, RDi 2021, 71.

Heute werden Datenschutz- und Datenwirtschaftsrecht oft gemeinsam als Datenrecht bezeichnet. Das ist erfreulich, wohnt dem doch die Erkenntnis inne, dass Datenschutz und Datennutzung gemeinsam gedacht werden müssen. Ohne Datenschutz kann keine grundrechtssensible Datennutzung erfolgen.

Das weltweit erste Datenschutzgesetz trat 1970 in Hessen in Kraft und ist dem Datenwirtschaftsrecht insoweit um Jahre voraus. Es stellt sich daher die Frage, was Datenschutz- und Datenwirtschaftsrecht voneinander lernen können – im positiven wie im negativen Sinne.

Hierzu werden zunächst die Perspektive und das Grundverständnis (A.) der Verfasser erörtert. Darauf folgt eine Untersuchung der Negativ- (B.) und Positivimplikationen (C.) des Datenschutzrechts und insoweit der Frage, was das Datenwirtschaftsrecht (nicht) vom Datenschutzrecht lernen sollte. Im Anschluss hieran wird erörtert, was beide Rechtsgebiete nur gemeinsam lernen können (D.). Der Beitrag schließt mit einem Fazit (E.).

A. Perspektive und Grundverständnis

Die Betrachtung potenzieller Lern- und Negativeffekte hängt von der Perspektive des Betrachtenden ab. Innerhalb des Data Acts z.B. unterscheiden sich die Interessen von Nutzern, Betroffenen, Dateninhabern und Dritten signifikant – es bestehen unterschiedliche Schutzbedürfnisse. Gleiches gilt für Verantwortliche, Auftragsverarbeiter, Aufsichtsbehörden und Betroffene in der DSGVO sowie für Dateninhaber, Datennutzer und Datenvermittlungsdienste im DGA. Dieser Beitrag nimmt eine wissenschaftliche Perspektive ein, um die Lern- und Negativeffekte frei von interessengeleiteten Annahmen zu erörtern.

Doch auch bei einer wissenschaftlichen Betrachtung ist das Grundverständnis entscheidend, mit dem man auf beide Rechtsgebiete blickt – insbesondere auf das Datenschutzrecht: Wird es als berechtigte Bremse im Interesse eines allüberlegenen Schutzes informationeller Selbstbestimmung angesehen, der keine Datennutzung als den besten Datenschutz begreift? Oder wird es als interessenausgleichendes Instrument betrachtet, das zwar rote Linien zieht, aber innerhalb des gesetzlichen Rahmens einen Korridor des Möglichen zeichnet, folglich ein Instrument ist, um Datennutzung zu ermöglichen und gar abzusichern?

Unser Verständnis ist das letztere. Die DSGVO ist niemals dafür angetreten, Datennutzungen und Datenverarbeitungen insgesamt zu verhindern.

Sie möchte vielmehr einen Interessenausgleich zwischen den Interessen der Verantwortlichen und Betroffenen an einem effektiven sowie umfassenden Grundrechtsschutz herstellen. Datenschutz ist kein Hindernis, sondern Chance und Standortvorteil, weil er Vertrauensgarant ist. Datenschutz ist Selbstbestimmung, Eigenverantwortung und Freiheit für alle Bürgerinnen und Bürger. Moderner Datenschutz steht einer digitalen Entwicklung mit Vorteilen für alle Bürgerinnen und Bürger nicht im Wege, sondern unterstützt sie.

Gleichzeitig ist Datennutzung essenziell für unsere Wirtschaft. Dass die DSGVO Datennutzungen nicht entgegensteht, legt sie selbst fest: In Art. 1 Abs. 1 DSGVO statuiert sie, dass sie auch Vorschriften „zum freien Verkehr" von personenbezogenen Daten enthält. Art. 1 Abs. 3 DSGVO ergänzt, dass der „freie Verkehr personenbezogener Daten in der Union […] weder eingeschränkt noch verboten werden" darf. Hier zeigt der Unionsgesetzgeber, dass ihm die Datenwirtschaft ein ebenso schützenswertes Interesse wie der Datenschutz ist. Beide sind im europäischen Allgemeininteresse stehende Eckpfeiler des digitalen Binnenmarkts[3]. *Das Datenschutzrecht ist daher keinesfalls wirtschaftsfeindlich*[4]. *Der Unionsgesetzgeber sieht personenbezogene Daten als selbstständiges Wirtschaftsgut an:* ErwGr. 9 und 10 DSGVO belegen, dass wirtschaftliche Betätigungen von der DSGVO erleichtert und der Wettbewerb geschützt werden soll[5]. Betroffenenschutz und Datennutzbarkeit sollen also nach dem gesetzgeberischen Willen Hand in Hand gehen.

B. Negativimplikationen des Datenschutzrechts

Lassen Sie uns zunächst einen Blick auf die negativen Implikationen des Datenschutzrechts werfen. Diese sollten dem Datenwirtschaftsrecht nicht als Vorbild dienen. Hier lassen sich v.a. zwei Punkte nennen: Die vielfache Unbestimmtheit der datenschutzrechtlichen Regelungen sowie deren reziprokes Verhältnis zu den signifikanten Bußgeld- und Schadensersatzrisiken der DSGVO (I.) sowie die fehlende Abstimmung der DSGVO mit verhaltenswissenschaftlichen Erkenntnissen (II.).

---

3 *Sydow*, in: Sydow/Marsch (Hrsg.), DSGVO BDSG, 3. Aufl. 2022, Art. 1 DSGVO Rn. 22; *Pötters*, in: Gola/Heckmann (Hrsg.), DSGVO BDSG, 3. Aufl. 2022, Art. 1 DSGVO Rn. 16.

4 *Hornung/Spiecker*, in: Simitis/Spiecker/Hornung (Hrsg.), Datenschutzrecht, 2. Aufl. 2025, Art. 1 DSGVO Rn. 42 ff.

5 *Spindler/Darby*, in: Spindler/Schuster (Hrsg.), Recht der elektronischen Medien, 4. Aufl. 2019, Art. 1 DSGVO Rn. 5.

I. Unbestimmtheit

Die vielfache Unbestimmtheit von Normen ist ein grundlegendes Problem des öffentlich-rechtlich geprägten Datenschutzrechts: Aufgrund der Vielzahl von unbestimmten Rechtsbegriffen und Abwägungsklauseln – allen voran der Interessenabwägung gemäß Art. 6 Abs. 1 lit. f DSGVO – besteht in vielen Verarbeitungsszenarien Rechtsunsicherheit. Diese Rechtsunsicherheit ist unausweichlich, um bei einer Betrachtung der sich gegenüberstehenden Grundrechtspositionen interessengerechte Lösungen zu finden. Dies mag als unterkomplex abgetan werden[6], führt aber mit einem „one size fits all"-Ansatz zur technikneutralen Zukunftsoffenheit des Datenschutzrechts.

Die DSGVO ist und bleibt eine Grundverordnung. Das zeigt sich z.B. in den Datenschutzgrundsätzen des Art. 5 DSGVO, die richtig und wichtig sind, aber vage bleiben. Dennoch sind sie zu verteidigen, da sie der DSGVO zu einem hohen Wirkungsgrad verhelfen und interessengerechte Lösungen unterstützen, die die Perspektive aller Akteure berücksichtigen. Der Gesetzgeber zeigt hierdurch, keinem Interesse per se den Vorrang gewähren zu wollen, sondern den *Ausgleich zwischen gleichermaßen schützenswerten Grundrechten herstellen zu wollen*[7].

Problematisch ist dennoch, dass der Verantwortliche zunächst alleingelassen wird in der Einschätzung der Rechtmäßigkeit einer Datenverarbeitung aufgrund einer Interessenabwägung.

Auch das oft praktizierte Ausweichen auf die Einwilligung gemäß Art. 6 Abs. 1 lit. a DSGVO kann den Unsicherheiten der Interessenabwägung nicht adäquat entgegentreten: Einerseits ist nicht immer gewährleistet, dass Betroffene eine Einwilligung abgeben können bzw. wollen. Andererseits sind die tatbestandlichen Voraussetzungen der Einwilligung nicht trivial: Die Vorgabe des Art. 4 Nr. 11 DSGVO, wonach die Einwilligung „freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich" abzugeben ist, ist keinesfalls selbsterklärend. Gleiches gilt für die von Art. 7 Abs. 2 S. 1 DSGVO geforderte Einwilligung „in verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache".

Hinzu tritt das Problem, dass nicht abschließend geklärt ist, ob neben der Einwilligung hilfsweise auf andere Rechtsgrundlagen ausgewichen werden darf. Indem der Verantwortliche bei einem Betroffenen eine Einwil-

6 *Roßnagel/Nebel/Richter*, ZD 2015, 455 (460).
7 *Masing*, NJW 2012, 2305 (2307).

ligung einholt, signalisiert er nämlich, dass es für die Zulässigkeit der Datenverarbeitung auf sein Einverständnis ankommen soll[8]. Es wäre widersprüchlich, wenn sich der Verantwortliche bei Ausbleiben oder Unwirksamkeit der Einwilligung alternativ auf einen gesetzlichen Zulässigkeitstatbestand berufen dürfte[9]. Dem Betroffenen würde dadurch eine Entscheidungsmacht suggeriert, die faktisch nicht besteht[10]. DSK und EDSA stellen sich daher auf den Standpunkt, dass ein Auswechseln der Rechtsgrundlage mit den Grundsätzen der Fairness und Transparenz gemäß Art. 5 Abs. 1 lit. a DSGVO nicht vereinbar sei[11]. Es gibt jedoch gerade keine Abstufung zwischen den einzelnen Erlaubnistatbeständen. Die Einwilligung ist also qualitativ nicht vorzugswürdiger als ein anderer Erlaubnistatbestand.

Obgleich die Einwilligung durch das strukturelle Ungleichgewicht, das z.B. auch zwischen Dateninhaber und Nutzer im DA besteht, an ihre Grenzen stößt, hält das Datenwirtschaftsrecht an ihr fest: So etwa für die Nutzung nicht-personenbezogener Daten durch Dateninhaber (Art. 4 Abs. 13 DA) oder für die Verarbeitung personenbezogener Daten durch Torwächter (Art. 5 Abs. 2 DMA). Diese Szenarien sehen – wie die DSGVO – darüber hinweg, dass es Situationen gibt, in denen ein Betroffener nicht selbstbestimmt entscheiden kann. Die Ursachen hierfür können vielfältig sein, z.B. durch Netzwerkeffekte, Informationsüberlastung, Drittbetroffenendaten oder strukturelle Unterlegenheitssituationen. Die Einwilligung vermittelt zwar den Eindruck von Selbstbestimmtheit, verkommt aber oft zu einer leeren Hülle. Im Verbraucherschutzrecht hat man vor Jahrzehnten Lösungen für den Mangel an materieller Selbstbestimmung gefunden – das Datenschutzrecht scheint sie bis heute nicht zur Kenntnis zu nehmen[12]. Es wäre insgesamt – für Datenschutz- und Datenwirtschaftsrecht gleichermaßen – wünschenswert, wenn die Einwilligung dort, wo sie schlicht nicht funktionieren kann, durch deutlichere Verbote oder Erlaubnisse des Gesetzgebers ersetzen würde.

Als wären die vorgenannten Rechtsunsicherheiten nicht genug, werden sie von einem signifikanten Bußgeldrisiko flankiert: Art. 83 Abs. 5

8 *Buchner/Kühling*, in: Kühling/Buchner (Hrsg.), DSGVO BDSG, 4. Aufl. 2024, Art. 7 DSGVO Rn. 17a.
9 *Ruschemeier*, ZD 2020, 618 (619); Uecker, ZD 2019, 248 (249).
10 *Buchner/Kühling*, in: Kühling/Buchner (Hrsg.), DSGVO BDSG, 4. Aufl. 2024, Art. 7 DSGVO Rn. 17a.
11 *DSK*, Kurzpapier Nr. 20, S. 3; *EDSA*, Leitlinien 05/2020, Rn. 123.
12 Vgl. insgesamt *Specht*, Konsequenzen der Ökonomisierung informationeller Selbstbestimmung, 2011.

lit. a DSGVO sieht u.a. für Verstöße gegen Art. 5 und 6 DSGVO „Geldbußen von bis zu 20 000 000 EUR oder im Fall eines Unternehmens von bis zu 4 % seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs" vor. Die aktuelle Bußgeldpraxis der Aufsichtsbehörden zeigt, dass diese Geldbußen keinesfalls zahnlose Tiger sind: Wegen Verstoßes u.a. gegen Art. 5 und 6 DSGVO hat z.B. die irische Aufsichtsbehörde in den letzten Jahren Bußgelder i.H.v. 405 Millionen € (2022 gegen Meta)[13], 345 Millionen € (2023 gegen TikTok)[14] und 310 Millionen € (2022 gegen LinkedIn)[15] verhängt. Ein weiteres Bußgeld i.H.v. mindestens 500 Millionen € ist dem Vernehmen nach gegen TikTok geplant[16]. Dieses reziproke Gegenspiel von einerseits Rechtsunsicherheiten aufgrund unbestimmter Rechtsbegriffe und andererseits Sanktionsrisiken aufgrund hoher Bußgeldvorschriften ist für datenverarbeitende Akteure eine große Abschreckung, die sie mitunter vor Verarbeitungen in der EU absehen lässt.

Eindeutige und klar handhabbare Rechtfertigungs- und Verbotstatbestände können hier sowohl im Datenschutz- als auch im Datenwirtschaftsrecht Abhilfe schaffen.

II. Uneinsichtigkeit

Das Datenschutzrecht krankt weiter daran, dass es keinerlei Reaktion auf verhaltenswissenschaftliche Erkenntnisse beinhaltet[17]. Ein Beispiel hierfür sind die Informationspflichten nach Art. 13 und 14 DSGVO: Betroffene werden oft mit Hinweisen überschüttet. Schnell unterliegen sie einem sog. „information overload"[18]. Die Informationspflichten kehren sich für sie dann ins Gegenteil. Betroffene können die Informationen nicht mehr

13 Abrufbar unter https://dataprotection.ie/en/news-media/data-protection-commission-announces-conclusion-two-inquiries-meta-ireland (zuletzt abgerufen am 17.10.2025).

14 Abrufbar unter https://dataprotection.ie/en/news-media/press-releases/DPC-announces-345-million-euro-fine-of-TikTok#fine (zuletzt abgerufen am 17.10.2025).

15 Abrufbar unter https://dataprotection.ie/en/news-media/press-releases/irish-data-protection-commission-fines-linkedin-ireland-eu310-million (zuletzt abgerufen am 17.10.2025).

16 Abrufbar unter https://www.heise.de/news/Bericht-Saftige-Datenschutz-Strafe-fuer-Tiktok-10339569.html (zuletzt abgerufen am 17.10.2025).

17 *Wette*, Privatheitsregulation im Datenschutzrecht, i. E.

18 *EDSA*, Guidelines 3/2022, Rn. 65 f.; *Art.-29-Datenschutzgruppe*, WP 260 rev.01, Rn. 11.

aufnehmen, weil sie in ihrer Länge und Komplexität ertrinken[19]. Lösungsmöglichkeiten wie „One Pager"[20], Bildsymbole[21] oder PIMS[22] werden zwar diskutiert und für zulässig erachtet, haben aber noch keinen nachhaltigen Einzug in die Praxis gefunden.

Es verwundert insoweit nicht, dass die Eurobarometer-Umfrage im Jahr 2019 zu beachtlichen Ergebnissen gekommen ist[23]: Lediglich 13 % der Befragten gaben an, Datenschutzhinweise vollständig zu lesen. 47 % der Befragten taten dies jedenfalls teilweise, während 37 % der Befragten Datenschutzhinweise gar nicht lesen. Verglichen mit der Eurobarometer-Umfrage aus dem Jahr 2015 zeigt sich, dass die Bereitschaft, Datenschutzhinweise zu lesen, sogar abnimmt[24].

Neben den Datenschutzhinweisen ist auch im Kontext der Einwilligung zu beachten, dass Betroffene nicht zwingend rational handeln. Gerade in Konstellationen, in denen Betroffene für das Erteilen einer datenschutzrechtlichen Einwilligung eine Gegenleistung erhalten, wie z.B. die Mitgliedschaft in einem sozialen Netzwerk oder den kostenfreien Bezug von Informationen, setzen sie sich mit den Rechtsfolgen ihrer Einwilligung oft nicht hinreichend auseinander. Menschen neigen dazu, kurzfristige Vorteile (z.B. Lesen eines Zeitungsartikels) zu überschätzen und langfristige Nachteile (z.B. die Beeinflussung durch personenbezogene Werbung aufgrund der Einwilligung, die zum Lesen eines Zeitungsartikels gegeben wurde) zu unterschätzen[25]. Ein „privacy calculus", der für Betroffene die Vorteile einer Datenpreisgabe mit deren faktischen Kosten verrechnet, führt insoweit oft zu verblüffenden Ergebnissen[26].

Auch im Datenwirtschaftsrecht droht ein „information overload"[27]: So sehen z.B. Art. 3 Abs. 2 und Abs. 3 DA umfassende Informationspflichten

19 *Ebner*, ZD 2022, 364 (365).

20 Das BMJV hat diese bereits 2016 befürwortet und untersucht, vgl. *Kettner/Thorun/Spindler*, Innovatives Datenschutz-Einwilligungsmanagement, Abschlussbericht vorgelegt beim Bundesministerium der Justiz und für Verbraucherschutz, 2016, S. 109.

21 *Art.-29-Datenschutzgruppe*, WP 260 rev.01, Rn. 11.

22 *Hunter/Ebert/Spiecker*, ZD 2024, 603; *Kühling/Sauerborn*, ZD 2022, 596.

23 *EU-Kommission*, Special Eurobarometer 487a "The General Data Protection Regulation", 2019, S. 47.

24 *EU-Kommission*, Special Eurobarometer 431 "Data Protection", 2015, S. 84.

25 Dieses Denkmuster wird häufig anlehnend an *Gartner* auch „Hype Cycle" genannt, vgl. https://t3n.de/news/was-ist-der-hype-cycle-757261/ (zuletzt abgerufen am 17.10.2025).

26 *Wette*, Privatheitsregulation im Datenschutzrecht, i. E.

27 *Hennemann/Steinrötter* NJW 2022, 1481 (1483); *Ebner*, ZD 2022, 364 (367).

für Verkäufer, Vermieter und Leasinggeber vor, wenn sie mit einem Nutzer einen Vertrag über ein vernetztes Produkt abschließen. Diese Informationspflichten stehen denjenigen der DSGVO in ihrem Umfang nicht nach. Unterdessen besteht die Problematik, dass die Modalitäten der Informationsbereitstellung im DA noch schmaler als in der DSGVO geregelt sind: Art. 3 Abs. 2 und Abs. 3 DA beschränken sich auf den Hinweis, dass die Informationen dem Nutzer „in klarer und verständlicher Art und Weise bereitgestellt" werden müssen. Hier muss der Gesetzgeber nachbessern und Verantwortung übernehmen, um nicht von Anfang an ellenlangen Texten Vorschub zu leisten[28], mit denen sich Verkäufer, Vermieter und Leasinggeber absichern möchten, gleichzeitig aber Nutzer mit der Menge an Informationen überfordern.

Eine Verantwortungsübernahme des datenwirtschaftsrechtlichen Gesetzgebers sollte darin bestehen, Regelung zur Form der Informationsübermittlung aufzuführen (elektronisch, maschinenlesbar, schriftlich etc.) sowie parallel zum Datenschutzrecht die Verwendung von One-Pagern, standardisierten Bildsymbolen und die softwaregestützte Aufbereitung der Informationen zu ermöglichen (z.B. durch PIMS)[29]. Auch Formularvorgaben für den Text der Einwilligung sowie ihre AGB-Kontrollfähigkeit scheinen sinnvoll.

III. Summa

Die dargestellten Schwächen des Datenschutzrechts sind signifikant. Nichtsdestotrotz sei darauf hingewiesen, dass sie dem öffentlichen Recht nicht fremd sind und das wohlwollende Ziel einer interessenausgeglichenen Verarbeitung personenbezogener Daten verfolgen. Der Gesetzgeber sollte auf die im Datenschutzrecht festgestellten Mängel dennoch möglichst frühzeitig legislativ reagieren, um sie im Datenwirtschaftsrecht gar nicht erst entstehen zu lassen.

C. Positivimplikationen des Datenschutzrechts

Ungeachtet der skizzierten Negativimplikationen gibt es auch Positivimplikationen des Datenschutzrechts, an die das Datenwirtschaftsrecht anknüp-

28 *Ebner*, ZD 2022, 364 (367).
29 *Ebner*, ZD 2022, 364 (367).

fen sollte. Dies betrifft veröffentlichte Hilfestellungen (I.), den zumindest in Ansätzen angelegten Schutz des Schwächeren (II.), effektive Zusammenarbeitsmechanismen (III.), Zweckprivilegierungen (IV.) sowie das Zusammenspiel von private und public enforcement (V.).

I. Veröffentlichte Hilfestellungen

Mit jedem Tag, den die DSGVO in Kraft ist, werden neue Hilfestellungen veröffentlicht, um ihre Vorschriften korrekt anzuwenden und umzusetzen. Hierzu zählen z.B. Standardvertragsklauseln[30] der Europäischen Kommission, Anwendungshilfen von privaten Verbänden wie die Praxishilfen[31] der GDD sowie Kurzpapiere[32] der DSK und Guidelines[33] des EDSA.

Sie stellen belastbare Argumentationshilfen in gerichtlichen wie aufsichtsbehördlichen Verfahren dar. Sie sind zudem eine niedrigschwellige Informationshilfe für die regulierten Akteure. Auch im Datenwirtschaftsrecht sollten Aufsichtsbehörden und Verbände an der Veröffentlichung von Hilfestellungsmaterialien festhalten, um den regulierten Akteuren die Navigation durch den Dschungel der Digitalrechtsakte zu erleichtern.

II. Schutz des Schwächeren

Ein weiterer Vorzug des Datenschutzrechts sind seine Instrumente gegen strukturelle Unterlegenheit. Diese zeigen sich z.B. im Kopplungsverbot gemäß Art. 7 Abs. 4 DSGVO: Dieses legt bei der Beurteilung der Freiwilligkeit einer Einwilligung einen besonderen Fokus darauf, ob die Erfüllung eines Vertrags von der Einwilligung zu einer Verarbeitung von personenbezogenen Daten abhängig gemacht wird, die für die Erfüllung des Vertrags nicht erforderlich ist. Dies ist eine begrüßenswerte Reaktion auf überlege-

30 Durchführungsbeschluss (EU) 2021/914 der Kommission vom 4. Juni 2021 über Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Drittländer gemäß der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates.

31 Abrufbar unter https://www.gdd.de/service/publikationen-und-aktionen/#gdd-praxis (zuletzt abgerufen am 17.10.2025).

32 Abrufbar unter https://www.datenschutzkonferenz-online.de/kurzpapiere.html (zuletzt abgerufen am 17.10.2025).

33 Abrufbar unter https://www.edpb.europa.eu/our-work-tools/general-guidance/guidelines-recommendations-best-practices_en (zuletzt abgerufen am 17.10.2025).

ne Marktmachtstellungen und hilft dort, wo eine Einwilligung zwar eine prinzipiell autonome Entscheidung gewährleistet, aber gleichzeitig eine zu kompensierende Unterlegenheitssituation besteht. Ein Instrument gegen strukturelle Unterlegenheit ist ebenfalls, dass auf Grundlage der Interessenabwägung nach Art. 6 Abs. 1 lit. f DSGVO keine sensiblen Daten i.S.d. Art. 9 Abs. 1 DSGVO verarbeitet werden dürfen. Der Unionsgesetzgeber möchte hiermit verhindern, dass Verantwortliche allein auf Grundlage einer von ihnen selbst durchgeführten Abwägung eigenmächtig mit der Verarbeitung sensibler Daten beginnen.

Der vorgehend skizzierte datenschutzrechtliche Schutz des Schwächeren sollte sich im Datenwirtschaftsrecht fortsetzen. Hier gilt es insbesondere zugunsten Betroffener, KMUs und Start-Ups sicherzustellen, dass sie mit wirksamen Instrumenten ausgestattet sind, um nicht der Marktmacht einzelner Akteure hilflos ausgesetzt zu sein. Gute Ansätze hierfür sind z.B. die Diskriminierungsfreiheit bei der Datenbereitstellung gemäß Art. 9 DA, der Schutz vor missbräuchlichen Vertragsklauseln gemäß Art. 13 DA und die besonderen Informationspflichten datenaltruistischer Organisationen gemäß Art. 21 DGA.

III. Zusammenarbeitsinstrumente

Ebenfalls positiv hervorzuheben sind die Zusammenarbeitsinstrumente des Datenschutzrechts. Diese bestehen sowohl auf nationaler als auch auf europäischer Ebene. Sie helfen dabei, unionsweit kohärente Entscheidungen zu treffen. Hierdurch wird für Verantwortliche und Aufsichtsbehörden Rechtssicherheit erzielt. Aufsichtsbehörden bekommen zugleich mehr Schlagkraft verliehen, indem sie Positionen abstimmen und damit kollektiv gegenüber grenzüberschreitenden Akteuren auftreten können.

National findet diese Abstimmung über die „Datenschutzkonferenz" (DSK) der Bundes- und 17 Landesdatenschutzbeauftragten statt. Die DSK arbeitet ohne gesetzliche Verankerung auf Grundlage ihrer Geschäftsordnung[34] zusammen. Gemäß Ziffer A.IV.3. ihrer Geschäftsordnung versucht sie, einheitliche Entscheidungen herzustellen. Ihre Entscheidungen sind aufgrund des föderalen Prinzips allerdings nicht bindend.

34 Abrufbar unter https://www.datenschutzkonferenz-online.de/media/dsk/Geschaeftsordnung_DSK_Stand_Februar-2024.pdf (zuletzt abgerufen am 17.10.2025).

Auf europäischer Ebene ist die Zusammenarbeit der Aufsichtsbehörden in den Art. 60 ff. DSGVO geregelt. Auch hier ist vorgesehen, dass die Aufsichtsbehörden einen Konsens erzielen (Art. 60 Abs. 1 DSGVO) und alle zweckdienlichen Informationen austauschen (Art. 60 Abs. 2 DSGVO). Sie kommen hierfür gemäß Art. 68 Abs. 1 DSGVO im Europäischen Datenschutzausschuss („EDSA") zusammen. Der EDSA kann – anders als die DSK – gemäß Art. 65 Abs. 1 DSGVO verbindliche Beschlüsse erlassen, die für alle Europäischen Datenschutzaufsichtsbehörden Rechtswirkung entfalten. Dies ist besonders schlagkräftig in den Fällen des Art. 65 Abs. 1 lit. a DSGVO: Eine von einem Sachverhalt betroffene Aufsichtsbehörde hat demnach die Möglichkeit, gegen eine Entscheidung der federführenden Aufsichtsbehörde einen Einspruch einzulegen. Wenn dieser Einspruch abgelehnt wird, kann die betroffene Aufsichtsbehörde einen verbindlichen Beschluss durch den EDSA herbeizuführen. Dies ist in der Vergangenheit mehrfach gegenüber der irischen Aufsichtsbehörde passiert, die aus Sicht anderer Aufsichtsbehörden unzureichende Aufsichtsverfahren geführt hat, z.B. gegenüber TikTok[35] und Meta[36]. Dies unterstreicht die Machtkonzentration im EDSA, der die Möglichkeit hat, federführende Aufsichtsbehörden in ihrer Entscheidungspraxis zu überstimmen.

Gesetzliche und verbindliche Kooperationsmechanismen sollten auch im Datenwirtschaftsrecht eingeführt werden. Auch dort ist es zwingend erforderlich, dass die Aufsichtsbehörden eine einheitliche Entscheidungspraxis an den Tag legen und aufeinander einwirken können. Hierdurch stellen sie einerseits Rechtssicherheit für länderübergreifende Akteure her und treten andererseits mit größerer Schlagkraft gegenüber diesen auf.

DGA und DA sehen in ihrer aktuellen Ausgestaltung lediglich allgemeine Pflichten zu Zusammenarbeit, Informationsaustausch und Amtshilfe vor, die ergänzungsbedürftig sind:

35 Verbindlicher Beschluss 2/2023 zu dem von der irischen Aufsichtsbehörde vorgelegten Streitfall betreffend TikTok Technology Limited (Artikel 65 DSGVO), abrufbar unter https://www.edpb.europa.eu/system/files/2024-11/edpb_bindingdecision_202302_ie_sa_ttl_children_de.pdf (zuletzt abgerufen am 17.10.2025).

36 Verbindlicher Beschluss 1/2023 zu dem von der irischen Aufsichtsbehörde vorgelegten Streitfall über die Datenübermittlung durch Meta Platforms Ireland Limited für ihren Facebook-Dienst (Artikel 65 DSGVO), abrufbar unter https://www.edpb.europa.eu/system/files/2024-01/edpb_bindingdecision_202301_ie_sa_facebooktransfers_de_0.pdf (zuletzt abgerufen am 17.10.2025).

1. Zusammenarbeit unter dem DGA

Der DGA normiert eine Zusammenarbeitspflicht sowohl im Rahmen der Überwachung von Datenvermittlungsdiensten (Art. 14 Abs. 7 DGA) als auch von datenaltruistischen Organisationen (Art. 24 Abs. 6 DGA): Hat ein Akteur seine Hauptniederlassung oder seinen gesetzlichen Vertreter in einem Mitgliedstaat, erbringt aber Dienste in anderen Mitgliedstaaten, so arbeiten die jeweils zuständigen Behörden zusammen und unterstützen einander.

Die konkrete Ausgestaltung für Zusammenarbeit, Informationsaustausch und Amtshilfe überlässt der DGA dem European Data Innovation Board (EDIB). Gemäß Art. 30 lit. j DGA obliegt dem EDIB u.a. die Aufgabe, für eine „Erleichterung der Zusammenarbeit zwischen den [zuständigen Behörden] mittels Kapazitätsaufbau und Informationsaustausch […] einschließlich der Abstimmung über Gebühren und Sanktionen sowie beim internationalen Zugang zu Daten" zu sorgen.

Neben der Zusammenarbeit im EDIB verbleibt allein die Möglichkeit zum Erlass von Durchführungs- oder delegierten Rechtsakten durch den Unionsgesetzgeber.

2. Zusammenarbeit unter dem DA

Auch im DA ist die Pflicht zur Zusammenarbeit nur rudimentär geregelt. Art. 22 Abs. 1 DA legt fest, dass die Akteure, denen im Rahmen des V. Kapitels des DA Daten bereitgestellt werden, zusammenarbeiten und sich gegenseitig unterstützen. Art. 22 Abs. 3 S. 1 DA ergänzt, dass wenn ein Akteur beabsichtigt, von einem Dateninhaber in einem anderen Mitgliedstaat die Bereitstellung von Daten zu verlangen, er dies zunächst der zuständigen Behörde dessen Mitgliedstaats mitteilen muss. Das Verlangen wird sodann von der zuständigen Behörde gemäß Art. 22 Abs. 3 S. 3 DA geprüft. Nach der Prüfung übermittelt die zuständige Behörde gemäß Art. 22 Abs. 4 DA entweder das Verlangen an den Dateninhaber oder lehnt es im Einklang mit den Art. 14 ff. DA ab.

Art. 37 Abs. 2 S. 2 DA ergänzt, dass wenn ein Mitgliedstaat mehrere zuständige Behörden für die Umsetzung des DA geschaffen hat, diese „bei der Wahrnehmung [ihrer] Aufgaben und Befugnisse" zusammenarbeiten. Zudem gibt Art. 37 Abs. 5 lit. f DA den Mitgliedstaaten auf, ihre Aufsichtsbehörden dazu zu verpflichten, mit „den zuständigen Behörden anderer Mitgliedstaaten und gegebenenfalls mit der Kommission oder dem EDIB

[zusammenzuarbeiten], um die einheitliche und effiziente Anwendung [des DA] zu gewährleisten, einschließlich des unverzüglichen Austauschs aller relevanten Informationen auf elektronischem Wege".

Eine konkretere Ausgestaltung findet unterdessen auch im DA nicht statt. Sie wird – wie im DGA – dem EDIB überlassen: Gemäß Art. 42 lit. b DA unterstützt dieser die einheitliche Anwendung des DA durch die „Erleichterung der Zusammenarbeit zwischen den zuständigen Behörden durch Kapazitätsaufbau und Informationsaustausch, insbesondere durch die Festlegung von Methoden für den effizienten Austausch von Informationen über die Durchsetzung der Rechte und Pflichten […] in grenzüberschreitenden Fällen, einschließlich der Abstimmung […] von Sanktionen".

3. Summa

Diese rudimentären Zusammenarbeitsmechanismen sind ein Anfang, um einheitliche Entscheidungen und den Informationsaustausch im Datenwirtschaftsrecht voranzubringen. Ergänzend gibt es die freiwillige Zusammenarbeit von Akteuren des öffentlichen Sektors, um ihre Erkenntnisse in der Digitalregulierung auszutauschen. Ein Beispiel hierfür ist das deutsche Digital Cluster Bonn: Dort kommen regelmäßig BaFin, BfJ, BSI, BKartA, BNetzA und BfDI zusammen. Ziel des Austauschs ist das Teilen von Wissen und Erfahrungen, um eine gemeinsame Haltung zu erarbeiten, die es ermöglicht, Gesetze kohärent anzuwenden.

Doch der freiwillige Austausch von Behörden benötigt mehr Nachdruck. Die nur rudimentären Zusammenarbeitsmechanismen von DA und DGA sehen im Wesentlichen Kooperationspflichten vor. Anders als die DSGVO sehen sie jedoch keine Konsequenzen vor, wenn sich mehrere beteiligte Behörden nicht einigen können. Art. 14 Abs. 7 DGA und Art. 24 Abs. 6 DGA können im Konfliktfall allein die Konsultation des EDIB anbieten. Gleiches gilt für Art. 37 DA.

Zur nachdrücklichen Rechtsdurchsetzung – insbesondere gegenüber marktmächtigen und grenzüberschreitenden Akteuren – bedarf es auch im Datenwirtschaftsrecht der Entscheidungskompetenz eines zentralen Gremiums mit klaren gesetzlichen Verfahren. Im Interesse von beaufsichtigten Stellen und Betroffenen ergibt es außerdem Sinn, einheitliche Verwaltungsakte verschiedener Behörden vorzusehen, die im Anwendungsbereich der Digitalrechtsakte, z.B. dem DA, zusammenarbeiten müssen. Verbindliche Vorabentscheidungen nach dem Vorbild des § 89 AO wären insoweit ein weiteres Instrument, um mehr Rechtssicherheit zu gewährleisten.

Die Schwächen des inländischen deutschen Abstimmungsprozesses innerhalb der DSK belegen, dass eine bloß allgemeine Abstimmung der Behörden nicht effizient ist. Es bedarf mindestens eines Once-Only-Prinzips und Schwerpunktzuständigkeiten, um eine effiziente und vorhersehbare Aufsicht für die beaufsichtigten Akteure zu gewährleisten sowie die Kapazitäten der Behörden zu entlasten. Der Abstimmungsprozess in Europa wird durch die im Entwurf vorliegenden Verfahrensverordnung[37] konkretisiert.

IV. Zweckprivilegierungen

Ebenfalls ein positiver Aspekt des Datenschutzrechts ist, dass es bestimmte Zwecke privilegiert. Hierzu zählt insbesondere die Öffnungsklausel des Art. 89 DSGVO für Forschungs-, Statistik- und Archivzwecke. Zugleich sieht Art. 23 DSGVO für bestimmte Zwecke eine Beschränkung der Betroffenenrechte vor. Hierzu zählen z.B. die Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten (Art. 23 Abs. 1 lit. d DSGVO) und die Durchsetzung zivilrechtlicher Ansprüche (Art. 23 Abs. 1 lit. j DSGVO).

Eine solche Zweckprivilegierung empfiehlt sich auch im Datenwirtschaftsrecht. Auch hier sollten dem Allgemeinwohl dienende Zwecke gefördert und gesetzgeberisch privilegiert werden. Differenzierungen nach privilegierten Verarbeitungszwecken sind dort bislang nur ansatzweise vorgesehen: Datenaltruismus wird z.B. gemäß Art. 2 Nr. 16 DA nur zugunsten von Zielen im nationalen[38] Allgemeininteresse vorgesehen. Die Mitgliedstaaten haben insoweit die Möglichkeit, die Zwecke vorzugeben, in denen sie Datenaltruismus ermöglichen möchten. ErwGr. 45 S. 1 bis S. 3 DA führen exemplarisch Zwecke auf, z.B. Gesundheitsversorgung, Bekämpfung des Klimawandels und Mobilität. Diese Privilegierungsziele sind zwar unbestimmter als diejenigen der DSGVO, dafür aber flexibler. Eine vergleichbare Zweckprivilegierung findet sich im DA für die primäre Bereitstellung von Daten wegen außergewöhnlicher Notwendigkeit gemäß Art. 14 ff. DA. Diese setzt sich auf Sekundärebene gemäß Art. 21 Abs. 1 DA fort: Demnach dürften die bereitgestellten Daten zu Forschungs- und Statistikzwecken weitergegeben werden.

37 Verordnung des Europäischen Parlaments und des Rates zur Festlegung zusätzlicher Verfahrensregeln für die Durchsetzung der Verordnung (EU) 2016/679.

38 *Hennemann*, in: Specht/Hennemann (Hrsg.), DA DGA, 2. Aufl. 2025, Art. 16 DGA Rn. 12.

In der Gesamtschau ist die datenschutzrechtliche Privilegierung einzelner Verarbeitungszwecke zu begrüßen. Sie ist Ausfluss einer Regulierung, die für herausgehobene Zwecke regulatorische Erleichterungen bringt. Hieran sollte im Datenwirtschaftsrecht angeknüpft werden. Verbesserungspotenzial besteht insbesondere für den DGA, der im Rahmen des Datenaltruismus selbst keine Zweckprivilegierung vorsieht, sondern diese den Mitgliedstaaten vorbehält. Effizienter wäre es, wenn der DGA selbst Zweckprivilegierungen vorsähe, um einerseits zugunsten grenzüberschreitend handelnder Akteure im Binnenmarkt Rechtssicherheit zu schaffen und andererseits zu schnellerer und effizienterer Geltung zu gelangen. Dazu braucht es aber – endlich – eine politische Diskussion darüber, zu welchen Zwecken Datenverarbeitungen privilegiert werden sollen und zu welchen Zwecken eben nicht.

V. Zusammenspiel aus private und public enforcement

Ein weiterer Vorteil des Datenschutzrechts ist die gesetzliche Verankerung von private enforcement, welches rechtsaktübergreifend zunehmend Eingang in das Unionssekundärrecht findet.

Dem Datenwirtschaftsrecht fehlt das Element des private enforcement weitestgehend[39]: Der DA sieht private enforcement zwar implizit vor[40], indem er in Art. 10 Abs. 13 DA im Kontext der Streitbeilegung vorsieht, dass diese „nicht das Recht der Parteien [berührt], wirksame Rechtsmittel bei einem Gericht eines Mitgliedstaats einzulegen“[41]. Es gibt im DA insoweit zivilrechtlich einklagbare Primäransprüche wie z.B. in Art. 3 ff. DA für den Datenzugang[42]. Dies gilt jedoch nicht für den Sekundärbereich, wenn Primärpflichten nicht erfüllt werden. Hier fehlt es an einem unionsweit harmonisierten Kompensationsinstrument, um z.B. Schäden aufgrund einer unterlassenen Datenbereitstellung einheitlich auszugleichen und nicht auf das divergierende mitgliedstaatliche Recht ausweichen zu müssen. Daher ist im DA auf das jeweils anwendbare nationale Recht zurückzugreifen, ins-

39 *Hennemann/Steinrötter*, NJW 2024, 1 (8).
40 A.A. *Schwamberger*, in: Specht/Hennemann (Hrsg.), DA DGA, 2. Aufl. 2025, Art. 37 DA Rn. 63.
41 *Schulz*, NZKart 2024, 426 (429).
42 *Hennemann/Steinrötter*, NJW 2024, 1 (8); *Wiebe*, GRUR 2023, 1569 (1570 ff.).

besondere das Vertrags-, Lauterkeits- und Deliktsrecht[43]. Der DGA äußert sich gar nicht zum private enforcement[44], sodass auch hier auf nationales Recht zurückzugreifen ist.

Wann im Unionssekundärrecht neben public enforcement zugleich private enforcement erforderlich ist, lässt sich der Rechtsprechung des EuGH[45] entnehmen: Dies ist immer dann der Fall, wenn das vorhandene public enforcement für die Effektivität der Durchsetzung nicht ausreicht[46]. Vollzugsdefizite der öffentlichen Hand im Rahmen des public enforcement, z.B. aufgrund von Kapazitätsengpässen, sind zwecks Kohärenz und Effizienz insoweit zwingend durch private Rechtsdurchsetzungsinstrumente zu ergänzen[47]. Diese haben zugleich den Vorteil, dass die Anspruchsteller unmittelbar von ihnen profitieren, z.B. durch Schadensersatzzahlungen, und insoweit ein höherer Anreiz zur Rechtsdurchsetzung besteht.

Die Gefahr eines ineffizienten public enforcement sah der Gesetzgeber auch im Datenschutzrecht – aufgrund der schieren Masse an tagtäglich stattfindenden Datenverarbeitungen vollkommen zu Recht – auf die Aufsichtsbehörden zukommen und führte daher richtigerweise Instrumente des private enforcement ein. Es steht begründet zu erwarten, dass entsprechende Vollzugsdefizite sich gleichermaßen im Datenwirtschaftsrecht zutragen werden. Folglich ist es die Aufgabe des Gesetzgebers, Instrumente des private enforcement auch dort zu implementieren.

Es bleibt zu beobachten, ob das public enforcement des Datenwirtschaftsrechts, das es in Art. 40 DA und Art. 34 DGA bei einem Verweis auf mitgliedstaatliche Sanktionen belässt, in seiner Effizienz mit dem Datenschutzrecht vergleichbar sein wird. Auch hier wäre ein unionsweit harmonisiertes Sanktionsregime wünschenswert, das von den nationalen Aufsichtsbehörden umgesetzt wird. Die nationalen Gerichte hätten die Möglichkeit, wie im Datenschutzrecht[48], auf der Basis von Vorabentschei-

43 *Determann*, in: Specht/Hennemann (Hrsg.), DA DGA, 2. Aufl. 2025, Einl. H. III.
44 *Schröder*, in: BeckOK Datenschutzrecht, Stand: 01.11.2024, Art. 12 DGA Rn. 89; *Schemmel*, in: BeckOK Datenschutzrecht, Stand: 01.11.2024, Art. 34 DGA Rn. 8.
45 EuGH, Urt. v. 16.2.2017, C-219/15, NJW 2017, 1161 – TÜV Rheinland.
46 *Schwamberger*, in: Specht/Hennemann (Hrsg.), DA DGA, 2. Aufl. 2025, Art. 37 DA Rn. 65.
47 *Richter*, ZEuP 2021, 634 (657 ff.); *Schröder*, in: BeckOK Datenschutzrecht, Stand: 01.11.2024, Art. 12 DGA Rn. 88; *Schemmel*, in: BeckOK Datenschutzrecht, Stand: 01.11.2024, Art. 34 DGA Rn. 9.
48 Vgl. im Überblick zu datenschutzrechtlichen Vorabentscheidungsverfahren *Leibold*, ZD-Aktuell 2025, 01156.

dungsverfahren gemäß Art. 267 AEUV unionsweit für eine einheitliche Entscheidungspraxis zu sorgen. Die in den letzten Jahren orchestrierende Judikatur[49] zum privatrechtlichen Schadensersatzanspruch gemäß Art. 82 Abs. 1 DSGVO belegt, welch signifikante Vorteile eine solche Vereinheitlichung mit sich bringt, indem von Anfang an für eine effiziente und vorhersehbare Rechtsdurchsetzung im Sinne aller beteiligten Akteure gesorgt wird.

D. Was Datenschutz- und Datenwirtschaftsrecht nur gemeinsam lernen können

Schließlich gibt es drei Themenkomplexe, die Datenschutz- und Datenwirtschaftsrecht nur gemeinsam lernen können, da sie hier an verwandten Mängeln leiden: Dies betrifft die Orchestrierung der Digitalrechtsakte (I.), die Verwendung von Öffnungsklauseln (II.) und die Präzisierung der Normgebung (III.).

I. Orchestrierung der Digitalrechtsakte

Wie eingangs bereits erläutert sind Datenschutz- und Datenwirtschaftsrecht eng miteinander verzahnt. Doch ihr Verhältnis ist legislativ nicht hinreichend vorgezeichnet.

DA, DGA und weitere Digitalrechtsakte lassen die DSGVO nämlich ausweislich ihres Normtextes unberührt, also parallel anwendbar. So sieht Art. 1 Abs. 5 DA vor, dass der DA „unbeschadet" der DSGVO gilt (S. 1) und im Falle eines Widerspruchs die DSGVO Vorrang genießt (S. 3). Parallel sieht Art. 1 Abs. 3 DGA vor, dass der DGA „unbeschadet" der DSGVO gilt (S. 2) und im Konfliktfall die DSGVO Vorrang genießt (S. 3).

Doch sitzt das Problem des Konfliktverhältnisses zwischen Datenschutz- und Datenwirtschaftsrecht tiefer, als der Wortlaut vermuten lässt: Kein Digitalrechtsakt lässt die DSGVO „unberührt". Sobald eine Nutzung personenbezogener Daten erfolgt, ist die DSGVO berührt. Nicht beantwortet werden Fragen nach der Zulässigkeit einer Ausfüllung der datenschutzrechtlichen Öffnungs- und Konkretisierungsklauseln durch das Datenwirtschaftsrecht sowie nach der Auslegung datenschutzrechtlicher Rechtsbegriffe und Interessenabwägungen mittels des Datenwirtschaftsrechts.

49 Vgl. im Überblick: *Schneider/Lennartz/Banken*, CR 2024, 450 ff.

Richtig ist daher: Nur im Konfliktfall wollte der Gesetzgeber einen Vorrang des Datenschutzrechts vorsehen. Wann ein Konflikt zwischen zwei EU-Rechtsakten – und somit auch zwischen Datenschutz- und Datenwirtschaftsrecht – vorliegt, kann der Rechtsprechung des EuGH entnommen werden[50]: Er entschied zur UGP-RL, dass ein Konflikt zwischen zwei EU-Rechtsakten vorliegt, wenn zwischen den Rechtsakten eine Divergenz besteht, die „unmöglich durch eine auf Ausgleich gerichtete Formel überwunden werden kann"[51]. Das bedeutet, dass wo immer ein widerspruchsfreies Kooperationsverhältnis zwischen der DSGVO und einem Digitalrechtsakt hergestellt werden kann, kein Konfliktfall besteht. Dies ist z.B. der Fall, wenn die DSGVO sich für eine solche Kooperation mittels Öffnungs- und Konkretisierungsklauseln offen zeigt oder ein Digitalrechtsakt unbestimmte Rechtsbegriffe bzw. Abwägungsklauseln der DSGVO ausfüllt[52]. Ein Konfliktfall liegt hingegen in zwei Fällen vor: Erstens, wenn ein Digitalrechtsakt weniger strengere Anforderungen an eine Verarbeitung personenbezogener Daten als die DSGVO stellt, und die DSGVO hierfür keine Öffnungsklausel vorsieht. Zweitens, wenn ein Digitalrechtsakt andere Voraussetzungen an eine Verarbeitung personenbezogener Daten stellt und dabei die Vorgaben der DSGVO abbedingen will, ohne dass die DSGVO hierfür eine Öffnungsklausel vorsieht. Die DSGVO geht in diesen Fällen vor[53].

Die skizzierte Systematik zeigt: Das Verhältnis zwischen Datenschutz- und Datenwirtschaftsrecht ist zwar mit den Gesetzestexten der Digitalrechtsakte und der Rechtsprechung des EuGH in den Griff zu bekommen. Erforderlich ist allerdings stets eine Einzelfallentscheidung, die weitere Rechtsunsicherheit in den Binnenmarkt bringt. Deshalb ist eine bessere Abstimmung der Rechtsakte untereinander und die konkrete Beantwortung der aufgeworfenen Fragen zum Verhältnis von Datenschutz- und Datenwirtschaftsrecht durch den Gesetzgeber sinnvoll. Es bedarf einer kohärenten Gesetzgebung, die beide Rechtsgebiete miteinander versöhnt. Solange diese nicht erreicht ist, ist es die Aufgabe von Datenschutz- und Datenwirtschaftsaufsicht, durch ständige Kooperation, Austausch und Abstimmung beide Rechtsgebiete in Einklang zu bringen.

50 Vgl. eingehend zum Nachfolgenden *Hennemann/Specht*, in: Specht/Hennemann (Hrsg.), DA DGA, 2. Aufl. 2025, Einl. und Art. 1 DA.
51 EuGH, Urt. v. 04.10.2018, C-105/17, MMR 2019, 101 Rn. 60.
52 *Specht-Riemenschneider*, ZEuP 2023, 638 (647 ff.).
53 *Specht-Riemenschneider*, ZEuP 2023, 638 (647 ff.).

II. Öffnungsklauseln

Erfreulicherweise kommen die Rechtsakte des Datenwirtschaftsrechts mit äußert wenig Öffnungsklauseln aus. Während die DSGVO ganze 69 Stück bereithält, müssen diese in DGA und DA mit der Lupe gesucht werden. Art. 2 Nr. 16 DGA und Art. 16 DGA sehen mitgliedstaatliche Regelungen z.B. für Datenaltruismus vor, und Art. 40 Abs. 1 S. 1 DA erlaubt den Mitgliedstaatlichen den Erlass von Sanktionen bei Verstößen gegen den DA.

Dennoch sind Öffnungsklauseln im Sinne der bezweckten Harmonisierung des EU-Digitalrechts kritisch zu sehen. Sie schaffen Rechtsunsicherheit. Es bedarf – soweit wie möglich – einer Verantwortungsübernahme des Gesetzgebers. Insbesondere für regulierte Akteure, die in mehr als einem Mitgliedstaat tätig sind, bedarf es für eine nachvollziehbare Regulierung mehr Vereinheitlichung. Ein gutes Beispiel hierfür ist die Öffnungsklausel des Art. 40 Abs. 1 S. 1 DA für mitgliedstaatliche Sanktionen: Wieso ist dies nötig? Der Schadensersatzanspruch nach Art. 82 Abs. 1 DSGVO ist ein Musterbeispiel dafür, wie ein zentraler Anspruch des Unionssekundärrechts durch Vorabentscheidungsverfahren vor dem EuGH gemäß Art. 267 AEUV unionsweit einheitlich und rechtssicher ausgelegt wird. Gleiches gilt für die Öffnungsklausel des Art. 16 DGA bezüglich Datenaltruismus: Wieso legt der Unionsgesetzgeber nicht selbst die Zwecke fest, in denen dieser praktiziert werden darf?

III. Präzisierung der Normgebung

Abschließend ist die Präzisierung der Normgebung anzuführen. Während die Technologieoffenheit und die Abstraktheit der DSGVO grundsätzlich zu begrüßen sind, um im Einzelfall interessengerechte Ergebnisse zu erzielen, sollte die DSGVO sich dennoch nicht an allen Stellen vage halten. Sie sollte, wo möglich, klare Aussagen treffen. Das schafft sie bereits gut z.B. in den inhaltlichen Vorgaben für Auftragsverarbeitungsverträge in Art. 28 Abs. 3 DSGVO. Dennoch besteht Verbesserungsbedarf: Es wäre von Vorteil, beispielsweise den Streit[54] um die Inhalte der Vereinbarung gemeinsam Verantwortlicher gemäß Art. 26 Abs. 1 S. 2 DSGVO dadurch zu lösen, dass nach dem Vorbild des Art. 28 Abs. 3 DSGVO qua Gesetz dessen Inhalte

54 Vgl. eingehend zu den formellen wie materiellen Ausgestaltungsmöglichkeiten *Schneider*, Gemeinsame Verantwortlichkeit, 2021, S. 113 ff.

vorgezeichnet werden. Ebenso könnte die allgemeingehaltene Interessenabwägung des Art. 6 Abs. 1 lit. f DSGVO dahingehend konkretisiert werden, dass bestimmte Verarbeitungsszenarien gesetzlich erlaubt oder verboten werden bzw. jedenfalls Kriterien für die Durchführung der Interessenabwägung qua Gesetz vorgesehen werden[55]. Eine solche Tendenz findet sich z.B. auch in Art. 13 Abs. 4 und Abs. 5 DA, die konkrete Beispiele für missbräuchliche Vertragsklauseln in Bezug auf Datenzugang und Datennutzung regeln. Auch in Großbritannien geht man diesen Weg der Konkretisierung, indem die Data Use and Access Bill z.B. in Ziffer 74 vorsieht, dass per Gesetz bestimmte Verarbeitungsszenarien sensibler Daten legitimiert oder untersagt werden können. Ähnlich geht man in der Schweiz vor, wo Art. 31 Abs. 2 DSG qua Gesetz das Ergebnis von Interessenabwägungen zur Legitimation bestimmter Verarbeitungsszenarien vorzeichnet.

Doch bietet auch das Datenwirtschaftsrecht Raum für mehr Präzision in der Normgebung: Exemplarisch anzuführen seien hier nur die äußerst abstrakt gehaltenen Modalitäten, unter denen ein Dateninhaber einem Nutzer gemäß Art. 4 Abs. 1 DA Daten bereitstellen muss. Der Unionsgesetzgeber hat hier nicht von den rechtlichen Unsicherheiten, die mit einer Vielzahl von unbestimmten Rechtsbegriffen innerhalb einer Definition ausgehen, wie sie sich z.B. für die datenschutzrechtliche Einwilligung darstellt, gelernt, sondern sich nochmals selbst übertroffen: Gemäß Art. 4 Abs. 1 DA hat der Dateninhaber dem Nutzer die Daten „unverzüglich, einfach, sicher, unentgeltlich, in einem umfassenden, gängigen und maschinenlesbaren Format und – falls relevant und technisch durchführbar – in der gleichen Qualität wie für den Dateninhaber kontinuierlich und in Echtzeit" bereitzustellen. Diese Umschreibung ist maximal rechtsanwenderunfreundlich und wird zwingenderweise zu divergierenden Auslegungen durch verschiedene Gerichte und Aufsichtsbehörden führen. Der DGA ist hier einen Schritt weiter und anwenderfreundlicher: Er ist erfreulich konkret gehalten, z.B. in den Bedingungen für die Weiterverarbeitung von Daten gemäß Art. 3 ff. DGA und für die Erbringung von Datenvermittlungsdiensten gemäß Art. 12 DGA sowie in den allgemeinen Eintragungserfordernissen datenaltruistischer Organisationen.

55 Vgl. mit ähnlichen Ansätzen der Entwurf von *Wendehorst* für eine KI-Datenschutz-VO, die z.B. bestimmte Verarbeitungsszenarien qua Gesetz verbietet und gesetzliche Kriterien für die Interessenabwägung zur Legitimation von Datenverarbeitungen zwecks KI-Training vorsieht: https://zivilrecht.univie.ac.at/fileadmin/user_upload/i_zivilrecht/Wendehorst/Workshop_Datenschutz/Draft_AI_Data_Protection_Regulation_WENDEHORST_24-12-20.pdf (zuletzt abgerufen am 17.10.2025).

E. Fazit

Die vorhergehende Untersuchung zeigt auf: Datenschutz- und Datenwirtschaftsrecht können noch viel voneinander lernen und miteinander erwachsen werden.

Nicht orientieren sollte sich das Datenwirtschaftsrecht an der Unbestimmtheit, Uneinsichtigkeit und Formalität, die das Datenschutzrecht an vielen Stellen prägen. Der Gesetzgeber sollte auf eine präzise Normgebung achten, die mit den Lebensrealitäten der verschiedenen Akteure übereinstimmt, um interessengerechte Ergebnisse zu erzielen und Auslegungsstreitigkeiten vorzubeugen.

Doch das Datenschutzrecht bietet zugleich nachahmenswerte Aspekte: Auch im Datenwirtschaftsrecht sollte an Hilfestellungen für die Rechtsanwender festgehalten, der Schutz der Schwächeren im Blick behalten, an die Zusammenarbeitsmechanismen des Datenschutzrechts angeknüpft sowie dessen Zweckprivilegierungen und private enforcement nachgeahmt werden.

Schließlich gibt es Punkte, die Datenschutz- und Datenwirtschaftsrecht nur gemeinsam lernen können: Dies betrifft die bessere Abstimmung der Digitalrechtsakte untereinander, um dem Rechtsanwender die Navigation durch das EU-Digitalrecht zu erleichtern. Zudem sollte der Unionsgesetzgeber insgesamt zurückhaltender von Öffnungsklauseln Gebrauch machen und auf eine präzise Normgebung achten.

Vieles das ausgearbeiteten Verbesserungspotenzials kann durch den Gesetzgeber aufgegriffen und gelöst werden. Doch das geht nicht von heute auf morgen. Bis zu einer finalen Lösung bedarf es einer Selbstregulierung durch Abstimmung der Behörden, einen proaktiven und kommunikativen Beratungsansatz der Behörden sowie den Dialog in und mit Branchenverbänden, um interessengerechte Leitlinien und Best Practices für alle Rechtsanwender zu schaffen.

Informationelle Sozialpflichtigkeit

Kai von Lewinski[*]

Der Staat greift in großer Not oder jedenfalls bei außergewöhnlicher Notwendigkeit auf Daten Privater zu – das ist das Szenario der Art. 14 bis 22 des EU-Datengesetzes (Data Act, DA)[1]. Was uns in diesen Ausnah-

* Kai von Lewinski ist Inhaber des Lehrstuhls für Öffentliches Recht, Medien- und Informationsrecht an der Universität Passau. Der Verf. dankt seinem Assistenten Wiss. Mit. *Peer Sonnenberg* für die Unterstützung bei dem Beitrag und für die sehr hilfreichen kritischen Diskussionen.

1 Verordnung (EU) 2023/2854 des Europäischen Parlaments und des Rates v. 13.12.2023 über harmonisierte Vorschriften für einen fairen Datenzugang und eine faire Daten-

mefällen sehr plausibel vorkommt und uns – nebenbei – an die Polizeipflichtigkeit des Nichtstörers aus dem Studium erinnert[2], führt zu einer grundrechtssystematischen Frage: Geht es beim Schutz von Daten um Eigentum[3]? Während die genaue dogmatische Antwort auf der einfachgesetzlichen bzw. sekundärrechtlichen Ebene angesichts der ausführlichen Regelungen des Data Act zunächst dahinstehen kann, stellt sich bei genauerem Hinsehen dann doch die grundsätzliche Frage, ob hier das Informationelle Selbstbestimmungsrecht (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG) einschlägig ist oder Art. 14 GG bzw. in unserer europäisierten Datenwelt das Datenschutzgrundrecht des Art. 8 GRCh oder der Eigentumsschutz des Art. 17 GRCh[4].

Kapitel V der VO (EU) 2023/2854, also die Art. 14–22 Data Act (DA), beantwortet diese grundlegende rechtskonzeptionelle und solchermaßen auch grundrechtsdogmatische Frage nicht[5]. Bei den Datenbereitstellungsverpflichtungen handelt es sich um fremd- bzw. gemeinschaftsnützige Grundrechtseingriffe. Diese könnte man als „informationelle Sozialpflichtigkeit[6]“ bezeichnen. Als Begriff wäre das (jedenfalls) für die deutsche Grundrechtsdogmatik recht anschlussfähig, einmal in Richtung des Eigentumsgrundrechts (insb. Art. 14 Abs. 1 S. 2 u. Abs. 2 GG), dann aber auch in Richtung Informationelle Selbstbestimmung (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG). Zudem gäbe es in den europäischen Grundrechten hierfür normtextliche Anknüpfungsstellen (Art. 8 Abs. 2 S. 1 GRCh: Personenbezogene „Daten dürfen nur […] auf einer […] gesetzlichen geregelten legitimen Grundlage verarbeitet werden.“; Art. 17 Abs. 1 S. 2 u. 3 GRCh: „Niemandem darf sein Eigentum entzogen werden, es sei denn aus Gründen des öffentlichen Interesses[.] Die Nutzung des Eigentums kann gesetzlich geregelt werden, soweit dies für das Wohl der Allgemeinheit erforderlich ist.“).

---

nutzung sowie zur Änderung der Verordnung (EU) 2017/2394 und der Richtlinie (EU) 2020/1828 (Datenverordnung) (ABl. EU L v. 22.12.2023).

2 Z.B. *Erbel*, JuS 1985, 257 ff.

3 Erster Problemaufriss bei *v. Lewinski*, in: Specht/Hennemann (Hrsg.), DGA/DA, 2. Aufl. 2025, Art. 14 DA Rn. 49.

4 Diese grundrechtsdogmatische Frage der Grundrechte im Mehrebenensystem soll hier einstweilen offenbleiben. Sie ist angesichts des Art. 345 AEUV, der die Eigentumsordnung der Mitgliedstaaten ausdrücklich unberührt lässt, zweifellos eine Doktorfrage, v.a. in Verbindung mit der BVerfG-Rechtsprechung (BVerfGE 152, 152 ff. – Recht auf Vergessen I).

5 *v. Lewinski*, in: Specht/Hennemann (Hrsg.), DGA/DA, 2. Aufl. 2025, Art. 14 DA Rn. 49.

6 *v. Lewinski*, in: Auerhammer (Hrsg.), DSGVO/BDSG, 8. Aufl. 2024, Einf. Rn. 32; ähnlich schon *ders.*, Auernhammer (Hrsg.), DSGVO/BDSG, 5. Aufl. 2017, Einf. Rn. 30: „informationelle Sozialbindung“.

A. Einführung

Doch: „Dateneigentum gibt es nicht!“[7], „Daten sind keine Ware“[8] – so hieß es jahrelang im Datenschutz[9] und heißt es mit Blick auf dessen persönlichkeitsrechtliche Verwurzelung noch immer[10]. Und mit dem Schutz unternehmensbezogener Daten, um die es im Kontext des DA ganz hauptsächlich geht, beschäftigt sich der Datenschutz schon mal gar nicht – Unternehmen stehen in der festgefügten Welt des Datenschutzes ja auf der „anderen Seite“.

Aus der Ecke des Immaterialgüterrechts kann dem aber entgegengehalten werden, dass immaterielles, „geistiges“ Eigentum gerade auch in einem wirtschaftlichen Kontext sehr wohl möglich ist, wie seit über 150 Jahren in Gestalt der (inzwischen revidierten) Berner Übereinkunft (RBÜ[11]) und vieler weiterer Abkommen über den gesamten Erdball[12] zu besichtigen ist. Auch werden in der Wissenschaft zunehmend Begründungsansätze für ein Dateneigentum diskutiert[13].

Wenn wir nun die grundrechtliche Brille aufsetzen, dann sehen wir zwei unterschiedliche Bilder. Denn diese grundrechtliche Brille ist durch unsere dogmatische Vorprägung in einerseits Eigentumsgrundrecht und andererseits Datenschutzgrundrecht eine Art 3D-Brille, durch die das eine Auge dies und das andere jenes wahrnimmt. Das eine sieht eigentumsgrundrechtlich, das andere datenschutzrechtlich. Das soll nicht als Sehbehinderung aufgefasst werden, sondern als Möglichkeit, unseren Gegenstand plastisch und auch in der Tiefendimension zu erfassen.

---

7 Zum (dogmatischen wie rechtspolitischen) Streitstand zum Dateneigentum vor Einführung des Data Acts, s. ausführlich *Kühling/Sackmann*, ZD 2020, 24 f., die schon rechtspolitisch die Einführung eines Datengesetzes (als Inhalts- und Schrankenbestimmung) ablehnen; *Zech*, Information als Schutzgegenstand, 2012, S. 215 ff.; *v. Lewinski/Rüpke/Eckhardt*, Datenschutzrecht, 3. Aufl. 2025, § 3 Rn. 17h Rn. 65 m.w.N.

8 Kritisch insb. *Simitis*, NJW 1998, 2473 (2477); vgl. aber *v. Lewinski/Rüpke/Eckhardt*, Datenschutzrecht, 3. Aufl. 2025, § 13 Rn. 28 f.

9 BVerfG, Urt. v. 15.12.1983 – 1 BvR 209/83 u.a., BVerfGE 65, 1, 43 f. – Volkszählung; vgl. *v. Lewinski*, Die Matrix des Datenschutzes, 2014, S. 53 f.; dafür aber z.B. *Fezer*, MMR 2017, S. 3 ff.

10 Zur Diskussion *Buchner*, Informationelle Selbstbestimmung im Privatrecht, 2006, S. 184 ff.

11 Berner Übereinkunft zum Schutz von Werken der Literatur und Kunst v. 9.9.1886 (RGBl. 1887 S. 493).

12 S. nur *Schack*, Urheber- und Urhebervertragsrecht, 10. Aufl. 2021, § 27.

13 Z.B. *Amstutz*, AcP 218 (2018), 438 ff. (Dateneigentum als Sacheigentum); *Hoeren*, MMR 2019, 5 ff. (Datenbesitz als Dateneigentum).

Dieser Beitrag will zunächst durch das eine und dann durch das andere Brillenglas schauen. Zunächst wird „Dateneigentum" durch die Linse des Art. 14 GG und des Art. 17 GRCh fokussiert (→ B.). Dann wird geschaut, ob das Konzept von „Informationeller Selbstbestimmung" (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG) und „Datenschutz" (Art. 8 GRCh) auch auf juristische Personen ausgedehnt werden und für nicht-personenbezogene Daten von Unternehmen eine taugliche Antwort geben kann (→ C.). Schließlich wird eine Synthese dieser beiden grundrechtlichen Sichtweisen versucht (→ D.), um damit die Problemlage, die sich beim hoheitlichen Zugriff auf Daten diesseits und jenseits des Ausnahmefalls ergibt, passend adressieren zu können.

B. Informationelle Elemente des Eigentumsgrundrechts

„Eigentum" ist in unserer Vorstellung ursprünglich anfassbar und material und besitzhaft[14]. Schon das Raubtier verteidigt „seine" Beute, der Höhlenmensch wird es genauso gemacht haben, das Kind im Kindergarten hinsichtlich seines Spielzeugs ebenso. Doch ist Eigentum nicht notwendigerweise tangibel, sondern kann durchaus immaterial sein (II.). Für unsere Perspektive besonders spannend sind die Inhalts- und Schrankenbestimmungen, die sich auch auf informationelle Aspekte beziehen und dadurch belegen, dass Eigentum durchaus eine informatische Komponente hat (III.). Auffällig ist der Befund, dass bislang – soweit ersichtlich – noch kein prominenter Fall von „Datenenteignung" (IV.) die juristische Öffentlichkeit oder gar die Gerichte erreicht hätte.

I. Vorfrage: Abgrenzung von Inhalts- zu Schrankenbestimmungen

Die Ausgestaltung von Eigentum wird überkommenerweise mit dem Begriffspaar „Inhalts- und Schrankenbestimmungen" (vgl. Art. 14 Abs. 1 S. 2 GG) bezeichnet, deren genaue Unterscheidung und Abgrenzung überraschend wenig beleuchtet wird.

14 Dass deutsche Juristen und Zivilrechtler kategorial zwischen Eigentum und Besitz unterscheiden, ist hierbei natürlich nicht übersehen.

Soweit ersichtlich, wird im Schrifttum die Abgrenzung zwischen Inhalts- und Schrankenbestimmungen als ein Streit ohne tiefergehende rechtsdogmatische Bedeutung angesehen, da es letztendlich egal sei, ob das Eigentum streng definiert wird oder ihm strenge Grenzen gezogen werden; im Ergebnis wird damit das Problem regelmäßig auf die Eingriffsebene verschoben[15]. Wenn dies überhaupt diskutiert und begründet wird, sehen die einen in jeder inhaltlichen Begrenzung des normgeprägten Eigentums zugleich eine Bestimmung dessen Inhalts; dogmatisch handele es sich nach dieser Sichtweise um eine einheitliche Konstituierung des Eigentums[16]. Andere meinen, Inhalts- und Schrankenbestimmung beträfen jeweils eigene Funktionsbereiche: Während die Inhaltsnorm das Eigentum und verbundene Befugnisse konstituiere, beinhalteten Schrankenbestimmungen Handlungs-, Unterlassungs-, und Duldungspflichten[17]. In der Konsequenz bilde die Institutsgarantie die primäre Grenze der Inhaltsbestimmung und das Übermaßverbot die primäre Grenze der Schrankenbestimmung. Vermittelnd wird vorgeschlagen, sowohl Inhalts- als auch Schrankenbestimmung als Begriffe der Eingriffsdogmatik zu verstehen, da auch Inhaltsbestimmungen als abstrakt-generelle Regelungen grundrechtlich geschützte Positionen beschränken können[18].

Auch wenn eine vertiefte Begründung an anderer Stelle erfolgen muss, wird hier eine am Wortlaut orientierte Auslegung vertreten. Entsprechend ihrer Funktionsbereiche konstituiert die Inhaltsbestimmung nach hier vertretener Auffassung den Schutzbereich und die Schrankenbestimmung die Schranken in Form von (informationellen) Handlungs-, Unterlassungs- und Duldungspflichten.

II. Inhaltsbestimmung durch den Gesetzgeber

Der Gesetzgeber kann nicht nur Dateneigentum schaffen, sondern es auch daten- und informationsbezogen ausgestalten. Damit sind nicht die Inhalts-

15 *Papier/Shirvani*, in: Dürig/Herzog/Scholz (Hrsg.), Grundgesetz, 104. ErgLfg. 2024, Art. 14 GG Rn. 417; a.A. *v. Lewinski*, Der Staat 59 (2020), 277 (284).

16 *Wieland*, in: Dreier (Hrsg.), Grundgesetz, 3. Aufl., 2018, Art. 14 Rn. 92 m.w.N.; ähnlich jetzt *Kempny,* in: Dreier (Hrsg.), Grundgesetz, 4. Aufl. 2023, Art. 14 Rn. 181.

17 *Wendt*, in: Sachs (Hrsg.), Grundgesetz, 8. Aufl. 2018, Art. 14 Rn. 55 m.w.N.

18 So wohl *Sieckmann*, in: Friauf/Höfling (Hrsg.), Berliner Kommentar, Bd. 5, 44. ErgLfg. 2014, Art. 14 Rn. 104 f.

und Schrankenbestimmungen von Dateneigentum gemeint, sondern datenbezogene Inhalts- und Schrankenbestimmungen von Eigentum gleich welcher Art.

Jedenfalls ist weder jedes Immaterialgut verfassungshoch und primärrechtlich geschützt, noch wäre alles, an dessen Schutz es ein Interesse gibt, stets Eigentum. Vielmehr ist die inhaltliche Ausgestaltung des Eigentums, die Umreißung seines Schutzbereichs, dem einfachen Gesetzgeber überlassen (Normgeprägtheit des Eigentums). Art. 14 Abs. 1 S. 2 Var. 1 GG formuliert das ausdrücklich so, in Art. 17 Abs. 1 GRCh findet dies einen Ausdruck durch die Qualifikation des geschützten Eigentums, nämlich des „rechtmäßig erworbenen".

I. Eigentum durch Daten

Es ist uns gut vertraut, dass Eigentum konkret teilweise erst dadurch entsteht, dass Informationen fließen oder Daten an den Staat gegeben werden. Eigentum wird oft informationell dadurch manifest, dass es besonders gesichert und dokumentiert werden muss. Das landläufige Instrument hierfür sind Register, wie sie vor allem für das Grundeigentum wie auch für Immaterialgüter verbreitet sind.

Eigentum an Grundstücken ist nur durch Grundbucheintrag möglich (§ 873 BGB i.V.m. § 13 GBO). Und selbst die Aufgabe des Eigentums muss vermerkt sein (§ 875 BGB). Ohne Eintragung erwirbt man kein „Grundeigentum". Es müssen also Daten fließen und verarbeitet werden.

Gewerbliche Schutzrechte müssen, damit ihre Schutzwirkung entsteht, ebenfalls bei einer öffentlichen Stelle (Patent- und Markenämter) gemeldet werden[19]. Ein anschauliches Beispiel ist das Markenrecht: Die für Art. 14 GG maßgebliche Ausschließlichkeitsfunktion des Markenschutzes ergibt sich einfachgesetzlich aus § 14 i.V.m. § 4 MarkenG, wenn dort tatbestandlich die Eintragung vorausgesetzt wird. Fehlt diese, fehlt es gleichzeitig an einem ausschließlichen Schutzgut im Sinne eines vermögenswerten Rechts nach Art. 14 Abs. 1 GG. „Eigentum" ohne Anmeldung entsteht gar nicht erst.

19 § 9 i.V.m. § 34 Abs. 1 PatG; § 14 Abs. 1 i.V.m. § 4 MarkenG; § 27 Abs. 1 DesignG; § 11 GebrMG; § 5 Abs. 1 Nr. 2 HalblSchG; § 1 Abs. 1, § 16 Abs. 2, § 8 Abs, 1 u. § 22 Abs. 1 SortSchG.

Die Liste der Beispiele lässt sich weiter verlängern: So fällt die Bergbauberechtigung nach §§ 7–9 BBergG ebenso wie etwa das Jagd- und Fischereirecht sowie altrechtliches Wasserrecht[20] in den Schutzbereich von Art. 14 GG[21]. Diese Rechtspositionen werden nur aufgrund eines vorangegangenen Antrages (z.B. § 10 BBergG) erteilt und verliehen. Ein solcher Antrag muss notwendigerweise Angaben über das begehrte vermögenswerte Recht enthalten, so dass auch hier Daten fließen und Information verarbeitet werden muss.

2. Immaterialgüter als Eigentum

Es ist unstreitig, dass der primär- und verfassungsrechtliche Eigentumsbegriff weiter ist als der zivilrechtliche Sacheigentumsbegriff und auch Immaterialgüterrechte einschließt[22]. Was sich beim Grundgesetz nicht direkt aus dem Normtext ergibt, aber in der Sache unbestritten ist, kann im Absatz 2 von Art. 17 GRCh ausdrücklich nachgelesen werden: „Geistiges Eigentum wird geschützt[23]."

Doch weder bei den körperlichen Sachen noch bei Immaterialgütern ist alles und immer geschützt und geschützt gewesen. Selbst bestimmte körperliche Sachen sind zivil- und eigentumsgrundrechtlich nicht eigentumsfähig[24]. Nicht-körperliche Gegenständen sind überhaupt erst im 19. und 20. Jahrhundert als rechtliche Kategorie entdeckt worden, ihr Schutz(umfang) wird in der Tendenz durch den Gesetzgeber immer noch

20 BVerfG, Beschl. v. 24.2.2010 – 1 BvR 27/09, SächsVBl. 2010, 140 ff. – Alte Wasserrechte konnten nach § 21 Abs. 1 WHG vom Inhaber angemeldet werden, damit sie im Wasserbuch anerkannt werden. Eine rechtliche Pflicht hierzu bestand nicht, eine Nichtanmeldung führte aber zum Erlöschen.

21 *Papier/Shirvani*, in: Dürig/Herzog/Scholz (Hrsg.), Grundgesetz, 104. ErgLfg. 2024, Art. 14 Rn. 324 ff.

22 BVerfGE 95, 267 (300); *Papier/Shirvani*, in: Dürig/Herzog/Scholz (Hrsg.), Grundgesetz, 104. ErgLfg. 2024, Art. 14 Rn. 160; *Dederer*, in: Kahl/Waldhoff/Walter (Hrsg.), Bonner Kommentar, Bd. 5, 188. ErgLfg. 2017, Art. 14 (Eigentum), Rn. 8, 75; *Depenheuer/Froese*, in: Huber/Voßkuhle (Hrsg.), Grundgesetz, Bd. 1, 8. Aufl. 2024, Art. 14 Rn. 114 f., 148.

23 *Buschmann*, EuGH und Eigentumsgarantie, 2017, S. 99.

24 Zu nennen wären hier beispielsweise Körperteile (inkl. Leichen), Zellen, mangels Grundrechtsträgerschaft öffentliches Eigentum (etwa Art. 89 Abs. 1 GG, § 4, § 4a hmbWaG), abstrakte natürliche Gemeingüter wie Luft oder Wasser (§ 4 Abs. 2 WHG), Himmelskörper.

eher ausgeweitet[25]. Immer wieder kommen neue Immaterialgüter hinzu (z.B. Presseverleger-Leistungsschutzrecht, §§ 87f ff. UrhG), manchmal können aber auch wieder welche wegfallen (z.B. geographischen Herkunftsbezeichnungen für weinrechtliche Kleinlagen[26]).

3. Eigentumsfähigkeit von Daten

Unser Thema ist aber „Daten". Daten sind, wie der Name schon sagt, etwas Gegebenes, etwas (einfach) Daseiendes. Doch gibt es ein „allgemeines Dateneigentum" nicht[27]. Denn es fehlt ohne voraussetzungsvolle Regelungen insoweit an der Schutzfähigkeit, wie sie nach Art. 14 GG gefordert wird: Es gibt (noch) keine Bestimmungen, die einem Berechtigten Rechtspositionen „in der Weise [zuordnet] […], dass er die damit verbundenen Befugnisse nach eigenverantwortlicher Entscheidung zu seinem privaten Nutzen ausüben darf"[28]. Insbesondere auf tatsächlicher Ebene können Dritte schwer bis gar nicht von der Datennutzung ausgeschlossen werden (Nicht-Exklusivität), vielmehr sind Nutzung und Rechte nebeneinander möglich (Nicht-Rivalität[29]; z.B. Innehabung, Zugang, Bezug, Leistungs-[30] und Investitionsschutz).

Allerdings ist der Gesetzgeber durchaus frei, auch Daten einer Person exklusiv, ausschließlich, also dinglich zuzuweisen. Mit einer solchen Verdinglichung von Daten[31] (und ihrer ausschließlichen Zuweisung an eine Person) geht einher, dass diese dann den Gewährleistungen des Eigentumsgrundrechts unterfallen[32]. Unsere Rechtsordnung kennt dies durchaus vereinzelt, etwa in der Form von gesammelten und sortierten Daten in einer Daten-

25 Vgl. etwa zur Genese (oder dessen Ansätze) eines „Medieninhalt-Schutzes" im UrhG *v. Lewinski,* Der Staat 59 (2020), 277 (280 ff.).

26 BVerfGE 78, 58 (75) – weinrechtliche Kleinlagen.

27 Zum (dogmatischen wie rechtspolitischen) Streitstand zum Dateneigentum noch vor Einführung des Data Acts ausführlich *Kühling/Sackmann*, ZD 2020, 24 ff.; allgemein und umfassend *Giegerich*, Das verfassungsrechtliche Dateneigentum nach Art. 14 Abs. 1 S. 1 des Grundgesetzes, 2024, sowie *Weiß*, Dateneigentum, 2025.

28 BVerfGE 83, 201 (209); 101, 239 (258); 112, 93 (107); 115, 97 (111 f.); 123, 186 (258).

29 Hierzu und zum folgenden *v. Lewinski*, Der Staat 59 (2020) 277 (288 ff.).

30 Vgl. *Zech*, Information als Schutzgegenstand, 2012, S. 151 m.Bez.a. die Arbeitstheorie nach *John Locke*.

31 Rechtstechnische Möglichkeiten hierzu bei *Kevekordes*, Daten als Gegenstand absoluter Zuordnung, 2022; *v. Lewinski/Rüpke/Eckhardt*, Datenschutzrecht, 3. Aufl. 2025, § 13 Rn. 29.

32 *Michl*, NJW 2019, 2729 (2931 f.); *v. Lewinski*, Der Staat 59 (2020), 277 (293).

bank (Datenbankleistungsschutzrecht, §§ 87a ff. UrhG) oder auch dem Datenbankwerk (§ 4 Abs. 2 UrhG).

III. Schrankenbestimmung durch Gesetz

Nicht nur die Inhaltsbestimmung ist dem Gesetz überwiesen, sondern auch – wie bei anderen Grundrechten ebenfalls – das Bestimmen von Schranken. Dies ergibt sich jeweils ganz ausdrücklich aus Art. 14 Abs. 1 S. 2 Var. 2 GG und Art. 17 Abs. 1 S. 3 GRCh.

Nach diesen Schrankenbestimmungen folgen Pflichten aus dem Eigentum, die auch informationeller Natur sein können. Mit Eigentum waren schon immer Datenbereithaltungs- und Datenbereitstellungspflichten verbunden gewesen. Sie haben häufig die Gestalt von Meldepflichten, die v.a. im Anlagen- und Umweltrecht erheblichen Umfang und damit auch erhebliche Informationsmengen betreffen können.

> Die im Folgenden aufgeführten Melde- und Datenbereitstellungspflichten knüpfen häufig an den „eingerichteten und ausgeübten Gewerbebetrieb" an (z.B. die Gewerbesteuer sowie Umsatzsteuer- und Handelsregistervorschriften, § 23 WpHG, § 137 AO oder § 43 GwG). Die Rechtsprechung und v.a. das BVerfG würden diese Sachverhalte aber überkommenerweise über Art. 12 GG lösen[33].

1. Steuerrecht

Das Steuerrecht kennt unterschiedliche Besteuerungsgegenstände. Die Verbindung zum Eigentum ist am deutlichsten[34] bei den Realsteuern, die an einen tatsächlichen Gegenstand anknüpfen, der im Falle der Grundsteuer

33 Während das BVerfG in früherer Rechtsprechung noch die Substanz der Sach- und Rechtsgesamtheit des eingerichteten und ausgeübten Gewerbebetriebes für von Art. 14 GG erfasst ansah, ist er mittlerweile davon abgerückt (vgl. *Dederer*, in: Kahl/Waldhoff/Walter (Hrsg.), Bonner Kommentar, Bd. 5, 188. ErgLfg. 2017, Art. 14 (Eigentum), Rn. 162 f.). Jedenfalls wird bei den hier genannten Melde- und Bereitstellungspflichten nicht in den Betriebsbestand eingegriffen, sondern lediglich in die Rentabilität seiner Geschäftsführung. Solche Fragen betreffen den Schutz des Erwerbs und nicht des Erworbenen und unterliegen daher nicht Art. 14 GG (vgl. BVerfGE 45, 142 (173); 77, 84 (118)).

34 Allerdings ist die Eingriffsqualität von Steuern in Bezug auf das Eigentum nicht unumstritten. Zwar sieht das BVerfG (BVerfGE 115, 97 (111) – Halbteilung) in der Finanzgewalt des Staates einen unmittelbaren und damit klassischen Eingriff.

sich tatsächlich auch auf das Immobiliareigentum bezieht, im Falle der Gewerbesteuer auf den stehenden Gewerbebetrieb (§ 2 Abs. 1 S. 1 GewStG).

Bei der Grundsteuer ist Steuerschuldner, wem das Grundstück zuzurechnen ist (§ 10 GrStG), was regelmäßig der Eigentümer ist (§ 39 Abs. 1 AO; zu Ausnahmen s. § 39 Abs. 2 AO). Hieran knüpfen sich entsprechende Anzeige- (z.B. § 19 GrStG) und Erklärungspflichten (z.B. § 228 Abs. 2 BewG).

Mit der Gewerbesteuer sind inländische „stehende Gewerbebetriebe" (§ 2 Abs. 1 S. 1 GewStG) belastet. Hierbei verweist das Gesetz auf § 15 Abs. 1 S. 1 Nr. 1 EStG, der seinerseits eine Gewerbeanmeldung nach § 14 GewO voraussetzt.

Auch weitere Steuern könnten genannt werden (wofür man sich allerdings weit ins Unterholz der Dogmatik der einzelnen Abgabenarten hineinbegeben müsste): Soweit man, was umstritten ist, das Vermögen als eigentumsfähige Position versteht[35], wären die entsprechenden Erklärungspflichten Ausfluss von Schrankenbestimmungen. Da der konkrete Lohnanspruch des Arbeitnehmers gegen den Arbeitgeber dem Eigentumsgrundrecht unterfällt[36] und der Arbeitnehmer einkommensteuerrechtlich zur Abgabe einer Steuererklärung verpflichtet sein kann, ist dies dann ebenfalls eine Schranke des Eigentums.

2. Sicherheitsrecht

Während es bei der polizeirechtlichen Zustandsstörerhaftung vor allem auf die tatsächliche Sachherrschaft ankommt (z.B. § 18 Abs. 1 Abs. 2 S. 2 BPolG; Art. 8 Abs. 1, Abs. 2 S. 2 bayPAG bzw. Art. 9 Abs. 2 S. 1, S. 2 Hs. 2 bayLStVG), kann ebenso der Eigentümer als Ausdruck seiner Sozialpflichtigkeit polizeilich in Anspruch genommen werden (§ 18 Abs. 1 S. 1, Abs. 2 S. 1 BPolG;

Im Schrifttum wird auf das „faktische Eingriffsäquivalent" (*Dederer*, in: Kahl/Waldhoff/Walter (Hrsg.), Bonner Kommentar, Bd. 5, 188. ErgLfg. 2017, Art. 14 (Eigentum), Rn. 185 ff., 581, 1150) oder die Freiheitseinbuße durch die Lenkungswirkung (*Papier/Shirvani*, in: Dürig/Herzog/Scholz (Hrsg.), GG, 104. ErgLfg. 2024, Art. 14 Rn. 283 ff.) abgestellt. Andere aber lehnen dies ab, wenn ein Eingriff bzw. ein „faktisches Eingriffsäquivalent" keine entsprechende Verhaltenslenkung beinhalte (so ausdrücklich zur Grundsteuer *Wernsmann*, NJW 2006, 1169 (1171 f.); anders *Drüen*, in: Stenger/Loose (Hrsg.), Bewertungsrecht – BewG/ErbStG/GrStG, 170. ErgLfg. 2024, Grundsteuer und Verfassungsrecht, Rn. 43; vgl. *Jarass*, in: Jarass/Pieroth (Hrsg.), Grundgesetz, 18. Aufl. 2024, Art. 14 Rn. 28 m.w.N.).

35 Das BVerfG sprach hier von einem „konsolidierten Vermögen" (BVerfGE 93, 121), welches eigentumsfähig sei.

36 *Schmidt*, in: Erfurter Kommentar zum Arbeitsrecht, 25. Aufl. 2025, Art. 14 GG Rn. 24.

Art. 8 Abs. 2 S. 1 bayPAG bzw. Art. 9 Abs. 2 S. 2 Hs. 1 bayLStVG)[37]. Das heißt zwar, dass Eigentum nicht zwangsläufig eine Störereigenschaft begründet, es aber zu einer solchen bei ordnungsgemäßer Störerauswahl durchaus führen kann. Aus Schutz- und Verkehrssicherungspflichten können sich unter Umständen (zivil- und strafrechtliche) reaktive Informationspflichten ergeben (z.B. bei (Wild-)Unfällen oder einsturzgefährdeten Gebäuden). Präventive Meldepflichten ohne spezialgesetzliche Konkretisierung (also nur aus § 18 BPolG, Art. 8 bayPAG usw. erwachsend) gibt es nicht (jedenfalls nicht, wenn man mit dem BVerwG[38] eine Pflicht zur Eigensicherung ablehnt).

Bislang singulär nur in Bayern ist die polizeirechtliche Standardbefugnis zur Datensicherstellung gemäß Art. 25 Abs. 3 bayPAG, das allerdings nicht an (an Daten nicht ohne weiteres bestehendes) Dateneigentum angeknüpft, sondern an die Dateninhaberschaft. Wenn aber die Dateninhaberschaft als Eigentum zu qualifizieren wäre, wäre ein polizeiliche Datensicherstellung ein Eigentumseingriff.

3. Bevölkerungsschutzrecht

Eine allgemeine bevölkerungsschutzrechtliche Pflicht zur Datenbereitstellung oder, umgekehrt, eine Befugnis zum Datenrequirieren gibt es im deutschen Recht nicht[39]; vereinzelte Regelungen finden sich in dem für den Bevölkerungsschutz insoweit zentralen Bundesleistungsgesetz (BLG) und sektorspezifischen Vorsorge- und Leistungsgesetzen[40]. Genannt werden können die allgemeine Auskunftspflicht (§ 15 BLG), die freilich nicht unmittel-

37 Ob nun der Eigentümer oder der Inhaber der Sachherrschaft in Anspruch zu nehmen ist, ist eine Frage der ordnungsgemäßen Störerauswahl im Einzelfall. Zentral kommt es auf die Verhältnismäßigkeit der Inanspruchnahme des Eigentümers an, welche deshalb unsachgemäß sein könnte, weil sie zu keiner gerechten Lastenverteilung führt (vgl. *Steiner*, in: Schmidbauer/Steiner (Hrsg.), Bayerisches Polizeiaufgabengesetz, 4. Aufl. 2014, Art. 8 Rn. 3, 6 f.), Über die Subsidiaritätsklausel (§ 18 Abs. 2 S. 2 BPolG; Art. 8 Abs. 2 S. 2 bayPAG bzw. Art. 9 Abs. 2 S. 2 Hs. 2 bayLStVG) hinaus gibt es indes keine typisierende Vorzeichnung der ordnungsgemäßen Störerauswahl im Rahmen der Zustandsstörereigenschaft.

38 BVerwG, DVBl. 1986, 360; s. auch *Denninger*, in: Lisken/Denninger (Hrsg.), Handbuch des Polizeirechts, 4. Aufl. 2007, E. (Polizeiaufgaben), S. 299, Rn. 109.

39 *v. Lewinski*, in: Specht/Hennemann (Hrsg.), DGA/DA, 2. Aufl. 2025, Art. 16 DA Rn. 18 m.w.N.; *v. Lewinski*, GSZ 2025, 55.

40 Umfangreiche Nachweise bei *Erkens*, in diesem Band, S. 77 (88).

bar an eine Eigentümerstellung anknüpft und auch nicht unmittelbar auf das Zurverfügungstellen von Daten gerichtet ist, sondern die Bereitstellung von Leistungen (i.S.v. § 2 Abs. 1 Nrn. 1–10 BLG) ermöglichen soll. Vergleichbare sektorspezifische Regelungen finden sich noch in einer Reihe von weiteren Versorge- und Leistungsgesetzen (z.B. § 14 WiSiG[41], ESVG-Datenübermittlungsverordnung[42], Mineralöldatengesetz[43]). Diese nur punktuellen Regelungen werden nun durch die Art. 14 bis 22 DA überformt und gesamthaft geregelt[44].

4. Wirtschafts- und Umweltrecht (Anlagenrecht)

Das (Öffentliche Wirtschafts-)Recht nimmt zwar mehr und mehr Abstand von „echten" Meldepflichten, um die Informationsverarbeitungskapazitäten der Öffentlichen Hand nicht zu überfordern. Stattdessen werden Private verpflichtet, Daten und Informationen vorzuhalten und auf Anforderung zur Verfügung zu stellen. Hiermit sind dann auch Strukturierungs- und Formatvorgaben verbunden, die auf die unternehmerische Datenhaltung rückwirken, was man nicht nur als Eingriff in die unternehmerische Freiheit (Art. 12 Abs. 1 GG) verstehen kann, sondern auch als einen solchen in (die Struktur von) Datengesamtheiten, die, wie §§ 87a ff. UrhG zeigt, ein tauglicher Gegenstand von Eigentum sind.

Lediglich exemplarisch für solche Datenbereithaltungspflichten seien hier das Wasserrecht (§ 88 Abs. 2, § 8 Abs. 3 S. 2 WHG), das Bodenrecht (Art. 1 S. 1 bayBodSchG i.V.m. § 4 Abs. 3 S. 1 Var. 3, Abs. 4 BBodSchG) und das Stoffrecht genannt (§ 16d ChemG i.V.m. ChemGiftInfoV, wo zwar auf den „Hersteller, Einführer oder Verwender" abgestellt wird, dieser ist aber in vielen Fällen nach § 948 BGB Eigentümer (geworden)). Vergleichbar mit diesem Feld sind des weiteren aktive Meldepflichten bei gefährlichen

41 Dazu *Erkens*, in: Freudenberg/v. Lewinski, (Hrsg.), Handbuch Bevölkerungsschutz, 2024, § 55 Rn. 85 ff.

42 Dazu *Erkens*, in: Freudenberg/v. Lewinski, (Hrsg.), Handbuch Bevölkerungsschutz, 2024, § 48 Rn. 141 ff.

43 Dazu *Erkens*, in: Freudenberg/v. Lewinski, (Hrsg.), Handbuch Bevölkerungsschutz, 2024, § 49 Rn. 147 ff.

44 *v. Lewinski*, in: Freudenberg/v. Lewinski (Hrsg.), Handbuch Bevölkerungsschutz, 2024, § 11 Rn. 145; *v. Lewinski*, in: Specht/Hennemann (Hrsg.), DGA/DA, 2. Aufl. 2025, Art. 14 DA Rn. 41.

Gegenständen, allen voran etwa die Hundehaltung[45]. Ferner zu nennen ist die allgemeine Regel des § 29 GewO.

5. Kapitalmarktrecht

Das Wertpapier- und Kapitalmarktrecht kennt bestimmte wertpapierrechtliche Mitteilungspflichten (§§ 20 f. AktG), also die Pflicht zur Weiterleitung von Informationen bzw. Angaben, wenn der Wertpapierbesitz an einer Aktiengesellschaft (= Eigentum) einen bestimmten Anteil überschritten hat[46].

6. Meldung natürlicher Personen und Registrierung von Fahrzeugen

Und selbst im allgemeinen Melderecht für jedermann kann man informationelle Schrankenbestimmung des Wohneigentums finden: Nach § 17 Abs. 1 BMG ist meldepflichtig, wer „eine Wohnung bezieht". Tatbestandsmäßig ist hier zwar der Bezug, der aber regelmäßig[47] an Immobilieneigentum oder das von Art. 14 Abs. 1 GG umfasste Wohnmietverhältnis[48] anknüpft.

Ähnlich verhält es sich mit vielen Fahrzeugen, die man zwar ohne informationelle Schranken zum Eigentum haben kann, die dann aber ein recht nacktes Recht darstellen, weil sie dann z.B. aus Gründen der Sicherheit des Verkehrs nicht im öffentlichen Raum bewegt werden können (allen voran PKWs, §§ 1 Abs. 1; 34 StVG, aber auch Schiffe, § 10 SchRegO, oder Luftfahrzeuge, § 64 Abs. 5 LuftVG).

---

45 Vgl. für eine allgemeine Pflicht verbunden mit einer Pflichthaftpflichtversicherung § 13 hmbgHundeG oder § 2 Abs. 5 S. 3 thürTierGefG. Für eine an die Gefährlichkeit der Hunde anknüpfende Pflicht auch ohne Anknüpfung an eine Haftpflichtversicherung § 3 Abs. 1 hessHundeVO oder Art. 37 bayLStVG.

46 S. allgemein § 33 WpHG zu wertpapierhandelsrechtlichen Schwellenwerten des Wertpapierbesitzes, der eine Meldepflicht auslöst.

47 Ausnahmen sind das Mit-Wohnen aufgrund von familienrechtlichen Bindungen oder Unterhaltsverpflichtungen oder aus Gefälligkeit.

48 BVerfGE 89, 1, 6; zustimmend statt vieler *Dederer*, in: Kahl/Waldhoff/Walter (Hrsg.), Bonner Kommentar, Art. 14 (Eigentum), Rn. 100 f. m.w.N.: kritisch *Depenheuer*, NJW 1993, 2561; *Depenheuer/Froese*, in: Huber/Voßkuhle (Hrsg.), Grundgesetz, Bd. 1, 8. Aufl. 2024, Art. 14 Rn. 157 ff.

IV. Praktisch kein Ausgleich für informationelle Eigentumseingriffe

Schon allgemein sind Inhalts- und Schrankenbestimmungen grundsätzlich entschädigungslos hinzunehmen (vgl. Art. 14 Abs. 1 S. 2 GG); nur in (atypischen) Sonderfällen werden sie als ausgleichspflichtig angesehen. Enteignungen sind nur unter den Voraussetzungen des Art. 14 Abs. 3 GG[49] möglich. Jedoch führen die Spezifika von Immaterialgütern, wie Daten es sind (Nichtrivalität, Nichtexklusivität, Nichtverbrauch)[50], dazu, dass ein Ausgleich oder eine Entschädigung für den Datenzugriff einstweilen noch kein großes Thema gewesen ist. Immaterielle und datenbezogene Informations- und Meldepflichten bedeuten vergleichsweise so geringe Inhaltsbestimmungen und Schranken, dass sie – soweit ersichtlich – die Schwelle zur Ausgleichspflicht noch in keinem Fall überschritten haben[51]. Ausgleichs- und Entschädigungsregelung wie in § 5c Abs. 8 BSI-G oder Art. 20 DA sind bislang singulär.

„Zwangslizenzen" in Bezug auf Urhebernutzungsrechte wären rechtskonstruktiv durchaus denkbar, der Gesetzgeber wählt freilich regelmäßig[52] den Weg über urheberrechtliche Schranken (insb. §§ 44a ff. UrhG), die dann eigentumsgrundrechtlich keine Enteignung nach Art. 14 Abs. 3 GG bedeuten, sondern „nur" Inhalts- und Schrankenbestimmungen darstellen. Und Urheberrechte können schon von vornherein nicht enteignet werden, weil sie unentziehbar im (Urheber-)Persönlichkeitsrecht gründen[53].

Anders ist dies bei Leistungsschutzrechten und gewerblichen Schutzrechten. Wenn sie dem Inhaber entzogen werden, wäre dies ohne weiteres eine Enteignung. Zwangslizenzvorschriften wie § 13 PatG[54] oder § 12 SortSchG kann man deshalb als eine die Sozialbindung konkretisierende

49 Auf den praktisch nicht bedeutsamen Art. 15 GG (Sozialisierungen) sei hier nur der Vollständigkeit halber hingewiesen.

50 *Schröder*, in: Bomhard/Schmidt-Kessel (Hrsg.), EU Data Act, 2025, Kap. V, Einf. Rn. 1.

51 Die hier in den Sinn kommende Pflichtexemplar-Entscheidung, der Fall der ausgleichpflichtigen Inhalts- und Schrankenbestimmung, kann hierfür aber nicht herangezogen werden. Denn sie betrifft nicht den Inhalt des damals streitgegenständlichen Buches (also nicht das Immaterialgut), sondern knüpft an die hohen Herstellungskosten (bei niedriger Auflage) an (also an das Sacheigentum).

52 Zu Ausnahmen *Ansorge*, Zwangslizenzen als Mittel der Pandemiebekämpfung, 2024.

53 Umfassend *Oekonomides*, in: Mitarbeiter-FS Ulmer, Enteignung der Urheberrechte?, 1973, S. 25–37; *Hirsch Ballin,* UFITA (1956) 196 (211 f.).

54 Vgl. *Körner*, GRUR 1970, 387 (389); *v. der Osten*, GRUR 1958, 465 (471); *Scharen*, in: Benkard (Hrsg.), Patentgesetz, 12. Aufl. 2023, § 13 Rn. 1 m.w.N. Zuletzt *Huber,* Die patentrechtliche Zwangslizenz auf dem Prüfstand, 2025.

Schrankenbestimmung oder eine entschädigungspflichtige Enteignung verstehen.

Hinsichtlich der spezialgesetzlich angeordneten Ausgleichspflicht nach Art. 20 DA ist die Einordnung in die Kategorien des deutschen Rechts der staatlichen Ersatzleistungen noch offen. Soweit deutsches Recht zur Anwendung kommt, ist zwischen einem Aufopferungsanspruch und dem enteignenden Eingriff zu unterscheiden[55]. Diese beiden Rechtsinstitute sind danach zu differenzieren, in welche der von den beiden Anspruchsgrundlagen geschützten Rechtsgüter eingegriffen wird: Der Aufopferungsanspruch beschränkt sich nach ständiger Rechtsprechung auf nicht-vermögenswerte Rechtsgüter[56]. Aus Art. 20 Abs. 1 lit. a sublit. ii DA wird jedoch deutlich, dass die Verpflichtung gerade auf im Rechtsverkehr erwerbliche Daten abzielt, der Datenbestand also einen gewissen Vermögenswert hat. Bei Eingriffen in vermögenswerte Rechtsgüter i.R.d. enteignenden Eingriffs besteht jedoch nur ein Ausgleichsanspruch für das erbrachte Sonderopfer, wenn es sich bei der Verpflichtung zu einer Datenübermittlung um einen Eingriff in das Eigentum handelt[57].

Eigentlich sind nur Löschverpflichtungen im eigentlichen Sinne „Datenenteignungen[58]". Daneben genannt werden kann hier eine Vorschrift wie Art. 25 Abs. 3 bayPAG, der primär auf den staatlichen Zugriff auf Daten abzielt, aber auch gestattet den früheren Dateninhaber von der Inhaberschaft auszuschließen. Und aus einer ganz anderen Perspektive könnte man die datenschutzrechtlich oftmals geforderte Anonymisierung als enteignenden Eingriff (bei der betroffenen Person wie auch dem Verantwortlichen) verstehen.

55 *v. Lewinski*, in: Specht/Hennemann (Hrsg.), DGA/DA, 2. Aufl. 2025, Art. 20 DA Rn. 26.

56 *Ossenbühl/Cornils*, Staatshaftungsrecht, 6. Aufl. 2013, S. 134.

57 *Ossenbühl/Cornils*, Staatshaftungsrecht, 6. Aufl. 2013, S. 134.

58 Allerdings geht das BVerfG davon aus, dass die Vernichtung von Eigentum (z.B. Asservaten und Restlaufzeiten von KKWen) keine Enteignung sei, da der Staat anders als in der typischen Enteignungssituation kein Eigentum begründen will (keine Zueignungsabsicht), sondern defensiv handelt, indem er eine fremde Eigentümerposition erlöschen lässt (BVerfGE 20, 351 (359); BVerfGE 22, 387 (422); BVerfGE 110. 1 (24 f.)).

V. Zwischenergebnis

Der grundrechtliche Eigentumsschutz beschränkt sich nicht auf die agrarische und industrielle Welt (wie Art. 15 GG das vielleicht nahelegen würde). Vielmehr reichen sowohl der Schutzbereich als auch die Inhalts- und Schrankenbestimmung in die digitale Welt und die Informationsgesellschaft hinein[59], auch wenn die Frage des Ausgleichs für staatliche Eingriffe einer näheren Behandlung harrt.

C. Dingliche Elemente des Schutzes von Daten

Nachdem zunächst (B.) nach den informationellen Gehalten des Eigentums gefragt worden war, soll nun durch das andere Glas unserer dogmatischen 3D-Brille nach den dinglichen Gehalten der Informationellen Selbstbestimmung und des Schutzes von Daten geschaut werden.

I. Absolute Rechte an Daten

Absolute Rechte an Immaterialgütern gibt es im Urheberrecht durchaus und zahlreich[60]. Nach immaterialen Zuordnungen im Datenrecht muss man dagegen etwas länger suchen. Und wenn man solche findet, sind sie durchaus etwas weicher, relativer, weniger „absolut"; dies soll hier mit dem Begriff der „Quasidinglichkeit" umschrieben sein.

1. Personenbezogene Daten als Gegenstand „relativer absoluter Rechte"

Nächstliegend sind personenbezogene Daten, die, durch Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG bzw. Art. 8 GRCh geschützt, ein absolutes Recht vermitteln. Das ist freilich nur im begrenzten Kosmos der vom Datenschutzrecht abgebildeten Beziehung zwischen verantwortlicher Stelle und Betroffenem (heute: Verantwortlichem und betroffener Person) so, wo (durch das gesetzestechnische Verbot mit Erlaubnisvorbehalt) das Mitbestimmungsrecht über die personenbezogene Verarbeitung der betroffenen Person zugewie-

59 Hierzu jetzt umfassend *Gierschner*, Das verfassungsrechtliche Dateneigentum nach Art. 14 Abs. 1 S. 1 GG, 2024.

60 *Zech*, Information als Schutzgegenstand, 2012, S. 406 ff.

sen wird, wie sich aus dem Erlaubnistatbestand der Einwilligung (Art. 6 Abs. 1 lit. a DSGVO) sowie den Betroffenenrechten ergibt. Entfällt der Personenbezug (etwa durch eine Anonymisierung) oder wird der sachliche Anwendungsbereich des Datenschutzrechts verlassen (etwa im privaten und familiären Bereich, Art. 2 Abs. 2 lit. c DSGVO), entfällt das Mitbestimmungsrecht und es besteht gerade keine absolute, *gegenüber jedermann geltende* Rechtsposition.

Außerdem berechtigt nach der Volkszählung-Entscheidung das „Recht auf informationelle Selbstbestimmung", wie ausdrücklich in Leitsatz und Entscheidung formuliert ist, nur „grundsätzlich" zur freien Entscheidung über die Preisgabe und Verwendung der „eigenen" persönlichen Daten zu bestimmen[61]. Das „Informationelle Selbstbestimmungsrecht" ist keinesfalls allgemein im Sinne einer absoluten Verfügungsbefugnis zu verstehen; es unterliegt vielmehr immer der Einzelfallabwägung gegen Gemeinschaftsinteressen, zumal personenbezogene Informationen stets auch ein Abbild sozialer Realität und damit gemeinschaftsgebunden und gemeinschaftsbezogen sind[62].

Lediglich von sehr vereinzelten Stimmen im Schrifttum wird (eine Form von) Dateneigentum bereits auf Grundlage der DSGVO anerkannt. Die Erlaubnistatbestände des Art. 6 Abs. 1 DSGVO werden dann als Inhalts- und Schrankenbestimmung verstanden, zumindest dann, wenn es auf die Einwilligung ankommt[63]. Dafür müsste freilich Art. 6 DSGVO in seinem Anwendungsbereich geteilt werden und nur ein Teil davon, nämlich Art. 6 Abs. 1 lit. a DSGVO, wäre als Inhalts- und Schrankenbestimmung zu verstehen. Doch kennt die DSGVO gerade kein Primat der Einwilligung. Auch an anderen Stellen wie den Betroffenenrechten wird keinesfalls eine Verfügungsbefugnis des Betroffenen begründet, sondern vielmehr einzelne Anspruchsgrundlage innerhalb des Rahmens einer objektiven Datenschutzregulierung.

In Richtung Verdinglichung von personenbezogenen Daten weist allerdings die mittlerweile gesetzgeberischerseits anerkannte und eingeräumte Möglichkeit des „Bezahlens mit Daten" (§ 312 Abs. 1a und § 327 Abs. 3 BGB

61 BVerfGE 65, 1 (Ls. 1, 43).
62 BVerfGE 65, 1 (43 f.).
63 Vgl. etwa *Bijok*, ZfDR 2021, 75 (93).

in Umsetzung der Digitale-Inhalte-Richtlinie (EU) 2019/770[64]). Das Recht auf informationelle Selbstbestimmung erscheint dann (nur noch) als „Verfügungsbefugnis" und nicht mehr als Abwehrrecht[65].

2. Geschäftsgeheimnisschutz

Verfassungsrechtlich anerkannt ist der Schutz von Daten, die ein Betriebs- und Geschäftsgeheimnis darstellen[66]. Dabei hat das BVerfG allerdings die Berufsfreiheit aus Art. 12 Abs. 1 GG herangezogen und offengelassen, ob auch Art. 14 Abs. 1 S. 1 GG einschlägig ist[67].

Jedenfalls aber hat der Gesetzgeber sich aufgrund europarechtlicher Vorgaben dazu entschlossen, den (Geschäfts-)Geheimnisschutz mit dem GeschGehG quasidinglich auszugestalten: Die primäre Schutzwirkung des GeschGehG ergibt sich aus dem Verbot gemäß § 4 GeschGehG, ein Geschäftsgeheimnis in unbefugter oder sonst treuwidriger Weise zu erlangen bzw. aus den dazu akzessorischen Ansprüchen gemäß §§ 6 ff. GeschGehG. Dem Geheimnisherrn wird dadurch ein faktisches Ausschließlichkeitsrecht kraft Geheimseins gewährt[68]. Ist die Geheimhaltung allerdings nicht mehr gegeben, dann endet das Geheimnis und damit die Schutzwirkung des Geschäftsgeheimnisses, sodass die sich aus dem GeschGehG ergebende Rechtsposition flüchtig ist und eben nicht (mehr) dem Geheimnisherrn mit rechtlicher Ausschließlichkeitsbefugnis zugeordnet wird. Ähnlich wie beim Data Act entspringt aus den begrenzten Zuweisungen des GeschGehG also nur ein „unvollkommenes Immaterialgüterrecht"[69], welches zwar einfachgesetzlich etwa über § 823 Abs. 1 BGB geschützt ist, gleichzeitig aber keine Zuweisung einer absoluten Rechtsposition i.S.v. Art. 14 Abs. 1 S. 1 GG begründet.

64 Richtlinie (EU) 2019/770 v. 20.5.2019 über bestimmte vertragsrechtliche Aspekte der Bereitstellung digitaler Inhalte und digitaler Dienstleistungen (ABl. EU L 136 v. 22.5.2019, S. 1).

65 *Behrendt*, Entzauberung des Rechts auf informationelle Selbstbestimmung, 2023, S. 393, relativierend aber freilich S. 203.

66 BVerfGE 115, 205 (220); *Dederer*, in: Kahl/Waldhoff/Walter (Hrsg.), Bonner Kommentar, Bd. 5, 188. ErgLfg. 2017, Art. 14 (Eigentum), Rn. 55; *Papier/Shirvani*, in: Dürig/Herzog/Scholz (Hrsg.), GG, 104. ErgLfg. 2024, Art. 14 Rn. 204.

67 BVerfGE 115, 205 (248); BVerfGE 137, 185 (261).

68 *Horeth*, Intellectual Property in Innovationskooperationen, 2020, S. 253.

69 *Ohly*, GRUR 2014, 1 (8). – Diese Begrifflichkeit fällt bereits in der Debatte zum Data Act (vgl. *Hennemann/Steinrötter*, NJW 2024, 1 (7)).

3. Data Act

Bezeichnenderweise schafft deshalb auch der Data Act keine Data Ownership[70], sondern spricht nur von Dateninhaberschaft (Data Holder)[71]. Auch die Erwägungsgründe, die von „geeigneten technischen Schutzmaßnahmen" sprechen (ErwGr. 57 DA), deuten darauf hin, dass es für Daten nicht um einen rechtlichen, sondern wie beim Geschäftsgeheimnisschutz um tatsächlichen Schutz geht.

Man könnte nun fragen, ob die Dateninhaberschaft (Art. 2 Nr. 13 DA) als eine Verdinglichung angesehen werden könnte. In der Literatur lassen sich vereinzelt Andeutungen erkennen, dass mit dem Data Act ein zumindest eigentumsähnliches Regime der Verfügungsbefugnisse von Dateninhaber und Nutzer geschaffen worden sein soll[72]. Die h.M. zum Data Act freilich räumt mangels Ausschließlichkeitsfunktion keine eigentumsfähige Rechtsposition ein[73]: Die Verfügungsbefugnis von Dateninhaber oder Nutzer scheitert daran, dass sie sich gegenseitig nicht verbieten können, die produzierten Daten anderweitig zu monetarisieren[74]. Auch sind die nicht-ausschließlichen Nutzungszuweisungen und -beschränkungen durch den Data Act kein „Nukleus eines Schutzrechts"[75]. Insoweit belässt es der Data Act bei dem überkommenen Ausgangspunkt, dass der Dateninhaber eine rein faktische Verfügungsmacht über „seine" Daten besitzt. Diese Verfügungsgewalt wird punktuell mit vertraglichen Mitteln schuldrechtlich zugunsten des Nutzers modifiziert[76]. Eine Exklusivitätsstellung des Nutzers besteht daher im dinglichen Sinne zwar nicht, dennoch aber hat er faktisch über

70 *Macher/v. Ballestrem*, GRUR-Prax 2023, 661 (Rn. 1).

71 Zur Begrifflichkeit vgl. Art. 2 Nr. 13 DA. Dass diese Begrifflichkeit nicht mit der Eigentümerstellung verwechselt werden sollte, ergibt sich schon aus ErwGr. 6 u. ErwGr. 20 DA, wonach kein ausschließlicher Rechtsanspruch auf die Daten begründet werden soll. Ebenso knüpft der konzeptionell oft parallellaufende Data Governance Act (DGA) ebenfalls an die Dateninhaberschaft an (vgl. Art. 2 Nr. 8 DGA). Der DGA verbietet sogar ausweislich seines Art. 4 die auch nur faktische bzw. vertragliche Begründung eines ausschließlichen Datennutzungsrechts.

72 Spuren lassen sich erkennen bei *Kraft/Schumann*, GRUR-Prax 2024, 324 (325); *Stögmüller*, NJW 2023, 3762 (3763); *Hennemann/Steinrötter*, NJW 2024, 1 (7).

73 Zusammenfassend zur Diskussion *Specht-Riemenschneider*, MMR 2022, 809; *Specht-Riemenschneider,* ZRP 2022, 137 (138); kritisch etwa *Funk*, CR 2023, 421 (424).

74 *Hennemann/Steinrötter*, NJW 2024, 1 (7); *Wiebe*, GRUR 2023, 1569 (1572).

75 So aber *Hennemann/Steinrötter*, NJW 2024, 1 (Rn. 36).

76 *Wiebe*, GRUR 2023, 1569 (1572).

Art. 4 Abs. 13 DA die Möglichkeit, über „seine" Daten in dem Sinne frei zu verfügen, dass er keine Nutzungsverträge schließt[77].

4. Datenbankleistungsschutzrecht

Umfassend verdinglicht sind Daten in der besonderen Aggregatform der Datenbank (§§ 87a ff. UrhG) (und der Datenbankwerke, § 4 Abs. 2 UrhG). Gegenstand des absoluten Rechts sind allerdings nicht die Daten und auch nicht die Struktur als solche, sondern ihre Gesamtheit und besonderen Anordnung.

II. Beschränkung zugunsten überwiegendem Allgemeininteresse

Schon das „Recht auf informationelle Selbstbestimmung" wurde – wie erwähnt – in der Volkszählung-Entscheidung mit dem einschränkenden Zusatz versehen, dass dieses Recht bedeute, (nur) „grundsätzlich" selbst über die Verarbeitung der einen selbst betreffenden Daten bestimmen zu können[78]. Dieser einschränkende Zusatz, der durchaus prominent auch in den Leitsätzen auftaucht[79], wird aber weder in der Entscheidung selbst begründet, noch ist er – soweit ersichtlich – in der fachlichen und wissenschaftlichen Diskussion seitdem speziell thematisiert worden[80].

1. Sozialbindung schon mangels Ausschließlichkeit

Die Sozialbindung (in Form von Inhalts- und Schrankenbestimmungen) stutzt ein absolutes Recht wieder auf das Maß zurück, das nach Auffassung des Gesetzgebers seiner Sozialbindung entspricht. Dies ist allerdings überhaupt nur bei absoluten Rechten nötig, weil die anderen kraft ihrer Nicht-Ausschließlichkeit bereits für die Allgemeinheit greifbar und nutzbar sind.

---

77 *Bomhard/Merkle*, RDi 2022, 168.

78 BVerfGE 65, 1 (43).

79 BVerfGE 65, 1 (Ls. 1).

80 Vgl. *Marsch*, Das europäische Datenschutzgrundrecht, 2018, S. 99 ff.; *Guggenberger*, Irrweg informationeller Privatautonomie, 2023, S. 49 m.w.N.; s.a. *Albers*, Informationelle Selbstbestimmung, 2005, S. 156 ff., 238; *Bull*, Informationelle Selbstbestimmung – Vision oder Illusion, 2009, S. 61 ff.

2. Datenaltruismus

Die (daten- und digitalpolitische) Idee, dass Daten einer gewissen Sozialpflichtigkeit unterliegen sollten, hat sich in der rechtswissenschaftlichen Diskussion bereits unter dem Begriff des „Datenaltruismus" verfestigt. Im einfachen Recht ist dieses Konstrukt bisher allenfalls in den Art. 16 ff. DGA ausgeformt worden. Dabei handelt es sich nicht um eine sozialgebundene Inpflichtnahme von Dateninhabern, sondern vielmehr um Incentivierungen für eine freiwillige „Datenspende" zur Förderung bestimmter Allgemeinwohlbelange[81]. In ihrer Funktion als solche knüpfen die Regelungen nicht etwa an die Dateninhaberschaft an, sondern konkret an eine „datenaltruistische Tätigkeit" (Art. 18 lit. a DGA) des Spenders.

Würde man hier – trotz des Anwendungsvorrangs der EU-Grundrechte oder wegen Art. 345 AEUV – eine mitgliedstaatliche deutsche grundrechtsdogmatische Betrachtungsweise anlegen, wären die Regelungen mehr der Berufsfreiheit aus Art. 12 Abs. 1 GG (also den „Erwerb" von Daten) als der Eigentumsgarantie aus Art. 14 Abs. 1 GG (also den erworbenen Daten) zuzuordnen.

III. Zwischenergebnis

Daten sind nicht der natürliche und naheliegende Gegenstand für dingliche Rechte. Rechtlich und rechtskonstruktiv ist eine Verdinglichung von Daten aber durchaus denkbar, insbesondere für bestimmte Aggregatzustände und Darreichungsformen (z.B. Datenbanken). Allerdings steht das Recht hier noch sehr am Anfang einer Entwicklung, so dass sowohl die Konturen eines dinglichen Datenrechts wie auch dessen Inhalts- und Schrankenbestimmungen noch nicht recht zu erkennen sind.

D. Offene Fragen und Arbeitsfelder

Was kann man nun aus diesem Befund lernen, dass das Eigentumsgrundrecht durchaus informationelle Komponenten und Elemente hat? Und dass das Daten(schutz)recht eine gewisse Tendenz hin zur Verdinglichung kennt? Kann man die beiden Bilder zu einem tiefenscharfen Gesamtbild

81 Vgl. dazu Art. 2 Nr. 16 DGA und ErwGr. 45 DGA.

zusammenschieben? (Wahrscheinlich können wir es noch nicht, weil das Datenrecht als Rechtsgebiet noch zu jung ist, wir unsere dogmatischen Sehfertigkeiten erst noch ausbilden müssen…)

I. Dogmatische Verselbständigung informationeller Pflichten?

Zunächst aber könnte man jedenfalls, etwa von der Warte der Angemessenheit, Kriterien entwickeln, um Schutzbereichsgrenzen, Schranken (und Schranken-Schranken) für Eingriffe in Datenrechte zu beschreiben und zu systematisieren. Hierdurch könnte man sich von den dogmatischen Pfaden und Pfadabhängigkeiten lösen, die notwendigerweise damit verbunden sind, wenn man nicht von einer vorhanden (mitgliedsstaatlichen!) Grundrechtsfigur her denkt, sondern quasi von hinten aufgezäumt von einer allgemeinen und damit abstrakten Verhältnismäßigkeitsprüfung her.

II. Aufgabe der Unterscheidung zwischen unternehmensbezogenen und allgemeinen Daten?

Im deutschen Recht schon wegen der Menschenwürdebasierung, im europäischen Recht wegen der ausdrücklichen Anordnung in Art. 8 Abs. 1 GRCh („[j]ede Person“) gilt das herkömmliche Datenschutzrecht nur für natürliche Personen. Der Umkehrschluss, dass Datenschutz deshalb für juristische Personen ausgeschlossen wäre, ist allerdings nicht zwingend; in anderen Rechtsordnungen (Österreich[82], Schweiz[83]) ist der Anwendungsbereich des (einfachgesetzlichen) Datenschutzrechts weiter (gewesen) und hat(te) auch juristische Personen umfasst. Da sich bislang gravierende Schutzlücken nicht aufgetan haben, sind (in der deutschen Rechtsprechung) einstweilen Entscheidungen des Bundesverfassungsgerichts, die auch juristische Personen ausdrücklich in den personalen Schutzbereich

82 Bis zum Inkrafttreten der DSGVO und der damit verbundenen Revision des österreichischen Datenschutzgesetztes 2018 hat das alte Datenschutzgesetz in seinem § 4 Nr. 3 auch die juristische Person in den Kreis der Betroffenen eingeführt.

83 Bis 2023 galt das Schweizer Datenschutzgesetz gemäß seines Art. 2 S. 1 auch für das Verarbeiten von Daten juristischer Personen.

der Informationellen Selbstbestimmung einbezogen haben, vereinzelt geblieben[84].

Aber auch von der dogmatisch anderen Seite, vom Eigentumsgrundrecht her, hatte es einzelne Vorstöße gegeben: So sprach das Bundesverfassungsgericht davon, dass für Unternehmen der „in […] Art. 14 GG verbürgte grundrechtliche Datenschutz einen Schutz gegen unbegrenzte Erhebung, Speicherung, Verwendung oder Weitergabe individualisierter oder individualisierbarer Daten" gibt[85]. Später hieß es dann: „Zu diesen [von Art. 14 GG geschützten] vermögenswerten Rechten könnten auch die vermögensrechtlichen Bestandteile des allgemeinen Persönlichkeitsrechts […] zählen"[86]. Hieraus folgert *Hans-Georg Dederer*, es könne einen grundrechtlichen Schutz an Unternehmensdaten in der Form vermögenswerter Bestandteile des Rechts auf informationelle Selbstbestimmung geben, soweit es sich um Daten mit beträchtlichem wirtschaftlichem Wert handelt[87]. Das BVerfG hat genauere Konturen allerdings offengelassen.

III. Ausgestaltung privater Datenräume?

Als Eingriff in die (Berufs- und) Eigentumsfreiheit ist für Melde- und Datenbereithaltepflichten eine gesetzliche Grundlage erforderlich (und regelmäßig auch vorhanden). Sie stellt aber bislang nur auf den Aufwand der Datenbereitstellung als solcher ab, nicht aber auch auf die Anpassung interner Prozesse, die Daten in einem bestimmten Format bereitzuhalten, was dann auch eine Rückwirkung auf das Unternehmen hat und damit auf das informationelle Selbst; betroffen ist also auch eine „unternehmerische Informationelle Selbstbestimmung"[88].

Wenn Private Daten nicht mehr proaktiv an die Behörden melden, sondern sie nur vorhalten müssen (s.o. B.III.3 u. 4.), dann ist dies nicht

84 BVerfGE 118, 168 (Rn. 153 ff.); BVerfGE 128, 1 (Rn. 156); BVerfGE 147, 50 (Rn. 237); angedeutet bereits in BVerfGE 67, 100 (142).

85 BVerfGE 84, 239.

86 BVerfG, GRUR-RR 2009, 375.

87 *Dederer*, in: Kahl/Waldhoff/Walter (Hrsg.), Bonner Kommentar, 188. ErgLfg. 2017, Art. 14 (Eigentum), Rn. 51 ff.

88 Hier wäre freilich noch (neben der Existenz eines solchen unternehmerischen Rechts auf informationelle Selbstbestimmung) zu fragen, ob nicht vorrangig die Berufsfreiheit betroffen ist, zumal ein Datenauskunftsverlangen von nicht-rivalen Daten mehr die Erwerbstätigkeit als die Innehabung und Verwendung vorhandener Vermögensgüter betrifft (Abgrenzung nach BVerfGE 30, 292 ff.).

nur eine bürokratische Erleichterung, sondern auch ein informationeller Eingriff in die Berufsfreiheit. Denn die Datenvorhaltungs- und -bereitstellungspflicht bedingt Vorgaben für eine Auswahl und Formatierung. Der Staat ordnet also nicht mehr nur die Schnittstelle (Formular, Erhebungsbogen), sondern den Datenraum des Privaten als solchen. Meldepflichten Privater hat es schon immer gegeben. Sie wurden und werden insbesondere durch (staatliche) Formulare auch formatiert; Private müssen ihre Daten und Informationen für diese Schnittstelle ordnen. Unbeleuchtet und unterbelichtet ist bislang die (staatliche) Machtausübung durch die Format- und Strukturierungsvorgaben (z.B. ESG-Kriterien, bestimmte Messpunkte und Messdichte usw.). Sie führen nicht nur zu einem bestimmten Aufwand, sondern auch dazu, dass dadurch bestimmte Daten vorhanden sind/sein müssen und andere nicht.

E. Schluss: Freihaltung der digitalen Allmende

Bedacht werden muss allerdings bei aller Verdinglichung und der damit verbundenen Vorteile, dass eine hinreichende digitale Allmende bestehen bleibt[89]. Daten sind wie jede Information grundsätzlich frei. Das Immaterialgüterrecht schützt immer nur bestimmte Aspekte, also nur eine bestimmte Gestaltgebung (z.B. das „Werk") für eine bestimmte Zeit („Schutzfrist") und nur bestimmte Aspekte („Urheberpersönlichkeitsrecht", „Urheberverwertungsrecht"; „Leistungsschutzrechte"). Insoweit ist anschaulich von den Rechten des Geistigen Eigentums als „Inseln im Meer der Nachahmungsfreiheit" gesprochen worden[90].

Die Schaffung von Immaterialgütern trägt zum Funktionieren von Datenmärkten bei. Zwar müssen nicht alle Daten in allen Aggregationsstufen zu Immaterialgütern verdinglicht werden (und werden es auch nie sein). In dem Maße der Verdinglichung jedoch wird die Rechtsposition der Dateninhaber gegenüber (allen) anderen Marktakteuren gestärkt. Doch darf die Position von Dateninhabern auch nicht zu stark sein und werden, und es dürfen Daten auch nicht zu weitgehend verdinglicht werden, damit sie nicht einzelnen Akteuren (Rechteinhabern) exklusiv (im Rechtssinne: absolut) zugewiesen sind. Vielmehr muss der Gesetzgeber das öffentliche

89 Überblick über die ökonomischen Grundlagen speziell im Zusammenhang mit dem DA *Rohner*, EuDIR 2025, 10 (14 f.).

90 So etwa Ohly, GRUR 2017, 90 (91).

und individuelle Interesse an der Datennutzung mit den Verwertungsinteressen der Dateninhaber zu einem Ausgleich bringen[91]. Bei der rechtstechnischen Ausgestaltung hat er dabei einen weiten Spielraum[92]. Insb. kann er wählen, ob er weitreichende Immaterialgüter an Daten durch ebenfalls weitreichende Schrankenbestimmungen ausbalanciert oder für bestimmte Daten bewusst keinen Immaterialgüterschutz schafft (etwa für das einzelne Datum); besonders letzteres kann man als „informationelle Allmende[93]" bezeichnen.

Die immaterialgüterrechtliche Verdinglichung von Daten kann rechts- und medienpolitisch durchaus auch grundsätzlich kritisiert werden. Hier ist es die Aufgabe des Rechts, in praktischer Konkordanz einen Ausgleich zu finden zwischen den Interessen der Dateninhaber einerseits und der Allgemeinheit und ihrer Teile andererseits. Dies geschieht rechtstechnisch durch die Definition des Anwendungsbereichs des Immaterialgüterrechts und vor allem mittels der urheberrechtlichen Schranken, wodurch eine hinreichend große „informationelle Allmende" gewährleistet sein und bleiben soll.

91 *v. Lewinski*, Der Staat 59 (2020), 277 ff.; vgl. *Eschenbach,* Der verfassungsrechtliche Schutz des Eigentums, 1996, S. 434.

92 Vgl. *Beyerbach,* ZGE 2014, 182 ff.; speziell zu Leistungsschutzrechten *Anger,* Verwandte Schutzrechte, 2022.

93 *v. Lewinski*, Medienrecht, 2020, § 9 Rn. 8.

Blaulicht und Abschleppwagen auf der Datenautobahn: Eine kleine Rundreise durch das Datenrecht

Moritz Hennemann[*]

A. Vorab: Eine kleine Daten(rechts)geologie

Wenn es im Folgenden um „Blaulicht" und „Abschleppwagen" auf den Datenautobahnen gehen soll, ist zunächst eine kleine datenrechtsgeographische Kartierung erforderlich. Mit dieser Kartierung sollen zum einen der Datenzugang in Fällen außergewöhnlicher Notwendigkeit nach den Art. 14 ff. DA, die im Zentrum dieses Tagungsbandes stehen, in das *bigger picture* des Datenrechts einsortiert werden. Zum anderen sollen dadurch gleichzeitig „weiße Flecken" auf der datenrechtlichen Landkarte deutlicher hervortreten.

* Moritz Hennemann ist Inhaber des Lehrstuhls für Zivilrecht mit Informationsrecht, Medienrecht und Internetrecht sowie Direktor des Instituts für Medien- und Informationsrecht der Universität Freiburg. Die Vortragsform wurde beibehalten.

I. Von Landschaften und Wimmelbildern

Blickte man als Geograph zunächst auf „Datenlandschaften" – auf die mannigfaltigen Datenökosysteme unserer Gesellschaft und digitaler Gesellschaften weltweit –, wäre man mit einem riesigen Mosaik zerklüfteter Landschaftsfragmente konfrontiert[1]. Fragmentierte Datensätze fänden sich hier ebenso wie Datensilos. Das zu überblickende Feld wäre ebenso weit wie die Begriffe „Daten" und „Nutzung"[2]. Führten alle stattfindenden datenbasierten Interaktionen zu einer zwischen den Beteiligten verlaufenden Straße, wir hätten uns wohl alle schon mindestens einmal im Stau, auf der Überholspur oder auch in einer Baustelle mit langsamer Geschwindigkeit wiedergefunden. Das wird umso deutlicher, wenn man sich vor Augen führt, dass Einbahnstraßen gerade nicht die Regel sind. Private interagieren mit anderen Privaten, sie „tauschen" Daten gegen Entgelt und nutzen Datenbestände gemeinsam in Datenpools. Staatliche Akteure treten genauso als Datenzugangsgewährende wie als Datenverlangende auf. Private, auch Verbraucherinnen und Verbraucher, mögen ihre Daten gegenüber einem Akteur monetarisieren sowie gleichsam und gleichzeitig einem anderen spenden.

Blickt man sodann auf die aktuelle und damit verbundene Datenregulierung ist das Bild kein anderes. *Heiko Richter* hat treffenderweise von einem „Wimmelbild" gesprochen[3]. Während man auf einem Wimmelbild am Ende alles finden kann, ist das im Datenrecht allerdings nicht immer so einfach. Das Datenrecht besteht aus einer Vielzahl von sich ergänzenden (und teils weniger ergänzenden) Regulierungsschichten. Es gibt leider kein umfassendes unionales oder (das Unionsrecht ergänzende) nationales Datengesetzbuch[4]. Kohärenz ist nicht *King*, sondern Überlappungen und Friktionen[5]. Das Datenrecht reicht mindestens von der Datenschutz-Grundverordnung (DSGVO) über das Open Data-Recht bis hin zu den

1 Dieses Bild wurde zuerst verwendet in *Hennemann*, Ein Datengesetzbuch für alles - Tagesspiegel Background Digitalisierung und KI, abrufbar unter https://background.tagesspiegel.de/digitalisierung-und-ki/briefing/ein-datengesetzbuch-fuer-alles (zuletzt abgerufen am 17.10.2025).

2 In Anlehnung an *Richter*, DNG, 2. Aufl. 2025, Einl. Rn. 3.

3 *Richter*, IIC 55 (2024), 179.

4 Zur Perspektive eines nationalen Datengesetzbuchs siehe *Hennemann,* Ein Datengesetzbuch für alles - Tagesspiegel Background Digitalisierung und KI, abrufbar unter https://background.tagesspiegel.de/digitalisierung-und-ki/briefing/ein-datengesetzbuch-fuer-alles (zuletzt abgerufen am 17.10.2025)

5 Siehe stellvertretend nur *Specht-Riemenschneider*, ZEuP 2023, 638.

Neuregelungen des Data Act und des Data Governance Act. Sektorspezifische Regelungen wie das Geodatenzugangsgesetz oder auch die Informationsfreiheitsgesetze treten hinzu. Neuregelungen sind fast an der Tagesordnung.

II. *Multiple Use* und mehrdimensionale Zielprojektionen

Dabei eint zumindest die jüngeren Datenrechtsakte der Wunsch nach mehr Datennutzung[6]. Daten sollen mehr freiwillig geteilt werden. Teilweise werden Teilungspflichten bzw. Zugangsgewährungsansprüche statuiert (etwa Art. 4 f. DA). Die Infrastruktur von Datenmärkten ist ebenso im Blick (etwa Art. 10 ff. DGA) wie der Datenzugang in Notstandslagen (Art. 14 ff. DA). Diese Zielsetzungen sind grundsätzlich begrüßenswert. Damit einher gehen bessere strukturelle Bedingungen für Dateninnovation, für das Entstehen eines echten Datenbinnenmarkts und für mehr Datenaltruismus – zugunsten von Gesellschaft, Wirtschaft und Staat, zugunsten von Innovation und Gemeinwohl[7].

Die Regelsetzer denken richtigerweise in Datenökosystemen und Datenräumen – und projizieren konsequenterweise politische Zielbilder in mehreren Dimensionen[8]. Das nicht-rivale Gut Daten, ein *multiple use*-Gut, soll gesamtgesellschaftlich erfasst, gerahmt und fruchtbar gemacht werden. Dafür stehen nicht zuletzt der Datenzugang nach Art. 14 ff. DA zugunsten staatlicher Stellen in Fällen außergewöhnlicher Notwendigkeit[9] – und damit die Frage nach dem Grad einer „informationelle[n] Sozialpflichtigkeit" (*v. Lewinski*[10]).

---

6 Siehe nur *Kommission*, Eine europäische Datenstrategie, COM(2020) 66 final.

7 Siehe auch BT-Drs. 20/13090, S.13.

8 Zum konzeptionellen Ansatz Gemeinsamer Europäischer Datenräume siehe SWD(2022), 45 final und SWD(2024) 21 final.

9 Hierzu *Wienroeder*, in: Hennemann u.a. (Hrsg.), Data Act – An Introduction, 2024, S. 151 ff.; *Schröder*, MMR 2024, 104. Zur Diskussion um die Art. 14 ff. DA während des Gesetzgebungsverfahrens siehe *Höne/Knapp*, ZGI 2023, 168 sowie *Wienroeder*, in: Hennemann u.a. (Hrsg.), The Data Act Proposal – Literature Review and Critical Analysis: Part II (Art. 14-22), University of Passau IRDG Research Paper Series No. 23-02 (Januar 2023), abrufbar unter https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4340312 (zuletzt abgerufen am 17.10.2025).

10 *v. Lewinski*, in: Specht/Hennemann (Hrsg.), DGA/DA, 2. Aufl. 2025, Art. 14 DA Rn. 49; *v. Lewinski,* in diesem Band, S. 37 ff.

III. „Neue Daten braucht das Land"?

Der gesamtgesellschaftliche Ansatz ist für das Datenrecht die richtige Stoßrichtung. Gleichzeitig ist der aktuelle Ansatz zumindest partiell lückenhaft. Dabei soll es im Folgenden nicht um die Infrastrukturebene gehen. Nicht überall sind Datenautobahnen vorhanden, sondern vielleicht nur Datenlandstraßen oder Datenfeldwege. Ebenso gilt mein Interesse im vorliegenden Kontext nicht den wichtigen Fragen von Standards und Formaten von Datensätzen. Vielmehr soll es mit einem datenrechtsholistischen Blick um die vorhandene Datenrechtsarchitektur gehen – und um die damit verbundenen „weißen Flecken". Mit Blick auf die Schwerpunktsetzung dieses Tagungsbandes gilt zwar nicht pauschal „neue Daten braucht das Land"[11]. Es wird aber deutlich werden, dass die geopolitischen, wirtschafts- und industriepolitischen, sicherheits- und verteidigungspolitischen Dimensionen von Datengenerierung, Datennutzung und Datentransfer nicht nur offensichtlich sind, sondern auch bislang nicht immer hinreichend im Fokus standen.

B. Die regulatorische Grundkonfiguration von Datenautobahnen

Umgekehrt können diese Dimensionen nicht ohne die regulatorische Grundkonfiguration des Datenautobahnnetzes, sprich nicht ohne die Arten des Datenverkehrs, die Verkehrsteilnehmer und die zugrundeliegenden Verkehrsregeln, bewertet werden.

I. Arten des Datenverkehrs

Die Arten des Datenverkehrs umfassen dabei nicht-personenbezogenen ebenso wie personenbezogenen Daten. Sektorspezifische Daten der Privatwirtschaft stehen ebenso in Rede wie Kategorien besonders geschützter Daten des öffentlichen Sektors.

11 In Anlehnung an das Lied von *Ina Deter* („Neue Männer braucht das Land").

II. Verkehrsteilnehmer

Der Datenverkehr findet mit und zwischen einer Vielzahl von Akteuren statt. Akteure, die Daten generieren, nutzen und tauschen (wollen oder müssen) – und deren Interessen regulatorisch auszutarieren sind: staatliche und private, kommerziell agierende und nicht kommerziell agierende Akteure. NGOs genauso wie Hersteller von *Internet of Things*-fähigen Geräten. Oder in anderen Worten: *private-to-private*, *business-to-business*, *business-to-consumer*, *business-to-government*, *government-to-government* und so weiter. Besonders „auf die Straße gesetzt" wurden vom Unionsgesetzgeber mittels des Data Governance Act zum einen Datenvermittlungsdienste, also etwa Datenschutz-Cockpit-Anbieter ebenso wie *matching*-Plattformen zum Abschluss von Datenverträgen (eine Art Uber oder AirBnB für Datensätze[12]), und zum anderen datenaltruistische Organisationen[13]. Warum diese Akteure etwa im Kontext der Art. 14 ff. DA nicht mitbetrachtet bzw. auch mit geregelt wurden, ist nicht ganz klar – und auch nicht ganz verständlich.

III. Verkehrsregeln

Freilich gelten auf den Datenautobahnen unbeschadet des jeweils betroffenen Akteurs ein paar grundlegende Verkehrsregeln – oder vielleicht genauer: Verkehrsvektoren. Dazu zählt zunächst ein Primat des Datenmarktes und damit von Datenverträgen. Ausgangs- und Leitparameter sind der Datenvertrag – *Contract is King!* – und damit freiwillige Vereinbarungen. Der Data Act setzt zusammen mit dem Data Governance Act auf eine umfassende Kontraktualisierung – vornehmlich im privaten Sektor, aber auch soweit staatliche Akteure beteiligt sind[14]. Das (Daten-)Vertragsrecht *führt* im Datenrecht[15]. Dies unterstreicht im Kontext des vorliegenden Tagungsbandes Art. 15 Abs. 1 lit. b DA ebenso wie Art. 1 Abs. 6 DA. Letzterer hebt die Möglichkeit (und implizit auch den Vorrang) freiwilliger Verträge über einen Datenaustausch zwischen privaten und staatlichen Akteuren

12 *Hennemann/v. Ditfurth*, NJW 2022, 1905.

13 Hierzu im Einzelnen *Hennemann*, in: Specht/Hennemann (Hrsg.), DGA/DA, 2. Aufl. 2025, Art. 18 DGA Rn. 8 ff.

14 Siehe hierzu *Hennemann*, in: Specht/Hennemann (Hrsg.), DGA/DA, 2. Aufl. 2025, Einl. Rn. 59, 140 und 183; *Hennemann/Steinrötter*, NJW 2024, 1 (7); *Hennemann*, in: Hennemann u.a. (Hrsg.), Data Act – An Introduction, 2024, S. 26 ff.

15 *Hennemann/Steinrötter*, NJW 2024, 1 (6).

hervor. Gleichzeitige Folge der Kontraktualisierung – und damit keine *reine* Marktlösung – ist eine zunehmende, wenn auch nicht umfassende „FRANDisierung" der Datenvertragsbeziehungen (sprich *fair, reasonable and non-discriminatory)*[16]. Vertragsbestimmungen müssen oftmals fair und angemessen sowie nichtdiskriminierend ausgestaltet sein. Dies gilt etwa im Kontext des Data Act genauso wie – schon länger – im Kontext des Open Data-Rechts, das wiederum „eine funktionale Nähe zum Wettbewerbsrecht"[17] aufweist. In diesem Sinne sind Innovation, Wettbewerb, Monetarisierungschancen, aber eben auch *Fairness* zentrale Verkehrsvektoren.

Ist damit Art der typischen Fahrzeuge und Straßen geklärt, können wir uns der Geschwindigkeit auf den Datenautobahnen zuwenden. Unbeschadet vertraglicher Absprachen kann hier mit guten Gründen das Datenschutzrecht als wesentliche, zu beachtende Verkehrsregel verstanden werden – eine Regel, die oftmals zu Stoppschildern oder zumindest zu Geschwindigkeitsreduktionen führen kann (und führt).

Schließlich hilft es zu wissen, wie weit man fahren darf. Weitere und besonders im hiesigen Kontext besonders bedeutsame Reglungen sind die Transferbestimmungen, sprich Regelungen zur Frage, ob und inwieweit Daten ins EU-Ausland, in sogenannte Drittländer, übermittelt werden dürfen bzw. welche Maßnahmen zu treffen sind, um einen Zugriff staatlicher Stellen aus Drittstaaten möglichst zu verhindern. Aus einer übergeordneten Perspektive geht es hierbei um Fragen des Datenaußenwirtschaftsrechts – dieses ist bislang nur als regulatorisches Stückwerk in den Art. 44 ff. DSGVO, Art. 32 DA, Art. 5 Abs. 9 ff. und Art. 31 DGA sowie im allgemeinen Außenwirtschaftsrecht vorhanden – und nicht wirklich kohärent geregelt[18]. Nicht nur insoweit gilt: Von einer *Datenrealpolitik* sind wir noch ein gutes Stück entfernt[19].

16 Hierzu – auch die Grenzen im B2B-Kontext aufzeigend – *Denga*, ZfPW 2024, 427.

17 *Richter*, DNG, 2. Aufl. 2023, Einl. Rn. 53.

18 Im Einzelnen *Hennemann*, in: Krenzler/Herrmann/Niestedt (Hrsg.), EU-Außenwirtschafts- und Zollrecht, 24. Aufl. 2024, DAWR Rn. 1 ff.

19 Siehe hierzu *Hennemann/Specht*, Datenrealpolitik ist gefragt, Tagesspiegel Background Digitalisierung & KI (27. Juni 2022), abrufbar unter https://background.tagesspiegel.de/digitalisierung-und-ki/briefing/datenrealpolitik-ist-gefragt (zuletzt abgerufen am 17.10.2025); *Hennemann*, Datenrealpolitik – Datenökosysteme, Datenrecht, Datendiplomatie, University of Passau IRDG Research Paper Series No. 22-18 (November 2022), abrufbar unter https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4267390 (zuletzt abgerufen am 17.10.2025); *Hennemann,* Ein Datengesetzbuch für alles, Tagesspiegel Background Digitalisierung und KI, abrufbar unter https://backgr

C. Abschleppwagen auf Datenautobahnen oder: Wer hilft bei mangelndem Datennachschub?

Da es doch verschiedentlich auf unseren Datenautobahnen stockt, da die Ressource Daten teils knapp ist, quasi der Daten-Sprit (oder auch der Daten-Spirit?!) ausgeht, bestehen verschiedene „private Abschleppwagen". Solche Helfer sollen neuen Schwung erzeugen und neue Dateninnovationen befördern – und damit potenziell auch den für den Staat im Falle außergewöhnlicher Notwendigkeit zur Verfügung stehenden „Datenfuhrpark" verbessern.

I. Datenzugang als Fixpunkt des Datenrechts

Zentraler „Turbo" sind die durch den Data Act eingeführten Datenzugangsrechte (Art. 4 f. DA) in *private-to-private*-Konstellationen – zugunsten des Nutzers von IoT-Geräten und auf Nutzerwunsch zugunsten Dritter. Solche Dritte können kommerzielle ebenso wie etwa datenaltruistisch agierende Akteure sein, allerdings keine Gatekeeper im Sinne des Digital Market Act (Art. 5 Abs. 3 und Art. 6 Abs. 2 lit. d DA). Diese zunächst wettbewerbs- und wohl auch ein wenig industriepolitisch induzierten Schranken gegenüber den größten Verkehrsteilnehmern sollen strukturell zu einer Datendezentralisierung beitragen. Die Datenzugangsrechte dienen deswegen mindestens mittelbar auch staatlichen Stellen. Denn durch die Dezentralisierung vergrößert sich strukturell die Anzahl potenzieller Dateninhaber. Der Dateninhaber dient zwar zunächst nur dem Nutzer als „Datentankstelle". Der Datenzugang des Nutzers ist allerdings auch strukturelle Vorbedingung für ein (durch Datenvermittlungsdienste befördertes) freiwilliges Datenteilen – und damit eine höhere Datenzirkulation, die sich im Endeffekt (etwa im Falle außergewöhnlicher Notwendigkeit) auch wiederum zugunsten des Staates auswirken kann.

---

ound.tagesspiegel.de/digitalisierung-und-ki/briefing/ein-datengesetzbuch-fuer-alles (zuletzt abgerufen am 17.10.2025).

II. Datenaltruismus

Auf Freiwilligkeit setzt der Unionsgeber auch und gerade im Kontext des Datenaltruismus[20]. Vor allem für Non-Profit-Organisationen, für Forschungseinrichtungen sowie für bestimmte staatliche Stellen besteht damit ein weiterer Kanal zu Daten. Die Corona-Datenspende-App des Robert Koch-Instituts ist hier sicher das eingängigste Beispiel[21].

Soweit der Unionsgesetzgeber allerdings mit den Art. 16 ff. DGA auf die Etablierung datenaltruistischer Organisationen setzt, besteht noch Luft nach oben[22]. Es wurden bislang keine hinreichenden Anreize statuiert, um als datenaltruistische Organisation tätig zu werden, insbesondere keine datenschutzrechtlichen Privilegierungen[23]. Möglicherweise kann ein zukünftiges Forschungsdatengesetz oder auch eine Modifikation oder Ergänzung der DSGVO hier künftig abhelfen.

III. Nicht zu vergessen: Das Open Data-Recht

Schließlich ist der Staat selbst im Open Data-Kontext ein Lieferant von Daten, der strukturell dazu beiträgt, dass im Privatsektor wiederum bessere und genauere Daten bzw. aus Open Data abgeleitete Daten vorliegen. Davon mag der Staat dann wiederum in Fällen außergewöhnlicher Notwendigkeit profitieren.

D. Blaulicht auf Datenautobahnen oder: Wer hat (manchmal) Vorfahrt? Und zu wessen Gunsten?

Stellt sich noch die Frage, wer eigentlich – manchmal zumindest – „Vorfahrt" auf den allfälligen Datenautobahnen hat – und zu wessen Gunsten

20 Hierzu *Hennemann*, in: Specht/Hennemann (Hrsg.), DGA/DA, 2. Aufl. 2025, Art. 16 DGA Rn. 3 ff.

21 Siehe abrufbar unter https://corona-datenspende.github.io/en/ (zuletzt abgerufen am 17.10.2025).

22 Es haben sich innerhalb der EU bislang nur zwei datenaltruistische Organisationen registriert, siehe abrufbar unter https://digital-strategy.ec.europa.eu/en/policies/data-altruism-organisations (zuletzt abgerufen am 17.10.2025).

23 *Hennemann*, in: Specht/Hennemann (Hrsg.), DGA/DA, 2. Aufl. 2025, Art. 16 DGA Rn. 20, 23.

sich eine etwaige Vorfahrt auswirkt. Oder anders ausgedrückt: Für wen wird der Weg zusätzlich freigemacht?

I. Der Datenzugang nach Art. 14 ff. DA

Dabei kann man die Datenzugangsansprüche nach Art. 14 ff. DA als „Blaulicht"-Einsatz bezeichnen. Ganz grundlegend ist dabei zu berücksichtigen, dass selbst der Datenzugang zugunsten staatlicher Stellen in den Art. 14 ff. DA in mehrfacher Sicht keine allgemeine Vorfahrt des Staates bedingt. Zunächst greifen die Art. 14 ff. DA nur in Ausnahmefällen. Die Hürden sind vergleichsweise hoch, wenn damit freilich auch ein potenzieller Anker für ein weites Verständnis von Krisenlagen angelegt sein mag. Zum anderen ist stets die nicht-rivale Natur von Daten zu bedenken. So tritt selbst der zu Recht Zugang verlangende Staat nicht in eine echte Konkurrenz zum Dateninhaber. Es findet keine „Datenenteignung" statt. Daten sind durch den Staat zweckgebunden zu nutzen und anschließend zu löschen (Art. 19 Abs. 1 lit. c DA) – und der Dateninhaber kann sie natürlich weiterhin und auch parallel nutzen. Gleichwohl sind die Regelungen eine Ausprägung des wohl allgemeineren Ansatzes des „Unternehmenswissen[s] als Regulierungsressource"[24].

II. Das Primat der Datenmärkte

Vielmehr ist zu unterstreichen, dass der „Blaulicht"-Einsatz die Ausnahme und nicht die Regel ist. Das Primat der Datenmärkte und damit die Beschaffung von Daten am Markt ist das Leitbild. Das Regel-Ausnahme-Verhältnis im Falle des Art. 15 Abs. 1 lit. b DA unterstreicht dies. Dort heißt es: „alle anderen ihr zur Verfügung stehenden Mittel ausgeschöpft hat, um (…) Daten zu erlangen, darunter der Erwerb von nicht-personenbezogenen Daten auf dem Markt durch Angebot von Marktttarifen".

Nur hinweisen möchte ich in diesem Zusammenhang darauf, dass auch in anderen digitalrechtlichen Kontexten auf eine Inpflichtnahme Privater gesetzt wird. So sieht etwa Art. 36 DSA einen Krisenreaktionsmechanismus

24 So der schöne Titel einer thematisch etwas anders gelagerten, bankaufsichtsrechtlichen Arbeit von *Voß* (Unternehmenswissen als Regulierungsressource – Der aufsichtsrechtliche Zugriff auf bankinterne Strukturen, 2019).

vor[25]; Art. 48 DSA spezielle Krisenprotokolle. ErwGr. 91 S. 1 DSA führt insofern aus: „In Krisenzeiten kann es erforderlich sein, dass Anbieter sehr großer Online-Plattformen zusätzlich zu [sonstigen Pflichten] (…) dringend bestimmte spezifische Maßnahmen ergreifen[26]."

III. Weitergabe an die Forschung

Liegen die Voraussetzungen der Art. 14 ff. DA gleichwohl vor, ist zu bedenken, dass richtigerweise Forschungseinrichtungen und statistische Ämter eine der zentralen „dritten" Profiteure der gesetzgeberischen Konstruktion im Data Act ist[27]. Hiervon profitieren auch und gerade private Forschungseinrichtungen, wenn damit auch teils umfassende Pflichten bzw. unter anderem die Verantwortlichkeit für die Sicherheit der Daten einhergeht (siehe Art. 19 Abs. 4 i.V.m. Art. 21 Abs. 3 DA) – worauf etwa *Meinhard Schröder* jüngst hingewiesen hat[28].

E. Regulierungsdesiderate und -perspektiven

Es stellt sich nach alledem die Frage, wo denn nun im Kontext des vorliegenden Tagungsbandes zentrale Handlungsbedarfe bestehen.

I. Allgemeine Verkehrssicherheit, Effizienz und Gemeinwohl

So mag zunächst angenommen werden, dass die aktuellen Regulierungsschichten eine grundsätzlich adäquate allgemeine Verkehrssicherheit auf den Datenautobahnen herstellen. Insbesondere auch durch Vorgaben zur

25 Siehe hierzu *Kuhlmann/Trute*, GSZ 2022, 115 (121 f.).

26 Nach ErwGr. 91 S. 2 DSA tritt eine Krise ein, „wenn außergewöhnliche Umstände eintreten, die zu einer ernsthaften Bedrohung der öffentlichen Sicherheit oder der öffentlichen Gesundheit (…) führen können. Solche Krisen könnten auf bewaffnete Konflikte oder terroristische Handlungen, einschließlich neu entstehender Konflikte oder terroristischer Handlungen, Naturkatastrophen wie Erdbeben und Wirbelstürme sowie auf Pandemien und andere schwerwiegende grenzüberschreitende Bedrohungen für die öffentliche Gesundheit zurückzuführen sein.".

27 Übrigens nicht nur im Kontext der Art. 14 ff. DA, sondern etwa auch im Kontext des Datenzugangs zugunsten eines Dritten im Rahmen des Art. 9 Abs. 4 DA.

28 *Schröder*, MMR 2024, 104 (108).

IT-Sicherheit und – etwa im Data Act – zur Interoperabilität. Dass die bestehende Regelungslandschaft vollkommen effizient operiert und deswegen das Gemeinwohl umfassend befördert, ist allerdings mindestens mit Zweifeln versehen[29].

II. Industrie-, sicherheits- und verteidigungspolitische Zielsetzungen? Oder: Mehr Datenaußenwirtschaftsrecht?

Sind wir – um im obigen Bild zu bleiben – eigentlich ausreichend vorbereitet, wenn es in den Datenlandschaften nicht nur „brennt" oder Hochwasser entstehen, sondern die äußere Sicherheit in Frage steht? Der Blick in den Data Act und den Data Governance Act hilft naturgemäß nicht weiter. Fragen der nationalen Sicherheit und der Verteidigung sind eine nationale Domäne. Hier muss der aktuelle nationale Regulierungsbestand, sprich die Leistungs- und Sicherstellungsgesetze, bewertet, evaluiert und wohl auch modernisiert werden – etwa durch ein eigenes Datenleistungsgesetz, um legitime Interessen der Sicherheits- und Verteidigungspolitik auch schon zu Friedenszeiten abzubilden, notwendige Datenbestände aufzubauen und damit auch dem geopolitischen Umfeld gerecht zu werden[30].

Auf jeden Fall in den Blick zu nehmen sind die Herausforderungen, die mittelbar aus dem vornehmlich privatwirtschaftlichen grenzüberschreitenden Datentransfer resultieren, sprich private Datentransfers in EU-Drittländer (inklusive in Staaten, die wir nicht als „trusted partners" einstufen). Für personenbezogene Daten besteht mit den Art. 44 ff. DSGVO ein umfassendes Transferregime. Dieses folgt allerdings – mit Blick auf die Genese verständlich – im Wesentlichen einer datenschutzrechtlichen Logik. Die wirtschaftspolitische, industriepolitische, sicherheitspolitische und verteidigungspolitische Dimension kommt hier – wenn überhaupt – nur sehr mittelbar zum Zuge. Nur partiell besser ist die Lage bei nicht personenbezogenen Daten. Hier haben die Art. 32 DA, Art. 31 DGA und Art. 5 Abs. 9 ff. DGA (letztere im Kontext der Weiterwendung von Kategorien besonders geschützter Daten des öffentlichen Sektors, sprich im erweiter-

29 Siehe nur jüngst *Draghi*, The future of European competitiveness – In-depth analysis and recommendations (9. September 2024), abrufbar unter https://commission.europa.eu/topics/strengthening-european-competitiveness/eu-competitiveness-looking-ahead_en (zuletzt abgerufen am 17.10.2025).

30 Siehe hierzu *Erkens,* in diesem Band, S. 77 ff., *v. Lewinski,* GSZ 2025, 55 (61 ff.).

ten Open Data-Kontext) bislang nur ein partielles Transferregime statuiert. Hier finden sich vornehmlich industrie- und innovationspolitische Instrumente, die auch eine Reflexwirkung zugunsten der sicherheits- und verteidigungspolitischen Dimension aufweisen. Im Übrigen kann natürlich auch das allgemeine Außenwirtschaftsrecht in Bezug auf Datentransfers in Stellung gebracht werden[31]. Daten sind eben ein *multiple use*-Gut. Hier ist allerdings noch eine Vielzahl von Fragen offen. Ein umfassendes unionales oder nationales Datenaußenwirtschaftsrecht steht im Übrigen – wie bereits angedeutet – noch aus.

III. Ein nationales Datengesetzbuch?

Auf nationaler Ebene bestehen freilich weitere Optionen. Dies gilt vor allem natürlich in Bezug auf Materien, die dezidiert nationale Domänen sind – wie etwa im Bereich der Verteidigung[32]. Denkbar sind weitere sektorspezifische Datennutzungs- und Datenzugangsgesetze. Aktuell diskutiert wird dies etwa in Bezug auf ein Forschungsdatengesetz[33]. Ebenso ist es eine lohnenswerte Perspektive, dass wir mittelfristig die nationalen Regelungen in einem nationalen Datengesetzbuch bündeln[34]. Kohärenz und Systematik würden erhöht. Friktionen würden abgebaut. Vor allem wäre damit notgedrungen ein rechtspolitisches Innehalten verbunden, das vielleicht auch dazu dient, zweckmäßig Prioritäten zu setzen und überflüssige doppelte Standards ab-

31 Siehe *Hennemann*, in: Krenzler/Herrmann/Niestedt (Hrsg.), EU-Außenwirtschafts- und Zollrecht, 24. Aufl. 2024, DAWR Rn. 105 ff.

32 Siehe allgemein zur Mitwirkung der Wirtschaft *Erkens*, in: Freudenberg/v. Lewinski (Hrsg.), Handbuch Bevölkerungsschutz – Grundlagen, Recht, Praxis, 2024, S. 1007 ff.; siehe allgemein zu den Sicherstellungsgesetzen *Erkens*, in: Freudenberg/Kuhlmey (Hrsg.), Krisenmanagement, Notfallplanung, Zivilschutz – Festschrift anlässlich 60 Jahre Zivil- und Bevölkerungsschutz in Deutschland, 2021, S. 567 (605 ff.).

33 *BMBF*, Eckpunkte BMBF – Forschungsdatengesetz (28. Februar 2024), abrufbar unter https://www.bmftr.bund.de/SharedDocs/Downloads/DE/gesetze/forschungsdatengesetz/sonstige/Eckpunktepapier.html (zuletzt abgerufen am 17.10.2025).

34 Hierzu *Hennemann,* Ein Datengesetzbuch für alles - Tagesspiegel Background Digitalisierung und KI, abrufbar unter https://background.tagesspiegel.de/digitalisierung-und-ki/briefing/ein-datengesetzbuch-fuer-alles (zuletzt abgerufen am 17.10.2025); *Hennemann/Wendehorst,* Ein nationales „Datengesetzbuch"? – Erste Überlegungen zu dem datenrechtlichen Vorhaben im Koalitionsvertrag von CDU, CSU und SPD (15. April 2025), abrufbar unter https://uni-freiburg.de/jura-medienrecht/wp-content/uploads/sites/34/74b487873ff2942cde10b53a3791f76ce3e22f07a6e16ce9c924b9a14558.pdf.

zubauen. Das geht sicher nicht von heute auf morgen. Mittelfristig möglich ist es allerdings schon – den politischen Willen dazu vorausgesetzt.

Datenbereitstellung im äußeren Notstand. Zum staatlichen Informationsbedarf in Krise und Krieg

Transkript[*] des Vortrages von Harald Erkens[**]

Über die Gelegenheit, hier in Passau zu Ihnen über dieses Thema sprechen zu dürfen, freue ich mich sehr. Erlauben Sie mir, drei Dinge voranzustellen.

Erstens: Ich komme als Praktiker aus dem Bundesministerium der Verteidigung nicht ohne Demut in ein akademisches, ja professorales Umfeld. Die Praxis nämlich, auch die Praxis der Bundesregierung, stumpft bisweilen ab. Das ist in meinem Fall nicht ausschließlich, aber doch in hohem Maße verschiedenen Tätigkeiten während der letzten Jahre geschuldet, bei denen selten Zeit blieb, den jeweiligen rechtlichen Gegenstand in aller Sorgfalt zu wägen, um schließlich zu einer Entscheidung zu kommen, die auch den Anforderungen rechtlicher Dogmatik gerecht wird: zunächst im Corona-Krisenstab des Bundesministeriums für Gesundheit, sodann im Krisenstab Flutkatastrophe und schließlich im Sonderstab Ukraine zu Beginn des Krieges. Ich bemühe mich zwar redlich, die Bindung zu meinem verehrten akademischen Lehrer, dem Bonner Staatsrechtler Josef Isensee, aufrechtzuerhalten, was mich bislang auch vor vielerlei Übel bewahrt hat. Gleichwohl muss ich festhalten: Wer einmal in den Untiefen der Verwaltungspraxis seine akademische Unschuld verloren hat, der gewinnt sie nicht wieder. Sehen Sie mir deshalb bitte die eine oder andere Stumpfheit nach.

---

* Bei diesem Beitrag handelt es sich um eine Niederschrift des mündlichen Vortrags des Referenten. Daraus ergibt sich der etwas ungewöhnliche Stil des Textes als geschriebene Rede und ohne Fußnoten.

** Harald Erkens ist Referent im Bundesministerium der Verteidigung.

Das zweite, das ich voranstellen möchte – Herr Professor von Lewinski hat es bereits angedeutet: Ich bin weder Datenrechtler noch vertraut mit dem Datenschutzrecht. Meine einzige Berührung mit dem Recht des Datenschutzes war eine neunmonatige Tätigkeit in der Projektgruppe DSGVO des Gesundheitsministeriums, gegen die ich mich nicht wehren konnte. Es ging seinerzeit um das Zweite Datenschutz-Anpassungs- und Umsetzungsgesetz zur Adaption des bereichsspezifischen Datenschutzrechts des Bundes an die Datenschutz-Grundverordnung der EU. Das war ein Gesetzentwurf von ungefähr 600 Seiten Umfang. Ich selbst habe das, vorsichtig ausgedrückt, wie den Ausgang eines gegen mich gerichteten Disziplinarverfahrens empfunden. Langer Rede kurzer Sinn: Ich bin überzeugt, als Bundesbeamter meinen Anteil an Datenrecht und Datenschutzrecht jedenfalls bis zum Erreichen der Altersgrenze geleistet zu haben.

Eine dritte und letzte Anmerkung: Ich spreche hier zu Ihnen nicht als Vertreter der Bundesregierung, sondern als Privatperson. Das heißt, dass der bisweilen stumpfe Praktiker bei Ihnen an der Universität Passau Zuflucht sucht unter dem Schirm von Art. 5 Abs. 3 des Grundgesetzes. Sollte ich also irgendetwas sagen, das Ihnen womöglich allzu stumpf erscheint, machen Sie bitte nicht meinen Dienstherrn dafür haftbar. Ich gebe hier ausschließlich meine eigene Auffassung wieder.

A. Kein Thema für den supranationalen Gesetzgeber

Genug der Vorrede. Mein Auftrag besteht darin, Ihnen etwas über die Datenbereitstellung im äußeren Notstand und insbesondere im Spannungs- und Verteidigungsfall zu sagen. Um dies gleich vorwegzunehmen: Die gesamte Rechtsmaterie des äußeren Notstandes entzieht sich der Regelungskompetenz der Europäischen Union. Sie ist deshalb auch nicht Gegenstand der EU-Datenverordnung, neudeutsch: Data Act. Vielmehr handelt es sich hierbei um Recht, das bis auf Weiteres einem nationalen Vorbehalt unterliegt.

Ich habe bereits in der ersten Hälfte dieser Tagung gelernt, dass in Art. 15 Abs. 1 lit. a Datenverordnung die außergewöhnliche Notwendigkeit der Datennutzung zur Bewältigung eines öffentlichen Notstandes geregelt ist. Und freundlicherweise liefert Art. 2 Nr. 29 Datenverordnung auch gleich die Legaldefinition dessen, was unter öffentlichem Notstand zu verstehen ist. Dort wird im Grunde beschrieben, was innerstaatlich das Grundgesetz in Art 35 Abs. 2 S. 2 und Abs. 3 S. 1 unter der Überschrift des Katastrophennot-

stands regelt, nämlich die Naturkatastrophe und der besonders schwere Unglücksfall. Letzterer ist menschlichen bzw. technischen Ursprungs und in seinem Schadensausmaß bzw. in seinem Schadenspotenzial mit der Naturkatastrophe vergleichbar. In Art. 2 Nr. 29 Datenverordnung werden neben Naturkatastrophen exemplarisch gesundheitliche Notlagen wie auch Notlagen im Bereich der Cybersicherheit genannt, die innerstaatlich unter Art. 35 Abs. 2 u. 3 GG zu subsumieren wären.

All dies sind Szenarien, die nichts mit dem äußeren Notstand, also mit dem Krieg und seinem Vorfeld, zu tun haben – oder jedenfalls nicht unmittelbar. Worüber ich mich heute mit Ihnen unterhalten möchte, entzieht sich also supranationaler Regelung. Dem deutschen Notstandsrecht sind dagegen datenrechtliche Regelungen für Krise und Krieg alles andere als fremd, wie Sie im Folgenden sehen werden, wenngleich die einschlägigen Normen im Laufe von Jahrzehnten Patina angesetzt haben.

Stichwort Patina: Noch vor wenigen Jahren hätten Sie womöglich gedacht, hier spreche ein Rechtshistoriker, hier komme jemand, der aus dem Gruselkabinett des Kalten Krieges berichten wolle und Vorschriften in die Hand nehme, die, wenn sie auch nicht außer Kraft gesetzt, so doch jedenfalls von der Zeit überholt sind. Die eine oder andere Regelung mag tatsächlich veraltet sein, aber alles, was ich Ihnen hier und jetzt im übertragenen Sinne auf den Tisch legen werde, ist geltendes Recht.

B. Die Renaissance der Machtpolitik und die Rückkehr des Krieges

Warum befassen wir uns heute wieder mit diesen Dingen und mit Gesetzen, die aus den Tiefen des Ost-West-Konfliktes stammen? Warum müssen wir uns mit Gegenständen beschäftigen, die, um ehrlich zu sein, in den drei Jahrzehnten nach Ende des Kalten Krieges niemand mehr anfassen wollte und die hierzulande auch niemand mehr angefasst hat? Bei der Bundeswehr, ebenso in anderen Armeen der westlichen Welt, gilt: Handlungsleitend ist, was der Gegner tut. Und spätestens seit dem 24. Februar 2022 haben wir mit der Vollinvasion der russischen Streitkräfte in die Ukraine eine neue Lage in Europa. Mit dem Ende des Kalten Krieges, jenes Super-Konflikts, der die Weltpolitik über vier Jahrzehnte lang beherrscht und nahezu jeden Bereich des öffentlichen wie privaten Lebens beeinflusst hatte, war der NATO einstweilen der Gegner abhandengekommen. Das nordatlantische Bündnis suchte und fand seine Aufgabe im Internationalen Krisenmanagement (IKM) und war bestrebt, als – etwas despektierlich

ausgedrückt – internationaler Feuerwehrmann überall auf der Welt Brände zu löschen.

Spätestens seit 2022 bekommen wir, freilich ungewollt, eine Lektion in geopolitischer Realität. Die drei klassischen Machtfaktoren, nämlich wirtschaftliche Potenz, militärische Stärke und territorialer Zugriff, erweisen sich gerade nicht als überwundenes Inventar des 19. und 20. Jahrhunderts, sondern vielmehr auf unbestimmte Zeit als die harte Währung der Geopolitik. Hier kommt ein Zitat in den Sinn, das *Thomas Jefferson* zugeschrieben wird. *Jefferson* hat es dem Vernehmen nach zwar nie so gesagt, aber wenn er es auch nicht gesagt hat, so ist es doch gut erfunden. Die Aussage lautet: „Frieden ist jener kurze und glorreiche Moment im Laufe der Geschichte, in dem alle herumstehen und nachladen." Aus dieser Perspektive zeigen sich die drei Jahrzehnte nach dem durch den Untergang des Sowjet-Imperiums besiegelten Ende des Kalten Krieges als eine Art Zwischenkriegszeit. Ungleich besser verbürgt ist das Zitat des griechischen Geschichtsschreibers *Thukydides*, der vor 2.500 Jahren gesagt hat: „Der Starke tut, was er will; der Schwache duldet, was er muss." Es mag im Lichte dieses Zitats bitter klingen, doch die Welt bleibt, wie sie ist und wie sie immer schon war. Die Euphorie der 1990er Jahre, die der Historiker *Andreas Rödder* in der Rückschau als den „unipolaren Moment" beschreibt und die davon ausgeht, dass sich die Demokratie endgültig gegen die Diktatur durchgesetzt habe, war in ihrer Prämisse zu schön, um wahr zu sein. Dieser Erkenntnis hat sich auch die NATO nicht verschlossen, als sie sich 2022 auf dem Gipfel von Madrid eine neue Struktur gegeben hat – ein Schritt, der so bedeutend ist, dass im Bündnis von einer Welt „vor Madrid" und einer Welt „nach Madrid" gesprochen wird.

Was wir innerhalb der NATO, abgesehen von der neuen Struktur und dem damit verbundenen Kräfteansatz, die ich im Folgenden kurz skizzieren werde, seitdem erlebt haben, ist, wenngleich der Begriff in den letzten Jahren überstrapaziert wurde, genau das: eine echte Zeitenwende. Die Rede ist von dem Beitritt Schwedens und Finnlands zur NATO, undenkbar bis vor wenigen Jahren. Der Beitritt dieser beiden Länder zur Allianz ist aus drei Gründen von einer nicht zu unterschätzenden Bedeutung. Erstens: Der strategische Raum des Bündnisses gewinnt ganz erheblich an Tiefe. Zweitens: Die Streitkräfte Schwedens und Finnlands sind zwar zahlenmäßig nicht besonders groß, aber gut ausgerüstet, gut ausgebildet und durch gemeinsame Manöver mit der NATO vertraut. Drittens – und das halte ich für besonders interessant: Mit dem Beitritt Schwedens und Finnlands kommen zwei Völker hinzu, zwei Gesellschaften, die in hohem Maße physisch

wie psychisch resilient sind. In Schweden wurde beispielsweise vor einigen Jahren eine Zivilschutzbroschüre an alle Haushalte verteilt mit dem sinngemäßen Titel „Im Fall von Krise oder Krieg". Das war für die Schweden kein Anlass zu kollektivem Hyperventilieren, wie es in anderen Ländern der westlichen Welt der Fall wäre, sondern vielmehr zu sachlich-nüchterner Kenntnisnahme der Realität und zu entsprechender Reaktion. Hier zeigt sich der Staat, der seine ureigene Aufgabe, die nicht nur Staatsaufgabe, sondern Staatszweck schlechthin ist, ernst nimmt: die Sicherheit seiner Bürger zu gewährleisten.

Zur neuen Struktur der NATO und ihrem Kräfteansatz: Wer am 31. Dezember 2024 in der alten Welt der NATO Response Force (NRF) einschläft, wacht am 1. Januar 2025 in der neuen Welt des NATO Force Model (NFM) auf. Ab dem Neujahrstag werden wir bündnispolitisch in einer neuen Welt – cum grano salis: in einer neuen alten Welt – leben. Die NATO, die zu ihrer Kernaufgabe der kollektiven Bündnisverteidigung zurückkehrt, wird künftig nicht mehr in Jahresscheiben, Kontingenten und Rotation denken und planen, sondern mit dauerhaft gestellten Kräften in ganz anderen Größenordnungen und in anderen zeitlichen Dimensionen. Die Rede ist von militärischen Großverbänden über die Größenordnung der Brigade hinaus. Zu einer Brigade gehören rund 5.000 Soldaten. Aufsehenerregend war in der Vergangenheit schon, wenn einmal von einer Division die Rede war. Das sind bei den NATO-Streitkräften üblicherweise drei Brigaden, also ungefähr 15.000 Soldaten. Die aktuellen Planungen der NATO bewegen sich erstmals seit Ende des Kalten Krieges nun auch wieder auf der Korps-Ebene. Ein Korps besteht in der Regel aus drei Divisionen, bildet also einschließlich der Unterstützungskräfte einen Truppenkörper von mindestens 50.000 Soldaten. Wer nach 1990 von Korps sprach, der meinte lediglich deren Stäbe, nicht aber die Truppen. Im Gegensatz dazu beabsichtigt die NATO, in der nahen Zukunft mehrere Korps entlang der gesamten Ostflanke des Bündnisgebietes von Finnland bis Bulgarien aufzustellen.

Das nordatlantische Bündnis hat sich auf dem Gipfel von Madrid 2022 mit dem NATO Force Model – es hieß zunächst New Force Model – ein Konzept gegeben, das drei Phasen („Tiers") unterscheidet. Innerhalb dieser Phasen müssen auf einem Zeitstrahl, der mit dem D-Day, d.h. mit dem Angriff auf die NATO, beginnt, militärische Großverbände innerhalb kürzester Zeit einsatzbereit sein. Tier 1 beschreibt die Phase von Tag 1 bis Tag 10, in der 100.000 Soldaten mit dem dazugehörigen Material ins Feld gebracht werden. Wenn nach zehn Tagen die Situation nicht bereinigt ist, wovon freilich auszugehen ist, zieht Tier 2 scharf, und wir haben einen

Umfang von weiteren 200.000 Soldaten in dem Zeitraum von Tag 11 bis Tag 30. Sollte bis dahin noch keine Entscheidung herbeigeführt worden sein – und auch damit muss gerechnet werden –, folgt mit Tier 3 ein „All in"-Szenario. Wir sprechen dann zusätzlich von 500.000 Soldaten auf einem Zeitstrahl von Tag 31 bis Tag 180, also insgesamt von 800.000 Soldaten. Zum Vergleich: Die NATO Response Force hatte einen Umfang von rund 50.000 Soldaten.

Ein letzter Punkt in diesem Zusammenhang: Sie haben sicherlich auch schon davon gehört, dass die Zeiten endgültig vorbei sind – wenn es sie überhaupt je gegeben hat –, in denen die Welt binär codiert war auf Krieg und Frieden. Längst hat sich ein diffuser dritter Aggregatzustand zwischen Krieg und Frieden etabliert. Rechtlich sind wir zwar nach wie vor im Normalzustand, im Grundbetrieb, also im Frieden. Die Eskalationsstufen der Notstandsverfassung, auf die ich nachher eingehen werde, sind, salopp gesagt, weit weg. Aber wenn Sie sich ansehen, welche hybriden Aktivitäten der Gegner gegenüber der Bundesrepublik Deutschland wie auch gegenüber anderen Bündnisstaaten entfaltet, also Maßnahmen, die für sich allein betrachtet nicht militärischer Natur sind, die aber den ins Visier genommenen Staat planvoll und systematisch schwächen sollen, dann werden Sie feststellen: Das ist nicht tiefster Frieden.

C. Deutschlands Rolle im Bündnis

Was ist bei alledem nun die Rolle der Bundesrepublik Deutschland? Die Beschreibung der sicherheits- und verteidigungspolitischen Lage beginnt aktuell oftmals mit der stereotypen Feststellung: „Deutschland ist nicht mehr Frontstaat". Das stimmt. Deutschland ist nicht mehr der Frontstaat des Kalten Krieges. Es gibt nicht mehr zwei deutsche Staaten, deren Grenze die Sollbruchstelle des Dritten Weltkriegs ist. Die Zeiten sind vorbei, in denen in der Bundeswehr im Frieden 500.000 Mann und in der Verteidigungsaufstellung, also bei Mobilmachung der Reserve, 1,3 Millionen Mann unter Waffen standen. Vorbei sind glücklicherweise die Zeiten, in denen allein in der alten Bundesrepublik über 5.000 Nuklearsprengköpfe lagen. Zum Vergleich: Heute haben wir im Rahmen der nuklearen Teilhabe eine zweistellige Zahl an taktischen Nuklearwaffen der USA, die auf einem Fliegerhorst in Rheinland-Pfalz gelagert werden. Vorbei sind auch die Zeiten, in denen die Staaten des Warschauer Paktes aufgrund ihrer konventionellen Überlegenheit aus dem Stand mit 100 Divisionen, bei voller Mobilmachung

mit 200 Divisionen einen Angriff gegen die NATO hätten vortragen können. Das sind zweifellos andere Größenordnungen als heute. Kurzum: Wir befinden uns nicht mehr in der Situation, in der sich zwei über allen Maßen bewaffnete Supermächte unmittelbar gegenüberstehen und einander die gegenseitige totale Vernichtung zusichern.

Gleichwohl vermittelt der Satz, Deutschland sei nicht mehr Frontstaat, eine trügerische Sicherheit. Deutschland ist in einer exponierten Rolle als logistische Drehscheibe und als Aufmarschgebiet der NATO, was einerseits an der geographischen Lage der Bundesrepublik, andererseits an ihrem Potenzial als stärkste Wirtschaftsmacht Europas liegt. Die NATO unterhält mehrere Marschrouten, die sie „Lines of Communication" nennt, und fast alle dieser Marschrouten führen über das Bundesgebiet. Zwar werden von den 800.000 Soldaten, von denen ich gerade im Zusammenhang mit dem NATO Force Model gesprochen habe, nicht alle das Bundesgebiet betreten, aber eben doch die meisten. In Zahlen ausgedrückt: Wir gehen davon aus, dass in den ersten 60 Tagen nach Aktivierung der „Drehscheibe Deutschland" – das beginnt auf der Zeitachse bereits vor einem möglichen Angriff auf die NATO – jeden Tag 11.000 Soldaten mit 4.000 Fahrzeugen (Rad und Kette) und 5.000 Containern durch Deutschland verlegen.

Im Bündnis ist Deutschland in einer dreifachen Rolle. Erstens: Wir sind Truppensteller (Troop Contributing Nation) in allen Dimensionen, das heißt zu Lande, zu Wasser, in der Luft, im Cyber- und Informationsraum sowie im Weltraum. Zweitens: Wir sind Transitnation, das heißt militärische Großverbände werden mit Mensch und Material durch die Bundesrepublik Deutschland verlegen, was sich einfacher anhört, als es ist, sowohl rechtlich als auch tatsächlich. Denken Sie angesichts der Zahlen, die ich Ihnen soeben genannt habe, an den Zustand unserer Brücken, Straßen, Schienen usw. Drittens: Wir sind Aufnahmestaat („Host Receiving Nation"), wir nehmen also die Streitkräfte der verbündeten Staaten auch für einen längeren Zeitraum im Bundesgebiet auf. Das ist unsere dreifache Rolle im Bündnis. Wenn Deutschland dieser Rolle gerecht werden will – und hierzu gibt es keine seriöse Alternative –, dann wird dies, um es klar zu sagen, die Anstrengung aller Kräfte von Staat und Gesellschaft erfordern.

Und nun sage ich Ihnen auch, warum ich von der vermeintlich beruhigenden Aussage, Deutschland sei nicht mehr Frontstaat, wenig halte. Bereits in einer aufwachsenden Krise, etwa im Spannungsfall, erst recht aber bei einem bewaffneten Angriff auf das Bündnisgebiet, namentlich an der Ostflanke der NATO, wird der Gegner nicht abwarten, bis nachrückende Kräfte den vorderen Rand der Verteidigung erreicht haben werden. Der

Gegner – und das ist beileibe keine neue Erkenntnis – wird dort Wirkung entfalten, wo das logistische Nervenzentrum für den Nachschub ist. Das bedeutet, dass Autobahnkreuze, Eisenbahnknotenpunkte, Logistikzentren, Flughäfen, Binnenhäfen und Seehäfen in der Bundesrepublik Deutschland nicht mehr nur Ziel von Cyberattacken sind, wie es bereits jetzt der Fall ist, sondern dann auch Ziel von kinetischer Waffenwirkung werden, etwa durch ballistische Raketen oder bewaffnete Drohnen. Machen Sie sich keine Illusionen: Der Betrieb der „Drehscheibe Deutschland" wird in einem scharfen Szenario der Bündnisverteidigung an der Ostflanke, mag diese auch an der Ostgrenze Polens und im Baltikum verortet sein, auch für uns nicht gewaltfrei ablaufen.

Um die Bedarfe zu decken, die in diesem Zusammenhang entstehen, stehen uns mehrere Möglichkeiten offen. Die Streitkräfte haben zunächst ihre eigenen Fähigkeiten. Ich habe allerdings bei der NATO gelernt, dass nicht nur die Bundesrepublik Deutschland, sondern auch die übrigen Verbündeten gerade einmal rund 20 % ihrer Bedarfe mit eigenen Kräften und Fähigkeiten decken können. Das bedeutet, dass die Streitkräfte der NATO-Bündnisstaaten, über einen groben Leisten geschlagen, zu 80 % auf andere Akteure angewiesen sind. Das können staatliche Akteure sein, hierzulande etwa die Polizeien von Bund und Ländern oder das THW, es können ebenso private Akteure sein, etwa Unternehmen der gewerblichen Wirtschaft wie Logistikbetriebe, die Nahrungsmittelwirtschaft, die Automobilindustrie oder Mineralölkonzerne. Leistungen werden auch durch die Streitkräfte zunächst einmal „eingekauft" mit den Mitteln der vertraglichen Leistungserfüllung, also im Wege der Privatautonomie. Wenn aber die Bedarfsdeckung über den Markt mit unverhältnismäßigen Schwierigkeiten verbunden ist oder diese Quelle ganz versiegt, können Bedarfe ebenso im Wege des Rechtszwangs gedeckt werden. Hier befinden wir uns dann im Bereich des Notstandsrechts, bei den Vorsorge- und Sicherstellungsgesetzen, die im Normalzustand überwiegend „gesperrt" sind und auf die ich sogleich näher eingehen werde.

D. Die Notstandsverfassung als rechtliches Koordinatensystem

Die Vorsorge- und Sicherstellungsgesetze, die in ihrer Summe das einfachgesetzliche Notstandsrecht der Bundesrepublik Deutschland bilden, bewegen sich in einem übergeordneten rechtlichen Koordinatensystem. Dieses Koordinatensystem ist die Notstandsverfassung, über die ich hier nur in

aller Kürze referieren möchte. Die Notstandsverfassung, die nicht etwa eine Ausnahme *vom* Grundgesetz, sondern vielmehr eine Ausnahme *im* Grundgesetz darstellt, sieht neben zwei Tatbeständen des inneren Notstandes, die ich vorhin kurz erwähnt habe, die aber im hiesigen Zusammenhang vernachlässigt werden können, vier Tatbestände des äußeren Notstandes vor, von denen drei wiederum eine Eskalationsleiter innerhalb des Kontinuums Frieden – Krise – Krieg bilden.

Am oberen – scharfen – Ende steht der Verteidigungsfall. „Verteidigungsfall" ist nichts anderes als der grundgesetzliche Begriff für „Krieg". Ich erwähne ihn an erster Stelle, obwohl ich weiß, dass es unter dramaturgischen Gesichtspunkten geschickter wäre, die Darstellung im Frieden beginnen zu lassen und bis zum Schießkrieg zu steigern. Ich fange aber deshalb am oberen Ende der Eskalation an, weil der Verteidigungsfall der einzige Tatbestand des äußeren Notstandes ist, der im Grundgesetz legaldefiniert wird. Die vorgelagerten Tatbestände sind – so jedenfalls die herrschende Meinung – inhaltlich auf den Verteidigungsfall ausgerichtet.

Der verfassungsändernde Gesetzgeber von 1968 hat eine beinahe rührende Sorgfalt aufgebracht, um das Szenario eines Krieges auf deutschem Boden in rechtliche Formen zu gießen, der mit an Sicherheit grenzender Wahrscheinlichkeit der Auftakt zum Dritten Weltkrieg unter Einsatz konventioneller, atomarer, biologischer und chemischer Waffen gewesen wäre und der somit die albtraumhaften Bilder der Apokalypse womöglich noch überboten hätte.

Der Verteidigungsfall wird in Art. 115a Abs. 1 S. 1 GG legaldefiniert als eine Situation, in der das Bundesgebiet mit Waffengewalt angegriffen wird oder ein solcher Angriff unmittelbar droht. Formal gibt es drei Wege, die Feststellung zu treffen, dass eine solche Situation eingetreten ist. Das reguläre Verfahren gem. Art. 115a Abs. 1 u. 3 GG sieht so aus, dass die Bundesregierung die Feststellung beim Deutschen Bundestag beantragt. Dieser stellt den Verteidigungsfall mit qualifizierter Zweidrittelmehrheit fest. Das heißt, es muss mindestens die Hälfte der gesetzlichen Mitglieder im Saal sein; von diesen wiederum müssen zwei Drittel für den Antrag stimmen. Dem muss der Bundesrat seinerseits mit Zweidrittelmehrheit zustimmen. Sodann ist die Feststellung durch den Bundespräsidenten im Bundesgesetzblatt zu verkünden. Mein akademischer Lehrer sagte einmal sinngemäß zu mir: „Sehen Sie, im freiheitlichen Rechtsstaat muss sogar der nukleare Weltuntergang noch bürgernah und transparent sein".

Das Grundgesetz bleibt freilich bei diesem aufwendigen Verfahren nicht stehen. Es sieht in Art. 115a Abs. 2 GG ein subsidiäres Verfahren vor: die

ersatzweise Feststellung des Verteidigungsfalls durch den Gemeinsamen Ausschuss, wenn der Deutsche Bundestag in der kritischen Situation nicht sogleich handlungsfähig ist. Die Bezeichnung „Gemeinsamer Ausschuss" mag unüberbietbar langweilig sein, doch verbirgt sich dahinter das „siebte Verfassungsorgan", das Kriegsparlament der Bundesrepublik Deutschland, geregelt in einem eigenen Abschnitt der Bundesverfassung in Art. 53a GG.

Sollte der bewaffnete Angriff auf die Bundesrepublik Deutschland schon begonnen haben, aber gerade keines der zuständigen Verfassungsorgane handlungsfähig sein, beispielsweise – so nennen wir das gelegentlich bei der Bundeswehr – im Falle einer tagzeitunüblichen Lichterscheinung über der Bundeshauptstadt, dann gilt der Verteidigungsfall gem. Art. 115a Abs. 4 S. 1 GG als festgestellt und verkündet, ohne dass hierzu irgendjemand tätig werden müsste. Aber wir sprächen nicht von „German Over-Engineering", wenn nicht die formale Festlegung des (zunächst rechtlich fingierten) Zeitpunktes gem. Art. 115a Abs. 4 S. 2 GG durch das Staatsoberhaupt nachgeholt werden müsste, sobald die Umstände es erlauben.

Was bedeutet das für diejenigen Gesetze, die, wie im Folgenden gezeigt wird, Regelungen für die notstandsbedingte Datenbereitstellung enthalten? Auf der obersten Eskalationsstufe, im Verteidigungsfall, sind sämtliche Vorsorge- und Sicherstellungsgesetze auf einen Schlag zur Anwendung freigegeben.

Das gleiche gilt für die Vorstufe des Verteidigungsfalls, für den Spannungsfall, der nichts anderes ist als das zentrale Mobilmachungsinstrument der Bundesrepublik Deutschland. Der Spannungsfall ist geregelt in Art. 80a Abs. 1 S. 1 Alt. 1 GG, wenngleich nicht legaldefiniert. Letzteres ist kein Versäumnis des verfassungsändernden Gesetzgebers, sondern im Gegenteil ein Nachweis seiner Weitsicht, denn die Situation einer „politischen Vorwarnzeit", in der der Krieg buchstäblich in der Luft liegt, lässt sich nicht auf die abstrakten Tatbestandsmerkmale einer Legaldefinition bringen. Im Spannungsfall jedenfalls sind die Vorsorge- und Sicherstellungsgesetze, die weitreichende Regelungen zur Datenbereitstellung enthalten, ebenfalls auf einen Schlag anwendbar. Die Mehrheit unter den Staatsrechtlern definiert den Spannungsfall als Anspannung der außen- und verteidigungspolitischen Konfliktlage, die einen Angriff auf das Bundesgebiet, mithin den Eintritt des Verteidigungsfalls, befürchten lässt. Ich selbst verwende hierfür eine Faustformel: Spannungsfall bedeutet, dass der Eintritt des Verteidigungsfalls wahrscheinlicher ist als sein Nichteintritt. Der Spannungsfall wird vom Deutschen Bundestag gem. Art. 80a Abs. 1 S. 2 GG mit Zweidrittelmehrheit festgestellt.

Unterhalb des Spannungsfalls bewegt sich der in Art. 80a Abs. 1 S. 2 GG geregelte Zustimmungsfall. Dieser ist sozusagen der kleine Bruder des Spannungsfalls. Er wird in der Literatur auch als die leise Variante des Spannungsfalls bezeichnet. Sollten Sie in Ihrem akademischen Umfeld noch nie von der Eskalationsstufe des Zustimmungsfalls gehört haben, grämen Sie sich nicht. Die Basisdokumente der Bundesregierung bis zum Weißbuch 2016 und bis zur Konzeption Zivile Verteidigung aus demselben Jahr schweigen sich über den Zustimmungsfall ebenfalls aus, mutmaßlich deshalb, weil ihn die Autoren dieser Dokumente ebenso wenig kannten. Seit der Konzeption der Bundeswehr aus dem Jahr 2018 taucht der Zustimmungsfall aber wieder in der Wahrnehmung der Bundesexekutive auf.

Die Vorsorge- und Sicherstellungsgesetze können im Zustimmungsfall durch Parlamentsbeschluss sowohl sukzessive als auch (jedenfalls nach überwiegender Auffassung) en bloc freigeben werden. Im Zustimmungsfall greift die soeben genannte Faustformel nicht. Der Eintritt des Verteidigungsfalls ist nicht wahrscheinlicher als sein Nichteintritt, aber die außenpolitische Konfliktlage ist immerhin derart angespannt, dass die Situation sofortiges Handeln erfordert, das über die rechtlichen Möglichkeiten des Normalzustandes hinausgeht. Es muss also gehandelt werden, wenn auch nicht sogleich mit dem „großen Besteck".

Der einzige Tatbestand des äußeren Notstandes, der jemals aktiviert worden ist, wenngleich erst zehn Jahre nach Ende des Kalten Krieges, in dem und für den er geschaffen worden war, ist der Bündnisfall. Der Bündnisfall ist im Grundgesetz naturgemäß nicht abschließend geregelt. Das Grundgesetz zeichnet den Bündnisfall lediglich vor: Es öffnet sich in Art. 80a Abs. 3 GG für internationales und supranationales Recht. Daher fallen unter die Bündnisklausel auch die Regelungen in Art. 42 Abs. 7 EUV oder Art. 222 AEUV. Doch die entscheidende Regelung kennen Sie alle, denn spätestens seit Beginn des russischen Angriffskrieges gegen die Ukraine ist die Norm in aller Munde: Art. 5 Nordatlantikvertrag. Wegen der unverändert hohen Bedeutung des nordatlantischen Bündnisses für die Freiheit und Sicherheit in Deutschland und Europa wird Art. 80a Abs. 3 GG auch mit voller Legitimation als die „NATO-Klausel" des Grundgesetzes bezeichnet.

Wird einer der Bündnispartner in Nordamerika oder Europa mit Waffengewalt angegriffen, dann betrachten die Bündnispartner dies als Angriff gegen alle. Es gibt allerdings keine Automatismen bei den Rechtsfolgen. Vielmehr können die Staaten nach eigenem Ermessen darüber entscheiden, welche konkreten Maßnahmen der Bündnissolidarität sie ergreifen. Zum

Portfolio gehört in der Bundesrepublik Deutschland auch die Freigabe der Vorsorge- und Sicherstellungsgesetze, allerdings mit einer Ausnahme: Das Arbeitssicherstellungsgesetz, das Maßnahmen des Arbeitszwangs ermöglicht, bleibt wegen der Regelung in Art. 12a Abs. 5 S. 1, Abs. 6 S. 2 GG im Bündnisfall gesperrt.

E. Die einfachrechtlichen Notstandsgesetze

Die Vorsorge- und Sicherstellungsgesetze bilden, wie bereits erwähnt wurde, das Konvolut der einfachrechtlichen Notstandsgesetze der Bundesrepublik Deutschland und so gewissermaßen die „Reserve des Rechts". Es handelt sich um Gesetze, die weitreichende staatliche Eingriffe in nahezu allen Bereichen des öffentlichen Lebens ermöglichen, um eine kriegsbedingte Gefahrenlage – in selteneren Fällen auch eine friedenszeitliche Notlage – in den Griff zu bekommen.

Ein kurzer Überblick: Es handelt sich hierbei um das Bundesleistungsgesetz (BLG), das Wirtschaftssicherstellungsgesetz (WiSiG), das Wassersicherstellungsgesetz (WasSiG), das Verkehrssicherstellungsgesetz (VerkSiG), das Verkehrsleistungsgesetz (VerkLG), das Arbeitssicherstellungsgesetz (ASG), das Energiesicherungsgesetz (EnSiG), das Erdölbevorratungsgesetz (ErdölBevG) sowie das Ernährungssicherstellungs- und -vorsorgegesetz (ESVG). Die Regelungen des früheren Post- und Telekommunikationssicherstellungsgesetzes (PTSG a. F.) sind 2021 in das Telekommunikationsgesetz (TKG) bzw. 2024 in das Postgesetz (PostG) überführt worden. Daneben gibt es einzelne Notstandsregelungen in an sich „notstandsfremden" Gesetzen, etwa in der Straßenverkehrsordnung (StVO), im Verwaltungsverfahrensgesetz (VwVfG) des Bundes wie der Länder, im Bundesbeamtengesetz (BBG), im Beamtenstatusgesetz (BeamtStG), im Infektionsschutzgesetz (IfSG) oder im Betäubungsmittelgesetz (BtMG). Darüber hinaus besteht vor dem Hintergrund der Erfahrungen in der Corona-Pandemie, insbesondere aber im Hinblick auf die „Zeitenwende", die politische Absicht, ein Gesundheitssicherstellungsgesetz zu schaffen und auf diese Weise eine Lücke innerhalb der Notstandsgesetze zu schließen, die seit den Zeiten des Kalten Krieges moniert wird.

Diese Gesetze haben im Wesentlichen eines gemeinsam: Sie befinden sich, von Ausnahmen abgesehen, in einem Standby-Modus, sie stehen also unter Anwendungsvorbehalt. Um Missverständnissen entgegenzuwirken: Diese Gesetze sind geltendes Recht. Sie sind verkündet und ausgefertigt,

sonst wären es keine Gesetze. Sie sind gerade keine geheimen Schubladengesetze, die das Licht scheuen müssten. Es handelt sich gewissermaßen um Gesetze „auf Abruf". Ein Verwaltungsakt, der im tiefsten Frieden auf der Grundlage einer solchermaßen gesperrten Norm erlassen würde, wäre nicht etwa rechtswidrig; er wäre nichtig.

Wie funktioniert nun die Bedarfsdeckung, von der vorhin die Rede war, auf der Grundlage dieser Gesetze? Die Zeiten, in denen ein schneidiger Offizier in die bürgerliche Stube trat, den Bedarf seiner Einheit anmeldete und der brave Bürger gern gab, was er hatte, weil es ja der guten Sache dient, sind vorbei. An die Stelle einer solchen Bedarfsdeckung „auf Zuruf" ist ein rechtsstaatliches Verfahren getreten, das ich exemplarisch anhand des BLG darstellen möchte. Stellen Sie sich eine rechtliche Bühne vor, auf der vier Beteiligte stehen, von denen zwei allerdings in den allermeisten Fällen identisch sind. Wir haben zunächst einen Bedarfsträger. Das kann die Bundeswehr sein, es kann aber auch jede andere Stelle von Bund, Land, Kommune oder auch ein Sozialversicherungsträger sein. Dieser Bedarfsträger wendet sich an die Anforderungsbehörde, die eine Stelle der allgemeinen Verwaltung ist – in der Regel auf der Kreisstufe, also Landkreis oder kreisfreie Stadt. Seitens dieser Anforderungsbehörde wird bei Vorliegen der gesetzlichen Voraussetzungen der Leistungspflichtige herangezogen, um seinen jeweils benötigten Beitrag zu leisten. So kann ein Spediteur verpflichtet werden, seine LKW den eigenen oder auch den verbündeten Streitkräften zur Verfügung zu stellen. Es gibt Verfahrensvereinfachungen in der Phase der Mobilmachung und im Verteidigungsfall, wodurch sich der jeweilige Truppenteil statt an die allgemeine Verwaltung an eine Stelle der Bundeswehrverwaltung wendet. Ausgeschlossen ist dagegen, dass der uniformierte Arm direkt auf den Leistungspflichtigen zugreift. Auf diese Weise soll Selbstbedienung verhindert werden. Es liegt in der Natur der Sache, dass der Leistungsempfänger, der die konkrete Leistung benötigt, an ihrer Anforderung auch das größte Interesse hat. Sein Urteil über Erforderlichkeit und Angemessenheit der Inpflichtnahme eines Privaten wäre selten objektiv. Dies sind also die Beteiligten: Bedarfsträger, Anforderungsbehörde, Leistungspflichtiger und Leistungsempfänger.

Was sind neben der Anforderung einer konkreten Leistung oder der Requirierung einer beweglichen oder unbeweglichen Sache, von denen hier schon die Rede war, die einzelnen Instrumente des Notstandsrechts? Hier ist in erster Linie das Prinzip „Sicherstellung durch Rechtsverordnung" zu nennen. Wenn Sie beispielsweise das WiSiG zur Hand nehmen, werden Sie feststellen, dass in diesem Gesetz, jedenfalls auf erste Sicht, wenig

geschrieben steht. Das WiSiG enthält jedoch weitreichende Ermächtigungen zugunsten der Bundesregierung zum Erlass von Rechtsverordnungen. Und diese Rechtsverordnungen haben es freilich in sich, denn mit ihnen kann die Bundesregierung – um es auf den Punkt zu bringen – die freie und soziale Marktwirtschaft umstellen auf eine Planwirtschaft, oder um es noch deutlicher zu sagen: auf Kriegswirtschaft. Ob das heute in der Praxis funktionieren würde und ob der Staat sich überhaupt zum Unternehmer eignet, das sind ganz andere Fragen, die über das Recht hinausweisen. Wir begnügen uns hier mit der Darstellung der Rechtslage.

Sodann gibt es das Prinzip „Sicherstellung durch Leistungen". Das bedeutet, dass natürliche Personen, juristische Personen des Privatrechts sowie Personenvereinigungen unmittelbar auf der formell-gesetzlicher Grundlage in Anspruch genommen werden, um beispielsweise Werkleistungen zu erbringen. Der Kfz-Mechaniker kann bereits im tiefsten Frieden und erst recht unter Notstandsbedingungen zu Instandsetzungsarbeiten an einem Fahrzeug der Bundeswehr oder des THW, an einem Rettungswagen oder einem Polizeifahrzeug verpflichtet werden, wenn der Bedarf anderweitig nicht oder jedenfalls nicht rechtzeitig gedeckt werden kann. Es gilt bei allen Vorsorge- und Sicherstellungsgesetzen der Grundsatz der Subsidiarität.

Ebenso kann der Einzelne unter Androhung von Sanktionen verpflichtet werden, den Besitz oder sogar das Eigentum an beweglichen und unbeweglichen Sachen an den Bedarfsträger zu übertragen. Ein einfaches Beispiel, nachdem wir bereits über den Spediteur gesprochen haben: Im Kalten Krieg war es gängige bundesrepublikanische Praxis, dass auch auf den Fahrzeugen eines Fleischereibetriebes ein Bereitstellungsbescheid nach § 36 Abs. 3 BLG lag. Im Verteidigungsfall werden diese Fahrzeuge nämlich benötigt für den Transport von Leichen. Der Bereitstellungsbescheid hat zwar keinen Einfluss auf Eigentum und Besitz an dem Fahrzeug. Sollte aber der Tag kommen, an dem das Fahrzeug benötigt wird und der Bereitstellungsbescheid zum Leistungsbescheid erstarkt, kann die zuständige Behörde auf vorhandene Dubletten der Fahrzeugpapiere zurückgreifen, um das Verfahren zu beschleunigen. In diesem Zusammenhang muss ich allerdings darauf hinweisen, dass entsprechende Datenbestände – das gilt nicht nur für die Kfz-Datei – seit Ende des Kalten Krieges kaum noch gepflegt worden sind und heute erst wieder mühevoll aufgebaut werden müssen. Ich werde zum Schluss noch einmal darauf zurückkommen.

Es gibt darüber hinaus die Möglichkeit, dass der Staat den Sektor der gewerblichen Wirtschaft im Ganzen oder auch einzelne Sektoren (beispiels-

weise Wasser, Ernährung, Energie) seiner Regulierung unterwirft. Der Staat kann ebenso in den Kapitalmarkt eingreifen und Börsen- und Wechselkurse festlegen.

Es gibt außerdem – daran werden Sie sich aus der Wirtschafts- und Energiekrise infolge des russischen Angriffs auf die Ukraine erinnern – Spezialmaßnahmen, die in den letzten zwei, drei Jahren in das EnSiG hineingeschrieben worden sind. Die Rede ist von Enteignung, Treuhandverwaltung oder Stabilisierungsmaßnahmen. Sie alle kennen auch die Pressemeldungen, die sich jeweils damit verbinden: Eine Enteignung wurde bei Nordstream erwogen, wenngleich sich die Sache dann anders erledigt hat. Bei der Treuhandverwaltung denken Sie zutreffend an Rosneft und Gazprom Germania, im Zusammenhang mit Stabilisierungsmaßnahmen an Uniper.

F. Im Besonderen: Datenrechtliche Bestimmungen

Das gesamte Instrumentarium der Notstandsgesetze liefe jedoch in der Praxis leer, wenn diese Gesetze nicht auch Auskunfts-, Melde- und sonstige Mitwirkungspflichten regeln würden. Die Zwangsbefugnisse bei der Inanspruchnahme Privater, die ich Ihnen vorgestellt habe, wären wirkungslos, wenn die zuständige Behörde nicht wüsste – um im Beispiel zu bleiben –, was der Spediteur auf dem Hof stehen hat, welches Fahrzeug der Fleischereibetrieb unterhält, über welches Potenzial ein Unternehmen der Nahrungsmittelwirtschaft, der Wasserwirtschaft oder der Mineralölbranche verfügt.

Das bedeutet, dass die jeweils zuständige staatliche Stelle bereits im tiefsten Frieden Zugriff auf diese Daten haben muss. Und deswegen haben wir es hier typischerweise mit denjenigen Vorschriften innerhalb der Vorsorge- und Sicherstellungsgesetze zu tun, die, von Ausnahmen abgesehen, nicht erst zur Anwendung freigegeben werden müssen, sondern bereits im Grundbetrieb zur Verfügung stehen. Wenn Sie quer durch das deutsche Notstandsrecht gehen, werden Sie diesbezüglich auf ein Proprium von Maßnahmen treffen, das sämtlichen Vorsorge- und Sicherstellungsgesetzen eigen ist[1]. Natürlichen und juristischen Personen sowie nicht rechtsfähigen

1 Im Einzelnen handelt es sich um folgende Vorschriften: § 15 BLG, § 14 WiSiG, § 18 WasSiG, § 15 VerkSiG, § 8 VerkLG, §§ 24, 25 ASG, § 10 EnSiG, §§ 33-38 ErdölBevG, § 15 ESVG, § 190 TKG, § 110 PostG.

Personenvereinigungen wird die Pflicht auferlegt, Auskünfte zu erteilen, wenn die zuständige Behörde dies verlangt.

Es liegt nahe, dass die Vorsorge- und Sicherstellungsgesetze auch Betretungsrechte der zuständigen Behörden statuieren. Die Behörde hat das Recht zur Einsichtnahme in die Geschäftsunterlagen, zur Vornahme von Besichtigungen sowie von Prüfungen, beispielsweise zur Entnahme von Proben bei einem Unternehmen der Wasserwirtschaft.

Das datenrechtliche Instrumentarium wäre ein stumpfes Schwert, wenn es nicht auch sanktionsbewehrt wäre. Deswegen sehen ausnahmslos alle Vorsorge- und Sicherstellungsgesetze Sanktionsregelungen vor. In allen Fällen existieren Ordnungswidrigkeitentatbestände, in den meisten Fällen darüber hinaus auch Straftatbestände. Wird die sanktionsbewehrte Handlung unter bestimmten objektiven Bedingungen oder aus bestimmten Beweggründen begangen, dann steigert sich das Unrecht dieser Handlung zur Kriminalstraftat.

Wo das Gesetz eine sanktionsbewehrte Auskunfts-, Melde und Mitwirkungspflicht statuiert, besteht freilich immer die Gefahr, dass der Einzelne in eine Situation gerät, die mit dem Grundsatz *Nemo tenetur se ipsum accusare* unvereinbar ist, also mit dem Verbot des Zwangs zur Selbstbezichtigung. Deswegen enthalten die Vorsorge- und Sicherstellungsgesetze nicht nur Regelungen, mittels derer die zuständige Behörde auf die erforderlichen Daten zugreifen kann, sondern umgekehrt auch Vorschriften, die dem Schutz des Auskunftspflichtigen dienen, ebenso dem Personenkreis, der in § 383 Abs. 1 Nr. 1 bis 3 ZPO genannt wird (Verlobte, Ehegatten, Angehörige). Inhaltlich richtet sich das Ganze auf mögliche Strafverfahren, auf Besteuerungsverfahren oder auf Strafverfahren wegen einer Steuerstraftat oder auf Bußgeldverfahren wegen einer Steuerordnungswidrigkeit.

In die gleiche Richtung weisen schließlich Verwertungsverbote bezüglich solcher Kenntnisse, deren Verwendung nicht ausschließlich dem Zweck des jeweiligen Notstandsgesetzes dient. Der Zweck der Datenerhebung und der Datennutzung ist hier also eng umrissen durch das jeweilige Notstandsgesetz.

G. Ausblick

Meine Ausführungen haben sich – nach dem Versuch einer Darstellung der aktuellen sicherheits- und verteidigungspolitischen Situation – im Wesentlichen auf die Darstellung der Rechtslage beschränkt. Über den Vollzug

dieser Gesetze in der Praxis habe ich dagegen sehr wenig gesagt. Gestatten Sie mir daher zum Schluss die Bemerkung, dass an allen Ecken und Enden der Exekutive 30 Jahre Friedensdividende spürbar sind, also der flächendeckende Rückbau von Kapazitäten der militärischen wie der zivilen Verteidigung nach dem Ende des Kalten Krieges, der sich nach meiner Auffassung heute mehr und mehr als Friedenshypothek erweist. Wir verfügen derzeit nicht nur nicht über die einschlägigen Daten, obwohl wir die Ermächtigungsgrundlagen für deren Erhebung haben. Es mangelt behördlicherseits auch weitgehend an Strukturen und Fähigkeiten zum Vollzug der Vorsorge- und Sicherstellungsgesetze. Wir haben es schlicht verlernt.

Und schließlich: Es fehlt trotz vielbeschworener Zeitenwende in der Gesellschaft noch weitgehend das Bewusstsein dafür – neudeutsch: das Mindset –, dass der Staat zu derlei Eingriffen schon im Grundbetrieb und erst recht unter Notstandsbedingungen ermächtigt ist. Zwar war dies auch während des Kalten Krieges in der Bevölkerung nie ein beliebtes Thema. Aber um ein letztes Mal das Beispiel zu bemühen: Der Spediteur wusste zumindest abstrakt, dass eine Regelung existiert, die es dem zuständigen Beamten der Kommunalverwaltung erlaubt, bereits im Frieden mit einem Bereitstellungsbescheid in der Hand auf den Hof zu kommen. Wer heute als Angehöriger der allgemeinen Verwaltung, womöglich gemeinsam mit einem Vertreter der Wehrverwaltung, auf den Hof der Spedition tritt und dem Geschäftsführer mitteilt, dass mehrere seiner Fahrzeuge – untechnisch gesprochen – nun der Bundesrepublik Deutschland gehören, sollte sich auf eine robuste Reaktion gefasst machen.

Gleichwohl: Die Maßnahmen, zu denen die Notstandsgesetze den Staat ermächtigen – darin die datenrechtlichen Regelungen zur Deckung des staatlichen Informationsbedarfs in Krise und Krieg – sind Bestandteil einer wirkungsvollen zivilen Verteidigung, die in der Summe mit der militärischen Verteidigung den hochkomplexen Organismus der Gesamtverteidigung bildet. Sie sind deshalb Teil einer wirkungsvollen Abschreckung. Und nur diese Abschreckung ist es, die einen potenziellen Angreifer davon abhält, den Zusammenhalt des nordatlantischen Bündnisses – und damit der westlichen Welt – auf die ultimative Probe zu stellen.

Die Außergewöhnliche Notwendigkeit als Voraussetzung von Datenbereitstellungsverlangen nach Art. 14 Data Act

Marie Wienroeder[*]

Das Kapitel V des Data Acts regelt die Bereitstellung von Daten an öffentliche Stellen wegen einer außergewöhnlichen Notwendigkeit. Nach der zentralen Norm des Art. 14 DA sind Dateninhaber zur Bereitstellung von Daten verpflichtet, wenn eine öffentliche Stelle den Nachweis erbringt, dass eine außergewöhnliche Notwendigkeit der Nutzung bestimmter Daten besteht. Diese Nachweispflicht wird auch als Anforderung an das Datenbereitstellungsverlangen nach Art. 17 Abs. lit. b DA wiederholt. Schon nach Art. 14 DA muss die außergewöhnliche Notwendigkeit im Hinblick auf die Erfüllung ihrer rechtlichen Aufgaben im öffentlichen Interesse bestehen. Zentraler Begriff ist also die außergewöhnliche Notwendigkeit, nicht der Notstandsbegriff, der nur einen Unterfall der Definition der außergewöhnlichen Notwendigkeit darstellt[1]. Gerade an diesem Grundbegriff zeigt sich der Ausnahmecharakter der Vorschrift: Es genügt gerade nicht allein, dass die Datennutzung im öffentlichen Interesse und gemeinwohlorientiert wäre[2]. Wann diese außergewöhnliche Notwendigkeit gegeben ist, ist in Art. 15 Abs. 1 DA definiert. ErwGr 63 ergänzt insoweit nur, dass es sich um Umstände handelt, die unvorhersehbar sind, während Umstände, die geplant

* Marie Wienroeder ist wissenschaftliche Mitarbeiterin am Lehrstuhl für Europäisches und Internationales Informations- und Datenrecht an der Universität Passau.

1 *v. Lewinski*, in: Specht/Hennemann (Hrsg.), DGA/DA, 2. Aufl. 2025, Art. 15 DA Rn. 7.

2 Vgl. *v. Lewinski*, in: Specht/Hennemann (Hrsg.), DGA/DA, 2. Aufl. 2025, Art. 15 DA Rn. 3.

oder terminiert werden können bzw. regelmäßig und häufig eintreten, gerade keine außergewöhnliche Notwendigkeit begründen.

Für die Bewältigung eines öffentlichen Notstands ist direkt ersichtlich, worin die außergewöhnliche Notwendigkeit und die Unvorhersehbarkeit liegen. Insofern wurde diese Grundlage zur Datenbereitstellung auch überwiegend begrüßt[3]. Deutlich kritischer wird jedoch die Pflicht zur Datenbereitstellung in anderen als Notstandslagen betrachtet[4], auch wenn nur nicht-personenbezogene Daten verlangt werden können. Es sei nicht klar, worin in diesen Fällen die außergewöhnliche Notwendigkeit bestehe[5]. Insofern ist auch weniger eindeutig, ob die Voraussetzung der Unvorhersehbarkeit stets erfüllt sein wird.

Um zu beantworten, was gerade in Nicht-Notstandslagen die „Außergewöhnlichkeit" bzw. „Unvorhersehbarkeit" ausmacht, möchte ich zunächst die einzelnen Aspekte der Definition in Art. 15 Abs. 1 DA, insbesondere lit. b, auslegen. Die folgende Darstellung stellt die einzelnen (Teil-)Voraussetzungen der Tatbestände nach Art. 15 Abs. 1 lit. a DA denjenigen nach Art. 15 Abs. 2 lit. b DA gegenüber. Um die Parallelen und Unterschiede aufzuzeigen und daraus Argumente für die Auslegung zu entwickeln, soll diese Gegenüberstellung auch der Auslegung der einzelnen Tatbestände im Folgenden zugrunde liegen.

	Art. 15 Abs. 1 lit. a DA	**Art. 15 Abs. 1 lit. b DA**
Gemeinsame Voraussetzungen	Zeitlich befristet Im Umfang begrenzt	Zeitlich befristet Im Umfang begrenzt
Parallele Voraussetzungen	Bewältigung eines öffentlichen Notstands	Erfüllung einer bestimmten im öffentlichen Interesse ausgeübten Aufgabe, die rechtlich ausdrücklich vorgesehen ist (Bsp. Statistik o. Eindämmung/Überwindung eines Notstands) Dabei Tätigwerden auf Grundlage des Unionsrechts o. des nationalen Rechts

3 *Hilgendorf/Vogel*, JZ 2022, 380 (388); *Höne/Knapp*, ZGI 2023, 168 (169); *Leistner/Antoine*, IPR and the use of open data and data sharing initiatives by public and private actors, 2022, S. 109; *Redeker*, CR 2024, 293 (294); *Schaller/Zurawski*, ZD-Aktuell 2022, 01169; *Specht-Riemenschneider*, MMR-Beilage, 2022, 809 (826).

4 *Hilgendorf/Vogel*, JZ 2022, 380 (388); *Höne/Knapp*, ZGI 2023, 168 (170); *Redeker*, CR 2024, 293 (294); *Schaller/Zurawski*, ZD-Aktuell 2022, 01169.

5 *Redeker*, CR 2024, 293 (294).

	Daten zur Bewältigung erforderlich	Durch Fehlen an Erfüllung gehindert
	Können nicht unter gleichwertigen Bedingungen auf andere Weise rechtzeitig u. wirksam beschaffen werden	Alle anderen ihr zur Verfügung stehenden Mittel ausgeschöpft hat, um solche Daten zu erlangen – darunter der Erwerb von nicht-personenbezogenen Daten auf dem Markt durch Angebot von Marktarifen – oder die Inanspruchnahme bestehender Verpflichtungen zur Bereitstellung von Daten – oder der Erlass neuer Rechtsvorschriften, die die rechtzeitige Verfügbarkeit der Daten gewährleisten könnten
Rechtsfolge	Pflicht zur Bereitstellung sowohl personenbezogener als auch nicht-personenbezogener Daten (einschließlich Metadaten)	Pflicht zur Bereitstellung ausschließlich nicht-personenbezogener Daten (einschließlich Metadaten)

A. Voraussetzungen: „Zeitlich befristet" und „Begrenzter Umfang"

Die zeitliche Befristung und der begrenzte Umfang der außergewöhnlichen Notwendigkeit zur Datennutzung sind als Voraussetzungen der Definition am Anfang des Art. 15 Abs. 1 DA vorangestellt und zentral für ihr Verständnis – sie sorgen für eine grundsätzliche Begrenzung des Anspruchs auf Datenbereitstellung[6].

Dass die außergewöhnliche Notwendigkeit zeitlich befristet sein muss, bedeutet zunächst, dass es sich nicht um einen Dauerzustand handeln darf, sondern es einen Endpunkt geben muss. Daraus folgt aber keine klare Begrenzung der möglichen Dauer. Diese kann aber in Zusammenschau mit den anderen Voraussetzungen zumindest etwas weiter eingegrenzt werden. Zum einen durch die Abgrenzung von der Bewältigung eines Notstands zur Überwindung desselben im Falle des lit. a. Im Fall von lit. b währt die Befristung maximal so lange, bis genügend Zeit vergangen ist, um die Daten

6 *v. Lewinski*, in: Specht/Hennemann (Hrsg.), DGA/DA, 2. Aufl. 2025, Art. 15 DA Rn. 3.

mit anderen Mitteln – etwa dem Erlass von Rechtsvorschriften – zu erlangen. Die konkrete Dauer hängt im Ergebnis stets vom Einzelfall ab. Fraglich ist daher vor allem, ob und wie konkret die Befristung im Zeitpunkt des Bereitstellungsverlangens schon benannt werden muss. Oder könnte sogar die weitere Entwicklung der Situation abgewartet werden? Nach Art. 14, 17 Abs. 1 lit. b DA besteht eine Nachweispflicht der staatlichen Stelle, dass die Voraussetzungen der außergewöhnlichen Notwendigkeit vorliegen. Diese besteht somit auch für die Voraussetzung, dass diese zeitlich befristet ist. Allerdings wird es gerade in solchen Ausnahmesituationen auch typisch sein, dass man nicht von Anfang an einen konkreten Zeitpunkt der Befristung benennen kann. Dann müssten jedenfalls die Umstände, unter denen die außergewöhnliche Notwendigkeit beendet wird, klar bezeichnet werden, sodass die Befristung wenigstens bestimmbar ist.

Die Voraussetzung des begrenzten Umfangs der außergewöhnlichen Notwendigkeit der Datennutzung kann man zum einen auf die verlangte Datenbereitstellung beziehen, aber auch auf die Situation, die die außergewöhnliche Notwendigkeit bedingt. Bezogen auf die Situation der außergewöhnlichen Notwendigkeit bedeutet dies parallel zur zeitlichen Befristung, dass sie begrenzbar und von anderen Sachverhalten abgrenzbar sein muss. Eine „allgemein schwierige Lage" kann demnach nicht genügen. Es muss um eine klar abgrenzbare und bezeichnete Notwendigkeit der Datennutzung gehen, der genaue Umfang muss aber im Einzelfall bestimmt werden[7]. Bezüglich der Datenbereitstellung korrespondiert diese Anforderung mit der Voraussetzung, dass es um die Nutzung bestimmter Daten geht.

B. Voraussetzung: Öffentlicher Notstand und Erfüllung einer Aufgabe im öffentlichen Interesse

Art. 15 Abs. 1 lit. a DA setzt die Bewältigung eines öffentlichen Notstands voraus. In Art. 2 Nr. 29 DA wird der „öffentliche Notstand" definiert als eine zeitlich begrenzte Ausnahmesituation, die sich negativ auf die Bevölkerung der Union oder eines Mitgliedstaats bzw. eines Teils davon auswirkt und das Risiko schwerwiegender und dauerhafter Folgen für die Lebensbedingungen, die wirtschaftliche Stabilität oder die finanzielle Stabilität birgt. Darüber hinaus sind nur zeitlich begrenzte Ausnahmesituationen erfasst;

7 *v. Lewinski*, in: Specht/Hennemann (Hrsg.), DGA/DA, 2. Aufl. 2025, Art. 15 DA Rn. 39.

dauerhafte Krisen bzw. Krisenfolgen, die zum Normalzustand werden, können gerade keine außergewöhnliche Notwendigkeit begründen[8]. Dies würde auch der von ErwGr. 63 genannten Unvorhersehbarkeit und zeitlichen Begrenztheit widersprechen.

Der öffentliche Notstand soll nach den einschlägigen Verfahren des Unionsrechts oder des nationalen Rechts festgestellt und amtlich ausgerufen werden, dazu zählen auch Verfahren internationaler Organisationen (ErwGr. 64). Unter die Ausrufung nach den Verfahren internationaler Organisationen würde die Ausrufung einer „gesundheitlichen Notlage internationaler Tragweite" durch die WHO fallen[9]. Diese Voraussetzung stellt eine Parallele zur Voraussetzung dar, dass die Aufgabe nach Art. 15 Abs. 1 lit. b DA rechtlich ausdrücklich vorgesehen sein muss. Beide Voraussetzungen bezwecken Rechtssicherheit für den Dateninhaber[10].

Erfasst ist nur die akute Bewältigung des Notstands, nicht hingegen die Eindämmung bzw. Überwindung und auch nicht die Vorbeugung vor zukünftigen Notstandslagen. In diesen Fällen ist dann unter Umständen ein Übergang zur Datenbereitstellung nach lit. b denkbar, soweit deren Voraussetzungen vorliegen.

Der Data Act nennt in Art. 2 Abs. 29 DA als Beispiele ausdrücklich Notfälle im Bereich der öffentlichen Gesundheit, infolge von Naturkatastrophen, einschließlich solcher, die durch den Klimawandel und die Umweltzerstörung noch verschärft werden, und von Menschen verursachte Katastrophen größeren Ausmaßes, einschließlich schwerer Cybersicherheitsvorfälle. In der Literatur werden verschiedene weitere konkrete Beispiele genannt, etwa die Corona-Pandemie, Umweltkatastrophen wie Waldsterben oder Waldbrände, Dürreperioden, oder auch Meteoriteneinschläge, Erdbeben und Kernkraftunfälle[11]. Ausgenommen sind hingegen Notstände

8 *v. Lewinski*, in: Specht/Hennemann (Hrsg.), DGA/DA, 2. Aufl. 2025, Art. 15 DA Rn. 13.

9 z.B. im Juli 2022 bezüglich des Affenpocken-Ausbruchs: abrufbar unter https://www.tagesschau.de/ausland/europa/who-affenpocken-109.html (zuletzt abgerufen am 17.10.2025).

10 *Wienroeder*, in: Hennemann u.a. (Hrsg.), Data Act – An Introduction, 2024, S. 155; *v. Lewinski*, in: Specht/Hennemann (Hrsg.), DGA/DA, 2. Aufl. 2025, Art. 15 DA Rn. 18.

11 *v. Lewinski*, in: Specht/Hennemann (Hrsg.), DGA/DA, 2. Aufl. 2025, Art. 15 DA Rn. 12, m.w.N.

im Kriegs- und Verteidigungsfall, für diese fehlt die Zuständigkeit der EU, entsprechende Beispiele werden im Data Act insofern auch nicht genannt[12].

Im Gegensatz dazu setzt Art. 15 Abs. 1 lit. b DA die „Erfüllung einer bestimmten im öffentlichen Interesse ausgeübten Aufgabe, die rechtlich ausdrücklich vorgesehen ist" voraus. Konsequent und sinnvollerweise ist nach Art. 17 Abs. 1 lit. h DA die Rechtsvorschrift, aus der sich die Aufgabe ergibt, auch im Datenbereitstellungsverlangen anzugeben. Die Art der Rechtsnorm, in der die Aufgabe ausdrücklich vorgesehen werden muss, ist nicht weiter konkretisiert, somit genügen auch untergesetzliche Normen, wie zum Beispiel Verordnungen[13].

Als Beispiele für solche Aufgaben werden amtliche Statistiken oder die Eindämmung oder Überwindung eines öffentlichen Notstands genannt. Die sehr unterschiedlichen Beispiele zeigen, dass damit wohl keine sachliche Einschränkung verbunden ist und auch Aufgaben aus anderen Sachbereichen erfasst sind, solange sie ausdrücklich rechtlich vorgesehen sind. Die genannten Fälle können aber als Beispiele für den Grad der geforderten Bestimmtheit dienen. Die Verhinderung von öffentlichen Notstandssituationen ist anders als im ursprünglichen Entwurf des Data Acts nicht mehr ausdrücklich als taugliche Situation genannt, kann aber natürlich auch eine rechtlich ausdrücklich vorgesehene Aufgabe sein.

Trotz Verwendung des Begriffs „Aufgabe" dürften Aufgabennormen regelmäßig zu allgemein[14] und weit formuliert sein, um das Merkmal einer „bestimmten Aufgabe" zu erfüllen. Dagegen dürften Normen, die konkreten Maßnahmen zur Erfüllung dieser allgemeinen „Aufgaben" enthalten die Voraussetzung erfüllen. Unter Umständen könnten Aufgabennormen, die schon sehr konkrete Tätigkeiten benennen ebenfalls dieser Anforderung genügen. Gerade mit Blick darauf, dass Art. 15 DA eine unionsrechtliche Norm ist, sollte es nicht darauf ankommen, ob eine Norm als „Aufgabennorm" nach deutschem Rechtsverständnis einzuordnen ist, sondern ob

12 Vgl. *v. Lewinski*, in: Specht/Hennemann (Hrsg.), DGA/DA, 2. Aufl. 2025, Art. 15 DA Rn. 8 (nach Rn. 10 aber Niederschlagung von Aufständen und Bürgerkriegen); *v. Lewinski,* GSZ 2025, 55; *Erkens,* in diesem Band, S. 77 (78 f.).

13 *v. Lewinski*, in: Specht/Hennemann (Hrsg.), DGA/DA, 2. Aufl. 2025, Art. 15 DA Rn. 28.

14 Vgl. *v. Lewinski*, in: Specht/Hennemann (Hrsg.), DGA/DA, 2. Aufl. 2025, Art. 15 DA Rn. 28.

die in der Norm genannte Aufgabe hinreichend „bestimmt" ist, also genau umrissen[15] ist.

Am Beispiel des Bayerischen Rettungsdienstgesetzes[16] (bayRDG) würde das bedeuten, dass etwa Art. 4 Abs. 1 bayRDG, wonach die Landkreise die Aufgabe haben, den öffentlichen Rettungsdienst sicherzustellen, zu allgemein gehalten wäre, um eine bestimmte Aufgabe i.S.v. Art. 15 Abs. 1 lit. b DA darzustellen. Die Festlegung der notwendigen Versorgungsstruktur nach Art. 5 Abs. 1 bayRDG oder Sicherung der Qualität rettungsdienstlicher Leistungen nach Art. 12 Abs. 1 bayRDG wären jedoch als bestimmte Aufgaben anzusehen.

Außerdem wird ein „Tätigwerden auf Grundlage des Unionsrechts oder des nationalen Rechts" vorausgesetzt. Dies ist deutlich allgemeiner als die Voraussetzung einer Aufgabe, die rechtlich ausdrücklich vorgesehen ist. Es ist vor allem fraglich, worin die eigenständige Bedeutung dieser Voraussetzung liegt. Die Voraussetzung erscheint eher vorgelagert, das heißt bezogen auf ein Tätigwerden, in dessen Rahmen dann die spezifische Aufgabe zu erfüllen wäre. Daher kann sie als Tätigwerden im Zuständigkeitsbereich der öffentlichen Stelle verstanden werden.

C. Daten zur Bewältigung erforderlich und durch Fehlen der Daten an Erfüllung gehindert

Nach Art. 15 Abs. 1 lit. a DA dürfen die Daten nur zur Bewältigung des Notstands erforderlich sein, somit ist eine Abgrenzung zu anderen Stadien des Umgangs mit einem Notstand (Vorbeugen, Eindämmen, Überwindung) zwingend erforderlich[17]. Erfasst ist also nur die akute Phase des Notstands, die Abgrenzung zwischen den verschiedenen Phasen der Auseinandersetzung mit dem Notstand ist aber stets einzelfallabhängig[18]. Da von dieser Abgrenzung einerseits die unterschiedlichen Tatbestandsvoraus-

15 Bestimmt auf Duden online: abrufbar unter https://www.duden.de/node/131622/revision/1365072 (zuletzt abgerufen am 17.10.2025).

16 Abrufbar unter https://www.gesetze-bayern.de/Content/Document/BayRDG/true (zuletzt abgerufen am 17.10.2025).

17 *Petel,* Chapter V of the Data Act – What is the European Concept of „B2G data sharing" in the Data Act Proposal, in: Ducuing/Margoni/Schirru (Hrsg.), CiTiP Working Paper Series – White Paper on the Data Act Proposal, 2022, S. 47 (48); *Wienroeder*, in: Hennemann u.a. (Hrsg.), Data Act – An Introduction, 2024, S. 156.

18 *v. Lewinski*, in: Specht/Hennemann (Hrsg.), DGA/DA, 2. Aufl. 2025, Art. 15 DA Rn. 22.

setzungen von lit. a und lit. b und andererseits auch die die verschiedenen daran geknüpften Rechtsfolgen (Zugang zu personen- oder nicht-personenbezogenen Daten, aber auch die unterschiedliche Ausgleichspflicht nach Art. 20 DA) abhängen, ist eine Abgrenzung zwingend notwendig. Gerade auch hier ist also wie oben gezeigt, die zeitliche Komponente relevant.

Die Datennutzung muss zur Bewältigung gerade erforderlich sein, also zur Bewältigung unbedingt notwendig sein.

Die zentrale Voraussetzung für Art. 15 Abs. 1 lit. b DA ist, dass die Stelle ohne die Daten an der Erfüllung einer Aufgabe gehindert wäre. Es ist somit zu bestimmen, wann dies der Fall ist. Das Wort „hindern" kann sowohl unmöglich machen bedeuten als auch erschweren/stören[19]. In der zweiten Bedeutungsvariante könnte diese Voraussetzung also sogar als weiter zu verstehen sein als „erforderlich" in lit. a[20]. Das heißt, diese Voraussetzung hat für die Tatbestandsebene keine starke einschränkende Wirkung. Dies wird aber durch die deutlich stärker eingrenzenden folgenden Voraussetzungen ausgeglichen. Aber auch wenn damit nicht zwingend notwendig zur Erfüllung gemeint ist, wird es wohl nicht genügen, wenn die Aufgabe nur „nicht bestmöglich erfüllt" werden kann.

Weiter setzt Art. 15 Abs. 1 lit. b DA voraus, dass das Fehlen spezifischer Daten die Behörde an der Erfüllung der Aufgabe hindert. In lit. a werden hingegen die „verlangten Daten" genannt. Dieser deutliche Unterschied zwischen lit. a und lit. b spricht dafür, dass die Voraussetzung „spezifische Daten" eine eigenständige Bedeutung hat. Dagegen spricht, dass in beiden Fällen des Art. 15 Abs. 1 DA nach Art. 17 I lit. a DA angegeben werden muss, welche Daten benötigt werden und schon Art. 14 DA von „bestimmten Daten" spricht, was dann also für den gesamten Art. 15 Abs. 1 DA gilt. Daher scheinen nur einige wichtige Voraussetzungen immer wieder betont zu werden.

D. Anforderungen an alternative Beschaffung der Daten

Nach Art. 15 Abs. 1 lit. a DA ist Voraussetzung des Datenbereitstellungsverlangens, dass die Daten nicht unter gleichwertigen Bedingungen auf andere

19 „Hindern" auf Duden online; abrufbar unter https://www.duden.de/node/145110/revision/1427611 (zuletzt abgerufen am 27.11.24).

20 Vgl. *v. Lewinski*, in: Specht/Hennemann (Hrsg.), DGA/DA, 2. Aufl. 2025, Art. 15 DA Rn. 30.

Weise rechtzeitig und wirksam beschafft werden können. Die Datenbereitstellung nach Art. 14, 15 Abs. 1 lit. a DA ist also subsidiär zu anderen Beschaffungsmethoden, aber da die alternative Beschaffung unter gleichwertigen Bedingungen möglich sein müsste, nicht *ultima ratio*[21].

Als Beispiele für Alternativen sind die Nutzung öffentlicher Datenbanken oder die freiwillige Bereitstellung angegeben. Die freiwillige Bereitstellung wird dabei wohl nicht identisch zu „Angebot von Marktttarifen" in lit. b sein. Es ist nicht notwendig, dass es gar keine alternative Beschaffungsmöglichkeit gäbe, sondern genügt, wenn diese keine gleichwertigen Bedingungen hätte. Dies könnte man also schon dann als erfüllt ansehen, wenn diese Alternative nur gegen Entgelt bestünde, da die Datenbereitstellung nach Art. 15 Abs. 1 lit. a DA nach Art. 20 Abs. 1 DA entgeltfrei wäre. Die Gleichwertigkeit der Bedingungen könnte sich aber etwa auch auf Datenqualität, Art des Zugriffs oder „Lizenzbedingungen" beziehen. Eventuell muss auch unterschieden werden, ob die konkrete Bedingung Auswirkungen auf die Bewältigung des Notstands, insbesondere deren Rechtzeitigkeit und Wirksamkeit, hat. Dann müsste die Ungleichwertigkeit von Bedingungen, die keinen relevanten Einfluss auf die Bewältigung des Notstands hätten, unter Umständen ignoriert werden.

Die Beschaffung auf andere Weise müsste auch rechtzeitig und wirksam möglich sein. Dies ist eigentlich selbstverständlich, denn sonst würden sie den Zweck der Bewältigung des Notstands, der von Eilbedürftigkeit gekennzeichnet ist, nicht erfüllen.

Art. 15 Abs. 1 lit. b DA setzt hingegen voraus, dass alle anderen zur Verfügung stehenden Mittel ausgeschöpft wurden, um solche Daten zu erlangen. Dass zunächst alle anderen zur Verfügung stehenden Mittel auszuschöpfen sind, zeigt, dass das Datenbereitstellungsverlangen in diesen Fällen *ultima ratio* ist[22]. Welche Anstrengungen muss die öffentliche Stelle also unternehmen, um alle ihr zur Verfügung stehenden Mittel ausgeschöpft zu haben? Schon nach Art. 1 Abs. 10 DA haben freiwillige Vereinbarungen immer Vorrang. Art. 15 Abs. 1 lit. b DA nennt konkret weitere Möglichkeiten, die vorrangig zu nutzen sind. Auch diese sind nicht abschließend, es handelt sich jedoch um besonders relevante Beispiele.

In diesem Zusammenhang wurde auch kritisiert, dass für diese Voraussetzung nicht direkt ersichtlich ist, worin die „außergewöhnliche Notwen-

21 *Höne/Knapp*, ZGI 2023, 168 (169 f.); *Schröder*, MMR 2024, 104 (105).
22 *Höne/Knapp*, ZGI 2023, 168 (169 f.).

digkeit" liegt – genügt es beispielsweise, dass der Gesetzgeber es versäumt hat, rechtzeitig spezielle Normen für den Datenzugang zu erlassen[23]? Mit Blick auf diese Fragen sollen daher die von Art. 15 Abs. 1 lit. b DA angeführten alternativen Möglichkeiten im Folgenden näher beleuchtet werden.

I. Erwerb von nicht-personenbezogenen Daten auf dem Markt

Zunächst sollen die nicht-personenbezogenen Daten durch Angebot von Markttarifen auf dem Markt erworben werden. Ausgenommen sind dabei nach Art. 15 Abs. 3 DA Fälle, in denen die Daten für die Erstellung von Statistiken benötigt werden und dafür der Erwerb von Daten nach nationalem Recht untersagt ist.

Diese alternative Beschaffungsmöglichkeit wirft die Frage auf, ob es dabei nur um bereits angebotene Daten geht oder ob die öffentliche Stelle auch proaktiv Verträge aushandeln muss[24]. Für letzteres spricht die Formulierung „Angebot von Marktpreisen", die man so verstehen kann, dass die öffentliche Stelle einen Vertrag anbietet. Dann bleibt aber fraglich, wie sich der „Marktpreis" bestimmen lässt[25]. Dies spricht wiederum dafür, dass es einen existierenden Markt für diese Art von Daten geben muss. Gerade wenn nur ein Anbieter für die benötigten Daten existiert, besteht die Gefahr, dass ein Monopol bei der Preisgestaltung ausgenutzt werden kann. Hier wird jedoch gerade der Unterschied zu Art. 15 Abs. 1 lit. a DA relevant, denn die Alternative muss nicht unter gleichwertigen Bedingungen möglich sein, sondern es müssen alle anderen Mittel ausgeschöpft werden. Die Dateninhaber, von denen die Daten erworben werden können, und diejenigen, die für ein Datenbereitstellungsverlangen in Betracht kommen, dürften allerdings häufig dieselben sein. Dadurch ist ein Anreiz für die Dateninhaber gegeben, zu einem Vertragsschluss mit der öffentlichen Stelle zu kommen[26].

23 *Redeker*, CR 2024, 293 (294).

24 Vgl. *Wienroeder*, in: Hennemann u.a. (Hrsg.), Data Act – An Introduction, 2024, S. 156; *MPIIC*, Position Statement 2022, S. 50 f.

25 Vgl. *Wienroeder*, in: Hennemann u.a. (Hrsg.), Data Act – An Introduction, 2024, S. 156; *MPIIC*, Position Statement 2022, S. 50 f.

26 Vgl. *Krämer et al.*, Data Act: Towards a balanced EU data regulation, CERRE report 2023, S. 63; *Wienroeder*, in: Hennemann u.a. (Hrsg.), Data Act – An Introduction, 2024, S. 155.

II. Inanspruchnahme bestehender Verpflichtungen

Unter die Inanspruchnahme bestehender Verpflichtungen zur Bereitstellung von Daten fallen sowohl bestehende Verträge, bestehende Rechtsvorschriften, die zur Datenbereitstellung verpflichten, wie auch existierende Verpflichtung im Rahmen von Auftragsvergaben. Das bedeutet, dass nur dann eine außergewöhnliche Notwendigkeit besteht, wenn die Daten, die bereits „beschaffbar" sind, nicht ausreichen.

III. Erlass neuer Rechtsvorschriften

Die alternative Beschaffung durch den Erlass neuer Rechtsvorschriften, die rechtzeitig die Verfügbarkeit gewährleisten könnten, steht deutlich in Bezug zu den Voraussetzungen „unvorhersehbar" und „zeitlich begrenzt".

Fraglich ist, ob durch Rechtsvorschriften nur formelle Gesetze, die vom Parlament erlassen wurden, erfasst sind oder auch Rechtsverordnungen und andere untergesetzliche Vorschriften, die auch durch die Verwaltung erlassen werden können. Für die Beschränkung auf formelle Gesetze sprechen rechtsstaatliche Erwägungen[27]. Dagegen spricht jedoch, dass alle anderen zur Verfügung stehenden Mittel ausgenutzt werden sollen. Dies muss den Erlass von Rechtsvorschriften durch öffentliche Stelle selbst umfassen. Insbesondere steht der Erlass von Gesetzen der öffentlichen Stelle letztlich auch nicht selbst zur Verfügung, sie könnte dafür nur lobbyieren.

Die drei genannten Beschaffungsmöglichkeiten sind nicht abschließend. Denkbar wären etwa auch Datenspenden aus der Zivilgesellschaft. Diese haben aber den Nachteil, dass sie häufig weniger umfassend sein werden und womöglich vorab nicht klar ist, welche Daten bzw. welche Menge an Daten dadurch beschafft werden kann. Dennoch sollte diese Möglichkeit zumindest erwogen werden. Selbstverständlich sind auch die in Art. 15 Abs. 1 lit. a DA genannten Möglichkeiten der Nutzung öffentlicher Datenbanken und freiwilliger Bereitstellung von Daten zu berücksichtigen.

27 *v. Lewinski*, in: Specht/Hennemann (Hrsg.), DGA/DA, 2. Aufl. 2025, Art. 15 DA Rn. 34.

E. Fazit

Anhand der vorangegangenen Auslegung kann nun klarer untersucht werden, was Unvorhersehbarkeit im Fall von Art. 15 Abs. 1 lit. b DA bedeutet.

Die Erfüllung einer rechtlich vorgesehenen Aufgabe wird typischerweise vorhersehbar sein. Indem ErwGr. 75 einräumt, dass Fälle einer außergewöhnlichen Notwendigkeit, die keine Notstandslage betreffen, häufiger auftreten können, wird diese Anforderung für Fälle nach Art. 15 Abs. 1 lit. b DA bereits etwas eingeschränkt. Das Element der Unvorhersehbarkeit wird zudem ausdrücklich nur in den Erwägungsgründen genannt, insofern ist schon fraglich, ob es die Anwendbarkeit von Art. 15 Abs. 1 lit. b DA wirklich ausschließen sollte, wenn alle anderen Voraussetzungen erfüllt sind.

Die Unvorhersehbarkeit könnte sich in Fällen nach Art. 15 Abs. 1 lit. b DA aber auch darauf beziehen, dass die öffentliche Stelle ohne die Daten, die bereitgestellt werden sollen, an der Erfüllung gehindert werden wird. Ist es also etwa absehbar, dass diese Daten zur Erfüllung der Aufgabe gebraucht werden, aber der Gesetzgeber versäumt es, eine Befugnisnorm zu schaffen, bzw. die öffentliche Stelle versäumt es, diese rechtzeitig zu beschaffen – dann ist die Notwendigkeit der Datennutzung nicht unvorhersehbar. Aus hiesiger Sicht hängt die Frage der Vorhersehbarkeit in den Fällen nach lit. b also eng mit der Ausschöpfung der alternativen Möglichkeiten zusammen. Ist die Notwendigkeit der Datennutzung vorhersehbar (und damit nicht außergewöhnlich), dann besteht typischerweise auch die Gelegenheit, sie mit alternativen Mitteln zu beschaffen.

Daran schließt sich jedoch die Frage an, ob es auch genügt, dass es nicht vorhersehbar war, dass die alternative Beschaffung misslingt. Dafür spricht, dass auch in diesem Fall die Gesamtsituation, dass ohne die Datenbereitstellung die Aufgabe nicht erfüllt werden kann, nicht vorhersehbar war. Wenn aber trotz Absehbarkeit die alternative Beschaffung versäumt wird, sind die Voraussetzungen nicht erfüllt.

Welche Anstrengungen müssen also von der öffentlichen Stelle unternommen werden? Wenn klar ist, dass mithilfe alternativer Mittel die Daten nicht rechtzeitig beschafft werden können, dann wird es genügen, diese Unmöglichkeit nachzuweisen. Der vergebliche Versuch muss also nicht zwingend unternommen werden. Ansonsten müssen aber alle Alternativen ermittelt und verfolgt werden; Art. 15 Abs. 1 lit. b DA ist insofern deutlich.

Wie ist dagegen die Situation zu bewerten, wenn zwar erkannt wird, dass entsprechende Rechtsvorschriften erlassen werden müssen, aber keine Mehrheit für ein Gesetz zustande kommt? Oder auch, wenn wie Ende

2024 die Regierungskoalition aufgelöst wird, bevor ein geplantes Gesetz beschlossen wird? In diesen Situationen würde einerseits das alternative Mittel dann doch nicht zur Verfügung stehen, andererseits ist dann die spätere Verhinderung der Aufgabenerfüllung vorhersehbar. Gerade aus demokratischer Perspektive überzeugt es nicht, fehlende Mehrheiten für eine spezielle Norm zur Datenbereitstellung später durch Datenbereitstellungsverlangen nach Art. 14 DA auszugleichen.

Anders ist dies jedoch zu beurteilen, wenn die Vertragsverhandlungen scheitern, wenn die öffentliche Stelle versucht, die Daten zu Marktpreisen zu erwerben. Zwar muss die öffentliche Stelle nachweisen, dass sie ein ernsthaftes Angebot unterbreitet hat und versucht hat, eine Einigung zu erzielen. Scheitert dies jedoch, dann steht diese Möglichkeit tatsächlich in so nicht vorhersehbarer Weise nicht zur Verfügung.

Zu wessen Lasten gehen Planungs- und Einschätzungsfehler? Die Vorhersehbarkeit kann im Ergebnis nur aus ex ante Perspektive beantwortet werden. Ein mögliches daraus entstehendes Ungleichgewicht zugunsten der öffentlichen Stelle kann durch die Nachweispflicht ausgeglichen werden. Die öffentliche Stelle muss also nachweisen, was im Vorfeld bekannt war, welche Möglichkeiten erwogen wurden und woran die alternativen Mittel zur Beschaffung gescheitert sind.

Durch den Vorrang alternativer Mittel zur Datenbereitstellung, wodurch das Datenbereitstellungsverlangen nach Art. 14 DA nur dann vorgesehen ist, wenn alle anderen Mittel scheitern, wird somit sichergestellt, dass es sich tatsächlich um Ausnahmesituationen handelt, die eine außergewöhnliche Notwendigkeit begründen.

Rechtsschutz gegen Datenverlangen

Meinhard Schröder[*]

A. Einführung

Die europäische Verordnung über harmonisierte Vorschriften für einen fairen Datenzugang und eine faire Datennutzung („Datenverordnung" oder – auch im deutschsprachigen Raum verbreiteter – „Data Act", im Folgenden „DA") zielt als Element der im Februar 2020 veröffentlichten „Datenstrategie" der Europäischen Union[1] darauf ab, Hindernisse für die Nutzung von Daten zu eliminieren. Die Ermöglichung „datengetriebener Geschäftsmodelle" steht zwar im Vordergrund, aber der Data Act ermöglicht es in gewissem Umfang auch, auf das Fehlen von Daten zur Erfüllung öffentlicher Aufgaben zu reagieren: Kapitel V Data Act sieht vor, dass Dateninhaber in Fällen außergewöhnlicher Notwendigkeit durch die öffentliche Hand zur Bereitstellung von Daten verpflichtet werden können (sog. Datenverlangen[2]). Damit werden Daten in privater Hand für die Erfüllung öffentlicher Aufgaben nutzbar gemacht; es kommt (ungeachtet des Streits

* Meinhard Schröder ist Inhaber des Lehrstuhls für Öffentliches Recht, Europarecht und Informationstechnologierecht an der Universität Passau.

1 *Europäische Datenstrategie*, COM (2020) 66 final, S. 4 ff.

2 Der Data Act ist in der Begriffsverwendung inkohärent: Teils ist von Datenverlangen, teils auch von Datenbereitstellungsverlangen die Rede, gemeint ist aber dasselbe. Siehe

darüber, was unter dem Begriff der „Bereitstellung", die nach dem Data Act verlangt werden kann, zu verstehen ist[3]) zu hoheitlich angeordneten B2G-Datenströmen[4].

Dass öffentliche Stellen von Privaten Daten verlangen oder an solche Daten gelangen können, ist kein Novum, wie beispielsweise Volkszählungen von der Antike bis zur Gegenwart belegen[5]. Rechtsstaatlich eingehegte Befugnisse für die „hoheitliche Datenbeschaffung" bestehen nicht erst seit der Entstehung des Datenschutzrechts, das allerdings (bezogen auf personenbezogene Daten) die mitunter hypertrophe Präzisierung dieser Befugnisse mit sich gebracht hat, sondern schon viel länger, etwa in Form der Befugnis zur strafprozessualen Sicherstellung von Datenträgern (und damit mittelbar auch von Daten), gestützt auf § 94 StPO. Mit der zunehmenden Ubiquität von Daten in der Gesellschaft und der gleichzeitigen Bedeutung für die Erfüllung staatlicher Aufgaben hat der Staat die Befugnisse für seine Datenbeschaffung ausgeweitet. Neben detailliert geregelten Pflichten zur Offenbarung personenbezogener Daten für verschiedenste Verwaltungsangelegenheiten liegt ein Schwerpunkt im Strafprozess- und Gefahrenabwehrrecht, wo mittlerweile beispielsweise Online-Durchsuchungen (§ 100b StPO, § 49 BKAG usw.) oder auch die präventivpolizeiliche Sicherstellung von Daten (Art. 25 Abs. 3 BayPAG) detailliert geregelt sind. Insbesondere im Wirtschaftsverwaltungsrecht finden sich zudem zahlreiche Normen, die Wirtschaftsteilnehmer zu Auskünften verpflichten und den Aufsichtsbehörden die Nachschau ermöglichen; beispielhaft genannt sei nur § 29 GewO. Eine solche Auskunft kann sich jedenfalls auf das Vorhandensein bestimmter Daten beziehen; teilweise wird sogar angenommen, dass eine Vorlagepflicht von Geschäftsunterlagen (und damit dann wohl auch von Daten) bestehe[6]. Zumindest können „Prüfungen und Besichtigungen" im Rahmen einer Nachschau auch (geschäfts-) datenbezogen sein.

Kapitel V des Data Acts stellt gegenüber diesen mehr oder weniger klassischen Vorschriften einen Paradigmenwechsel dar: Mithilfe der weiten

zu den legistischen Mängeln des Data Act *Schröder*, in: Bomhard/Schmidt-Kessel (Hrsg.), Data Act, 2025, Einf. Kapitel V Rn. 2.

3 *Schröder*, in: Bomhard/Schmidt-Kessel (Hrsg.), Data Act, 2025, Art. 14 DA Rn. 15.

4 *Schröder*, MMR 2024, 104 (105).

5 Siehe zur Rechtsgeschichte des Datenschutzes (und damit auch hoheitlicher Datenverlangen) *v. Lewinski/Rüpke/Eckhardt*, Datenschutzrecht, 3. Aufl. 2025, § 2.

6 Vgl. zum Meinungsstand *Schröder*, in: Korte/Repkewitz/Schulze-Werner (Hrsg.), GewO, 327. ErgLfg. 2021, § 29 Rn. 42.

Fassung des Begriffs „außergewöhnliche Notwendigkeit" in Art. 15 DA[7] normiert der europäische Gesetzgeber in Art. 14 DA im Grundsatz eine Generalklausel für Datenverlangen. Begrenzt wird ihre Reichweite einerseits situativ durch das Erfordernis der „außergewöhnlichen Notwendigkeit" und andererseits durch die in Art. 15 Abs. 1 lit. a und b DA in unterschiedlicher Intensität zum Ausdruck gebrachte Subsidiarität gegenüber anderen Mitteln der hoheitlichen „Datenbeschaffung". Die Vielzahl der in diesem Zusammenhang verwendeten unbestimmten Rechtsbegriffe und die in Art. 17 Abs. 1 und 2 DA detailliert geregelten formellen und materiellen Anforderungen an Datenverlangen lassen Kontroversen zwischen Dateninhabern und zu Datenverlangen berechtigten Stellen über die Rechtmäßigkeit konkreter Datenverlangen wahrscheinlich erscheinen, so dass der Frage des Rechtsschutzes gegen Datenverlangen auch im Kontext des Data Act erhebliche Bedeutung zukommen dürfte.

Der Data Act selbst gibt nur punktuell Antworten auf Rechtsschutzfragen, vor allem in Form von Beschwerderechten[8] und mit einem (weitgehend deklaratorischen) Verweis auf das Recht auf effektiven Rechtsschutz gegen Entscheidungen der zuständigen Behörden[9]. Erforderlich ist daher – unter Beachtung allgemeiner Rechtsschutzprinzipien (dazu B.) – der Rückgriff auf die allgemeinen Regelungen zum Rechtsschutz. Diese variieren in Abhängigkeit davon, welche Stelle ein Datenverlangen ausspricht. Bei Datenverlangen öffentlicher Stellen eines Mitgliedstaats i.S.d. Art. 2 Nr. 28 DA (dazu C.) kommt im Ausgangspunkt dessen Rechtsschutzsystem zur Anwendung; es kann aber aufgrund europarechtlicher Vorgaben zu modifizieren sein, sei es infolge des Anwendungsvorrangs konkreter Vorgaben des Unionsrechts, sei es zur Sicherung von dessen effektiver und nichtdiskriminierender Anwendung. Bei Datenverlangen europäischer Stellen (dazu D.) richtet sich der Rechtsschutz hingegen nach den Vorgaben des AEUV, die gegebenenfalls um Vorgaben des Data Act zu ergänzen sind. Besonders schwierige Fragen stellen sich, wenn der Dateninhaber nicht derselben Jurisdiktion unterliegt wie die Stelle, welche die Bereitstellung der Daten verlangt (dazu E.).

7 Dazu kritisch *Wienroeder*, in diesem Band, S. 95 ff.

8 Art. 17 Abs. 5, 20 Abs. 5, 21 Abs. 5, 38 Abs. 1 Data Act; zu Art. 18 Abs. 5 Data Act siehe noch detailliert unter C.II.3.

9 Art. 39 Data Act.

B. Erfordernis effektiven gerichtlichen Rechtsschutzes gegen Datenverlangen

Wie im Fall von Datenverlangen nach Kapitel V Data Act die verschiedenen Rechtsschutzbestimmungen konkret zusammenspielen, ist noch ungeklärt. Die zu entwickelnde Lösung muss den Rahmenbedingungen Rechnung tragen, die sich aus dem – sowohl im Unionsrecht wie auch im mitgliedstaatlichen Recht anerkannten – Gebot effektiven Rechtsschutzes ergeben.

Für Datenverlangen deutscher Stellen i.S.d. Art. 2 Nr. 28 DA ist die Garantie effektiven Rechtsschutzes aus Art. 19 Abs. 4 GG zu beachten. Zwar ist im Anwendungsbereich des Data Act auch Art. 47 Abs. 1 GRCh von Bedeutung, denn die Ausübung der im Data Act vorgesehenen Befugnisse ist Durchführung des Unionsrechts i.S.d. Art. 51 Abs. 1 Alt. 2 GRCh. Jedenfalls ergänzend (vgl. Art. 53 GRCh a.E.), nach Auffassung des Bundesverfassungsgerichts[10] sogar primär, sind aber auch die verfassungsrechtlichen Anforderungen an effektiven Rechtsschutz gegen die öffentliche Gewalt, die aus Art. 19 Abs. 4 GG entwickelt wurden, zu berücksichtigen, soweit sie nicht durch vorrangiges Unionsrecht verdrängt sind[11]. Bei Datenverlangen der Europäischen Kommission, der EZB oder einer Einrichtung der Union sind diese gemäß Art. 51 Abs. 1 Alt. 1 GRCh ohnehin an die Vorgaben der Grundrechtecharta und damit auch an das Gebot effektiven Rechtsschutzes aus Art. 47 Abs. 1 GRCh gebunden. Dieser Standard gilt als Mindeststandard auch bei Datenverlangen öffentlicher Stellen anderer Mitgliedstaaten.

Beide Grundrechtsverbürgungen verlangen, dass der Rechtsschutz effektiv bzw. wirksam ist – Art. 47 Abs. 1 GRCh schon im Normtext, Art. 19 Abs. 4 GG in der völlig unbestrittenen Interpretation durch Rechtsprechung[12] und Schrifttum[13]. Welche organisatorischen und verfahrensrechtlichen Vorkehrungen erforderlich sind, um die Effektivität des Rechtsschutzes zu gewährleisten, kann hier nicht umfassend erörtert werden; mit Blick auf Kapitel V Data Act erscheinen allerdings drei Punkte erwähnenswert.

10 Zur parallelen Anwendbarkeit der Grundrechtsebenen im nicht-vollharmonisierten Bereich und zur primären Orientierung am Grundgesetz vgl. BVerfGE 152, 152 („Recht auf Vergessen I").

11 Vgl. zum Anwendungsvorrang des Unionsrechts gegenüber weiterreichenden mitgliedstaatlichen Grundrechtsverbürgungen EuGH, Urt. v. 26.2.2013, C-399/11 – Melloni, EuZW 2013, 305 (Rn. 57 ff.).

12 Vgl. schon BVerfGE 8, 274 (326); aus neuerer Zeit BVerfGE 149, 346 Rn. 34.

13 Vgl. statt vieler *Schmidt-Aßmann*, in: Dürig/Herzog/Scholz (Hrsg.), GG, 92. ErgLfg. 2020, Art. 19 Abs. 4 GG Rn. 229.

I. Erforderlichkeit gerichtlichen Rechtsschutzes

Erstens könnte man mit Blick auf Art. 18 Abs. 2 DA, der dem Dateninhaber das Recht gibt, die Bereitstellung der Daten unter bestimmten Voraussetzungen zu verweigern, oder mit Blick auf den in Art. 18 Abs. 5 DA vorgesehenen Streitschlichtungsmechanismus in Frage stellen, ob es überhaupt gerichtlichen Rechtsschutzes gegen Datenverlangen bedarf. Hierin läge ein Verweis auf das anerkannte Institut des Rechtsschutzbedürfnisses, dessen Fehlen zur Unzulässigkeit eines Rechtsbehelfs führt. An das Vorliegen des Rechtsschutzbedürfnisses sind allerdings keine allzu hohen Anforderungen zu stellen[14]; typischerweise ist es schon durch die Belastung mit dem Hoheitsakt indiziert[15].

Für das Verweigerungsrecht gem. Art. 18 Abs. 2 DA erscheint es insofern sehr fraglich, ob sich durch seine Ausübung wirklich das gleiche Ergebnis „sachgerechter – insbesondere einfacher, umfassender, schneller oder billiger[16] – " als mit einer Klage (ggf. verbunden mit einem Antrag auf Eilrechtsschutz) erreichen lässt. Zwar hat die Verweigerung auf den ersten Blick eine ähnliche Wirkung wie die Suspendierung eines Verwaltungsakts. Damit kann aber allenfalls das Rechtsschutzbedürfnis für einen Eilantrag entfallen (dazu noch unten, C.II.2.)), nicht hingegen für ein Hauptsacheverfahren, das auf eine abschließende Klärung der Rechtslage zwischen den Beteiligten abzielt. Bei Verwaltungsakten bedarf es der Klage zudem, um den Eintritt der Bestandskraft zu verhindern[17]. Dieses Ergebnis wird auch gestützt durch einen Blick auf Parallelvorschriften, bei denen einer durch Verwaltungsakt ausgesprochenen Verpflichtung (Aussage-)Verweigerungsrechte entgegengehalten werden können, beispielsweise in § 29 GewO. Auch hier ist nicht davon auszugehen, dass das Verweigerungsrecht das Rechtsschutzbedürfnis für eine gerichtliche Klärung entfallen lässt[18]. Schließlich bringt auch Art. 18 Abs. 5 DA zum Ausdruck, dass ein Datenverlangen (unabhängig von der Verweigerung nach Art. 18 Abs. 2 DA) angegriffen werden kann[19].

14 BVerfGE 110, 77 (85); so auch *Schenke*, in: Kahl/Waldhoff/Walter (Hrsg.), Bonner Kommentar, 227. ErgLfg. 2024, Art. 19 Abs. 4 GG Rn. 318.
15 Vgl. *Ehlers*, in: Schoch/Schneider (Hrsg.), VwGO, Grundwerk, Vorbem. § 40 Rn. 80.
16 *Ehlers*, in: Schoch/Schneider (Hrsg.), VwGO, Grundwerk, Vorbem. § 40 Rn. 81.
17 Vgl. dazu *Redeker*, CR 2024, 293 (296).
18 Vgl. *Schröder*, in: Korte/Repkewitz/Schulze-Werner (Hrsg.), GewO, 327. ErgLfg. 2021, § 29 Rn. 52.
19 *Schröder*, in: Bomhard/Schmidt-Kessel (Hrsg.), Data Act, 2025, Art. 18 DA Rn. 30.

Mit Blick auf Art. 18 Abs. 5 DA mag man zudem erwägen, ob das dort vorgesehene Streitschlichtungsverfahren den gerichtlichen Rechtsschutz ersetzen soll. Ob der Unionsgesetzgeber das mit der erst im Trilog eingefügten Norm bezwecken wollte, ist unklar. Eine solche – dem Wortlaut nach wohl mögliche – Interpretation wäre allerdings nicht mit Art. 47 GRCh vereinbar, der genau wie Art. 19 Abs. 4 GG gerade Rechtsschutz durch ein Gericht und nicht durch eine Behörde fordert. In einer solchen Situation ist – ähnlich der verfassungskonformen Auslegung im deutschen Recht – eine primärrechtskonforme Auslegung vorzunehmen[20], die dann dazu führen muss, dass der Rechtsweg zu einem Gericht eröffnet bleibt.

II. Zulässigkeit von Vorverfahren

Sieht man in Art. 18 Abs. 5 DA die Normierung eines obligatorischen Vorverfahrens[21], wirft dies zweitens die Frage auf, ob dem gerichtlichen Rechtsschutz ein solches obligatorisches Verfahren vorgelagert werden darf. Schon ein Blick in das geltende Recht zeigt allerdings, dass obligatorische Vorverfahren verbreitet und keine Erfindung des Gesetzgebers des Data Act sind – zu nennen ist insbesondere das Widerspruchsverfahren in §§ 68 ff. VwGO. Vorverfahren werden, wenn sie durch sachgerechte Erwägungen (etwa die Entlastung der Justiz) veranlasst sind, grundsätzlich für zulässig erachtet und dürfen lediglich nicht durch ihre konkrete Ausgestaltung (etwa unbegrenzte Dauer) die Effektivität des gerichtlichen Rechtsschutzes konterkarieren, sodass dieser zu spät käme[22]. Im Rechtsschutzsystem der EU ist in Art. 263 Abs. 5 AEUV sogar ausdrücklich vorgesehen, dass Rechtsakte zur Gründung von Einrichtungen und sonstigen Stellen der Union vorsehen können, dass vor Erhebung von Nichtigkeitsklagen „besondere Bedingungen" erfüllt werden müssen. Hierzu werden insbesondere Vorverfahren gerechnet[23].

20 Dazu *Leible*, in: Riesenhuber (Hrsg.), Europäische Methodenlehre, 2006, § 6.
21 Dazu noch unten C.II.3.
22 BVerfGE 35, 65 (72); 40, 237 (256); *Schmidt-Aßmann*, in: Dürig/Herzog/Scholz (Hrsg.), GG, 92. ErgLfg. 2020, Art. 19 Abs. 4 GG Rn. 249.
23 Vgl. dazu *Dörr*, in: Grabitz/Hilf/Nettesheim (Hrsg.), Das Recht der Europäischen Union, 83. ErgLfg. 2024, Art. 263 AEUV Rn. 117 f.

III. Vorrang des Primärrechtsschutzes

Mit Blick auf Art. 20 DA ist drittens darauf hinzuweisen, dass der Rechtsschutz gerade mit Blick auf das konkret bedrohte subjektive Recht effektiv sein muss. Daraus resultiert ein grundsätzliches Prinzip des Vorrangs des Primärrechtsschutzes. Ansprüche auf eine Ausgleichszahlung, wie sie Art. 20 DA in bestimmten (nicht aber allen) Fällen vorsieht, oder gar auf öffentliche Anerkennung des Beitrags des Dateninhabers sind also nicht geeignet, den gerichtlichen Rechtsschutz gegen ein Datenverlangen zu substituieren. Dagegen lässt sich auch nicht anführen, dass das Bundesverfassungsgericht im Vergaberecht für den Unterschwellenbereich den Sekundärrechtsschutz für ausreichend erachtet hat[24]. Unabhängig davon, ob man diese Entscheidung für überzeugend hält[25], liegt in den Augen des Gerichts schon kein Fall vor, in dem effektiver Rechtsschutz gegen die öffentliche Gewalt gem. Art. 19 Abs. 4 GG erforderlich ist, da bei der Vergabe öffentlicher Aufträge keine Ausübung von Hoheitsgewalt im Sinne dieser Norm stattfinde[26]. Somit kann die Entscheidung nicht als Absage an das Prinzip des Vorrangs des Primärrechtsschutzes im Anwendungsbereich des Art. 19 Abs. 4 GG verstanden werden. Anders als im Vergaberecht tritt die öffentliche Hand bei Datenverlangen auch nicht wie ein „anderer Marktteilnehmer" auf, sodass die für das Vergaberecht entwickelten geringeren Anforderungen[27] auch nicht übertragbar erscheinen.

C. Rechtsschutz gegen Datenverlangen deutscher öffentlicher Stellen

Der Rechtsschutz gegen Datenverlangen deutscher öffentlicher Stellen i.S.d. Art. 2 Nr. 28 DA richtet sich im Ausgangspunkt nach deutschem Recht; hieran ändert sich auch nichts dadurch, dass eine Verordnung der EU vollzogen wird[28]. Insofern stellt sich einerseits mit Blick auf das ausdifferenzierte Rechtsschutzsystem der VwGO die Frage nach der Rechtsnatur von Datenverlangen und damit der richtigen Verfahrensart, andererseits ist die Einbettung der punktuellen Rechtsschutzvorgaben des Data Act in das nationale Recht von Interesse.

---

24 BVerfGE 116, 135 (155 ff.).
25 Kritik etwa bei *Siegel*, DÖV 2007, 237.
26 BVerfGE 116, 135 (149 f.).
27 *Siegel*, DÖV 2007, 237 (243) spricht von einer „bereichsspezifische[n] Ausnahme".
28 Zum dezentralen Rechtsschutzsystem vgl. *Wegener*, in: Calliess/Ruffert (Hrsg.), EUV/AEUV, 6. Aufl. 2022, Art. 267 AEUV Rn. 1.

I. Rechtsnatur von Datenverlangen und Verfahrensarten

Dateninhaber müssen nach Kapitel V Data Act die relevanten Daten nicht *ipso iure* bereitstellen, sondern nur auf „Verlangen" einer berechtigten Stelle. Nach deutschem Recht stellt ein Datenverlangen einen Verwaltungsakt i.S.d. § 35 S. 1 VwVfG bzw. seiner landesrechtlichen Pendants dar. Die Regelung liegt darin, die in Art. 14, 18 Abs. 1 DA vorgesehene Pflicht zur Datenbereitstellung für den konkreten Adressaten im konkreten Fall zu begründen. Die Einordnung als Verwaltungsakt kann auch nicht unter Berufung darauf in Frage gestellt werden, dass es infolge der in Art. 18 Abs. 5 DA vorgesehenen Verhandlungspflicht am hoheitlichen Charakter der Maßnahme fehle. Schon Art. 1 Abs. 6 UAbs. 1 DA lässt erkennen, dass zwischen der einseitigen Ausübung von Befugnissen und vertraglichen Vereinbarungen über die Weitergabe von Daten zu differenzieren ist. Die Einordnung des Art. 14 DA als einseitige Befugnisnorm wird auch durch die Verweigerungsmöglichkeiten des Adressaten gem. Art. 18 Abs. 2 DA nicht in Frage gestellt. Insofern kann ein Vergleich mit verwaltungsrechtlichen Auskunftsverweigerungsrechten[29] oder mit der Befugnis zur Beantragung eines Austauschmittels im Polizeirecht[30] angestellt werden. Auch in diesen Fällen können die Adressaten eines Verwaltungsakts Einwände erheben und den Eintritt der angeordneten Rechtsfolge abwenden, ohne dass deshalb die Verwaltungsaktqualität der Maßnahme in Frage stünde.

Konsequenz der Einordnung von Datenverlangen als Verwaltungsakte ist, dass sie mit dem Rechtsbehelf der Anfechtungsklage (§ 42 Abs. 1 Alt. 1 VwGO) anzugreifen sind. Dies gilt sowohl für den Adressaten eines Datenverlangens als auch für Dritte, deren Rechte, z.B. Geschäftsgeheimnisse, möglicherweise durch das Verlangen (oder seine Erfüllung) beeinträchtigt werden könnten[31]. Die Frage, ob es vor der Erhebung einer Anfechtungsklage eines Vorverfahrens gem. §§ 68 ff. VwGO bedarf, ist – unabhängig von einem möglichen Entfallen des Vorverfahrens nach Bundesrecht oder Landesrecht (§ 68 Abs. 1 S. 2 VwGO) – im Kontext der besonderen Anforderungen des Data Act zu beantworten (dazu sogleich II.3.).

29 Etwa in § 29 Abs. 3, dazu *Schröder*, in: Korte/Repkewitz/Schulze-Werner (Hrsg.), GewO, 327. ErgLfg. 2021, § 29 Rn. 56 ff.

30 Vgl. etwa Art. 5 Abs. 2 S. 2 bayPAG.

31 Dazu, auch zur Frage der Klagebefugnis, *Schröder*, in: Bomhard/Schmidt-Kessel (Hrsg.), Data Act, 2025, Art. 18 DA Rn. 38.

Ob Anträge auf Eilrechtsschutz gem. § 80 Abs. 5 VwGO (oder, im Fall von Dritten, gem. § 80a Abs. 3 VwGO) in Betracht kommen, hängt in erster Linie davon ab, ob ein Hauptsacherechtsbehelf gegen ein Datenverlangen gem. § 80 Abs. 1 S. 1 VwGO Suspensiveffekt entfaltet oder ob dieser aufgrund gesetzlicher (§ 80 Abs. 2 S. 1 Nrn. 1 – 3a VwGO) oder behördlicher (§ 80 Abs. 2 S. 1 Nr. 4 VwGO) Anordnung entfällt. Insofern bleibt abzuwarten, ob und inwieweit der deutsche Gesetzgeber in dem (aus anderen Gründen sowieso vor dem 12. September 2025 zu verabschiedenden[32]) Gesetz zur Implementierung des Data Act anordnen wird, dass die aufschiebende Wirkung von Rechtsbehelfen entfallen soll. Für die Fälle des Art. 15 Abs. 1 lit. a DA (Datenverlangen zur Notstandsbewältigung) würde eine solche Anordnung naheliegen, in Fällen des Art. 15 Abs. 1 lit. b DA (Datenverlangen in anderen Fällen) erscheint es sachgerechter, die Entscheidung über die sofortige Vollziehbarkeit der Behörde zu überlassen. Neben der Frage der Statthaftigkeit von Anträgen auf Eilrechtsschutz gegen Datenverlangen kann sich angesichts der Vorgaben des Unionsrechts auch die Frage stellen, ob überhaupt ein Rechtsschutzbedürfnis für Eilrechtsschutz besteht (dazu sogleich II.3.).

II. Einbettung der Vorgaben des Data Act in das System der Verwaltungsgerichtsordnung

Obwohl das Unionsrecht den Rechtsschutz in den von ihm erfassten Bereichen grundsätzlich den Mitgliedstaaten überlässt (vgl. auch Art. 19 Abs. 1 UAbs. 2 EUV), wird deren Verfahrensautonomie neben den generellen Grenzen der Äquivalenz und Effektivität[33] dadurch beschränkt, dass zwingenden Vorgaben des Unionsrechts Rechnung zu tragen ist. Im Data Act finden sich drei Vorschriften, deren Verknüpfung mit dem eben skizzierten Rechtsschutzsystem klärungsbedürftig erscheint.

32 Vgl. Art. 50 DA. Zu den zu regelnden Punkten gehört beispielsweise die Benennung der zuständigen Behörden gem. Art. 37 Abs. 1 DA oder die Festlegung von Sanktionen für Verstöße gem. Art. 40 DA.

33 Vgl. aus der ständigen Rechtsprechung des EuGH etwa *EuGH,* Urt. v. 12.5.2011, C-107/10, BeckRS 2011, 80513 Rn. 29 – Enel Maritsa Iztok 3; siehe auch *v. Danwitz*, Europäisches Verwaltungsrecht, 2008, S. 483 ff.

1. Beschwerderecht nach Art. 38 Abs. 1 Data Act

Art. 38 Abs. 1 DA räumt natürlichen oder juristischen Personen (egal ob Dateninhaber oder nicht) eine Beschwerdemöglichkeit ein, wenn sie „der Ansicht sind, dass ihre Rechte nach dieser Verordnung verletzt wurden". Die Vorschrift ist dem datenschutzrechtlichen Beschwerderecht (Art. 77 DSGVO) nachgebildet. Sie ermöglicht die Involvierung von Aufsichtsbehörden (hier der „zuständigen Behörde" i.S.d. Art. 37 DA) und dient gleichermaßen dem individuellen Rechtsschutz und der effektiven Durchsetzung des Datenrechts. Schon nach dem Wortlaut des Art. 38 Abs. 1 Data Act besteht die Beschwerdemöglichkeit allerdings „[unbeschadet] eines anderen verwaltungsrechtlichen oder gerichtlichen Rechtsbehelfs". Einer Einpassung in das verwaltungsprozessuale Rechtsschutzsystem bedarf es daher nicht, die Möglichkeiten der Beschwerde und des Rechtsschutzes nach der VwGO stehen nebeneinander und beeinflussen sich gegenseitig nur insoweit, als sich im Erfolgsfall der Verfahrensgegenstand des anderen Verfahrens erledigen kann[34].

2. Verweigerungsrecht des Dateninhabers nach Art. 18 Abs. 2 Data Act

Art. 18 Abs. 2 DA gibt dem Dateninhaber die Möglichkeit, die Erfüllung eines Datenverlangens (jedenfalls in der gestellten Form) unter bestimmten Voraussetzungen zu verweigern. Für ein Hauptsacheverfahren, das der gerichtlichen Klärung der Streitigkeit dient, entfällt das Rechtsschutzbedürfnis trotz dieser Möglichkeit der Einrede[35] nicht[36]. Anderes könnte im Eilrechtsschutzverfahren gelten: Wenn das Sofortvollzugsrisiko, das der Grund für die Existenz des § 80 Abs. 5 VwGO ist, aus anderen Gründen als der aufschiebenden Wirkung eines Hauptsachrechtsbehelfs nicht besteht, würde ein solches Verfahren die Rechtsstellung des Klägers womöglich nicht verbessern – ein klassischer Fall des fehlenden Rechtsschutzbedürfnisses[37].

34 Zur insoweit vergleichbaren Situation der parallelen Einlegung einer Landes- und einer Bundesverfassungsbeschwerde vgl. *Zuck*, ZAP 2007, 679 (684).

35 Zur Rechtsnatur vgl. *Schröder*, in: Bomhard/Schmidt-Kessel (Hrsg.), Data Act, 2025, Art. 18 DA Rn. 13.

36 Siehe oben B.I.

37 Zur Geltung der allgemeinen Anforderungen des Rechtsschutzbedürfnisses auch im Eilrechtsschutzverfahren vgl. *Schoch*, in: ders./Schneider (Hrsg.), VwGO, 41. ErgLfg. 2021, § 80 Rn. 492 ff.

Allerdings lässt sich kaum eine pauschale Aussage darüber treffen, in welchen Konstellationen welches Vorgehen einfacher oder effektiver ist. Lediglich für den Fall, dass der Dateninhaber die Erfüllung schon wirksam verweigert hat, erscheint es im Ausgangspunkt klar, dass es nicht zusätzlich einer gerichtlichen Suspendierung des Datenverlangens bedarf. Dies gilt auch mit Blick auf die mögliche Vollstreckung eines Datenverlangens: Ein Vollstreckungshindernis, das in der wirksamen Verweigerung wohl zu sehen ist[38], „schützt" genauso gut wie das Fehlen der Vollstreckbarkeit eines Verwaltungsakts mangels sofortiger Vollziehbarkeit – in jedem Fall fehlt es an einer der „allgemeinen Vollstreckungsvoraussetzungen"[39]. Sobald aber das Bestehen eines Verweigerungsrechts strittig ist, spricht viel dafür, die Zulässigkeit eines Verfahrens nach § 80 Abs. 5 VwGO nicht am Fehlen des Rechtsschutzbedürfnisses scheitern zu lassen. Bei Anträgen Dritter, denen der Data Act kein Verweigerungsrecht zuspricht, stellt sich die Frage ohnehin nicht.

3. Befassung der zuständigen Behörde nach Art. 18 Abs. 5 Data Act

Am problematischsten ist die Verknüpfung des in Art. 18 Abs. 5 DA vorgesehenen Streitschlichtungsmechanismus mit dem deutschen Verwaltungsprozessrecht. Art. 18 Abs. 5 DA lautet:

> „Wenn die öffentliche Stelle, die Kommission, die Europäische Zentralbank oder die Einrichtung der Union beabsichtigt, der Ablehnung des Datenverlangens eines Dateninhabers zu widersprechen, oder wenn der Dateninhaber Einspruch gegen das Verlangen einzulegen beabsichtigt und die Angelegenheit durch eine entsprechende Änderung des Verlangens nicht beigelegt werden kann, wird die nach Artikel 37 benannte zuständige Behörde des Mitgliedstaats, in dem der Dateninhaber niedergelassen ist, mit der Angelegenheit befasst."

Mit Widerspruch und Einspruch sind keine spezifischen Rechtsbehelfe gemeint, sondern es wird, wie sich aus der englischen und französischen Sprachfassung des Data Act klarer ergibt, die Situation beschrieben, dass gegen die Verweigerung der Erfüllung bzw. gegen das Datenverlangen vorgegangen werden soll. Die Norm erfasst damit sämtliche Streitigkeiten um

38 *Schröder*, in: Bomhard/Schmidt-Kessel (Hrsg.), Data Act, 2025, Art. 18 DA Rn. 43.
39 Zu deren Bedeutung für den Rechtsschutz vgl. BayVGH, BayVBl. 2021, 127 (Rn. 51 f.).

Datenverlangen sowohl aus der Perspektive der Behörde, deren Verlangen unerfüllt bleibt, als auch aus der Perspektive des Dateninhabers[40]. Nicht erfasst sind hingegen mögliche Einwendungen Dritter, etwa wegen Weitergabe ihrer personenbezogenen Daten oder wegen der Offenbarung von Geschäftsgeheimnissen – insofern bleibt nur der (klassische) Rechtsweg.

Art. 18 Abs. 5 DA sieht ein zweistufiges Verfahren vor, bestehend aus einem Versuch, den Streit zwischen der Stelle, die die Daten verlangt hat, und dem Dateninhaber durch Änderung des Datenverlangens (also letztlich Verhandlungen) beizulegen, und falls dies nicht gelingt, der Befassung der zuständigen Behörde. Unklar ist angesichts der auch in anderen Sprachfassungen anzutreffenden Passivkonstruktion, wer die Befassung der Behörde vornimmt. Naheliegend ist, dass es derjenige Beteiligte ist, der gegen den Status quo vorgehen möchte – bei einem Datenverlangen also der Dateninhaber, bei einer Erfüllungsverweigerung die Stelle, die die Daten verlangt hat[41]. Von der zuvor erwähnten allgemeinen Beschwerdemöglichkeit gem. Art. 38 Abs. 1 DA und auch von den „besonderen Beschwerderechten" gem. Art. 17 Abs. 5, Art. 20 Abs. 5 und Art. 21 Abs. 5 DA unterscheidet sich Art. 18 Abs. 5 DA insofern, als er das Verfahren nicht zur Disposition eines Beschwerdeführers stellt, sondern für obligatorisch erklärt („wird … befasst"). Damit stellt sich allerdings die Frage nach dem Verhältnis zum verwaltungsgerichtlichen Rechtsschutz, denn das Verfahren nach Art. 18 Abs. 5 Data Act vermag ein verwaltungsgerichtliches Verfahren jedenfalls nicht zu ersetzen, da es nicht den Anforderungen des Art. 19 Abs. 4 GG und des Art. 47 GRCh genügt[42].

Auf den ersten Blick erscheint es naheliegend, Art. 18 Abs. 5 DA als ein besonderes, europarechtlich vorgeschriebenes Vorverfahren zu verstehen, welches dann das Widerspruchsverfahren der §§ 68 ff. VwGO als lex specialis verdrängt[43]. Dem steht nicht entgegen, dass der „zuständigen Behörde" angesichts der geringen Regelungsdichte des Verfahrens wohl keine Kompetenz zur verbindlichen Streitentscheidung zukommt, sondern sie nur eine unverbindliche Stellungnahme abgeben kann[44]. In diesem Punkt unterscheidet sich das Verfahren des Art. 18 Abs. 5 DA zwar vom klassischen Widerspruchsverfahren, das (bei Nichtabhilfe durch die Ausgangs-

40 *Schröder*, in: Bomhard/Schmidt-Kessel (Hrsg.), Data Act, 2025, Art. 18 DA Rn. 30.
41 *Schröder*, in: Bomhard/Schmidt-Kessel (Hrsg.), Data Act, 2025, Art. 18 DA Rn. 32.
42 Siehe oben B.I.
43 *Schröder*, in: Bomhard/Schmidt-Kessel (Hrsg.), Data Act, 2025, Art. 18 DA Rn. 32; ebenso wohl schon *Redeker*, CR 2024, 293 (296).
44 *Schröder*, in: Bomhard/Schmidt-Kessel (Hrsg.), Data Act, 2025, Art. 18 DA Rn. 33.

behörde) zu einem klagefähigen Widerspruchsbescheid führt (§ 73 Abs. 1 S. 1 VwGO); dem Prozessrecht sind aber obligatorische Streitschlichtungsverfahren ohne verbindliche neue Entscheidung nicht fremd, wie etwa § 15a EGZPO zeigt. Dem Wortlaut des Art. 18 Abs. 5 DA entspräche auch die Einordnung des Verfahrens als zwar verpflichtendes, aber unverbunden neben einem gerichtlichen Verfahren stehendes Streitbeilegungsinstrument. Für die Qualifikation als Prozessvoraussetzung spricht aber, dass ein obligatorisches Streitbeilegungsverfahren wohl nur dann seinen prozessvermeidenden Zweck erfüllen kann, wenn es vor einem gerichtlichen Verfahren erfolgt, und dass eine Durchführung parallel zu einem Widerspruchsverfahren wenig sinnvoll wäre.

Diese Einordnung des Verfahrens gem. Art. 18 Abs. 5 DA führt allerdings zu Folgeproblemen, da es ein klassisches Vorverfahren nicht deckungsgleich ersetzen kann. Das gilt zunächst mit Blick auf die für den Eintritt bzw. die Verhinderung der Bestandskraft zentralen Rechtsbehelfsfristen. Die Erhebung eines Widerspruchs gem. § 70 Abs. 1 VwGO verhindert den Eintritt der Bestandskraft eines Verwaltungsakts. Diese Wirkung mag man dem verfahrenseinleitenden Akt nach Art. 18 Abs. 5 DA abstrakt auch zusprechen können, allerdings sind die vorgesehenen Beilegungsverhandlungen zwischen den Beteiligten kaum formalisiert. Zudem fehlt es, wie eben erwähnt, an einem Bescheid am Schluss des Verfahrens, an den die Klagefrist des § 74 Abs. 1 S. 1 VwGO anknüpfen könnte. Angesichts der erheblichen Folgen der Bestandskraft eines Verwaltungsakts erscheint diese Rechtsunsicherheit kaum akzeptabel. Überzeugender mag daher sein, von einem Fall des § 74 Abs. 1 S. 2 VwGO auszugehen und die Klagefrist schon mit der Bekanntgabe des Datenverlangens beginnen zu lassen. Das Verfahren nach Art. 18 Abs. 5 DA würde dann innerhalb des gerichtlichen Verfahrens stattfinden, das währenddessen gem. § 94 VwGO ausgesetzt werden müsste. Falls sich der Streit infolge des integrierten Vorverfahrens erledigt, erginge nur noch eine Kostenentscheidung gemäß § 161 Abs. 2 VwGO, andernfalls würde das Gericht in der Sache entscheiden.

Bei dieser Sichtweise stellt sich auch nicht die andernfalls auftretende und schwer zu beantwortende Frage, ob das Verfahren gem. Art. 18 Abs. 5 DA analog § 80 Abs. 1 S. 1 VwGO aufschiebende Wirkung entfaltet. Nach der hier vertretenen Auffassung ist dies weder der Fall noch erforderlich, da sich die aufschiebende Wirkung ausschließlich nach den Vorschriften über die förmlichen Rechtsbehelfe richtet. Die gegenteilige Auffassung wäre insbesondere bei Datenverlangen zur Notstandsbewältigung, deren Erfüllung womöglich keinen Aufschub duldet, problematisch und würde

dem Anliegen des Kapitels V Data Act zuwiderlaufen. In der Folge wird nach hier vertretener Auffassung, wenn die sofortige Vollziehbarkeit eines Verwaltungsakts infolge gesetzlicher oder behördlicher Anordnung gegeben und nicht gerichtlich suspendiert ist, das Verfahren gem. Art. 18 Abs. 5 DA auch keine Sperre gegen eine etwaige Vollstreckung entfalten können.

D. Rechtsschutz gegen Datenverlangen europäischer Stellen

Für Datenverlangen europäischer Stellen (Europäische Kommission, EZB oder Einrichtungen der Union) dürfte klar sein, dass sie Beschlüsse i.S.d. Art. 288 Abs. 4 AEUV darstellen. Als Rechtsbehelf kommt somit nur die Nichtigkeitsklage gem. Art. 263 AEUV in Betracht. Hieran ändert sich auch nichts dadurch, dass Datenverlangen europäischer Stellen stets das Verfahren gem. Art. 22 Abs. 3 und 4 DA durchlaufen müssen. Die Prüfung und Weiterleitung durch die zuständige Behörde des Mitgliedstaats, in dem der Dateninhaber niedergelassen ist, bietet diesem zwar einen zusätzlichen Schutz, da die zuständige Behörde das Wirksamwerden eines rechtswidrigen Datenverlangens verhindern kann, modifiziert aber im Fall der Übermittlung an den Dateninhaber weder die Rechtsnatur des Datenverlangens[45] noch das dafür relevante Rechtsschutzsystem.

Für den Adressaten eines Datenverlangens, also den Dateninhaber, bedarf es gem. Art. 263 Abs. 4 AEUV keiner über die Adressatenstellung hinausgehenden Klagebefugnis; sein Rechtsschutzbedürfnis[46] dürfte, wie im deutschen Recht, auch nicht infolge der Möglichkeit der Erfüllungsverweigerung gem. Art. 18 Abs. 2 DA entfallen. Dritte, beispielsweise Geschäftsgeheimnisinhaber oder betroffene Personen i.S.d. Datenschutzrechts, müssen dagegen die Voraussetzungen der individuellen und unmittelbaren Betroffenheit gem. Art. 263 Abs. 4 AEUV erfüllen. Dies dürfte trotz der engen Auslegung, die der EuGH dem Begriff der individuellen Betroffenheit gegeben hat[47], möglich sein, da selbst nach der „Plaumann-Formel" die Gefährdung eigener Rechte durch ein Datenverlangen zur Begründung der Klagebefugnis ausreichend erscheint. Speziell für Geschäftsgeheimnisinha-

45 *Schröder*, in: Bomhard/Schmidt-Kessel (Hrsg.), Data Act, 2025, Art. 22 DA Rn. 18.
46 Dazu etwa *Thiele*, Europäisches Prozessrecht, 2. Aufl. 2014, § 7 Rn. 88.
47 EuGH, Urt. v. 15.7.1963, C-25/62, BeckRS 2004, 72625 – Plaumann, bestätigt in EuGH, Urt. v. 25.7.2002, C-50/00 P, EuR 2002, 699 Rn. 32 ff. – Unión de Pequeños Agricultores.

ber lässt sich die Betroffenheit zudem mit ihrer gem. Art. 19 Abs. 3 DA erforderlichen Verfahrensbeteiligung[48] begründen.

Klärungsbedürftig scheint auch mit Blick auf das europäische Prozessrecht, ob das Verfahren gem. Art. 18 Abs. 5 DA ein Vorverfahren darstellt. Vorverfahren sind durch Art. 263 Abs. 5 AEUV grundsätzlich erlaubt, allerdings nur bei „Klagen von natürlichen oder juristischen Personen gegen Handlungen [von] Einrichtungen und sonstigen Stellen", die durch Sekundärrecht gegründet sind. Für Klagen gegen Datenverlangen von „Einrichtungen der Union" i.S.d. Art. 2 Nr. 27 DA wäre ein Vorverfahren demnach zulässig. Art. 18 Abs. 5 DA enthält aber keine Begrenzung auf diese Einrichtungen, sondern gilt seinem Wortlaut nach stets, also auch bei Datenverlangen der Europäischen Kommission oder der EZB. Insoweit erlaubt das Primärrecht aber kein Vorverfahren. Eine Reduktion des Anwendungsbereichs des Art. 18 Abs. 5 DA auf Datenverlangen von Einrichtungen der Union überzeugt als Lösung genauso wenig wie die Annahme, dass die Rechtsnatur des Verfahrens gem. Art. 18 Abs. 5 DA in Abhängigkeit davon variiert, wer ein Datenverlangen stellt. Einzige Lösung bleibt, das Verfahren als obligatorisch, aber im Grundsatz unabhängig von einem gerichtlichen Verfahren zu verstehen. Eine gewisse Synchronisation mit dem gerichtlichen Rechtsschutz lässt sich allerdings auch bei dieser Sichtweise über die Aussetzung des Gerichtsverfahrens herbeiführen, die das Unionsrecht in Art. 55 VerfO EuGH und, für Klagen von Dateninhabern oder Dritten relevanter, in Art. 69 VerfO EuG vorsieht. Dieses Ergebnis mag Anlass dazu geben, die Einordnung als Vorverfahren im nationalen Recht[49] auch wieder in Frage zu stellen. Angesichts der offenen Formulierung des Art. 18 Abs. 5 DA spricht allerdings einiges dafür, das Verfahren so tief wie möglich in das jeweilige Verwaltungsprozessrecht zu integrieren, was im nationalen Recht, bedingt durch den Anwendungsvorrang des Unionsrechts, leichter ist als im Unionsrecht, dessen Verwaltungsprozessrecht im Wesentlichen primärrechtlich geprägt ist.

Für die Frage des Eilrechtsschutzes ist bei Datenverlangen europäischer Stellen auf Art. 278 AEUV hinzuweisen. Danach haben Klagen keine aufschiebende Wirkung; eine solche kann aber durch den Gerichtshof der Europäischen Union im Einzelfall angeordnet werden. Angesichts dieser

48 Zur Verfahrensbeteiligung als die Klagebefugnis begründendem Umstand vgl. *Cremer*, in: Calliess/Ruffert (Hrsg.), EUV/AEUV, 6. Aufl. 2022, Art. 263 AEUV Rn. 42 m.w.N. aus der Rechtsprechung.

49 Oben C.II.3.

Grundentscheidung stellen sich die im deutschen Recht virulenten Fragen des Rechtsschutzbedürfnisses nicht – der Gerichtshof kann unter Berücksichtigung aller Umstände des Einzelfalls, einschließlich der durch etwaige Verweigerungsrechte i.S.d. Art. 18 Abs. 2 DA bestehenden Lage des Klägers, entscheiden, ob eine Aussetzung des Datenverlangens erforderlich ist. Die drohende Vollstreckung eines Datenverlangens ist in diesem Fall allerdings kein Argument, da Art. 299 Abs. 1 AEUV eine Vollstreckbarkeit nur für Beschlüsse, die eine Zahlungspflicht auferlegen, vorsieht. Andere Beschlüsse europäischer Stellen, und damit auch Datenverlangen, sind nur vollstreckbar, wenn das Sekundärrecht dies vorsieht[50], was im Fall des Data Act aber nicht der Fall ist. Insbesondere genügt der unspezifische Art. 22 Abs. 1 DA („Öffentliche Stellen, die Kommission, die Europäische Zentralbank und die Einrichtungen der Union arbeiten im Hinblick auf die kohärente Umsetzung dieses Kapitels zusammen und unterstützen sich diesbezüglich gegenseitig") nicht als Rechtsgrundlage für die Vollstreckung eines Datenverlangens einer unionalen Stelle im Inland. Auch die allgemeinen Vorschriften über die europäische Amtshilfe (§§ 8a ff. VwVfG) reichen hierfür nicht aus.

Trotz der fehlenden unmittelbaren Vollstreckbarkeit unionaler Datenverlangen wird ein Dateninhaber diese nicht ungestraft ignorieren können. Art. 40 Abs. 1 DA verpflichtet die Mitgliedstaaten, wirksame, verhältnismäßige und abschreckende Sanktionen für Verstöße gegen die Verordnung zu verhängen. Die Nichtbefolgung eines Datenverlangens ohne Verweigerungsgrund stellt einen Verstoß gegen Art. 18 Abs. 1 DA dar, mithin muss der deutsche Gesetzgeber zumindest eine Bußgeldvorschrift vorsehen. Diskutabel erscheint zudem, die Nichtbefolgung des Datenverlangens als Verletzung der Rechtsordnung und damit als Störung der öffentlichen Sicherheit anzusehen, die ein sicherheitsbehördliches Einschreiten (einschließlich etwaiger Vollstreckungsmaßnahmen) nach deutschem Recht rechtfertigt. Gegen diese Maßnahmen wäre Rechtsschutz dann vor den deutschen Gerichten zu suchen, wobei eine etwaige Bestandskraft des Beschlusses wohl berücksichtigt würde.

50 *Krajewski/Rösslein*, in: Grabitz/Hilf/Nettesheim (Hrsg.), Das Recht der Europäischen Union, 62. ErgLfg. 2017, Art. 299 AEUV Rn. 7.

E. Rechtsschutz gegen Datenverlangen öffentlicher Stellen anderer Mitgliedstaaten

Für Datenbereitstellungsverlangen öffentlicher Stellen aus anderen Mitgliedstaaten findet ebenfalls das in Art. 22 Abs. 3 und 4 DA vorgesehene Verfahren Anwendung. Der Data Act schließt eine Adressierung von Datenverlangen an in anderen Mitgliedstaaten ansässige Dateninhaber nicht aus, sondern sorgt im Gegenteil durch Art. 22 Abs. 4 lit. a dafür, dass diese an den Dateninhaber übermittelt und (in der deutschen Terminologie der §§ 41, 43 VwVfG) bekanntgegeben und wirksam werden. Es wird mithin der Erlass transnationaler Verwaltungsakte ermöglicht, die vorbehaltlich der Prüfung durch die zuständige Behörde das allgemeine Territorialitätsprinzip, dem die Ausübung von Staatsgewalt unterliegt[51], überwinden. Auch hier führen die Prüfung und Weiterleitung durch die zuständige Behörde des Mitgliedstaats, in dem der Dateninhaber niedergelassen ist, nicht zu einer Modifikation der Rechtsnatur des Datenverlangens oder des Rechtsschutzsystems – mit der Folge, dass Rechtsschutz vor den Gerichten des Mitgliedstaats zu suchen ist, dessen Stelle die Daten verlangt hat[52].

Im Grundsatz besteht somit ein „Herkunftslandprinzip für Datenverlangen". Während der Begriff „Herkunftslandprinzip" im Unionsrecht für die Wirtschaftsteilnehmer meist eine positive Konnotation hat (in dem Sinne, dass sie nur den Anforderungen ihres Sitzstaats unterliegen), kommt ihm hier durch die Anknüpfung an die handelnde Behörde eine negative Wirkung zu. Ein Dateninhaber, kann – ohne irgendeinen Bezug zu einem anderen Staat als seinem Sitzstaat zu haben – transnationalen Datenverlangen ausgesetzt sein, weil jede Behörde eines anderen Mitgliedstaats ein qualifiziertes Interesse an „seinen" Daten haben kann. Schutz dagegen bietet allein das in Art. 22 Abs. 3 und 4 DA vorgesehene Kontrollverfahren durch den Mitgliedstaat, in dem der Dateninhaber ansässig ist. Dagegen erscheint der Weg, Sanktions- und (indirekte) Vollstreckungsmaßnahmen nach innerstaatlichem Recht, die wie bei unionalen Datenverlangen im Raum stehen werden[53], abzuwarten, wenig empfehlenswert. Er ermöglicht es zwar, über die Fokussierung auf einen anderen Streitgegenstand ein transnationales Datenverlangen inzident vor deutsche Gerichte zu ziehen. Allerdings werden deutsche Gerichte bei der Prüfung der Rechtmäßigkeit

51 Dazu etwa *Maurer/Waldhoff*, Allgemeines Verwaltungsrecht, 24. Aufl. 2024, § 9 Rn. 68.

52 *Schröder*, in: Bomhard/Schmidt-Kessel (Hrsg.), Data Act, 2025, Art. 22 DA Rn. 26.

53 Dazu oben D.

des Datenverlangens eine etwaige Bestandskraft des Datenverlangens nach ausländischem Recht berücksichtigen müssen, so dass es dann nicht mehr zu einer inhaltlichen Überprüfung kommt.

F. Sekundäransprüche

Nach Erfüllung eines Datenverlangens kann Art. 20 DA Bedeutung erlangen, der unter bestimmten Voraussetzungen „Sekundäransprüche" einräumt. Die Vorschrift differenziert zwischen Datenverlangen zur Notstandsbewältigung und in anderen Fällen: Im Fall der Notstandsbewältigung ist im Grundsatz nur eine (antragsabhängige) öffentliche Anerkennung für die Bereitstellung vorgesehen (Art. 20 Abs. 1 DA); lediglich Klein- oder Kleinstunternehmen können einen Antrag auf eine „faire Gegenleistung" stellen (Art. 20 Abs. 3 i.V.m. Abs. 2 DA). Bei Datenanforderungen aus anderen Gründen als zur Notstandsbewältigung sind Klein- oder Kleinstunternehmen schon gar nicht zur Bereitstellung von Daten verpflichtet; im Übrigen kann eine faire Gegenleistung beantragt werden (Art. 20 Abs. 2 DA)[54].

Die Anerkennung oder Gegenleistung ist nicht davon abhängig, dass zuvor versucht worden sein muss, die Erfüllung eines womöglich rechtswidrigen Datenverlangens mithilfe von Art. 18 Abs. 2 DA, mithilfe des in Art. 18 Abs. 5 DA vorgesehenen Streitbeilegungsverfahrens oder mithilfe gerichtlichen Rechtsschutzes zu vermeiden. Anders als die meisten Aufopferungsansprüche im deutschen Recht der öffentlich-rechtlichen Ersatzleistungen[55] wird also kein Vorrang des Primärrechtsschutzes etabliert und es besteht die – angesichts des geringen Umfangs der Gegenleistung[56] aber wohl wenig attraktive – Möglichkeit des „dulde und liquidiere".

Auch für diese Sekundäransprüche gilt die Garantie effektiven Rechtsschutzes[57], so dass sie im Streitfall gerichtlich durchsetzbar sind. Das in Art. 20 Abs. 5 DA vorgesehene Beschwerdeverfahren wegen der Höhe der Gegenleistung vermag den gerichtlichen Rechtsschutz nicht zu ersetzen und ist auch nicht obligatorisch vor (oder während) einer etwaigen Klage auf Gewährung der Gegenleistung, die gem. § 40 Abs. 2 S. 1 VwGO vor den ordentlichen Gerichten zu erheben wäre, durchzuführen.

54 *Schröder*, in: Bomhard/Schmidt-Kessel (Hrsg.), Data Act, 2025, Einf. Kap. V Rn. 12.
55 Vgl. dazu *Papier/Shirvani*, in: MüKoBGB, 9. Aufl. 2024, § 839 BGB Rn. 5.
56 *Schröder*, in: Bomhard/Schmidt-Kessel (Hrsg.), Data Act, 2025, Art. 20 DA Rn. 8.
57 Vgl. oben B.III.

G. Fazit

Obwohl der Data Act nur wenige Regelungen zum Rechtsschutz gegen Datenverlangen enthält, bereiten diese beträchtliche Auslegungs- und Synchronisationsprobleme. Das gilt in besonderem Maße für den in Art. 18 Abs. 5 DA vorgesehenen obligatorischen Streitbeilegungsmechanismus. Unter Berücksichtigung der Anforderungen an effektiven Rechtsschutz ist die praktische Bedeutung dieser Bestimmung für den Rechtsschutz gegen Datenverlangen allerdings gering; zudem stellt sich zumindest im Fall von Datenverlangen zur Notstandsbewältigung, die naturgemäß eilbedürftig sind, die Frage, ob ein aus Verhandlungen und behördlicher Streitbeilegung bestehender Mechanismus nicht dysfunktional ist. Das Recht zur Verweigerung der Erfüllung von Datenverlangen gem. Art. 18 Abs. 2 DA ist demgegenüber aufgrund seiner großen Reichweite von hoher praktischer Bedeutung, lässt aber das Bedürfnis nach gerichtlichem Rechtsschutz nicht entfallen.

Der gerichtliche Rechtsschutz gegen Datenverlangen richtet sich im Kern nach dem Rechtsschutzsystem, dem die datenverlangende Stelle unterliegt. Bei Datenverlangen deutscher Stellen, die Verwaltungsakte darstellen, ist damit die Anfechtungsklage gem. § 42 Abs. 1 VwGO der Rechtsbehelf der Wahl; daneben wird dabei vor allem bei Datenverlangen zur Notstandsbewältigung dem Verfahren gem. § 80 Abs. 5 VwGO große Bedeutung zukommen, da, wenn nicht schon der Gesetzgeber die aufschiebende Wirkung von Rechtsbehelfen gegen solche Datenverlangen entfallen lässt, jedenfalls die datenverlangende Behörde von § 80 Abs. 2 S. 1 Nr. 4 VwGO Gebrauch machen wird.

Bei Datenverlangen europäischer Stellen richtet sich der Rechtsschutz gegen diese nach dem AEUV (Nichtigkeitsklage gem. Art. 263 AEUV). Da der Data Act keine Aussage zur Vollstreckung trifft, kommt nur eine Sanktionierung der Nichtbefolgung solcher Datenverlangen oder eine indirekte Vollstreckung über allgemeines Sicherheitsrecht in Betracht, wodurch die Frage der Rechtmäßigkeit von Datenverlangen inzident auch vor nationale Gerichte gebracht werden kann, wenn eine Prüfung nicht wegen Bestandskraft des Beschlusses ausscheidet.

Ähnlich ist die Lage auch bei Datenverlangen öffentlicher Stellen anderer Mitgliedstaaten. Sie stellen transnationale Verwaltungsakte dar, und der Rechtsschutz richtet sich nach dem Recht des Staates, in dem sie erlassen wurden. Auch hier können deutsche Gerichte in Streitigkeiten über Sanktionen für die Nichtbefolgung eines solchen Verlangens oder über

(indirekte) Vollstreckungsmaßnahmen zuständig sein; wie bei Datenverlangen europäischer Stellen wird aber gegebenenfalls die Bestandskraft eines Datenverlangens zu berücksichtigen sein.

Diskussionsbericht – Zu Vorfragen der Datenbereitstellung

Peer Sonnenberg[*]

A. Einleitung

Die Tagung wurde beendet mit einer Schlussdiskussion. Es waren alle Tagungsteilnehmer aufgerufen, die gehörten Beiträge Revue passieren zu lassen und Fragen sowohl an einzelne Speaker zu ihren Vorträgen als auch an die offene Runde zu der allgemeinen Thematik zu stellen. Die Moderation übernahm *Tristan Barczak*[1].

Im Laufe der Diskussion hat es im Wesentlichen drei thematische Schwerpunkte gegeben: Eine Datenbereitstellungspflicht, datenschutzrechtliche Kollisionen mit dem Datenrecht und die Regelungen zu Datenaltruismus und Datenvermittlungsdiensten gerade im Verhältnis zum Helferrecht. Dabei hatten alle drei Themen gemein, dass sie sich um die Bereitschaft und den rechtlichen Rahmen des Teilens von Daten (egal ob mit Privaten oder der öffentlichen Hand) drehten, sodass sie im Laufe der Diskussion zu einem einheitlichen Gespräch der Tagungsteilnehmer und Referenten verwoben werden konnten.

* Peer Sonnenberg ist wissenschaftlicher Mitarbeiter am Lehrstuhl für Öffentliches Recht, Medien- und Informationsrecht an der Universität Passau.

1 Prof. Dr. Tristan Barczak ist Inhaber des Lehrstuhls für Öffentliches Recht, Sicherheitsrecht und das Recht der neuen Technologien an der Universität Passau.

B. Gang der Diskussion

Barczak, der sich eingangs bei den Referenten und insbesondere bei dem Organisator *Kai von Lewinski*[2] bedankte, gab sodann die Diskussion in die offene Runde frei. Der erste Beitrag kam von *David Bomhard*[3] gerichtet an *Moritz Hennemann*[4]: *Bomhard* habe da immer den Gesetzgeber im Blick, der die Vorstellung hätte, man könne einfach den „Datenhahn" aufdrehen und dann könne der Gesetzgeber alles regeln mit den Daten. Hier rekurriert er auf die sehr bildliche Darstellung einer „Datenautobahn" von *Hennemann*[5]: Sähe man Daten als das die Autos betreibende Öl an[6], dann sei mit dem Vorhandensein dieses Öls noch nichts gewonnen. Vielmehr brauche man zusätzlich Fahrzeuge und Infrastruktur, was ggf. aus den Daten heraus entwickelt werden müsse. Folglich brauche man im Datenrecht doch erstmal die Zeit, ein passendes Ökosystem zu entwickeln, Datenpools aufzubauen und Experten entsprechend auszubilden, um die erhobenen Daten vernünftig auswerten zu können. Für *Bomhard* ist es damit zentral erforderlich, sich darauf zu konzentrieren, die Daten präventiv noch vor dem Ausnahmefall nutzbar zu machen. Dafür müsse schon jetzt ein entsprechendes Ökosystem aufgebaut werden und vor allem der „Sackgasse" des Datenschutzrechts irgendwie begegnet werden.

Hennemann pflichtete ihm bei. Man dürfe nicht bei den Art. 14 ff. DA stehenbleiben, sondern müsse schon – ggf. auf nationaler Ebene – die vorgelagerte Frage einer Datenbereithaltungspflicht adressieren. Dabei verweist er maßgeblich auf den Beitrag von *von Lewinski,* wo diese Stoßrichtung erstmalig ausgeführt wird und die mit einer Strukturierungspflicht

2 Prof. Dr. *Kai von Lewinski* ist Inhaber des Lehrstuhls für Öffentliches Recht, Medien- und Informationsrecht an der Universität Passau. Er hat zuvor zum Thema „Informationelle Sozialpflichtigkeit" vorgetragen.

3 Prof. Dr. *David Bomhard* ist Honorarprofessor für das Recht der Künstlichen Intelligenz sowie IT-, Software- und Datenrecht an der Universität Passau.

4 Prof. Dr. *Moritz Hennemann* ist Inhaber des Lehrstuhls für Zivilrecht mit Informationsrecht, Medienrecht, Internetrecht sowie Direktor des Instituts für Medien- und Informationsrecht an der Universität Freiburg. Er hat zuvor zum Thema „Blaulicht und Abschleppwagen auf der Datenautobahn" vorgetragen.

5 *Hennemann,* in diesem Band, S. 63.

6 Hier wird eine altbekannte Metapher aufgegriffen, welche die zentrale wirtschaftliche Relevanz von Daten hervorheben soll, vgl. *The Economist,* The world's most valuable ressource is no longer oil, but data (6. Mai 2017), abrufbar unter https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data (zuletzt abgerufen am 17.10.2025).

einhergeht[7]. Es sei zu erwägen, Unternehmen dazu zu verpflichten, bestimmte Datenbestände mit einer Vorstrukturierung vorzuhalten, so dass diese auch kurzfristig abrufbar sind. Eine solche Inpflichtnahme erfordere faktisch natürlich die Fachkompetenz auf staatlicher Seite, mit herausgegebenen Daten (technisch) umgehen zu können. *Hennemann* äußerte hier allerdings leise Zweifel, ob die (Notstandsverwaltungs-)Behörden derzeit schon hinreichend darauf vorbereitet sind, die verschiedensten Daten ggf. ganz unterschiedlicher Natur in allen Sachlagen auslesen und verwerten zu können. In der Tat, so *Hennemann,* seien hier Reallabore bzw. reale Übungsszenarien in einen beschränkten und geschützten Rahmen zu erwägen. Auf diese Weise könnte getestet werden, ob Behörden die übermittelten Daten tatsächlich benötigen und wie sie mit ihnen umgehen (können), oder ob Behörden nicht auf eine Dienstleistung des Dateninhabers bei der Datenauswertung angewiesen sind bzw. sein sollten.

Meinhard Schröder[8] blieb mit seiner Ergänzung bei der Metapher der Datenautobahn und merkte an, es gehe beim Datenrecht im Ausnahmefall nicht nur um ein Infrastrukturvorhaben. Anders als in den Fällen, in denen aufgrund einer Bedarfsanalyse Infrastruktur errichtet werde, müsse hier zunächst der Bedarf generiert werden. Es sei letztendlich ein Henne-Ei-Problem, was zuerst da sein müsse: der Bedarf oder die Infrastruktur? Beim Data Act scheine es, so *Schröder*, wie beim Data Governance Act mehr in die vorbereitende Richtung zu gehen, dass also juristische Infrastruktur ohne konkreten Bedarf entstehen soll. Gleichzeitig weist er darauf hin, dass für einen Datenaltruismus, der praktisch bei einem Infrastrukturvorhaben weiterhelfen könnte, schlicht die Anreize fehlen würden. Dies zeige sich nicht zuletzt in der schwachen Erfolgsquote des Datenvermittlungsdienstes[9].

Dass die Regelungen zu datenaltruistischen Diensten ohne echte Anreize ausgestaltet und deshalb äußerst unattraktiv seien, weiß *Hennemann* zu bestätigen. Insbesondere bezweifelt er, dass die Registerpublizität und die

---

7 *v. Lewinski*, in diesem Band, S. 37 (47), der auf entsprechende Tendenzen im Bevölkerungsschutz- und Anlagenrecht verweist.

8 Prof. Dr. *Meinhard Schröder* ist Inhaber des Lehrstuhls für Öffentliches Recht, Europarecht und Informationstechnologierecht an der Universität Passau. Er hat zuvor zum Thema „Rechtsschutz gegen Datenverlangen" vorgetragen.

9 Zzt. der Diskussion existierten in Europa nur 10 Datenvermittlungsdienste. Zzt. der Veröffentlichung ist diese Zahl immerhin auf 24 gestiegen, vgl. *Europäische Kommission,* EU-Register der Datenvermittlungsdienste, abrufbar unter https://digital-strategy.ec.europa.eu/de/policies/data-intermediary-services (zuletzt abgerufen am 17.10.2025).

Erlaubnis, ein entsprechendes Logo tragen zu dürfen, die Menge an Pflichten, die auf datenaltruistische Unternehmen zukommen[10], kompensieren können. Entsprechende anreizorientierten Regelungen wären in einem Umsetzungsgesetz zum Data Governance Act möglich (welches allerdings trotz abgelaufener Frist noch nicht final vorliegt[11]). Platz dafür wäre etwa im Vertrags- und AGB-Recht, im Vergaberecht oder im Steuerrecht (gerade neben allfälligen datenschutzrechtlichen Privilegierungen). Ebenso führe die Tätigkeit als Datenvermittlungsdienst zu einem sehr strengen Pflichtenkatalog (unter anderem eine Notifizierungspflicht[12]), der abschreckend wirke. Das Kalkül des Gesetzgebers, durch vergleichsweise strenge Regulierung besonders viel Vertrauen im Markt zu schaffen und dadurch die Nachfrage zu erhöhen, scheint *Hennemann* bisher nicht aufgegangen zu sein. *Hennemann* sieht auch Potenzial, soweit konkrete Anreize in Form von Privilegierungen gesetzt werden (etwa im Bereich des KI-Trainings oder in Bereichen, in denen keine sensiblen Daten verarbeitet werden).

Die genannten Schwächen des Datenaltruismus aufgreifend fragt *von Lewinski* sich und die Runde, ob der Datenaltruismus nicht vom Helferrecht im Bevölkerungsschutz – also gemeinnützige Organisationen wie dem DRK, den Johannitern oder dem THW – lernen könnte. Auf diesem Gebiet funktioniere im Notstandsfall altruistisches Handeln ja offenkundig. Was werde hier besser gemacht als beim EU-Gesetzgeber, fragt er *Hennemann*.

Hennemann zufolge sei es nur mehr als menschlich, anderen zu helfen – vor allem bei einem Unglücksfall. Das gebiete schon der Solidaritätsgedanke und die (hoffentlich nicht schwindende) zwischenmenschliche Nächstenliebe. So einfach sei es aber nicht beim Datenteilen. In der breiten Bevölkerung sei wohl das Bewusstsein noch nicht angekommen, welche Daten man habe, wie man sie teilen könne und welcher Gemeinwohlnutzen da-

10 Regelungen zum Datenaltruismus finden sich in den Art. 16 ff. DGA und umfassen etwa Registrierungs- und Transparenzpflichten, Unabhängigkeit von Organisationen zu Erwerbszwecken, Sicherheits- und Interoperabilitätsanforderungen und weitere Organisationspflichten.

11 Trotz Einleitung eines Vertragsverletzungsverfahrens vonseiten der Europäischen Kommission Ende Mai 2024 befand sich der Gesetzesentwurf eines deutschen Daten-Governance-Gesetz (DGG-E) zzt. der Diskussion noch im Beratungsverfahren im Digitalausschuss des Bundestages.

12 Die Pflichten eines Datenvermittlungsdienstes ergeben sich vornehmlich aus Art. 11 und 12 DGA. Nach Art. 11 Abs. 1 DGA muss ein Datenvermittlungsdienst seine Dienstleistung bei der zuständigen Aufsichtsbehörde – in Deutschland wohl die Bundesnetzagentur – anmelden. Diese Anmeldungen werden in einem Register der Europäischen Kommission geführt, Art. 11 Abs. 10 DGA.

raus erwüchse. Man denke hier nur an die Corona-Datenspende-App. Es gebe zwar bereits heute viele Möglichkeiten beispielsweise zu Forschungszwecken Daten zu spenden, daraus sei aber wohl noch keine allgemeine „Bewegung" geworden. *Hennemann* habe etwa noch keine Verkehrs-Apps gesehen, die aktiv nachfragen, ob die erhobenen Daten an universitäre Institute zur Verkehrsforschung „gespendet" werden – unbeschadet der Tatsache, ob die Daten überhaupt für die jeweiligen Forschungszwecke geeignet sind.

Zur Attraktivität von Datenspenden schlägt *Marie Wienroeder*[13] vor, man könne sich die Anreize digitaler Interaktion auf sozialen Netzwerken als Vorbild nehmen. Sie sieht den Vorteil des Helferrechts darin, dass physisches Anpacken gleichzeitig einem sozialen Zweck diene, indem man mit anderen interagiert und sozial aktiv wird – das gebe es bei der Datenspende im digitalen Raum so noch nicht.

Auch *Schröder* meint, dass die Helfertätigkeit beim DRK oder beim THW viel unmittelbarer einleuchte, während das Bedürfnis des Staates, Daten zu erlangen, vielleicht nicht so evident sei. Wenn man aber eine Datenbevorratungspflicht einführe, die durchaus zweckmäßig wäre, dann könne man gleichzeitig Anreize zur weiteren Bereitstellung erzeugen, da die Daten ohnehin schon entsprechend aufbereitet und bereitgehalten wären: Wer ohnehin zur teilungsfähigen Aufbereitung verpflichtet ist, für den sei es viel naheliegender, diese Aufbereitung weiter zu kommerzialisieren, indem entsprechende rechtliche Privilegien genutzt werden – eine Tätigkeit als Datenvermittlungsdienst könne damit durchaus an Attraktivität gewinnen.

Wenn das Stichwort Bevorratungspflicht fällt, dann muss man zugleich an die datenschutzrechtlich prominent diskutierte Frage der Vorratsdatenspeicherung denken. So wirft *Barczak* auch ein, dass eine solche Bevorratungspflicht wohl an den strengen Maßstäben der Rechtsprechung, insbesondere die des EuGHs[14], scheitern würde (es fällt der Begriff der „Glasper-

13 *Marie Wienroeder* ist wissenschaftliche Mitarbeiterin am Lehrstuhl für Europäisches und Internationales Informations- und Datenrecht an der Universität Passau. Sie hat zuvor zum Thema „Außergewöhnliche Notwendigkeit" vorgetragen.

14 Gemeint ist hier die beachtliche Kasuistik des EuGH zur Vorratsdatenspeicherung und Art. 7, 8 GRCh (vgl. EuGH, NJW 2014, 2169; ZD 2017, 124; NJW 2021, 531; NJW 2022, 3135; ZD 2022, 677; NJW 2024, 2099). Danach soll die Datenbevorratung v.a. auf das „absolut Notwendige" beschränkt sein, was etwa bei einer flächendeckenden und anlasslosen Speicherung regelmäßig nicht der Fall ist. Eine pauschale notstandsrechtliche Datenbereithaltungspflicht, bei der der Notstand sich noch nicht konkret

lenspielerei"). In der Tat lassen sich in der Praxis schwer die Erhebung von personenbezogenen wie nicht-personenbezogenen Daten voneinander trennen, zumal – wie *Barczak* auch anmerkt – die begriffliche Abgrenzung der beiden Konzepte kaum möglich ist.

Nicht nur aus datenschutzrechtlicher Perspektive sei eine Datenbevorratungspflicht problematisch, merkt *Johannes Erny*[15] an. Man müsse sich auch bewusst sein, dass eine Datenbevorratung mit einer erheblichen Speicherkapazität einhergehe, die Kosten verursache. Das gelte nicht nur finanziell, sondern auch aus Umweltgesichtspunkten, zumal große Datenspeicher einen hohen Energieverbrauch haben.

Während *von Lewinski* Umweltbedenken der allgemeinen politischen Debatte zuordnet, hält er rechtlich die durch eine Bevorratungspflicht verursachten unternehmerischen Organisationskosten für maßgeblich. Datenbanken seien vielseitig ausgestaltbar. Und wenn das Datenrecht praktisch so ausgestaltet werden solle wie etwa das Anlagen- oder Umweltrecht, dann bedeute das, Unternehmen müssten eine riesige Datenmenge in allen erdenklichen Dimensionen dezentral bereithalten und eine definierte Schnittstelle vorweisen, wodurch dem Staat ein punktueller Zugriff bei Bedarf ermöglicht werde. Hinter diesem Vorhalteprozess verbergen sich weitere betriebliche und technische Prozesse, aus denen erhebliche Kosten erwachsen können. Gerade diese Einwirkung auf die betriebliche Organisation müsste man sich bei einer Datenbereitstellungspflicht ganz genau anschauen. Die genannten umwelttechnischen Bedenken würden die Gemengelage freilich gut illustrieren.

Als nächstes meldete sich *Harald Erkens*[16] zu Wort, der drei Beispiele aus der Praxis der (Notstands-)Verwaltung anbringt, aus denen sich konkrete Probleme des Datenrechts im Ausnahmefall ergäben. Die Beispiele zeigten, so *Erkens*, dass es in den entsprechenden Datenschutzgesetzen unbedingt der Schaffung von Sondertatbeständen für Notstandssituationen

angedeutet hat, dürfte demnach mit dieser Rechtsprechung kollidieren, soweit auch personenbezogene Daten erfasst sind.

15 *Johannes Erny* ist wissenschaftlicher Mitarbeiter am Lehrstuhl für Öffentliches Recht mit Europäischen Verwaltungs-, Informations- und Umweltrecht an der Universität Freiburg.

16 *Harald Erkens* ist Referent im Bundesministerium der Verteidigung und hat zuvor zum Thema „Datenbereitstellung im Zivilschutz- und Verteidigungsfall" vorgetragen.

bedürfe[17]. Als erstes nennt er den Winter 2018/2019, in dem in Bayern u.a. Krankenhäuser und Pflegeheime eingeschneit waren. Damals benötigten die Katastrophenschutzbehörden Daten, vor allem die Adressen der zahlreichen ambulant gepflegten Personen, darunter auch Heimbeatmungspatienten, Dialysepatienten usw. Dennoch hatten sich die Pflegekassen unter Verweis auf die DSGVO und aus Furcht vor entsprechenden Sanktionen zunächst geweigert, personenbezogene Daten und insbesondere Gesundheitsdaten der Betroffenen zur Verfügung zu stellen und so Auskunft etwa über den Pflegegrad oder über besondere Umstände wie das Erfordernis eines Liegendtransports zu geben. Letztendlich konnten die Bedenken der Pflegekassen, zumindest bezogen auf den konkreten Einzelfall, mit einem Verweis auf Art. 9 DSGVO zerstreut werden. Gleichwohl sind die in der Folge erhobenen Forderungen nach Schaffung eines gesetzlichen Erlaubnistatbestandes etwa im SGB X, der in Notstandssituationen insoweit für Rechtssicherheit sorgen könnte, bis heute ohne Ergebnis geblieben. *Erkens*' zweites Beispiel bezieht sich auf die Corona-Warn-App. Diese sei aufgrund datenschutzrechtlicher Bedenken nicht so leistungsfähig gewesen, wie sie hätte sein können. Solche Fälle würden das bedauerliche Signal an die Öffentlichkeit senden, dass eine effektive Pandemiebekämpfung am Datenschutz scheitere – ganz gleich, ob diese Aussage in ihrer Einfachheit zutreffe oder nicht. Zuletzt nennt er das in den letzten Jahren zunehmend relevante Beispiel der Spontanhelfer. Diesen werde nämlich seitens der zuständigen Behörden sowie der Hilfsorganisationen eine Registrierung schon allein im Hinblick auf Versicherungsschutz und Haftungsprivilegierung empfohlen. Es gebe aber in der Praxis mannigfaltige Gründe, warum sich ein Spontanhelfer gerade nicht registrieren lassen wolle. Deshalb sollte auch hier über die datenschutzrechtliche Steuerungsmöglichkeit eine gesetzliche Grundlage geschaffen werden, was letztendlich auch der Attraktivität der Spontanhilfe zugutekommen könnte.

Barczak findet, diese Beispiele zeigten sehr schön, in welchem Dilemma man sich in der deutschen Debatte bewege. Das Datenschutzrecht habe gerade hierzulande eine gesellschaftspolitisch gut verankerte Tradition. Zwar gewichten wir kollidierende sicherheitspolitische Belange heute höher als wir es früher getan hätten. *Barczak* erinnert sich jedoch an seine Zeit als wissenschaftlicher Mitarbeiter am BVerfG, genauer bei *Johannes Masing*,

17 Dass es auch in an sich notstandsfremden Gesetzen spezifische Regelungen zum Notstand gibt, hat *Erkens* bereits in seinem Vortrag nachgewiesen, *Erkens,* in diesem Band, S. 77 (88, 91).

der dort maßgeblich am Datenschutz mitgewirkt hat[18]. Das Datenschutzrecht habe in Karlsruhe unglaubliche Blüten getrieben. *Barczak* sieht es daher skeptisch, ob man an dieser Stelle maßgeblich deregulieren könne.

In der letzten Frage, gestellt von *Hennemann* an *Barczak,* geht es um dessen Perspektive zum Begriff des personenbezogenen Datums und den daran hängenden Implikationen für eine praktisch wirksame Datenregulierung. Könne man nicht den Begriff des personenbezogenen Datums, der derzeit eher weit ausgelegt werde[19], unional einfachgesetzlich präzisieren, sodass zum Beispiel bei nicht sensiblen Daten oder anderen Kontexten, in denen es um große Datenmengen geht, modifizierende Regelungen getroffen werden können? Anderenfalls, so *Hennemann,* müsse man ohne eine Änderung der EuGH-Rechtsprechung auf längere Zeit mit der oben angesprochenen Sackgasse des Datenschutzrechts leben. Hierauf kann *Barczak* nur einen Blick in die Glaskugel werfen. Die DSGVO sei weiterhin – und hier schließe er den Kreis zum Eingangsreferat von *Louisa Specht-Riemenschneider*[20] – europäischer Goldstandard. Und dazu gehöre ja auch maßgeblich die Definition des personenbezogenen Datums. Vor diesem Hintergrund sieht *Barczak* – ohne sich auf unmittelbare Einblicke in den europapolitischen Betrieb zu berufen – keine Anzeichen von Änderungen oder internen Mehrheiten, geschweige denn von einer Änderung der EuGH-Rechtsprechung. Dass der EuGH von seiner strengen Lesart von Art. 4 Nr. 1 DSGVO abrückt, würde in gewissem Maße auch *judicial*

18 Prof. Dr. *Johannes Masing* war von 2008 bis 2020 zuständiger Berichterstatter für u.a. das Persönlichkeitsrecht und den Datenschutz am BVerfG. Als solcher bereitete er zentrale datenschutzrechtliche Urteile wie zur Vorratsdatenspeicherung (BVerfGE 125, 160), zur Kfz-Kennzeichenkontrolle (BVerfGE 150, 244) oder zum Recht auf Vergessenwerden (BVerfGE 152, 152; 152, 216) vor.

19 Nach dem EuGH ist die Anwendung der DSGVO „sehr weit und die von [ihr] erfassten personenbezogenen Daten vielfältig", vgl. nur *EuGH*, Urt. v. 7.5.2009, C-553/07, EuZW 2009, 546 Rn. 59 – Rijkeboer; *EuGH*, Urt. v. 20.12.2917, C-434/16, NJW 2018, 767 Rn. 33 – Nowak. Die Kontextspezifik und die beliebige Kombinierbarkeit können nahezu jedes Datum zu einem personenbezogenen machen. Vgl. zum Maßstab der indirekten Identifizierbarkeit etwa *EuGH*, Urt. v. 4.5.2022, T-384/20, BeckRS 2024, 3655 Rn. 45 ff. – OC.

20 Prof. Dr. *Louisa Specht-Riemenschneider* ist Inhaberin des Lehrstuhls für Bürgerliches Recht, Recht der Datenwirtschaft, des Datenschutzes, der Digitalisierung und der Künstlichen Intelligenz an der Rheinischen Friedrich-Wilhelms-Universität Bonn, sowie Bundesbeauftragte für den Datenschutz und die Informationssicherheit (BfDI). Sie hat zuvor zum Thema „Was kann das Datenrecht vom Datenschutzrecht lernen?" vorgetragen.

self-restraint bedeuten, was *Barczak* letztendlich als nicht realistische Perspektive bewertet.

Damit hat sich ein gutes Schlusswort zur Tagung gefunden. *Von Lewinski* schließt damit die Diskussion und bedankt sich insbesondere noch einmal bei *Louisa Specht-Riemenschneider* und *Moritz Hennemann* – eine hatte die Forschungsstelle FREDI geschaffen und angeschoben, der andere hatte sie maßgeblich weitergeleitet.

C. Fazit und Einordnung

Große Streitpunkte gab es also kaum. Einigkeit bestand vor allem darüber, dass eine vorgelagerte Datenbereithaltungspflicht, die insbesondere auf die Teilbarkeit und schnelle Abrufbarkeit der Daten abzielt, praktikabel und wünschenswert ist. Die rechtliche Umsetzbarkeit dieser Idee war hingegen unklar. Denn zumindest wenn es um personenbezogene Daten geht, legt der EuGH strenge Maßstäbe zur Vorratsdatenspeicherung an. Und selbst wenn Datenbereithaltungspflichten nur auf nicht-personenbezogene Daten abzielen, dann führt die weite Lesart des „personenbezogenen Datums" des EuGH unweigerlich zu Abgrenzungsschwierigkeiten im Einzelfall und damit zu einer faktischen Sperrwirkung durch das Datenschutzrecht. Dass der EuGH von diesen Rechtsprechungslinie (und aber auch das BVerfG hinsichtlich seiner weitreichenden[21] Konzeption des Rechts auf informationelle Selbstbestimmung[22]) zukünftig zugunsten etwa einer effektiveren Notstandsverwaltung abweichen wird oder dass es zu entsprechenden

21 So hat das BVerfG in seiner Volkszählung-Entscheidung konstatiert, es gebe keine belanglosen Daten mehr und es räumt dem Betroffenen eine Befugnis ein, *grundsätzlich* selbst über Preisgabe und Verwendung „seiner" persönlichen Daten zu bestimmen, BVerfGE 1, 65 (43 f.) – Volkszählung.

22 Zu entsprechenden (dogmatischen wie rechtspolitischen) Kritiken und Diskussionen gerade hinsichtlich der Reichweite dieses Rechts, vgl. etwa *Albers,* Informationelles Selbstbestimmungsrecht, 2005, S. 238, 355, 601 ff.; *Bull,* Informationelle Selbstbestimmung – Vision oder Illusion?, 2. Aufl. 2011, S. 45 ff., 63 f., 136 f. *Behrendt,* Die Entlarvung des Rechts auf informationelle Selbstbestimmung, 2023, S. 393 ff. und *passim*; *Hoffmann-Riem,* Informationelle Selbstbestimmung in der Informationsgesellschaft, AöR 123 (1998) 513 (531 f.); *Britz,* Informationelle Selbstbestimmung zwischen rechtswissenschaftlicher Grundsatzkritik und Beharren des Bundesverfassungsgerichts, in: Brandt u.a. (Hrsg.), Offene Rechtswissenschaft, 2010, S. 561; *Poscher,* Die Zukunft der informationellen Selbstbestimmung als Recht auf Abwehr von Grundrechtsgefährdungen, in: Gander u.a. (Hrsg.), Resilienz in der offenen Gesellschaft, 2012, S. 167 (182 ff.).

Gesetzesänderungen kommen könnte, ist den Diskutanten indes nicht ersichtlich. Unabhängig davon muss man sich bei vergleichbaren Vorhaben immer vor Augen führen, dass Datenbereithaltungspflichten nicht nur eine immense Speicherkapazität erfordern, sondern auch dass die erforderlichen betrieblichen und technischen Umstrukturierungen zu finanziellen Belastungen der Unternehmen führen und letztendlich deren Berufsausübung (Art. 12 I GG; Art. 15 I GRCh) beschränken.

Das zweite Takeaway dieser Debatte adressiert die Rolle des Datenaltruismus insbesondere in Kombination mit Datenvermittlungsdiensten. Gerade in Notstandsfällen könnte beidem eine zentrale Rolle zukommen. Gleichzeitig ist das freiwillige Datenteilen recht unattraktiv ausgestaltet, sodass nicht zu erwarten ist, dass sich viele Dateninhaber bereitwillig als Datenvermittlungsdienst oder gar datenaltruistische Organisation anbieten werden. Dennoch ist ungeklärt, wie die Attraktivität von Datenaltruismus gesteigert werden könnte. Ideen wären etwa die AGB-rechtliche Einbettung von freiwilligen Datenspenden oder die steuerliche Absetzbarkeit. Dabei scheint man (noch) nicht vom Helferrecht lernen zu können, da Datenaltruismus als allgemeine Bewegung noch nicht in der Gesellschaft angekommen ist. Während man etwa beim THW mit anpackt, sozial aktiv wird und damit entsprechend zwischenmenschlicher Nächstenliebe handelt, verbindet man die Datenspende nicht mit diesen Attributen – sie kann jederzeit per Knopfdruck von der Couch aus getätigt werden, ohne dass man die unmittelbaren Auswirkungen seines altruistischen Handelns spüren kann.

Letztendlich zeigte die Diskussion, dass rechtliche Instrumente als Rechtsfiguren und -formen zwar existent sind, aber immer noch zahlreiche technische und auch rechtliche Vorfragen der Bereitstellungsinfrastruktur sowie Kollisionsfragen zum Datenschutzrecht nicht ausreichend geklärt sind.