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.