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.