

MÄRZ 2025

13

Weizenbaum-Institut

Stellungnahme zum Referenten- entwurf eines Gesetzes zur Durchführung der Verordnung (EU) 2023/2854 (Data Act- Durchführungsgesetz – DA-DG)

AUTOR:INNEN

Jonathan Baumer \\\ Humboldt-Universität zu Berlin
Lisa Marksches \\\ Weizenbaum-Institut
Ceyda Erbay \\\ Humboldt-Universität zu Berlin
Herbert Zech \\\ Weizenbaum-Institut

Kontakt: herbert.zech@weizenbaum-institut.de

ÜBER DIESES PAPER

Die Stellungnahme wurde in einem kollaborativen Prozess von vier Forschenden am Weizenbaum-Institut erarbeitet. Im Anschluss an eine Analyse der Vorschriften des Referentenentwurfs im Abgleich zur wissenschaftlichen Diskussion rund um den Data Act und dessen Durchsetzung folgte die erste Erarbeitung von Schwerpunkten einer Stellungnahme in einer gemeinsamen Diskussion. Auf dieser Grundlage wurde die Stellungnahme anschließend in arbeitsteiligem Vorgehen von den vier Forschenden fertiggestellt.

In den Weizenbaum Policy Papers werden wissenschaftlich fundierte Stellungnahmen, Positionspapiere und Briefings zu aktuellen politischen Themen und Entscheidungsprozessen veröffentlicht.

ÜBER DAS WEIZENBAUM-INSTITUT

Das Weizenbaum-Institut ist ein Verbundprojekt und wird vom Bundesministerium für Bildung und Forschung (BMBF) und dem Land Berlin gefördert. Es betreibt interdisziplinäre Grundlagenforschung zur digitalen Transformation der Gesellschaft und liefert evidenzbasierte und wertorientierte Handlungsoptionen, damit die Digitalisierung nachhaltig, selbstbestimmt und verantwortungsvoll gestaltet werden kann.

Weizenbaum Policy Paper

Stellungnahme zum Referentenentwurf eines Gesetzes zur Durchführung der Verordnung (EU) 2023/2854 (Data Act-Durchführungsgesetz – DA-DG)

Weizenbaum-Institut

¶ Abstract

Der 2023 verabschiedete Data Act hat sich zum Ziel gesetzt, faire Zugangs- und Nutzungsregeln für Daten, die von Internet of Things-Geräten generiert wurden, zu schaffen. Die Ausgestaltung der Durchsetzung der Verordnung wird in Teilen auch dem nationalen Gesetzgeber überlassen. Hier setzt der Referentenentwurf eines Gesetzes zur Durchführung der Verordnung (EU) 2023/2854 (Data Act-Durchführungsgesetz – DA-DG) an. Diese Stellungnahme greift maßgebliche Aspekte des Entwurfs auf und analysiert sie. Ein Schwerpunkt der Betrachtung liegt auf der Stellung der Bundesnetzagentur als zentrale Durchsetzungsbehörde. Insbesondere die große Zahl von Fällen, die personenbezogene Daten zum Gegenstand haben, stellt hier eine Herausforderung dar, die durch eine Stärkung der Datenschutzbehörden gelöst werden könnte. Ebenso wird das zweigleisige Durchsetzungssystem, dessen behördliche Schiene im Referentenentwurf konkretisiert wird, im Rahmen der Stellungnahme diskutiert. Besonders im Fokus stehen hier die Position des Nutzers sowie der Umgang mit Geschäftsgeheimnissen. Die Betrachtung erfolgt hierbei stets mit Blick auf die Geeignetheit der Maßnahmen zur Erreichung der Ziele des Data Acts.

|| Inhalt

1	Einleitende Gedanken zur Durchsetzung der Verordnung (EU) 2023/2854	4
2	Zuständigkeitsvorschriften der §§ 2-4 DA-DG-E	6
2.1	§ 2 DA-DG-E: Zuständigkeit der Bundesnetzagentur als Ausgangspunkt	6
2.2	§ 3 DA-DG-E: Zuständigkeiten im Anwendungsbereich der DSGVO	7
2.3	§ 4 DA-DG-E: Zusammenarbeit mit anderen Behörden	12
3	Durchsetzungsmechanismen vor dem Ziel der Verordnung	13
3.1	Sanktionsregime	13
3.2	Die Position des Nutzers im DA-DG	14
3.3	Geschäftsgeheimnisse in der Durchsetzung des Data Acts	16
4	Zusammenfassung	18

1 Einleitende Gedanken zur Durchsetzung der Verordnung (EU) 2023/2854

Die Verordnung (EU) 2023/2854 vom 13. Dezember 2023 über harmonisierte Vorschriften für einen fairen Datenzugang und eine faire Datennutzung (Data Act / DA)¹ schafft ein horizontales Regelwerk von Datenzugangsrechten für Daten, die bei der Nutzung von vernetzten Produkten i.S.d. Art. 2 Nr. 5 DA (gemeinhin als Internet of Things-Produkte bekannt) und verbundenen Diensten, Art. 2 Nr. 6 DA, generiert werden. Kapitel IX des Data Acts ordnet die Durchsetzung im Wege einer behördlichen Überwachung², einem separaten Beschwerdemechanismus³ und Sanktionen⁴ an. Es treten sowohl Rechtsbehelfe gegen Entscheidungen der zuständigen Behörde⁵ als auch eine implizit vorausgesetzte Durchsetzung privatrechtlich einklagbarer Rechte⁶ hinzu. Die Konkretisierung der Durchsetzung der im Data Act angelegten Rechte obliegt jenseits des vom Data Act vorgegebenen Rahmens mehreren Akteuren: Auf europäischer Ebene wird die Europäische Kommission im Rahmen von delegierter Gesetzgebung gemäß Art. 45 DA i.V.m. Art. 29 Abs. 7 und Art. 33 Abs. 2 DA tätig, der EDIB (European Data Innovation Board) wird gemäß Art. 42 zur einheitlichen Anwendung beitragen und der Europäische Datenschutzbeauftragte tritt zur Datenschutzüberwachung im Rahmen des Data Acts gemäß Art. 37 Abs. 3 UAbs. 2 und Art. 40 Abs. 5 DA hinzu. Darüber hinaus obliegt sowohl den mitgliedstaatlichen Gerichten als auch dem Gerichtshof der Europäischen Union die gerichtliche Anwendung und Auslegung von Vorschriften zur Durchsetzung des Data Acts.

Schließlich werden die mitgliedstaatlichen Gesetzgeber in dem durch die Verordnung geschaffenen Rahmen tätig, um nationale Regeln für die Durchsetzung zu schaffen. Explizit vorgesehen ist dies in Bezug auf Vorschriften zur behördlichen Überwachung nach Art. 37 Abs. 5 DA und in Bezug auf Sanktionsvorschriften nach Art. 40 Abs. 1 DA. Gegenstand dieser Stellungnahme ist der Referentenentwurf eines Gesetzes zur Durchführung der Verordnung (EU) 2023/2854 (Referentenentwurf/DA-DG-E), welcher diesen vom Data Act vorgegebenen Rahmen ausfüllen soll. Insbesondere wird die Bundesnetzagentur (BNetzA) als zuständige Behörde i.S.d. Art. 37 Abs. 1 DA bestimmt, vgl. § 2 Abs. 1 DA-DG-E, und es werden ihr

¹ Verordnung (EU) 2023/2854 des Europäischen Parlaments und des Rates vom 13. Dezember 2023 über harmonisierte Vorschriften für einen fairen Datenzugang und eine faire Datennutzung sowie zur Änderung der Verordnung (EU) 2017/2394 und der Richtlinie (EU) 2020/1828 (Datenverordnung), ABl. L 22.12.2023, S. 1-71.

² Art. 37 DA.

³ Art. 38 DA.

⁴ Art. 40 DA.

⁵ Art. 39 DA.

⁶ Metzger/Schweitzer, ZEuP 2023, 42 (79); Wiebe, GRUR 2023, 1569 (1577).

Kompetenzen zur Überwachung der Verordnung, einschließlich der Erteilung von Bußgeldern als Sanktionen i.S.d. Art. 40 Abs. 1 DA, übertragen, vgl. §§ 6-18 DA-DG-E.

Während vereinzelt in Frage gestellt wird, inwiefern der starke Fokus des Data Acts auf eine behördliche Durchsetzung tatsächlich erforderlich ist und ob eine stärkere Betonung von oder gar die Beschränkung auf privatrechtliche Durchsetzungsmechanismen zu sachgerechteren Ergebnissen kommen würde,⁷ sind die mitgliedstaatlichen Gesetzgeber schon wegen der unmittelbaren Wirkung der Verordnung gemäß Art. 288 Abs. 2 S. 2 AEUV nicht befugt, die konkrete Anordnung der Durchsetzungsmechanismen des Data Acts durch den europäischen Gesetzgeber zu missachten. In Anbetracht dieser Grundsätze ist anlässlich der Beurteilung eines mitgliedstaatlichen Durchführungsgesetzes vorrangig zu erörtern, ob die Entscheidungen des nationalen Gesetzgebers im Rahmen der durch die Verordnung eröffneten Spielräume den vom Data Act verfolgten Zweck fördern können. Dabei konzentriert sich die Stellungnahme entsprechend dem Ansatz des Data Acts, konkret dessen Kapitel IX, auf die behördliche Durchsetzung der Verordnung. Dennoch sollte bereits an dieser Stelle darauf hingewiesen werden, dass mit dem Referentenentwurf selbst auch keine substantiellen Vorgaben zur privatrechtlichen Durchsetzung des Data Acts getroffen werden. Wie sich der materiell privatrechtliche Regelungsgehalt des Data Acts⁸ auf die behördliche Durchsetzung im Anwendungsbereich des Referentenentwurfs auswirkt, ist im Rahmen dieser Stellungnahme anzusprechen.

Der Data Act soll mittels Datenzugangs- und Datenweitergaberechten, Missbrauchskontrolle bei der vertraglichen Vereinbarung von Datenzugangsrechten und portabilitätserleichternden Pflichten von Datenverarbeitungsdiensten die Zugänglichkeit und Verfügbarkeit von Daten zur Eröffnung von Innovation und Märkten verbessern.⁹ Hierbei will der Data Act zugleich vermeiden, dass durch eine übermäßige Einschränkung der im Ausgangspunkt bestehenden Kontrolle der Dateninhaber, in der Regel die Hersteller von IoT-Produkten,¹⁰ Anreize gegen Investitionen in die Herstellung von IoT-Produkten geschaffen werden.¹¹

Zur Beurteilung, ob der Referentenentwurf grundsätzlich in einer vom Data Act vorgesehnen Weise den Spielraum zur Konkretisierung von nationalen Durchsetzungsmechanismen nutzt und ob hierbei dem dargestellten Ziel der Verordnung ausreichend Rechnung getragen wird, erfolgt zunächst eine Einordnung der Zuständigkeitsvorschriften der §§ 2-4 DA-DG-E. Anschließend soll nach einer allgemeinen Einordnung des Bußgeldregimes des § 18 DA-DG-E Stellung zu der Frage bezogen werden, ob und, wenn ja, wie sich die im Referentenentwurf vorgesehenen Durchführungsmechanismen auf die im Data Act maßgebliche

⁷ Drexel et al., Position Statement of the Max Planck Institute for Innovation and Competition of 25 May 2022 on the Commission's Proposal of 23 February 2022 for a Regulation on harmonised rules on fair access to and use of data (Data Act), Max Planck Institute for Innovation and Competition No. 22-05, 2022, Rn. 243-246; Henne-mann/Steinrötter, NJW 2024, 1 (8).

⁸ Vgl. an dieser Stelle nur Metzger, in: Sattler/Zech (Hrsg.), The Data Act: First Assessments, 2024, S. 67-81 (67).

⁹ Erwgr. 1-4 DA.

¹⁰ Eckardt/Kerber, European Journal of Law and Economics 57(1-2), 113 (120).

¹¹ Erwgr. 32 DA.

Position des Nutzers¹² auswirken und welche Rolle Geschäftsgeheimnisse bei der Durchsetzung spielen werden. Abschließend werden offene Fragen hervorgehoben und eine zusammenfassende Einschätzung gegeben.

2 Zuständigkeitsvorschriften der §§ 2-4 DA-DG-E

Die Regeln des Art. 37 DA eröffnen den Mitgliedstaaten Spielraum bei der Ernennung und Ausgestaltung der für die Durchsetzung des Data Acts zuständigen Behörde. Hier setzt der Referentenentwurf an und legt in seinem § 2 Abs. 1 die BNetzA als einzige zuständige Behörde i.S.d. Art. 37 Abs. 1 DA fest. Neben dieser Grundsatzentscheidung treffen §§ 3 und 4 DA-DG-E, wie auch durch Art. 37 Abs. 3 UAbs. 1 S. 1, Abs. 4 lit. a DA angeordnet, Bestimmungen hinsichtlich der Zuständigkeit der Aufsichtsbehörden im Rahmen der Verordnung (EU) 2016/679 (DSGVO)¹³ und der Zuständigkeit sektoraler Behörden. Diese Bestimmungen sind im Folgenden eingehender zu untersuchen.

2.1 § 2 DA-DG-E: Zuständigkeit der Bundesnetzagentur als Ausgangspunkt

Zunächst ist die Entscheidung für lediglich eine zuständige Behörde grundsätzlich zu begrüßen.¹⁴ Vereinzelt wurde die Zuständigkeit der BNetzA im Gleichlauf mit dem Entwurf eines Daten-Governance-Gesetzes¹⁵ (DGG-E) zur Bündelung der Kompetenzen bei der Überwachung von Verordnungen zur Datenwirtschaft als naheliegend angesehen.¹⁶ Eine abschließende Stellungnahme zur Ernennung der BNetzA als zuständige Behörde folgt im Rahmen der Erläuterung von Zuständigkeiten bei der Schnittstelle von Data Act und DSGVO und bezieht die Erwägungen zur Kohärenz mit dem DGG-E ein.

Die Ernennung einer einzigen zuständigen Behörde ermögliche laut der Begründung des Referentenentwurfs schließlich auch den Verzicht auf die Ernennung eines Datenkoordinators gem. Art. 37 Abs. 2 S. 1 DA.¹⁷ Diese Entscheidung wird bei der Auslegung der Vorschriften zur Zuständigkeit anderer Behörden zu berücksichtigen sein.

¹² Vgl. hierzu Eckardt/Kerber, Property rights theory, bundles of rights on IoT data, and the Data Act, European Journal of Law and Economics 57(1-2), 113, 2023.

¹³ Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG, ABl. L 119, 4.5.2016, S. 1-88.

¹⁴ Vgl. Gemeinsame Stellungnahme des EDSA und EDSB vom 4.5.2022 zum Vorschlag des Europäischen Parlaments und des Rates über harmonisierte Vorschriften für einen fairen Datenzugang und eine faire Datennutzung (Datengesetz), Rn. 98; Bitkom, Vorschläge zur nationalen Durchführung des Data Act, 2024, S. 5.

¹⁵ BT-Drucks. 20/13090, S. 7.

¹⁶ Bitkom, Vorschläge zur nationalen Durchführung des Data Act, 2024, S. 6.

¹⁷ Gesetzesbegründung des Data Act-Durchführungsgesetzentwurfs (Bearbeitungsstand 5.2.2025), S. 24.

2.2 § 3 DA-DG-E: Zuständigkeiten im Anwendungsbereich der DSGVO

§ 3 Abs. 1 DA-DG-E erklärt die/den Bundesbeauftragte(n) für den Datenschutz und die Informationsfreiheit (BfDI) als für die Überwachung der DSGVO im Rahmen des Data Acts zuständig. Um die Tragweite und Bedeutung dieser Regelung einzuschätzen, wird zunächst zusammenfassend das Zusammenwirken von DSGVO und Data Act dargestellt, bevor die Bedeutung und Auswirkung der Vorschrift des Referentenentwurfs zur Zuständigkeit der/des BfDI erörtert werden soll.

2.2.1 Das Verhältnis von DSGVO und Data Act

Gemäß Art. 1 Abs. 5 DA gelten die Vorschriften des Data Acts unbeschadet der Vorschriften zum Schutz personenbezogener Daten. Sofern personenbezogene Daten im Rahmen des Anwendungsbereichs des Data Acts betroffen sind, sind mithin die Vorschriften der DSGVO einzuhalten. Dies bedeutet insbesondere für die zentralen Vorschriften der Art. 4 Abs. 1 und Art. 5 Abs. 1 DA, dass bei einem Datenzugangsverlangen, welches zumindest auch (sensible) personenbezogene Daten betrifft, Datenverarbeitungsermächtigungen i.S.d. Art. 6 (und ggf. 9) DSGVO berücksichtigt werden müssen.¹⁸ Vermehrt wird davon ausgegangen, dass in einer nicht unerheblichen Zahl der Fälle von einem Personenbezug der vom Zugangsverlangen betroffenen Daten auszugehen sein kann.¹⁹ Dies ergebe sich nicht zuletzt aus der unklaren Abgrenzung und einer daraus folgenden Annahme von Personenbezug im Zweifel.²⁰ Der Anwendungsvorrang der DSGVO gegenüber dem Data Act hat mehrere Fragen aufgeworfen, welche für eine effektive Durchsetzung des Data Acts von großer Bedeutung sind, insbesondere die Feststellung der einschlägigen Verarbeitungsgrundlage des Art. 6 (und 9) DSGVO bei Datenzugangsverlangen und zusammenhängende Bedenken in Bezug auf eine mögliche „Flucht ins Datenschutzrecht“.²¹

2.2.2 Umsetzung des Data Acts im Anwendungsbereich der DSGVO nach dem Referentenentwurf

Ausgehend von der Anwendbarkeit der DSGVO postuliert bereits Art. 37 Abs. 3 UAbs. 1 S. 1 DA die Zuständigkeit der datenschutzrechtlichen Aufsichtsbehörde, sodass der nationale Gesetzgeber an diese Entscheidung grundsätzlich gebunden ist. Der Referentenentwurf stellt jedoch darüber hinaus in § 3 Abs. 5 und 6 klar, dass die Zuständigkeit der/des BfDI bei Anwendbarkeit der DSGVO im Rahmen der Durchsetzung des Data Acts zur Zuständigkeit der

¹⁸ Erwgr. 7 DA; Sattler, in: Sattler/Zech, (Hrsg.), *The Data Act: First Assessments*, 2024, S. 103-135 (105 f.). Darüber hinaus wird auch in Hinblick auf das Verhältnis zwischen dem Accessibility-by-Design-Gebot des Art. 3 Abs. 1 DA und den Grundsätzen der Datenminimierung und Speicherbegrenzung des Art. 5 Abs. 1 lit. c und e DSGVO über materielle Spannungen zwischen den Verordnungen diskutiert, vgl. Sattler, in: Sattler/Zech, (Hrsg.), *The Data Act: First Assessments*, 2024, S. 103-135 (112-114); Specht-Riemenschneider, ZEuP 2023, 638 (663).

¹⁹ Antoine, CR 2024, 73 (74); Bomhard/Merkle, RDi 2022, 168 (172); Metzger/Schweitzer, ZEuP 2023, 42 (76); Wiebe, GRUR 2023, 1569 (1574).

²⁰ Bomhard/Merkle, RDi 2022, 168 (172); Sattler, in: Sattler/Zech, (Hrsg.), *The Data Act: First Assessments*, 2024, S. 103-135 (126).

²¹ Siehe zur Diskussion: Antoine, CR 2024, 73 (74 f. und 79); Bomhard, MMR 2024, 71 (74); Hennemann/Steinrötter, NJW 2024, 1 (5 f.); Sattler, in: Sattler/Zech, (Hrsg.), *The Data Act: First Assessments*, 2024, S. 103-135 (119-129).

BNetzA hinzutritt und in diesen Verfahren die Behörden gemeinsam entscheiden.²² Zu beachten ist ferner, dass lediglich die BNetzA nach außen hin als verfahrensleitende Behörde auftritt, sodass gegenüber Beschwerdeführenden laut der Begründung des Referentenentwurfs keine Einschränkung des One-Stop-Shop-Prinzips zu befürchten sei.²³ Der teilweise festgestellte Klärungsbedarf²⁴ hinsichtlich der Kompetenzen der Datenschutzbehörden im Rahmen ihrer Zuständigkeit bei der Durchsetzung des Data Acts nach Art. 37 Abs. 3 UAbs. 1 sollte mit der vorgeschlagenen Lösung ausgeräumt sein, sofern die BNetzA als verfahrensleitende Behörde ihre Kompetenzen entsprechend des Durchführungsgesetzes ausübt, während für die/den BfDI die Kompetenzen nach dem BDSG, insbesondere dessen §§ 14, 16, einschlägig sind.

Mit Blick auf die Effizienz der behördlichen Überwachung der Durchführung, welche im Durchsetzungsmodell des Data Act an vorrangiger Stelle steht,²⁵ sollte die oben angeführte Häufigkeit der Anwendung der DSGVO im Rahmen des Data Acts Berücksichtigung finden. Die Gesetzesbegründung ordnet zudem bereits eine Konsultation der/des BfDI an, sobald ein Personenbezug der verfahrensgegenständlichen Daten zumindest im Raum steht.²⁶ Hiervon ausgehend wird eine Befassung der/des BfDI und ihre/seine (Mit-)Zuständigkeit nach § 3 Abs. 1 DA-DG-E bei der Durchsetzung des Data Acts mit Sicherheit sehr häufig, wenn nicht sogar Regelfall sein.

2.2.3 Sanktionen bei Verstößen gegen den Data Act im Anwendungsbereich der DSGVO

Abschließend ist in Bezug auf die Schnittmenge von Data Act und DSGVO auf eine offene Frage von nicht unerheblicher Bedeutung hinzuweisen: Der Referentenentwurf nimmt weder im Rahmen der Zuständigkeitsvorschriften des § 3 noch im Rahmen des Sanktionsregimes des § 18 DA-DG-E Bezug auf die Vorschrift des Art. 40 Abs. 4 DA, welche eine Sanktionsierung von Verstößen gegen Kapitel II, III und V des DA durch die Datenschutzbehörden vorsieht. Eine Umsetzung dieser Vorschrift nach dem im Referentenentwurf gewählten Modell der Mitzuständigkeit der/des BfDI nach § 3 Abs. 5 und 6 DA-DG-E wirft mehrere Fragen auf.

Art. 40 Abs. 4 DA knüpft an die Zuständigkeit der mitgliedstaatlichen Datenschutzaufsichtsbehörden und damit implizit auch an Art. 37 Abs. 3 DA an.²⁷ Die Durchsetzungszuständigkeit der Datenschutzaufsichtsbehörden soll gemäß Art. 40 Abs. 4 DA auch die Möglichkeit umfassen, bei Verstößen gegen Kapitel II, III und V des Data Acts unter entsprechender

²² Die Gesetzesbegründung des Data Act-Durchführungsgesetzentwurfs (Bearbeitungsstand 5.2.2025) spricht von mehrstufigen Verwaltungsakten.

²³ Gesetzesbegründung des Data Act-Durchführungsgesetzentwurfs (Bearbeitungsstand 5.2.2025), S. 26.

²⁴ Remke, MMR 2024, 117 (117); Schreiber/Pommerening/Schoel, Der neue Data Act, 2. Auflage 2024, § 9 Rn. 4.

²⁵ Drexel et al., Position Statement of the Max Planck Institute for Innovation and Competition of 25 May 2022 on the Commission's Proposal of 23 February 2022 for a Regulation on harmonised rules on fair access to and use of data (Data Act), Max Planck Institute for Innovation and Competition No. 22-05, 2022, Rn. 240.

²⁶ Gesetzesbegründung des Data Act-Durchführungsgesetzentwurfs (Bearbeitungsstand 5.2.2025), S. 27.

²⁷ Roth-Isigkeit, in: Wolff/Brink/v. Ungern-Sternberg (Hrsg.), BeckOK Datenschutzrecht, 50. Edition 2024, Art. 40 DA Rn. 7.

Anwendung von Art. 83 DSGVO zu sanktionieren. Die Vorschrift wurde teils in Bezug auf ihre Unklarheit kritisiert.²⁸

Der Referentenentwurf erwähnt die Vorschrift des Art. 40 Abs. 4 DA an keiner Stelle explizit. Es ist zu unterstellen, dass dabei richtigerweise von der direkten Anwendbarkeit dieser Norm ausgegangen wurde. Sollten zuständige Behörden nach Art. 40 Abs. 4 DA Bußgelder erteilen, bleibt dennoch die Frage, wie sich dies im Verhältnis zu den Zuständigkeiten nach dem Referentenentwurf verhält. In diesem Zusammenhang benennt § 18 Abs. 6 DA-DG-E als zuständige Verwaltungsbehörde für Ordnungswidrigkeiten i.S.d. § 18 DA-DG-E grundsätzlich die BNetzA vorbehaltlich Art. 37 Abs. 3 DA. Dieser Verweis auf Art. 37 Abs. 3 DA stellt die Bedeutung des § 3 Abs. 5 und 6 DA-DG-E unter folgenden Gesichtspunkten in Frage: Die Funktion letzterer Norm des Referentenentwurfs und ihre korrespondierende Begründung ist, wie bereits dargestellt, die Klärung der Fälle, in denen die DSGVO im Anwendungsbereich des Data Acts zu berücksichtigen ist, durch ein gemeinsames Verfahren.²⁹ Der Wortlaut des § 18 Abs. 6 DA-DG-E scheint jedoch von Fällen auszugehen, in denen durch die Anwendung des Art. 37 Abs. 3 DA, also bei Berücksichtigung der DSGVO im Rahmen des Data Acts, die Zuständigkeit der Datenschutzaufsichtsbehörde einen Vorbehalt zur Zuständigkeit der BNetzA darstellt. Nicht nur offenbart dieses Verständnis einen Widerspruch innerhalb des Referentenentwurfs, sondern ausgehend vom Data Act, spezifisch von Art. 40 Abs. 4, ist eine solche Deutung auch grundsätzlich angezeigt. Sofern der direkt anwendbare Art. 40 Abs. 4 DA die Datenschutzaufsichtsbehörde auf Grundlage ihrer Kompetenzen nach der DSGVO ermächtigt Bußgelder bei Verstößen gegen den Data Act zu erteilen, wäre dies *prima facie* grundsätzlich nicht mit dem Modell des § 3 Abs. 6 DA-DG-E vereinbar, wonach die BNetzA zur Durchsetzung des Data Acts mit Zustimmung der/des BfDI handelt. Diese Widersprüche erscheinen besonders dann schwerwiegend, wenn die Gesetzesbegründung davon ausgeht, eine Notwendigkeit eines Datenkoordinators nach Art. 37 Abs. 2 DA wäre aufgrund der alleinigen Zuständigkeit der BNetzA ausgeschlossen.³⁰

2.2.4 Stellungnahme zur effektiven Durchsetzung des Data Acts im Verhältnis von BfDI und BNetzA

Im Grundsatz ist sich den Stimmen anzuschließen, die ein Verfahren vor einer einzigen Behörde i.S.d. One-Stop-Shop-Prinzips befürworten.³¹ Vor dem Hintergrund der Kritik, vor welcher der Fokus des Data Acts auf behördliche Durchsetzung steht,³² und zur gerechten

²⁸ BR-Drucks. 130/1/22, Rn. 48; Remke, MMR 2024, 117 (121).

²⁹ Gesetzesbegründung des Data Act-Durchführungsgesetzentwurfs (Bearbeitungsstand 5.2.2025), S. 25-27. Dabei tritt die BNetzA ausweislich dieser Begründung alleine nach außen hin auf.

³⁰ Gesetzesbegründung des Data Act-Durchführungsgesetzentwurfs (Bearbeitungsstand 5.2.2025), S. 24.

³¹ Gemeinsame Stellungnahme des EDSA und EDSB vom 4.5.2022 zum Vorschlag des Europäischen Parlaments und des Rates über harmonisierte Vorschriften für einen fairen Datenzugang und eine faire Datennutzung (Datengesetz), Rn. 98; Bitkom, Vorschläge zur nationalen Durchführung des Data Act, 2024, S. 5.

³² Drexel et al., Position Statement of the Max Planck Institute for Innovation and Competition of 25 May 2022 on the Commission's Proposal of 23 February 2022 for a Regulation on harmonised rules on fair access to and use of data (Data Act), Max Planck Institute for Innovation and Competition No. 22-05, 2022, Rn. 243-246; Henne-mann/Steinrötter, NJW 2024, 1(8).

Umsetzung des Zwecks des Data Acts, durch einfache Datenzugänglichkeit Innovation und Märkten zu eröffnen, kann die Bedeutung eines effizienten und einfachen Verwaltungsverfahrens nicht überschätzt werden.³³ Ferner muss das Verwaltungsverfahren bei Konfliktlagen im Rahmen der Durchführung des Data Acts gegensätzliche Interessen zu einem Ausgleich bringen, der sowohl dem Ziel der Verordnung als auch anderen legitimen Interessen gerecht wird.

Hiervon ausgehend mag grundsätzlich angeführt werden, dass BfDI und BNetzA mit den unterschiedlich ausgerichteten Zwecksetzungen ihrer Rechtsgrundlagen und damit auch ihren gegensätzlichen Aufträgen³⁴ durch den in § 3 Abs. 5 und 6 DA-DG-E vorgesehenen Dialog einem Ausgleich beim Konfliktfall Data Act und DSGVO abhelfen können. Ferner spricht für die Zuständigkeit der BNetzA der angeführte Gleichlauf mit dem DGG-E.

Jenseits davon ist jedoch zu fragen, ob der vorgesehene Dialog zwischen BNetzA und BfDI der effizienten Durchsetzung dienlich ist. Eine reibungslose Umsetzung der behördlichen Struktur ist nicht zuletzt für die Klärung ausstehender materieller Fragen rund um das Verhältnis von Data Act und DSGVO unentbehrlich. Wie zuvor dargestellt, könnte das mehrstufige gemeinsame Verfahren den Regelfall nach § 3 Abs. 5 und 6 DA-DG-E darstellen, was zu berücksichtigende Koordinationsaufwände mit sich bringen würde. In Anbetracht dieser Aufwände und der deutlichen Regel des Art. 37 Abs. 2 DA zur Erforderlichkeit des Datenkoordinators bei mehreren zuständigen Behörden muss kritisch beleuchtet werden, ob die regelmäßige parallele Zuständigkeit von BfDI und BNetzA im Rahmen des gemeinsamen Verfahrens die Erforderlichkeit eines Koordinators nicht doch begründet.

Schließlich ist die Klärung des Verhältnisses von § 3 Abs. 6 DA-DG-E zu § 18 Abs. 6 DA-DG-E und Art. 37 Abs. 3 und Art. 40 Abs. 4 DA unerlässlich, wobei drei Lösungen denkbar sind:

Zunächst könnte die Durchsetzung von Verstößen gegen den Data Act bei Zuständigkeit der Datenschutzaufsichtsbehörde gemäß Art. 37 Abs. 3 DA konsequent nach dem Modell des § 3 Abs. 5 und 6 DA-DG-E gelöst werden. Diese Lösung könnte im Widerspruch zum Wortlaut des Art. 40 Abs. 4 DA stehen. Jedoch kann davon ausgegangen werden, dass Art. 40 Abs. 4 ohnehin implizit an Art. 37 Abs. 3 DA anknüpft,³⁵ sodass die Lösung über das Modell zur Umsetzung von Art. 37 Abs. 3 DA nicht grundsätzlich abwegig ist.

Alternativ und als explizite Ausnahme von §§ 2 Abs. 1, 3 Abs. 5 und 6 DA-DG-E könnte sich § 18 Abs. 6 DA-DG-E implizit auf Art. 40 Abs. 4 DA beziehen, womit die/der BfDI für die Verfolgung von Ordnungswidrigkeiten bei Anwendung von Art. 37 Abs. 3 DA alleinige Zuständigkeit besäße und ihre Kompetenzen nach Art. 83 DSGVO ausüben würde. In diesem Fall müsste die Zuständigkeit der BNetzA zur Durchsetzung von § 18 DA-DG-E

³³ So auch die Begründung selbst, vgl. Gesetzesbegründung des Data Act-Durchführungsgesetzentwurfs (Bearbeitungsstand 5.2.2025), S. 19 f.

³⁴ Bitkom, Vorschläge zur nationalen Durchführung des Data Act, 2024, S. 6.

³⁵ Roth-Isigkeit, in: Wolff/Brink/v. Ungern-Sternberg (Hrsg.), BeckOK Datenschutzrecht, 50. Edition 2024, Art. 40 DA Rn. 7.

konsequenterweise zur Einhaltung des Doppelbestrafungsverbots gesperrt bleiben.³⁶ Ange- sichts der unmittelbaren Wirkung des Art. 40 Abs. 4 DA und des Verweises in § 18 Abs. 6 DA-DG-E auf Art. 37 Abs. 3 DA könnte dieses Verständnis möglicherweise dem Referentenentwurf ohnehin zugrunde liegen.

Die dritte, weitreichendste und zugleich konsequenteste Lösung zum Widerspruch zwischen § 3 Abs. 6 DA-DG-E auf der einen und § 18 Abs. 6 DA-DG-E und Art. 40 Abs. 4 DA auf der anderen Seite wäre eine grundsätzliche, alleinige Zuständigkeit der Datenschutzaufsichtsbehörde(n) (Landesbeauftragte für Datenschutz und die/der BfDI) zur Durchsetzung, soweit das konkrete Verfahren persönliche Daten i.S.d. DSGVO betrifft und somit ohnehin eine durch Art. 37 Abs. 3 DA deklaratorisch verwiesene originäre Datenschutzkompetenz besteht.³⁷ Die Datenschutzaufsichtsbehörde würde als unmittelbar zuständige Stelle eine Einschätzung der Betroffenheit persönlicher Daten im gegenständlichen Verfahren vornehmen. Im Falle der Nicht-Betroffenheit würde die Datenschutzaufsichtsbehörde die Fortsetzung des Verfahrens durch die BNetzA eröffnen. Im Falle der Betroffenheit hingegen würde sie schon wegen ihrer originären Kompetenz das Verfahren alleine zu Ende führen. Das Verfahren würde hierdurch im Vergleich zur Regelung in § 3 Abs. 5 und 6 DA-DG-E verkürzt und vereinfacht. Ausgehend von der verbreiteten Annahme eines Personenbezugs von Daten im Zweifel³⁸ würde diese im Vergleich zum Referentenentwurf umgekehrte Lösung im Zweifel die alleinige Zuständigkeit der Datenschutzaufsichtsbehörden begründen. Komplexe, sich bereits jetzt abzeichnende Fragen zum Zusammenspiel zwischen DSGVO und Data Act würden der Behörde obliegen, welche diese Fragen mit dem entsprechenden Fachwissen beantworten kann – es handelt sich zu einem beachtlichen Teil um Fragen des Datenschutzrechtes, deren Komplexität ins Datenwirtschaftsrecht getragen werden,³⁹ der Sache nach also um datenschutzrechtliche Fragen. In dieser Konstellation bestünde schließlich eine konsequente Anwendbarkeit des Art. 40 Abs. 4 DA durch die Datenschutzaufsichtsbehörde.

Hinsichtlich des Gleichlaufs mit dem DGG-E ist darauf hinzuweisen, dass die europarechtlichen Grundlagen für die Durchsetzung dieser Gesetze im Hinblick auf Schnittstellen mit der DSGVO variieren: Der Data Governance Act (DGA)⁴⁰ beschränkt einen Vorrang der DSGVO in seinem Art. 1 Abs. 3 auf Konfliktfälle, wohingegen der Data Act einen allgemeinen Vorrang der DSGVO einräumt.⁴¹

³⁶ Vgl. Remke, MMR 2024, 117 (121).

³⁷ Anerkennend gegenüber dieser Möglichkeit: Steinrötter, GRUR 2023, 216; befürwortend bereits im Hinblick auf den Data Act selbst: Gemeinsame Stellungnahme des EDSA und EDSB vom 4.5.2022 zum Vorschlag des Europäischen Parlaments und des Rates über harmonisierte Vorschriften für einen fairen Datenzugang und eine faire Datennutzung (Datengesetz), Rn. 115.

³⁸ Bomhard/Merkle, RDi 2022, 168 (172); Sattler, in: Sattler/Zech, (Hrsg.), The Data Act: First Assessments, 2024, S. 103-135 (126).

³⁹ Sattler, in: Sattler/Zech, (Hrsg.), The Data Act: First Assessments, 2024, S. 103-135 (115-118).

⁴⁰ Verordnung (EU) 2022/868 des Europäischen Parlaments und des Rates vom 30. Mai 2022 über europäische Da- ten-Governance und zur Änderung der Verordnung (EU) 2018/1724 (Daten-Governance-Rechtsakt), ABl. L 152, 3.6.2022, S. 1-44.

⁴¹ Vgl. die Gegenüberstellung bei Specht-Riemenschneider, ZEuP 2023, 638 (670 f.)

Vermehrt wird die vorrangige Zuständigkeit von Datenschutzaufsichtsbehörden zur Durchsetzung des Data Acts unter dem Gesichtspunkt kritisiert, Datenschutzbehörden hätten lediglich einen Schutzauftrag, der dem Zweck des Data Acts entgegenstehe.⁴² Die Einordnung der Zwecksetzungen von Datenschutz und freier Datenwirtschaft in binäre Entscheidungen ist jedoch nicht durch die maßgeblichen Rechtsgrundlagen angezeigt und fördert auch nicht die Lösung von Konflikten zwischen effektivem Datenwirtschaftsrecht und grundrechtlich adäquaten Datenschutzrecht.⁴³ Schon Art. 1 Abs. 3 DSGVO erklärt zum Ziel der Verordnung, dass der freie Verkehr von personenbezogenen Daten in der Union nicht aus Datenschutzgründen eingeschränkt oder verboten werden darf. Zugleich ist die Aufrechterhaltung des Datenschutzes unter anderem Ziel des Data Acts,⁴⁴ welches mit der hier präsentierten Lösung nicht Gegenstand eines möglichen Konflikts zwischen zwei zuständigen Behörden sein müsste. Bei dem Vorschlag einer alleinigen Zuständigkeit von Datenschutzbehörden bei Betroffenheit personenbezogener Daten soll vielmehr die Chance gegeben werden, innerhalb einer Behörde interessengerechte und effiziente Ausgleiche zwischen Datenschutz und Datenzugang und -weitergabe zu finden.

2.3 § 4 DA-DG-E: Zusammenarbeit mit anderen Behörden

Art. 37 Abs. 4 DA schreibt vor, dass die Zuständigkeit sektoraler Behörden gewahrt bleiben muss. Diese Regelung soll § 4 DA-DG-E in nationales Recht umsetzen.⁴⁵ Die Gesetzesbegründung sieht mögliche Anwendungsfälle insbesondere für die Zuständigkeiten des Bundeskartellamts, des Bundesamts für Sicherheit in der Informationstechnik und des Kraftfahrt-Bundesamts gegeben. Mit Hinweis auf das Urteil des EuGH in der Rechtssache Meta zeigt Schulz⁴⁶ die mögliche kartellrechtliche Berücksichtigung der Wertungen des Data Acts auf, was die Relevanz der Zusammenarbeit der Behörden offenlegt. Eine ähnliche Schnittmenge offenbart sich beim Verwendungsverbot der Art. 4 Abs. 10 und Art. 6 Abs. 2 lit. e DA,⁴⁷ über deren Verletzung die BNetzA auch im Rahmen eines Sanktionsverfahrens entscheiden könnte.

§ 4 Abs. 2 DA-DG-E statuiert die Pflicht der BNetzA, sich mit zuständigen oberen Bundesbehörden im Rahmen ihrer sachlichen Zuständigkeiten ins Benehmen zu setzen. Benehmen ist als verwaltungsinterne Mitwirkungsform schwächer ausgestaltet als Formen der Zustimmung⁴⁸ und stellt die Entscheidung der verfahrensleitenden Behörde gerade nicht in Abhängigkeit einer verbindlichen Einschätzung der anderen Behörde.⁴⁹ Demnach mag es zunächst zweifelhaft erscheinen, ob diese Umsetzung der Anforderung des Wahrens der

⁴² Remke, MMR 2024, 117 (118), Bitkom, Vorschläge zur nationalen Durchführung des Data Act, 2024, S. 6.

⁴³ Vgl. Specht-Riemenschneider, ZEuP 2023, 638 (672).

⁴⁴ Erwgr. 7, Art. 1 Abs. 5 DA.

⁴⁵ Gesetzesbegründung des Data Act-Durchführungsgesetzentwurfs (Bearbeitungsstand 5.2.2025), S. 28.

⁴⁶ Schulz, NZKart 2024, 426 (430).

⁴⁷ Schulz, NZKart 2024, 426 (431 f.).

⁴⁸ So auch selbst die Gesetzesbegründung des Data Act-Durchführungsgesetzentwurfs (Bearbeitungsstand 5.2.2025), S. 29.

⁴⁹ Siegel, in: Stelkens/Bonk/Sachs (Hrsg.), Verwaltungsverfahrensgesetz, 10. Auflage 2023, § 58 Rn. 27.

sektoralen Zuständigkeit aus Art. 37 Abs. 4 lit. a DA genügt, insbesondere wenn die Entscheidung der sachlich zuständigen Behörde für die BNetZA nicht rechtsverbindlich ist.

Im Übrigen sollte jedoch beim Anwendungsbereich des § 4 DA-DG-E anknüpfend an Art. 37 Abs. 4 lit. a DA berücksichtigt werden, dass diese Vorschriften vom Anwendungsbereich des Data Acts begrenzt werden, welcher wiederum gemäß Art. 44 DA, insbesondere dessen Abs. 2, hinter sektoralem Datenrecht zurücktritt. Dass § 4 DA-DG-E mithin nur solche sachlich zuständigen sektoralen Behörden meint, deren Zuständigkeit sich gerade nicht aus besonderem Datenrecht ergibt, verdient Klarstellung und sollte bei der Auslegung der Vorschrift und ihrer Bedeutung berücksichtigt werden. Insbesondere für die oben aufgeworfene Frage der Anforderungen des Art. 37 Abs. 4 lit. a DA könnte es einschränkend zu berücksichtigen sein, dass diese Norm ihrem Anwendungsbereich nach auf solche Behörden beschränkt ist, die gerade nicht für sektorales Datenrecht, sondern nur für Fachbereiche im weiten Sinne zuständig sind. Die Schnittmengen zum Kartellrecht bleiben vor diesem Hintergrund jedoch von großer Bedeutung. Dies gilt insbesondere im Hinblick auf bestehende Kompetenzen und Fachwissen des Bundeskartellamts bei digitalen Märkten,⁵⁰ welche in einzelnen Anwendungsfällen erhebliche Beiträge zu Verfahren im Einzelnen, aber auch zur Lösung von Rechtsfragen bei Schnittmengen zwischen Data Act und Kartellrecht bieten können. Dabei ist im Gegensatz zum Verhältnis zwischen DSGVO und Data Act jedoch nicht mit einer vergleichbaren Häufigkeit der Schnittmengen zu rechnen.

3 Durchsetzungsmechanismen vor dem Ziel der Verordnung

3.1 Sanktionsregime

Art. 40 Abs. 1 DA ermächtigt den nationalen Gesetzgeber zum Erlass von Sanktionsvorschriften. Abs. 3 wiederum stellt nicht abschließende Kriterien auf, die bei der Verhängung von Sanktionen zu berücksichtigen sind. Anknüpfend hieran legt § 18 DA-DG-E gestaffelte Höchstsanktionsbeträge fest, die von der zuständigen BNetZA verhängt werden können. Zwar sprach sich Bitkom,⁵¹ als Interessenvertretung von Unternehmen, im Vorhinein gegen konkretisierende nationale Regeln aus, jedoch ist es vor dem Hintergrund des Bestimmtheitsgebots des Art. 103 Abs. 2 GG geboten, konkretisierende Vorschriften zu Ordnungswidrigkeitentatbestand und Bußgeldhöhe zu erlassen,⁵² insbesondere wenn der europäische Gesetzgeber hierfür den entsprechenden Spielraum eröffnet hat. Demnach ist die Entscheidung für einen gestuften Ordnungswidrigkeit- und Bußgeldkatalog in § 18 DA-DG-

⁵⁰ Siehe insbesondere § 32g GWB.

⁵¹ Bitkom, Vorschläge zur nationalen Durchführung des Data Act, 2024, S. 8.

⁵² Vgl. BVerfGE 38, 348 (371); 159, 223 (292).

E grundsätzlich zu begrüßen.⁵³ Neben den gesetzten Obergrenzen in § 18 Abs. 5 DA-DG-E werden zur Bestimmung der konkret zu erteilenden Bußgelder neben den Kriterien des Art. 40 Abs. 3 DA auch die Kriterien des § 17 OWiG herangezogen.⁵⁴ Einzelne Wirkungen der mit Bußgeld belegten Tatbestände werden neben anderen Durchsetzungsmechanismen im Folgenden hinsichtlich ihrer Übereinstimmung mit dem Regelungszweck und -ziel des Data Acts erörtert.

3.2 Die Position des Nutzers im DA-DG

3.2.1 Ausgangspunkt im Data Act

Die Umsetzung des nutzerzentrierten Ansatzes des Data Acts hängt maßgeblich von der Durchsetzung der dort eingeführten Normen ab. Hier setzt das DA-DG an, das einen Rahmen für die nationale Umsetzung bietet.

Dem Nutzer werden im Data Act neue Rechte zuteil, wodurch seine Position gestärkt wird. So gewährt Art. 3 Abs. 1 DA ein Recht auf Datenzugang im Wege eines Access-by-Design. Subsidiär wird mit Art. 4 Abs. 1 DA ebenso ein Anspruch des Nutzers auf Herausgabe geschaffen.⁵⁵ Ihm gebührt auch die Entscheidung darüber, wie im Folgenden mit den Daten verfahren wird. So bedarf die Nutzung der Daten durch den Dateninhaber gem. Art. 4 Abs 13 und 14 DA eines Vertrages mit dem Nutzer.⁵⁶ Ebenso kann der Nutzer die Daten selbst mit einem Datenempfänger teilen oder den Dateninhaber anweisen, dies zu tun, Art. 5 Abs. 1 DA. Der Nutzer nimmt somit eine Schlüsselposition im Regelungsregime des Data Acts ein.⁵⁷ Das Erreichen der vom Data Act verfolgten Ziele hängt daher maßgeblich davon ab, dass Nutzer von den ihnen verliehenen Rechten Gebrauch machen können und zu diesem Zwecke eine effiziente Durchsetzung ermöglicht wird. Andernfalls ist zu befürchten, dass die praktische Bedeutung des Data Acts hinter den gestellten Erwartungen zurückbleibt. Hier besteht wiederum Spielraum für den nationalen Gesetzgeber.

3.2.2 Durchsetzungsmöglichkeiten

Wie bereits eingangs erwähnt, wird im Rahmen des Data Acts auf eine zweigleisige Durchsetzung, bestehend aus privatrechtlicher und behördlicher Durchsetzung, gesetzt.⁵⁸

⁵³ Im Ergebnis ähnlich: Drexel et al., Position Statement of the Max Planck Institute for Innovation and Competition of 25 May 2022 on the Commission's Proposal of 23 February 2022 for a Regulation on harmonised rules on fair access to and use of data (Data Act), Max Planck Institute for Innovation and Competition No. 22-05, 2022, Rn. 242.

⁵⁴ Gesetzesbegründung des Data Act-Durchführungsgesetzentwurfs (Bearbeitungsstand 5.2.2025), S. 44.

⁵⁵ Wiebe, GRUR 2023, 1569 (1570 f.).

⁵⁶ Zech, in: Sattler/Zech, (Hrsg.), The Data Act: First Assessments, 2024, S. 53-66 (60 f.).

⁵⁷ Vgl. Bomhard/Merkle, RDI 2022, 168 Rn. 53; Zech, in: Sattler/Zech, (Hrsg.), The Data Act: First Assessments, 2024, S. 53-66 (64).

⁵⁸ Metzger/Schweitzer, ZEuP 2023, 42 (78 f.); Wiebe spricht insoweit von einem „Auseinanderfallen der anwendbaren Regeln für öffentlich-rechtliche und privatrechtliche Durchsetzung“, Wiebe, GRUR 2023, 1569 (1569).

Der DA-DG-E konkretisiert mit Hinblick auf die privatrechtliche Durchsetzung in § 5 die Voraussetzungen zur Zulassung für in Deutschland niedergelassenen Streitbeilegungsstellen gem. Art. 10 Abs. 5 DA. Die Zulassung kann hierbei insbesondere mit Nebenbestimmungen versehen werden (§ 5 Abs. 1 DA-DG-E), befristet werden (§ 5 Abs. 2 DA-DG-E) und mit Blick auf das gem. Art. 10 Abs. 5 lit. b DA erforderliche Fachwissen beschränkt werden (§ 5 Abs. 3 DA-DG-E).

Die außergerichtliche Streitbeilegung berührt gem. Art. 10 Abs. 13 DA nicht das Recht der Parteien, wirksame Rechtsmittel bei einem Gericht eines Mitgliedstaats einzulegen. Eine genauere Ausgestaltung dieser Option der privatrechtlichen Durchsetzung wird jedoch nicht weiter im Referentenentwurf aufgegriffen und ausgestaltet.

Im Rahmen der öffentlich-rechtlichen Durchsetzung ist zunächst auf Art. 38 DA zu verweisen, der natürlichen und juristischen Personen die Möglichkeit eröffnet, bei der zuständigen Behörde eine Beschwerde einzureichen. Dies wird in § 7 Abs. 1 DA-DG-E aufgegriffen, der statuiert, dass die BNetzA die Einhaltung des DA aufgrund einer Beschwerde gem. Art. 38 DA oder von Amts wegen prüft und sie durchsetzt. Sie ist dabei gem. § 7 Abs. 1 S. 3 DA-DG-E nicht an etwaige Anträge von Beteiligten gebunden. Das Ermitteln der Behörde von Amts wegen und die daraus möglicherweise resultierende Bußgeldandrohung könnten dazu beitragen, dass die Position des Nutzers gestärkt wird. Insbesondere Szenarien mit mehreren Nutzern stellen den Data Act vor Herausforderungen.⁵⁹ Die Anreize für den Einzelnen, seine Rechte durchzusetzen, können hier gering sein. Vorzugswürdig ist es daher, dass ein System auszustalten, dessen Durchsetzung nicht auf den einzelnen Nutzer angewiesen ist, sondern auch auf Untersuchungen von Amts wegen setzt. Deutlich wird dies beispielhaft an Art. 11 Abs. 1 S. 2 DA, der festhält, dass Nutzer an der Ausübung ihrer im Data Act beschriebenen Rechte nicht durch technische Schutzmaßnahmen gehindert werden dürfen. Ein Verstoß hiergegen wird in §§ 18 Abs. 3 Nr. 29 DA-DG-E als Ordnungswidrigkeit sanktioniert. Die Option einer Untersuchung von Amts wegen ist an dieser Stelle geeignet, als Anreiz für den Dateninhaber zu dienen, von vornherein schonend mit technischen Schutzmaßnahmen umzugehen. Weiterhin statuiert § 11 DA-DG-E, dass Beteiligte, die im Rahmen des Verwaltungsverfahrens zur Vorlage von Informationen verpflichtet sind (zumeist Dateninhaber), jene Teile, die Geschäfts- und Betriebsgeheimnisse enthalten, kennzeichnen müssen. Geschieht dies nicht, wird von der Zustimmung zur Einsicht ausgegangen. Auch dies trägt zu einem, aus Nutzersicht, beschleunigten Verfahren bei. Behördliches Handeln von Amts wegen, das auch Bußgeldandrohungen und Verwaltungsvollstreckung als öffentlich-rechtliche Mittel zur Durchsetzung des Datenzugangs beinhaltet, kann hier teilweise Abhilfe schaffen.

3.2.3 Schwächung der Position des Nutzers

Die starke Position des Nutzers könnte jedoch durch die an ihn adressierten Sanktionsmöglichkeiten im DA-DG-E geschwächt sein. Hier ist zunächst §§ 18 Abs. 5 Nr. 2 iVm Abs. 3 Nr. 12 DA-DG-E zu nennen, demzufolge die Nutzung der Daten nach Erlangung entgegen Art. 4 Abs. 10 DA als Ordnungswidrigkeit geahndet wird. Hierbei handelt es sich um das Verbot,

⁵⁹ Antoine, CR 2024, 1(4).

anhand der Daten (entweder durch den Nutzer selbst oder durch einen Dritten) Konkurrenzprodukte zu entwickeln oder Einblicke in die wirtschaftliche Lage, die Vermögenswerte und die Produktionsmethoden des Herstellers oder gegebenenfalls des Dateninhabers zu erlangen. Ebenfalls als Ordnungswidrigkeit ist gem. §§ 18 Abs. 5 Nr. 3 iVm Abs. 3 Nr. 6 DA-DG-E die Offenlegung von Geschäftsgeheimnissen entgegen Art. 4 Abs. 6 S. 1 DA oder Art. 5 Abs. 9 S. 1 DA sanktioniert. Wenngleich diese Durchsetzungsregeln aufgrund der Bußgeldandrohung von bis zu 500.000 Euro den Nutzer erheblich treffen können, ist hierin doch keine Abweichung von den Zielsetzungen und Grundpfeilern des Data Acts zu sehen. Auch der Dateninhaber soll hier nicht schutzlos gestellt sein. Zu beachten ist zudem, dass demgegenüber auch eine Vielzahl von Bußgeldvorschriften stehen, die die Position des Nutzers stärken: § 18 Abs. 2 Nr. 3, Abs. 3 Nr. 1, 3-5, 23-31 und Abs. 4 DA-DG-E.

3.2.4 Ergebnis

Von der Durchsetzung der Rechte des Nutzers hängt der Erfolg des Data Acts maßgeblich ab. Fraglich ist dabei, ob eine zweigleisige Durchsetzung von Ansprüchen hierfür ein geeignetes Mittel darstellen kann. Ein solches Modell wurde bereits im Rahmen der DSGVO verfolgt, die teils unter Durchsetzungsdefiziten leidet.⁶⁰ Es liegt hier jedoch nicht an dem nationalen Gesetzgeber, diese grundsätzliche Entscheidung zu treffen, sondern es ist vielmehr seine Aufgabe, eine konsequente Lösung im vom Data Act vorgegebenen Rahmen zu gestalten. Dabei sollten einfache Verfahrensstrukturen bevorzugt werden und vom Data Act hervorgehobene Interessen berücksichtigt werden, was mit Bezug auf den Nutzer grundsätzlich geschehen. Es bietet sich hier vielmehr sogar die Chance an, aus einem DSGVO-ähnlichen Verfahren Synergieeffekte nutzbar zu machen und im Ergebnis die Durchsetzung beider Rechtsakte effektiver zu gestalten. Die Regelungen, die im DA-DG-E getroffen wurden, wahrt die Position des Nutzers aus dem Data Act.

3.3 Geschäftsgeheimnisse in der Durchsetzung des Data Acts

Der Schutz von Geschäftsgeheimnissen ist im Data Act in Art. 4 Abs. 6, 7 und 8 sowie Art. 5 Abs. 9, 10 und 11 verankert. Hiermit wird verhindert, dass Dateninhaber gezwungen werden, sensible Geschäftsgeheimnisse preiszugeben.⁶¹ Gleichzeitig soll das unzulässige Berufen auf den Geschäftsgeheimnisschutz auch nicht den Datenzugang verhindern. Es ist daher besonders wichtig, hier einen interessengerechten Ausgleich zu schaffen, der zum einen das Teilen von Daten ermöglicht, zum anderen jedoch auch Geschäftsgeheimnisse in einem angemessenen Rahmen berücksichtigt.

Im Referentenentwurf finden sich Verfahrens- und Durchsetzungsnormen, die mit Hinblick auf dieses Spannungsfeld zu betrachten sind.

⁶⁰ Bergt, in: Kühling/Buchner, DS-GVO BDSG, 4. Auflage 2024, Vor Art. 77–84 DSGVO Rn. 3; Art. 84 DSGVO Rn. 22; Lühmann/Schumacher/Stegemann, ZD 2023, 131.

⁶¹ Grützmacher, CR 2024, 281; Pauly/Wichert/Baumann, MMR 2024, 211.

3.3.1 Geheimnisschutz im Rahmen des Verfahrens

So ist der bereits erwähnte § 11 DA-DG-E zu beachten, der maßgeblich den Umgang mit Geschäftsgeheimnissen während des Verwaltungsverfahrens regelt. Im Ergebnis ist der Geschäftsgeheimnisinhaber durch diese Norm zu einem vergleichsweise schnellen (unverzüglich nach Vorlage) Handeln verpflichtet, sofern er sich auf den Geschäftsgeheimnisschutz berufen möchte. Dies befördert einen zügigen Verfahrensablauf, indem eine Verschleppung des Verfahrens mit Hinweis auf den Geschäftsgeheimnisschutz erschwert wird. Dieser Ablauf ist bereits aus § 216 TKG bekannt.⁶²

3.3.2 Geheimnisschutz in der Durchsetzung des Data Acts

Im Bereich der Durchsetzung sind vor allem die §§ 18 Abs. 3 Nr. 6-11 DA-DG-E bedeutend. Hier werden bestimmte Verstöße im Umgang mit Geschäftsgeheimnissen als Ordnungswidrigkeit sanktioniert. So wird zwar die unbefugte Offenlegung von Geschäftsgeheimnissen gem. § 18 Abs. 3 Nr. 6 DA-DG-E sanktioniert. Dies ist jedoch nicht konträr zu den Regelungszwecken und -zielen des Data Acts. Spannender ist in diesem Zusammenhang, dass auch eine unzureichende Mitwirkung des Dateninhabers in den §§ 18 Abs. 3 Nr. 7-11 adressiert wird. §§ 18 Abs. 3 Nr. 7 DA-DG-E sanktioniert beispielsweise bereits, dass entgegen Art. 4 Abs. 6 S. 2 DA oder Art. 5 Abs. 9 S.2 DA bei Erhalt der Daten eine Maßnahme nicht oder nicht richtig vereinbart wurde. Das Konzept des Geschäftsgeheimnisschutz im Data Act wird somit im behördlichen Verfahren derart ausgestaltet, dass ein Vorgehen gegen dessen Missbrauch mit dem Ziel, den Datenzugang zu verhindern, ermöglicht wird. Gleichzeitig wird die bestehende Schutzposition weiter abgesichert. An dieser Stelle ist auch darauf hinzuweisen, dass auch der Nutzer sich auf Geschäftsgeheimnisschutz berufen kann, sobald er Kontrolle über die Daten hat.⁶³ Verstärkt wird dies zudem dadurch, dass Widerspruch und Klage gem. § 16 DA-DG-E keine aufschiebende Wirkung entfalten. Ferner wird eine fehlende Schriftschrift bei Verweigerung der Herausgabe von Daten unter Berufung auf den Geschäftsgeheimnisschutz auch sanktioniert, vgl. § 18 Abs. 3 Nr. 9 u. 11 DA-DG-E i.V.m. Art. 4 Abs. 7 S. 3, Abs. 8 S. 3 und Art. 5 Abs. 10 S. 3, Abs. 11 S. 3. Mit der Schriftschrift wird den Behörden ein Ermittlungsansatz geliefert, gegebenenfalls auch von Amts wegen, hinsichtlich der Rechtmäßigkeit der Verweigerung zu ermitteln.⁶⁴ Die Bußgeldtatbestände des § 18 Abs. 3 Nr. 7-11 bieten in diesem Zusammenspiel mithin starke Anreize gegen Overclaiming von Geschäftsgeheimnisschutz. Im Ergebnis ist der Interessenausgleich im Referentenentwurf gegeben.

⁶² Zu der dortigen Interessenlage Attendorn, in: Geppert/Schütz, Beck'scher TKG-Kommentar, 5. Auflage 2023, § 216 TKG Rn. 3ff; VG Köln, MMR 2023, 798 (Rz. 37ff.).

⁶³ Schmidt-Kessel, MMR 2024, 75 (81 f.); Zech, in: Sattler/Zech, (Hrsg.), The Data Act: First Assessments, 2024, S. 53-66 (62f.).

⁶⁴ Schreiber/Pommerening/Schoel, Der neue Data Act, 2. Auflage 2024, § 9 Rn. 33.

4 Zusammenfassung

Der erste Teil dieser Stellungnahme beleuchtete Zuständigkeitsregeln des Referentenentwurfs kritisch. Der äußerst präsente Zusammenhang zwischen Data Act und DSGVO als zentrale materielle Problemstellung des Data Acts wirkt sich schon aufgrund der Vorgaben des europäischen Gesetzgebers stark auf die Entscheidung des nationalen Gesetzgebers zur effektiven Durchsetzung des Data Acts aus. Der Referentenentwurf berücksichtigt diese Ausgangslage, jedoch wirft eine Analyse des konkret vorgeschlagenen Modells in §§ 2 und 3 DA-DG-E mehrere Fragen auf und führt schließlich zu der Erwägung, ob eine alleinige Zuständigkeit der Datenschutzaufsichtsbehörden für die Durchsetzung des Data Acts bei der Betroffenheit persönlicher Daten zu einer effektiveren Rechtsdurchsetzung führen würde. Auch das Verhältnis zu anderen sektoralen Behörden nach § 4 DA-DG-E wird untersucht, wobei die konkrete Anordnung in Art. 37 Abs. 4 lit. a DA möglicherweise sektoralen Behörden mehr Befugnisse einräumen soll, als der Verfahrensschritt des Benehmens gemäß § 4 Abs. 2 DA-DG-E zuweisen würde.

Anschließend wird in dieser Stellungnahme das Durchsetzungsregime des Referentenentwurfs beleuchtet. Innerhalb des DA-DG-E wird insbesondere die öffentlich-rechtliche Durchsetzung näher ausgestaltet. Dieses profitiert von der klaren Möglichkeit, die Einhaltung des Data Acts gem. § 7 Abs. 1 DA-DG-E von Amts wegen zu ermitteln. Verbunden mit klaren Sanktionskatalogen in § 18 DA-DG-E ist hierin ein Schritt hin zu einer effektiven Durchsetzung auf nationaler Ebene zu sehen. Fraglich bleibt künftig, inwieweit die vom Data Act avisierte zweigleisige Durchsetzung auch klarerer Regeln auch für die privatrechtliche Durchsetzung bedarf.

Diese Stellungnahme weist abschließend auf das Bedürfnis von Kohärenz bei der Auslegung materieller Fragen hin. Schon der Data Act selbst betraut mehrere unterschiedliche Stellen mit der Durchsetzung und Konkretisierung der einzelnen Vorschriften. Der nationale Gesetzgeber ist an Vorgaben zur Zuständigkeit auf europäischer Ebene gebunden, vermag jedoch auf nationaler Ebene einer Fragmentierung entgegenzuwirken. Dies kann zum einen durch deutliche Zuständigkeitsvorschriften in Umsetzung des Art. 37 DA und zudem durch Kooperation im Rahmen des vom Data Act vorgesehenen zweigleisigen Durchsetzungsmechanismus geschehen. Für letzteres wird eine effektive Implementierung von § 14 und § 17 DA-DG-E von großer Bedeutung sein, um eine einheitliche Auslegung materiellen Rechts vor unterschiedlichen Stellen in teils stark übergreifenden Rechtsgebieten, zwischen Datenschutz, Geschäftsgeheimnisrecht, Wettbewerbsrecht und Vertragsrecht, zu garantieren.

¶ Impressum

Weizenbaum-Institut

Stellungnahme zum Referentenentwurf eines Gesetzes zur Durchführung der Verordnung (EU) 2023/2854 (Data Act-Durchführungsgesetz – DA-DG)

Weizenbaum Policy Paper # 13

März 2025

ISSN 2748-5587 \ DOI [10.34669/WI.WPP/13](https://doi.org/10.34669/WI.WPP/13)

Weizenbaum-Institut e.V.

Hardenbergstraße 32 \ 10623 Berlin \ Tel.: +49 30 700141-001
info@weizenbaum-institut.de \ www.weizenbaum-institut.de

KOORDINATION: Dr. Moritz Buchner

Dieses Paper ist unter der [Creative Commons Attribution 4.0](#) (CC BY 4.0) lizenziert.

GEFÖRDERT VOM