21. Wahlperiode

Deutscher Bundestag

Ausschuss für Digitales
und Staatsmodernisierung

Ausschussdrucksache 21(23)44
vom 22. Januar 2026

Schriftliche Stellungnahme

des Sachverständigen Prof. Dr. David Bomhard
Aitava Rechtsanwaltsgesellschaft mbH

Öffentliche Anhörung am 28. Januar 2026

zu dem Gesetzentwurf der Bundesregierung

Entwurf eines Gesetzes zur Durchführung der 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
BT-Drs. 21/2998

Prof. Dr. David Bomhard
Rechtsanwalt

Aitava Rechtsanwaltsgesellschaft mbH Walhallastr. 36 80639 München

Deutscher Bundestag
Ausschuss für Digitales und Staatsmodernisierung
Platz der Republik 1
11011 Berlin

München, den 22. Januar 2026

Stellungnahme zum Entwurf eines Gesetzes zur Durchführung der 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, BT-Drs. 21/2998 (nachfolgend „Data Act-Durchführungsgesetz-E“)

Ausgangslage: Der Data Act als Innovationsbremse

Aus Perspektive der Rechtsanwender ist der Data Act (Verordnung (EU) 2023/2854) ein besonders eindrucksvolles Beispiel dafür, wie die jüngste Regulierungswut der EU Innovation ausbremst und für den Wirtschaftsaufschwung dringend anderweitig benötigte Ressourcen bindet. Systematische Fehler des EU-Gesetzgebers, offensichtlich ignorierte Fragen und gravierende Unterschiede in den (gleichsam geltenden) Sprachfassungen machen die praktische Implementierung des Data Act zu einem Minenfeld für Rechtsanwender und zu einem Compliance-Albtraum für betroffene Unternehmen.

In der Praxis zeigt sich zunehmend, dass der Data Act kaum etwas mit Innovation zu tun hat – im Gegenteil: Die Umsetzung des Data Act hat bei vielen deutschen Unternehmen bereits enorme Aufwände verursacht und Kosten verschlungen. Statt neue, innovative Produkte zu entwickeln, beschäftigen sich große Teams technischer Fachkräften (insb. Softwareentwickler) monatelang mit ungeklärten rechtsdogmatischen Fragen und Formalia rund um Data Compliance. Woran liegt das? Der Data Act ist zwar seit 12.09.2025 umzusetzen, jedoch fehlen rechtsverbindliche Guidelines und belastbare Use Cases. Zudem gibt es bislang keine nationale Behörde, die die Umsetzung begleitet.

Das führt dazu, dass viele Unternehmen im Regen der Rechtsunsicherheit stehen gelassen werden und bei der Auslegung des Data Act jeweils „das Rad neu erfinden“ müssen.

Beispiel Datennutzungsverträge: Die mit dem Data Act einhergehende Ineffizienz zeigt sich etwa am Roll-out von Datennutzungsverträgen, die zwischen Dateninhabern und Nutzern abzuschließen sind. Gemäß Art. 4 Abs. 13 Data Act dürfen Dateninhaber seit dem 12.09.2025 ohne Weiteres verfügbare Daten, bei denen es sich um nicht-personenbezogene Daten handelt, nur noch auf der Grundlage eines Vertrags mit dem Nutzer nutzen. Warum damit nicht-personenbezogene Daten strenger geschützt werden als personenbezogene Daten, lässt sich Managern und Engineers kaum sinnvoll erklären. Oftmals ist in komplexen Sachverhalten (wie z.B. Car Sharing) bereits unklar, wer genau Nutzer im Sinne des Data Act sein soll. Das bedeutet für Dateninhaber, dass häufig schon nicht eindeutig ist, mit welchen genauen Vertragspartnern überhaupt entsprechende Datennutzungsverträge abgeschlossen werden müssen, was naturgemäß den lückenlosen Rollout solcher Verträge erheblich erschwert. In den „*Frequently Asked Questions*“ der EU-Kommission finden sich hierzu teilweise widersprüchliche Aussagen und viel zu triviale Beispiele („*Sara goes on holiday to Portugal for 2 weeks and needs to rent a car*.“)[1]. Zudem ist unklar, was inhaltlich genau in solchen Datennutzungsverträgen geregelt werden muss und darf. Allein die von der EU-Kommission vorgeschlagenen Model Contractual Terms (MCTs) für das Verhältnis Dateninhaber-Nutzer („H2U“) sehen in der Mustervorlage 28 Seiten plus 10 Vertragsanlagen (!) vor, weichen erheblich vom Wortlaut des Data Act ab und sind nach einhelliger Meinung der Rechtsanwender völlig praxisfern und unbrauchbar. Bemerkenswert ist, dass es derzeit – soweit ersichtlich – kein einziges Unternehmen gibt, das diese MCTs tatsächlich wie vorgesehen verwendet, der Verstoß gegen Art. 4 Abs. 13 Data Act aber in Deutschland mit einem Bußgeld von bis zu EUR 100.000 (siehe unten) sanktioniert werden soll.

Die Liste konkreter Praxisbeispiele und täglicher Anwendererfahrungen, anhand derer sich die Divergenz von Wunsch und Wirklichkeit illustrieren lässt, ließe sich beliebig fortsetzen. Dies würde jedoch den Rahmen dieser Stellungnahme sprengen.

<u>Data Act-Durchführungsgesetz: Chance zur Schaffung von Rechtssicherheit</u>

Vor diesem Hintergrund steht der deutsche Gesetzgeber vor der Herausforderung, die negativen Auswirkungen des Data Act auf die deutsche Wirtschaft kurzfristig abzufedern. Im Kern geht es darum, die Vorgaben des Data Act nicht zu überdehnen, sondern stattdessen den durch den Data Act bereits angerichteten und noch drohenden Schaden möglichst zu verringern. Freilich sind die rein nationalen Handlungsspielräume und Gestaltungsmöglichkeiten unionsrechtlich begrenzt, aber dennoch vorhanden. Diese Spielräume sollten nun vom Bundesgesetzgeber schnellstmöglich genutzt werden, um mehr Rechtssicherheit insb. für Unternehmen bei der Anwendung des Data Act sicherzustellen.

Im Ergebnis bietet der aktuelle Data Act-Durchführungsgesetz-E einen weitgehend passablen und handhabbaren Durchführungsrahmen. Zu begrüßen ist, dass sich der Bundesgesetzgeber einigen im bisherigen Gesetzgebungsverfahren vorgetragenen Belangen der Praxis angenommen hat und hierauf

[1] Frequently Asked Questions Data Act Version 1.3, Seite 14, abrufbar unter https://digital-strategy.ec.europa.eu/en/library/commission-publishes-frequently-asked-questions-about-data-act.

eingegangen ist. Die jüngsten Anpassungen im Data Act-Durchführungsgesetz-E stellen größtenteils eine relative Verbesserung im Vergleich zum ursprünglichen Gesetzentwurf dar. Gleichzeitig gibt es noch offene Punkte, die aus Praxissicht einer dringenden Klärung bedürfen.

Im Einzelnen

- **Bundesnetzagentur als zuständige Behörde**

  Aus Praxissicht ist es wichtig, schnellstmöglich eine Behörde zu schaffen, die über das notwendige technische, rechtliche und wirtschaftliche Verständnis verfügt und zudem in der Lage ist, den Data Act mit Augenmaß anzuwenden und auszulegen. Zu begrüßen ist daher, dass § 2 Abs. 1 Data Act-Durchführungsgesetz-E die Bundesnetzagentur als zuständige Behörde für die Anwendung und Durchsetzung des Data Act benennt. Die Bundesnetzagentur dürfte geeignet sein, weil sie (anders als etwa die Datenschutzbehörden in Deutschland) als wirtschaftsnah gilt und viel Erfahrung mit Marktaufsicht in technologiegetriebenen Bereichen hat. Dies lässt auf eine praxisnahe und innovationsfreundliche Umsetzung des Data Act mit Augenmaß hoffen.

- **Anordnung von Maßnahmen durch die Bundesnetzagentur**

  Nach dem Wortlaut von § 7 Abs. 3 Data Act-Durchführungsgesetz-E soll die Bundesnetzagentur pauschal „*die erforderlichen Maßnahmen anordnen*“ können, um die Einhaltung des Data Act sicherzustellen, wenn die natürliche oder juristische Person einem Abhilfeverlangen nicht innerhalb einer gesetzten Frist nachkommt. Es handelt sich hierbei um eine offene, unspezifische Generalklausel, die massive Rechtsunsicherheit und unvorhersehbare Eingriffstiefe erzeugt. Mangels gesetzlicher Leitplanken und Konturen können Unternehmen insofern nicht belastbar antizipieren, welche konkreten Maßnahmen auf sie zukommen. Zudem erhöht diese Regelung das Risiko einer uneinheitlichen Verwaltungspraxis sowie einer Überdehnung der Anforderungen des Data Act im Einzelfall. Besonders kritisch ist zudem, dass es sich um eine überschießende Umsetzung des Data Act handelt, der solch umfassende Befugnisse zur Anordnung sämtlicher Maßnahmen gar nicht verlangt. Im Ergebnis ist daher zu empfehlen, § 7 Abs. 3 Data Act-Durchführungsgesetz-E nachzuschärfen und durch einen Katalog konkreter, abschließender Handlungsbefugnisse der Bundesnetzagentur einzugrenzen.

- **Festsetzung von Zwangsgeldern**

  § 7 Abs. 6 Data Act-Durchführungsgesetz-E soll der Bundesnetzagentur die Durchsetzung von Anordnungen oder Untersagungen mit Zwangsgeldern in Höhe von bis zu EUR 500.000 ermöglichen. Eine Differenzierung nach Adressaten (z.B. nach Unternehmensgröße) ist nicht vorgesehen. Dass der Bundesgesetzgeber für die Festsetzung von Zwangsgeldern alle denkbaren Fälle „über einen Kamm schert“, zugleich aber derart hohe Zwangsgelder vorsieht und sogar einen Höchstbetrag ermöglicht, der 20 (!) mal so hoch ist wie der in § 11 Abs. 3 VwVG (dort sind es max. EUR 25.000), dürfte unverhältnismäßig sein und wird auch nicht vom Data Act so vorgegeben. Art. 40 Abs. 5 lit. d Data Act verlangt lediglich die

Möglichkeit zur „*Verhängung wirksamer, verhältnismäßiger und abschreckender finanzieller Sanktionen*“. Zwangsgelder in Höhe von EUR 500.000 schießen weit über das Ziel eines nur präventiven Beugemittels hinaus und können – je nach Adressat – vielmehr existenzbedrohend sein. Bedenklich ist zudem, dass § 7 Abs. 6 Data Act-Durchführungsgesetz-E im Übrigen keinerlei Abstufung oder Eskalationsmechanismen vorsieht, zumal Unternehmen im Worst Case eine Doppel- oder Dreifachbelastung zudem mit Bußgeldern sowie zivilrechtlichen Klagen (siehe unten) droht. Der Bundesnetzagentur wird hier ein unnötig großer Ermessensspielraum eingeräumt. Dass derart hohe Zwangsgelder ausgerechnet zur Durchsetzung der unspezifischen Generalklausel in § 7 Abs. 3 Data Act-Durchführungsgesetz-E (siehe oben) dienen, wiegt aus Praxissicht doppelt schwer. Im Ergebnis ist daher zu empfehlen, den Maximalbetrag möglicher Zwangsgelder – in Orientierung an § 11 Abs. 3 VwVG – erheblich zu reduzieren und zudem sachgerechte Abstufungen vorzusehen.

- **Bußgeldvorschriften**

  § 15 Abs. 2 Data Act-Durchführungsgesetz-E sieht einen extensiven Ordnungswidrigkeitenkatalog vor, der Verstöße gegen nahezu alle Pflichten des Data Act mit Bußgeldern sanktioniert. Dies ist aus Praxissicht besonders kritisch, weil darunter auch Sanktionen für zahlreiche Pflichten geregelt werden, die aktuell auf Tatbestandsebene unklar sind und sich – mangels belastbarer Behördenverlautbarungen oder Rechtsprechung – nicht rechtssicher umsetzen lassen. Dies gilt unter anderem für Art. 4 Abs. 13 Data Act, der einen Abschluss von Datennutzungsverträgen mit sog. Nutzern verlangt (siehe oben) und für dessen Verstoß § 15 Abs. 2 Nr. 10, Abs. 4 Data Act-Durchführungsgesetz-E derzeit eine Geldbuße von bis zu EUR 100.000 vorsieht.

  Zumindest der Wortlaut in Art. 40 Abs. 1 Data Act (*„erlassen Vorschriften über Sanktionen, die bei Verstößen*“ – es heißt gerade nicht: „bei *allen* Verstößen“) kann so verstanden werden, dass die Mitgliedsstaaten nicht verpflichtet sind, Bußgelder für sämtliche Tatbestände des Data Act einzuführen. Im Ergebnis ist daher zu empfehlen, den Katalog in § 15 Abs. 2 Data Act-Durchführungsgesetz-E auf ausgewählte Pflichten, die für die Schutzzwecke des Data Act essenziell und zugleich im Detail transparent und inhaltlich klar sind, zu begrenzen. Im Übrigen sollten im Data Act-Durchführungsgesetz-E möglichst keine weiteren Bußgelder vorgesehen werden, zumal bei vielen Verstößen ohnehin eine parallele zivilrechtliche Rechtsdurchsetzung droht (siehe nächster Punkt). Mit Blick auf § 19 OWiG sollte noch klargestellt werden, dass ein Bußgeld nicht pro Nutzer bzw. Vertrag anfällt, sondern insgesamt nur einmal.

- **Zivilrechtliche Verankerung als offene Flanke**

  Der Data Act fußt auf vertraglichen und sonstigen zivilrechtlichen Rechtsbeziehungen zwischen den einzelnen Akteuren und muss daher in weiten Teilen zivilrechtlich „gedacht“ und umgesetzt werden. Viele wichtige Frage zur genauen zivilrechtlichen Durchsetzbarkeit werden vom Data Act allerdings nicht einmal im Ansatz beantwortet, insb. wenn bzw. weil es sich um nationales Privatrecht handelt. Soweit Pflichten zivilrechtlicher Natur sind, drohen u.a. Schadensersatz- und Unterlassungsansprüche im Verletzungsfall. Bemerkenswert ist, dass die privatrechtliche Bedeutung des Data Act – und damit die Möglichkeit bzw. Gefahr einer privaten Rechtedurchsetzung (private enforcement) weitgehend ungeklärt ist. Dies betrifft nicht abschließend insb. die privatrechtliche Dimension von Art. 3 Abs. 1 (access by design),

Art. 4 Abs. 1, Art. 5 Abs. 1 (Vereinbarungen im Zuge der Datenbereitstellung), Art. 4 Abs. 13 (Datennutzungsverträge), Art. 13 (Klauselkontrolle für spezielle B2B-Datenverträge) und Art. 25 Data Act (Mindestanforderungen für Cloudverträge).

Auch der aktuelle Data Act-Durchführungsgesetz-E klammert die zivilrechtliche Verankerung des Data Act aus und konzentriert sich auf die öffentlich-rechtliche Durchsetzung (public enforcement). Damit versäumt der Bundesgesetzgeber eine wichtige Chance, seine legislativen Gestaltungsmöglichkeiten zu nutzen und mehr Klarheit und Planbarkeit für das Daten-Zivilrecht zu schaffen, auf die Rechtsanwender (etwa bei der Vertragsgestaltung) dringend angewiesen sind. Aus Praxissicht wäre es sehr wünschenswert und daher zu empfehlen, zumindest auf nationaler Ebene ein Mindestmaß an Rechtssicherheit zu den konkreten zivilrechtlichen Auswirkungen des Data Act herzustellen, soweit dies möglich ist und nicht einheitlich auf EU-Ebene geschieht. Für viele Rechtsanwender stellt die Schaffung von zivilrechtlicher Klarheit ein „Must-have“ und nicht bloß ein „Nice-to-have“ dar. Der Data Act-Durchführungsgesetz-E würde einen optimalen Rahmen für die Verankerung mit nationalem Zivilrecht bieten und sollte daher entsprechend genutzt und nachgeschärft werden.

gez.
Prof. Dr. David Bomhard
Rechtsanwalt