

KOHÄRENTE UND EFFEKTIVE AUFSICHT ÜBER DEN DATA ACT SICHERSTELLEN

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

13. März 2025

Impressum

**Bundesverband der Verbraucherzentralen und Verbraucherverbände –
Verbraucherzentrale Bundesverband e.V.**

Team Digitales und Medien
digitales@vzbv.de

Rudi-Dutschke-Straße 17
10969 Berlin

Der Verbraucherzentrale Bundesverband e.V. ist im Deutschen Lobbyregister und im europäischen Transparenzregister registriert. Sie erreichen die entsprechenden Einträge [hier](#) und [hier](#).

INHALT

VERBRAUCHERRELEVANZ	3
ZUSAMMENFASSUNG	4
I. EINLEITUNG	5
II. GRUNDSÄTZLICHE ANMERKUNGEN	5
III. ANMERKUNGEN IM EINZELNEN	5
1. Zentrale Anlaufstelle	5
2. Umgang mit Verbraucherbeschwerden	6
3. Zusammenarbeit der Behörden	6
4. Zuständige Datenschutzaufsichtsbehörde und Zusammenarbeit mit der Bundesnetzagentur	7

VERBRAUCHERRELEVANZ

Der Data Act soll den Zugang zu und die Kontrolle der Verbraucher:innen über von ihnen generierte Daten stärken. Beispielsweise erhalten Nutzer:innen von vernetzten Haushaltsgeräten, Smartwatches oder vernetzten Autos mehr Rechte darüber, welche Unternehmen auf ihre Nutzungsdaten zugreifen dürfen und wie diese weiterverwendet werden können. Dies betrifft insbesondere vernetzte Produkte und digitale Dienstleistungen, bei denen bislang häufig Unklarheit darüber herrscht, wem die erzeugten Daten gehören und unter welchen Bedingungen sie genutzt werden dürfen. Ein zentrales Anliegen des Gesetzes ist es, Verbraucher:innen mehr Transparenz und effektive Durchsetzungsmechanismen für ihre Rechte an Daten zu bieten. Eine wirksame nationale Aufsichtsstruktur ist dabei von entscheidender Bedeutung, um eine konsistente Durchsetzung der Verbraucherrechte zu gewährleisten, Missbrauch effektiv zu verhindern und gleichzeitig den Schutz personenbezogener Daten aufrechtzuerhalten.

ZUSAMMENFASSUNG

- ❖ Es sollte klargestellt werden, dass die Bundesnetzagentur während der gesamten Dauer eines Beschwerdeverfahrens als Ansprechpartnerin der Beschwerdeführer:innen fungiert.
- ❖ Die Bundesnetzagentur sollte ein Beschwerdemanagementsystem einrichten müssen, das für Verbraucher:innen nicht nur leicht zugänglich und benutzerfreundlich ist, sondern auch eine transparente Nachverfolgung des Verfahrensverlaufs ermöglicht.
- ❖ Die Ziele, die mit der Benennung der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) als allein zuständige Datenschutzaufsichtsbehörde im Rahmen des Data Act (DA) verfolgt werden – insbesondere eine effizientere Aufsicht und kürzere Verfahren – werden mit dem Vorschlag voraussichtlich nicht erreicht werden können. Insbesondere befürchtet der Verbraucherzentrale Bundesverband (vzbv) Schwierigkeiten hinsichtlich der Abgrenzung zu den Befugnissen und Tätigkeiten der Landesdatenschutzbehörden. Vielmehr droht die vorgeschlagene Zuständigkeitsregelung die Verfahren zusätzlich zu verkomplizieren und zu verlängern.
- ❖ Falls der Gesetzgeber dennoch beschließt, die Benennung der BfDI als allein zuständige Datenschutzaufsichtsbehörde weiterzuverfolgen, muss im Vorfeld ein Mechanismus geschaffen werden, um die mit dem Vorschlag verbundenen Probleme zu lösen. Es wäre unangemessen, die Verantwortung für ein effektives und verbraucherfreundliches Verfahren allein den Aufsichtsbehörden zu überlassen. Für diese dürfte es aufgrund der Komplexität und der Abgrenzungsprobleme äußerst herausfordernd sein, diese Aufgabe unter Wahrung ihrer Unabhängigkeit sachgerecht zu erfüllen.

I. EINLEITUNG

Der Referentenentwurf des Bundesministeriums für Wirtschaft und Klimaschutz und des Bundesministeriums für Digitales und Verkehr eines Data Act-Durchführungsgesetzes (DA-DG) verfolgt das Ziel, die europäische Verordnung über harmonisierte Vorschriften für einen fairen Datenzugang und eine faire Datennutzung (Data Act, Verordnung (EU) 2023/2854) in Deutschland umzusetzen. Dabei steht insbesondere die Benennung einer zentralen Aufsichtsbehörde, ihre Zusammenarbeit mit anderen Institutionen sowie die Durchsetzung der neuen Vorschriften im Vordergrund.

Eine klare, kohärente und effiziente Behördenstruktur ist essenziell, um Doppelstrukturen, Kompetenzkonflikte und ineffiziente Rechtsdurchsetzung zu vermeiden. Der vzbv bedankt sich daher beim Bundesministerium für Wirtschaft und Klimaschutz (BMWK) und beim Bundesministerium für Digitales und Verkehr (BMDV) für die Gelegenheit, zum Referentenentwurf des DA-DG Stellung nehmen zu können.

II. GRUNDSÄTZLICHE ANMERKUNGEN

Die zunehmende Regulierung des digitalen Raums durch unterschiedliche europäische Rechtsakte – neben dem DA insbesondere der Digital Services Act (DSA), der Artificial Intelligence Act (AIA) und der Cyber Resilience Act (CRA) – stellt erhebliche Herausforderungen an die nationale Umsetzung und Aufsicht.

Vor diesem Hintergrund ist der Ansatz des DA-DG grundsätzlich zu begrüßen, eine klare Zuständigkeit der Bundesnetzagentur (BNetzA) für die Durchsetzung des Data Act festzulegen. Allerdings bleiben zentrale Fragen nach der langfristigen strategischen Organisation der Digitalaufsicht in Deutschland sowie nach der effektiven Abstimmung zwischen Markt-, Datenschutz- und Verbraucherschutzbehörden ungelöst. Hier bedarf es einer weitergehenden strukturellen Debatte über eine einheitliche Regulierungssystematik und koordinierte Durchsetzungsmechanismen.

Problematisch vor diesem Hintergrund ist insbesondere, dass – abweichend von der föderalen Aufsichtsstruktur in Deutschland – im Entwurf die BfDI als alleinige zuständige Behörde für Fragen des Datenschutzes im Kontext des Data Act benannt wird. Dies könnte zu fragmentierten Zuständigkeiten und ineffizienter Rechtsdurchsetzung führen, was dem Ziel einer kohärenten und effektiven Aufsichtsstruktur widerspricht.

III. ANMERKUNGEN IM EINZELNEN

1. ZENTRALE ANLAUFSTELLE

Die BNetzA wird in § 2 des Entwurfs als zentrale Behörde für die Anwendung und Durchsetzung des Data Act benannt. Neben der Durchsetzung der neuen Vorgaben sollen auch Informationsmaßnahmen sowie die Bearbeitung von Beschwerden zentral bei der BNetzA angesiedelt werden.

Dieser Vorschlag wird vom vzbv ausdrücklich begrüßt. Verbraucher:innen und Unternehmen benötigen eine zentrale Anlaufstelle, die je nach konkretem Anliegen als beratende Stelle, Durchsetzungsinstanz oder koordinierende Behörde fungiert. Dies trägt dazu bei, dass Verbraucher:innen gezielt Unterstützung und rechtliche Durchsetzung aus einer Hand erhalten. Besonders für Verbraucher:innen, die sich gegen unzulässige Datenpraktiken wehren möchten, ist es entscheidend, dass eine Behörde schnell und unbürokratisch Abhilfe schafft.

Die Komplexität digitaler Geschäftsmodelle und datengetriebener Märkte erfordert interdisziplinäre Expertise, insbesondere im Zusammenspiel mit Datenschutz-, Kartell- und Verbraucherschutzrecht.

Daher muss sichergestellt werden, dass die BNetzA auch tatsächlich über die notwendigen Ressourcen und Fachkompetenzen verfügt, um diese Rolle effektiv auszufüllen. Dazu gehören spezialisiertes Personal mit Fachkenntnissen im Datenrecht, technische Infrastruktur zur Analyse und Überprüfung datenbasierter Geschäftsmodelle sowie ausreichende finanzielle Mittel für Schulungen und den Ausbau digitaler Durchsetzungsmechanismen.

2. UMGANG MIT VERBRAUCHERBESCHWERDEN

Nach § 7 des Entwurfs übernimmt die BNetzA eine zentrale Rolle bei der Bearbeitung und Koordinierung von Beschwerden. Die vorgeschlagenen Mechanismen, insbesondere die zeitnahe Information der Beschwerdeführer:innen über den Fortgang des Verfahrens, sind zu begrüßen. Dies gilt insbesondere in Fällen, in denen eine Beschwerde an eine sektorale Aufsichtsbehörde oder die Datenschutzaufsicht weitergeleitet werden muss.

Ein koordinierter und effizienter Umgang mit Beschwerden ist entscheidend, um das Vertrauen in die Durchsetzung der neuen Regelungen zu stärken. Um die Effektivität des Beschwerdesystems zu gewährleisten, sollte klargestellt werden, dass die BNetzA während des gesamten Beschwerdeverfahrens als Ansprechpartnerin der Beschwerdeführer:innen fungiert, insbesondere im Fall einer Weiterleitung an eine andere Behörde. Es muss sichergestellt sein, dass Verbraucher:innen nicht zwischen verschiedenen Instanzen hin- und verwiesen werden.

Der vzbv weist zudem darauf hin, dass das Beschwerdeverfahren für Betroffene so niedrigschwellig und zugänglich wie möglich gestaltet werden muss. Zur Erfüllung ihrer Aufgaben als zentrale Beschwerdestelle sollte die BNetzA daher ein Beschwerdemanagementsystem einrichten, das nicht nur leicht zugänglich und benutzerfreundlich ist, sondern auch eine transparente Nachverfolgung des Verfahrensverlaufs ermöglicht. Dies kann etwa durch digitale Meldewege, klare Bearbeitungsfristen und eine effektive Schnittstelle zu anderen zuständigen Behörden sichergestellt werden.

Es sollte klargestellt werden, dass die BNetzA während des gesamten Beschwerdeverfahrens als Ansprechpartnerin der Beschwerdeführer:innen fungiert. Sie sollte außerdem ein Beschwerdemanagementsystem einrichten, das nicht nur leicht zugänglich und benutzerfreundlich ist, sondern auch eine transparente Nachverfolgung des Verfahrensverlaufs ermöglicht.

3. ZUSAMMENARBEIT DER BEHÖRDEN

Ähnlich wie § 19 Digitale-Dienste-Gesetz sieht § 4 des Entwurfs vor, dass die BNetzA mit anderen Aufsichtsbehörden kooperativ und vertrauensvoll zusammenarbeitet und

relevante Informationen austauscht, insbesondere mit dem Bundeskartellamt, dem Bundesamt für Sicherheit in der Informationstechnik (BSI) und dem Kraftfahrt-Bundesamt (KBA). Diese Behörden sollen insbesondere bei sektoralen Fragen der Datenaufsicht beteiligt und ihre Stellungnahmen berücksichtigt werden. Abschließende Entscheidungen der BNetzA sollen im Benehmen mit den jeweils betroffenen Bundesbehörden erfolgen.

Der vzbv begrüßt den Regelungsvorschlag, da eine frühzeitige und reibungslose Zusammenarbeit essenziell ist, um effiziente Entscheidungsprozesse und eine kohärente Aufsichtspraxis zu gewährleisten.

Um mögliche Friktionen von Beginn an zu vermeiden, sollten jedoch verbindliche Koordinierungsmechanismen sowie klare Verfahrensregeln etabliert werden. Dazu gehört insbesondere eine detaillierte Festlegung von Zuständigkeiten und Kommunikationswegen zwischen den beteiligten Behörden, wie etwa ein Fallmanagement-System. Ohne eine solche Struktur besteht die Gefahr ineffizienter Doppelprüfungen, Kompetenzüberschneidungen und unklarer Verantwortlichkeiten, die den effektiven Vollzug der Vorschriften erschweren könnten.

4. ZUSTÄNDIGE DATENSCHUTZAUF SICHTSBEHÖRDE UND ZUSAMMENARBEIT MIT DER BUNDESNETZAGENTUR

In § 3 des Entwurfs wird die BfDI als alleinig zuständige Behörde für Fragen des Datenschutzes im Kontext des Data Act benannt. § 3 legt außerdem fest, dass die BNetzA und BfDI im Rahmen der jeweiligen Zuständigkeiten kooperativ und vertrauensvoll zusammenarbeiten. Die BfDI unterstützt die BNetzA in allen Fragen des Datenschutzrechts (insbesondere schon bei der initialen Prüfung, ob Datenschutzrecht betroffen ist oder nicht) und wirkt stetig auf eine rasche und kohärente Entscheidungsfindung hin. Einzelheiten der Zusammenarbeit zwischen BNetzA und BfDI können bei Bedarf in Verwaltungsvereinbarungen geregelt werden.

Mit der Übertragung dieser Zuständigkeit auf die BfDI erhofft sich der Entwurf, dass zusätzliche Koordinierungs- und Abstimmungsprozesse vermieden, die Dauer der Beschwerdeverfahren erheblich verkürzt und einheitliche Entscheidungen sichergestellt werden. Insbesondere würde sichergestellt, dass eine in Beschwerdefragen abweichende Auslegung von datenschutzrechtlichen Anforderungen oder divergierende Vollzugspraxis aufgrund der Zuständigkeit von 18 unterschiedlichen Datenschutzaufsichtsbehörden auf Bundes-/Landesebene nicht zu einer zusätzlichen Belastung deutscher Unternehmen im Bereich der Datenschutz-Compliance führt. Dies ist im Kern nachvollziehbar, wirft jedoch eine Reihe von Problemen auf:

Zum einen ergeben sich vor dem Hintergrund der föderalen Ordnung der Bundesrepublik verfassungsrechtliche Fragen. Eine Übertragung der Aufsicht auf eine zentrale Bundesbehörde stellt eine wesentliche Kompetenzverschiebung dar. Dennoch könnte man aus Sicht des vzbv durchaus an geeigneter Stelle darüber diskutieren, ob und in welchem Umfang eine stärkere Zentralisierung der Datenschutzaufsicht als sinnvoll erachtet werden kann. Allerdings wäre nach Ansicht des vzbv dafür eine breite gesellschaftliche Debatte wünschenswert, etwa im Rahmen einer möglichen Anpassung des Bundesdatenschutzgesetzes. Eine überstürzte (Teil)Zentralisierung wäre nicht nur aus demokratischen und verfassungsrechtlichen Gesichtspunkten fragwürdig, vielmehr besteht auch die Gefahr ungewollter Nebeneffekte. Diese Nebeneffekte könnten nicht nur die Durchsetzung des Datenschutzes erschweren, sondern auch zu unerwünschten

Belastungen für Wirtschaft und Verbraucher:innen führen, was nicht nur den Datenschutz in der Sache, sondern auch in der öffentlichen Wahrnehmung weiter beschädigen könnte.

Solche Nebeneffekte sind auch bei der Zuweisung der Datenschutzaufsicht auf die BfDI entsprechend des vorliegenden Entwurfs zu erwarten. Insbesondere befürchtet der vzbv Schwierigkeiten hinsichtlich der Abgrenzung zu den Befugnissen und Tätigkeiten der Landesdatenschutzbehörden (LDA). Vor allem ist völlig unklar, wie „Datenverarbeitungen im Kontext des Data Act“ von „Datenverarbeitungen nach DSGVO“ abgegrenzt werden könnten. Schon innerhalb des Data Act ist die Abgrenzung zwischen datenschutzrechtlichen und allgemeinen Datenverarbeitungsvorschriften äußerst schwierig. Durch die vorgeschlagene Regelung wird jedoch eine weitere Ebene eingeführt, so dass nun nicht nur zwischen verschiedenen Regelwerken, sondern auch zwischen unterschiedlichen, unabhängigen Behörden die schwierige Abgrenzung erfolgen muss.

Statt einer Verkürzung von Beschwerdeverfahren und einer Vereinheitlichung der Aufsichtspraxis befürchtet der vzbv insbesondere, dass künftig mehrere unabhängige Datenschutzbehörden für im Kern identische Fälle zuständig sein könnten. Besonders für betroffene Verbraucher:innen und Unternehmen dürfte diese Trennung vollkommen unverständlich sein, da sie mit längeren Bearbeitungszeiten, widersprüchlichen Zuständigkeiten und möglicher Rechtsunsicherheit konfrontiert werden könnten. Dies könnte nicht nur die Durchsetzung von Datenschutzrechten erschweren, sondern auch das Vertrauen in die Wirksamkeit der behördlichen Aufsicht beeinträchtigen. Ein denkbare Beispiel:

Ein Medienbericht deckt ein schwerwiegendes Datenleck bei einer bundesweit tätigen Kfz-Werkstattkette auf. Laut den Berichten wurden personenbezogene Daten zahlreicher Kund:innen – darunter Namen, Adressen, Kfz-Kennzeichen, Werkstattbesuche, Diagnosedaten und Standortdaten – durch eine Sicherheitslücke ungeschützt ins Internet gestellt.

Kunde A bringt sein altes Auto bereits seit Jahren in die Kfz-Werkstatt. Er erfährt über die Presse von dem Vorfall. Die Kfz-Werkstatt bestätigt ihm auf Anfrage, dass auch sein Datensatz betroffen ist. Er reicht daraufhin Beschwerde bei der zuständigen LDA ein und argumentiert, dass seine personenbezogenen Daten durch unzureichende Sicherheitsmaßnahmen offengelegt wurden.

Kunde B vermutet hingegen, dass die Kfz-Werkstatt seine Daten im Rahmen einer Datenübermittlung nach dem Data Act erhalten hat. Er hatte seinen Fahrzeughersteller beauftragt, bestimmte Diagnosedaten sowie Standortdaten an die Werkstatt zu übermitteln. Er befürchtet nun, dass seine Daten während dieser Übermittlung kompromittiert wurden. Daher wendet er sich an die BNetzA, die daraufhin die BfDI einschaltet.

Auch Kunde C hat im Rahmen des Data Act von seinem Fahrzeughersteller Daten an die Kfz-Werkstatt übermitteln lassen. Als er aufgrund des Datenlecks eine Auskunft von der Werkstatt einfordert, stellt er fest, dass sein Datensatz betroffen ist und Standortdaten enthält, die vom Fahrzeughersteller übermittelt wurden – obwohl er einer Übertragung dieser Daten nie zugestimmt hatte. Aufgrund der unzulässigen Datenweitergabe sowie der Sicherheitslücke wendet er sich an die LDA und fordert eine Untersuchung.

Dieses Beispiel illustriert die Herausforderungen bei der unklaren Zuständigkeitsverteilung in der Praxis:

- ❖ Fall A: Hier ist die Zuständigkeit der LDA weitgehend unstrittig, da kein Bezug zum Data Act besteht. Die LDA wird hier möglicherweise gar nicht abschätzen können, dass das Datenleck für manche Betroffene einen Bezug zum Data Act haben könnte (wie in Fall B und C).
- ❖ Fall B: Die Zuständigkeit ist unklar:
 - Falls die Daten bei der Übermittlung zwischen Fahrzeughersteller und Kfz-Werkstatt offengelegt wurden, wäre die BfDI zuständig, da dies im Rahmen des Data Act erfolgte?
 - Falls die Sicherheitslücke in der Kfz-Werkstatt aufgetreten ist, wäre dann ebenfalls die BfDI zuständig, weil die Daten im Kontext des Data Act übermittelt wurden?
 - Dies würde jedoch bedeuten, dass in einem identischen Vorfall (Sicherheitslücke bei der Kfz-Werkstatt) in Fall A die LDA, in Fall B die BfDI zuständig wäre.
 - Oder wäre hier doch die LDA zuständig, da die Verarbeitung letztlich in der Sphäre der Kfz-Werkstatt stattfand und nach DSGVO zu bewerten ist?
- ❖ Fall C:
 - Hinsichtlich der unzulässigen Übertragung von Standortdaten an die Kfz-Werkstatt dürfte die BfDI zuständig sein, da es sich um eine Verarbeitung im Kontext des Data Act handelt.
 - Bezüglich der Sicherheitslücke gelten dieselben Überlegungen wie in Fall B.

Das Ergebnis zeigt, dass – abhängig von der Einordnung der Datenverarbeitung in der Kfz-Werkstatt – entweder in Fall B oder in Fall C sowohl die LDA als auch die BfDI zuständig sein könnten.

Da es in der Praxis kaum möglich sein dürfte, in jedem Fall klar zwischen „Datenverarbeitungen im Kontext des Data Act“ und „Datenverarbeitungen nach DSGVO“ zu unterscheiden, könnten vergleichbare Probleme auch dann auftreten, wenn eine Aufsichtsbehörde ein Unternehmen zu seinen Datenverarbeitungsprozessen berät, während eine andere unabhängige Behörde diese Prozesse im Rahmen ihrer Zuständigkeit beanstandet.

Aus Sicht des vzbv können daher die mit dem Regelungsvorschlag verfolgten Ziele – insbesondere eine effizientere Aufsicht und verkürzte Verfahren – kaum erreicht werden. Vielmehr dürfte die vorgeschlagene Zuständigkeitsverteilung zu einem erhöhten Abstimmungsbedarf zwischen den beteiligten Behörden, einer geringeren Einheitlichkeit in der Rechtsdurchsetzung sowie zu längeren Verfahren führen. Dies würde die Rechtsunsicherheit sowohl für Unternehmen als auch für betroffene Verbraucher:innen erhöhen und eine klare und verlässliche Durchsetzung des Datenschutzrechts erschweren.

Falls der Gesetzgeber dennoch beschließt, den kritisierten Vorschlag weiterzuverfolgen, muss im Vorfeld ein Mechanismus geschaffen werden, um die mit dem Vorschlag verbundenen Probleme zu lösen. Es wäre unangemessen, die Verantwortung für ein effektives und verbraucherfreundliches Verfahren allein den Aufsichtsbehörden zu überlassen. Für diese dürfte es aufgrund der Komplexität und der Abgrenzungsprobleme äußerst herausfordernd sein, diese Aufgabe unter Wahrung ihrer Unabhängigkeit sachgerecht zu erfüllen.