Stellungnahme
der unabhängigen Datenschutzaufsichtsbehörden der Länder
vom 13. März 2025

---

zu Entwurf eines Gesetzes zur Durchführung der Verordnung (EU) 2023/2854 (Data Act-Durchführungsgesetz – DA-DG) (Stand: 5. Februar 2025)

Ziel des Data Act ist es, die Verwendung von Daten, die bei der Nutzung von vernetzten Produkten und verbunden Diensten (z. B. Geräte in der Industrie, in der Verwaltung und in privaten Haushalten mit Verbindungen zum Internet) entstehen, zu verbessern und die sie betreffenden Regelungen unionsweit zu vereinheitlichen. Nutzerinnen und Nutzer sollen darüber entscheiden können, ob sie diese Daten erhalten oder ob sie an Dritte (z. B. Reparaturbetriebe) weitergegeben werden. Auch öffentliche Stellen haben einen Anspruch, dass ihnen in Notfällen die Daten aus der Gerätenutzung übermittelt werden.

Sind in den nutzungsgenerierten Daten auch personenbezogene Daten enthalten, richtet sich deren Verarbeitung nach der Datenschutzgrundverordnung (DSGVO). Im Fall eines Widerspruchs zwischen Data Act und DSGVO geht nach Art. 1 Abs. 5 S. 3 Data Act die DSGVO vor.

Nach Art. 37 Abs. 1 Data Act benennen die Mitgliedstaaten eine oder mehrere zuständige Behörden, die für die Anwendung und Durchsetzung des Data Act verantwortlich sind. Nach § 2 des Referentenentwurfs soll diese Zuständigkeit bei der Bundesnetzagentur (BNetzA) liegen.

In Art. 37 Abs. 3 S. 1 Data Act ist ferner geregelt, dass die für die Überwachung der Anwendung der DSGVO zuständigen Aufsichtsbehörden bezüglich des Schutzes personenbezogener Daten auch für die Überwachung der Anwendung der vorliegenden Verordnung zuständig sind. Die Aufsicht über die Verarbeitung personenbezogener Daten durch Verantwortliche aus dem nicht-öffentlichen Bereich ist gem. § 40 Abs. 1 Bundesdatenschutzgesetz (BDSG) i. V. m. dem Landesdatenschutzgesetz der jeweiligen Landesdatenschutzbehörde übertragen. Zudem regeln die Landesdatenschutzgesetze die Zuständigkeit der Landesdatenschutzbehörden für die öffentlichen Stellen des jeweiligen Landes. Im Gegensatz dazu soll nach § 3 des Referentenentwurfs die Zuständigkeit für die Überwachung der Anwendung der DSGVO im Rahmen des Data Act auf die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) übertragen werden.

Der Regelungsentwurf stößt auf mehrfache Bedenken:

1. Der Referentenentwurf verstößt gegen Unionsrecht.

a) Art. 37 Abs. 3 S. 1 Data Act bestimmt, dass die für die Überwachung der Anwendung der DSGVO

„zuständigen Aufsichtsbehörden (…) bezüglich des Schutzes personenbezogener Daten ***auch*** *für die Überwachung der Anwendung der vorliegenden Verordnung zuständig*“ sind.

Nach dem klaren Wortlaut der Verordnung will der europäische Gesetzgeber durch einen Gleichlauf der Zuständigkeiten nach Data Act und DSGVO eine Zuständigkeitszersplitterung vermeiden und knüpft daher ausdrücklich an die bestehende Zuständigkeitsordnung nach der DSGVO an. Danach wären die Landesdatenschutzbehörden im Rahmen ihres bereits zugewiesenen Aufgabenspektrums zur Kontrolle des Schutzes personenbezogener Daten gemäß DSGVO auch im Rahmen des Data Act die zuständigen Aufsichtsbehörden.

b) Die klare und abschließende Regelung in Art. 37 Abs. 3 S. 1 Data Act bietet keinen Anhaltspunkt für eine Befugnis der Mitgliedstaaten, abweichende Regelungen zu treffen. Im Gegensatz zu Art. 37 Abs. 1 Data Act werden in Abs. 3 die Mitgliedstaaten nicht aufgefordert, eine zuständige Behörde zu benennen. Vielmehr überträgt Abs. 3 die Zuständigkeit im Rahmen des Data Act unmittelbar auf die bereits zuständigen Behörden.

Eine Abweichung ist auch nicht gemäß Art. 51 Abs. 1 und 4 DSGVO möglich. Zwar geben diese Regelungen den Mitgliedstaaten die Befugnis, mehrere, auch sektoral differenzierte Datenschutzaufsichtsbehörden einzurichten. Doch wird diese allgemeine Befugnis durch die spezifischere und zeitlich spätere Leitentscheidung des Art. 37 Abs. 3 Data Act überlagert, wonach der nationale Gesetzgeber die Aufsicht nach DSGVO und die Datenschutzaufsicht bei der Überwachung des Data Act nicht auseinanderfallen lassen soll. Würde aber – wie in § 3 Abs. 1 des Referentenentwurfs vorgesehen – eine Abweichung von der bestehenden Zuständigkeitszuweisung vorgenommen, so käme es für die Adressaten des Data Act zu einem Auseinanderfallen der Aufsicht, da bei der Anwendung der DSGVO im Rahmen des Data Act eine andere Datenschutzbehörde zuständig wäre, als außerhalb des Rahmens. Die vorrangige Regelung des Art. 37 Abs. 3 Data Act geht daher auch aus sachlich überzeugenden Gründen davon aus, dass die Bewertung von Datennutzungsanliegen und die Beurteilung von Verarbeitungen dadurch erlangter personenbezogener Daten durch dieselbe Behörde gewährleistet werden sollte.

c) § 3 Abs. 6 des Referentenentwurfs verstößt auch gegen die Zuweisung von Aufgaben an die Datenschutzaufsichtsbehörden durch die DSGVO. Art. 57 Abs. 1 lit. f DSGVO überträgt den Datenschutzaufsichtsbehörden die Aufgabe, über das Ergebnis der aufsichtlichen Beschwerdeprüfung in Form eines Verwaltungsakts (so EuGH) zu entscheiden und die Beschwerdeführenden darüber zu unterrichten, unionsrechtlich bindend, d. h. ohne mitgliedstaatliche Abweichungsbefugnis. Art. 37 Abs. 3 S. 2 Data Act erklärt diese Aufgabenzuweisung ausdrücklich für sinngemäß anwendbar. Diese Aufgabe kann daher nicht der BNetzA übertragen werden.

Eine zusammengefasste Entscheidung i. S. v. § 3 Abs. 6 des Referentenentwurfs, in der die datenschutzaufsichtliche Bewertung letztlich alleine als Beurteilungsbeitrag einer gesamtverantwortlichen Data Act-Aufsichtsbehörde erscheinen würde, verkürzt diese unionsrecht-

lich zugewiesene Aufgabe und erschwert jedenfalls den durch Art. 78 DSGVO gewährleisteten Rechtsschutz betroffener Personen gegen datenschutzaufsichtliche Entscheidungen.

2. § 3 des Referentenentwurfs verstößt gegen die verfassungsrechtliche Verteilung der Verwaltungskompetenzen.

a) Entgegen der Grundregel des Art. 83 GG darf eine Verwaltungskompetenz nach Art. 87 Abs. 3 GG auf eine Bundesbehörde nur dann übertragen werden, wenn der Bund in diesem Sachbereich eine Gesetzgebungskompetenz hat. Der Entwurf verweist in seiner Begründung auf S. 19 auf die Gesetzgebungskompetenz des Bundes gemäß Art. 74 Nr. 11 GG für das „Recht der Wirtschaft“. Die vom Data Act erfassten Geräte werden jedoch nicht nur in der „Wirtschaft“ eingesetzt. Sie finden in vielen anderen Bereichen Anwendung, die nicht zum Bereich der Wirtschaft zu zählen sind und der Gesetzgebungskompetenz der Länder unterliegen, wie z. B. medizinische Versorgung, Lehre und Forschung, Schulen, Kultureinrichtungen, Medien, Gerichte, Vereine, Verbände und Kammern.

b) Ganz allgemein fehlt es an einer Ausnahme, die eine Aufsicht der BfDI über Landesbehörden ausschließt. Landesbehörden können als Nutzer, Dateninhaber oder als Datenempfänger vom Data Act erfasst sein. Je nach Auslegung des Begriffs „im Rahmen der Verordnung“ in § 3 Abs. 1 des Referentenentwurfs (s. 1.) ist die Verarbeitung personenbezogener Daten durch Landesbehörden in einem breiteren oder schmaleren Umfang erfasst. In jedem Fall widerspricht es aber grundlegenden föderalen Ordnungsprinzipien, wenn eine Bundesbehörde die Datenverarbeitung von Landesbehörden überwacht.

c) Dies betrifft insbesondere eine spezielle Konstellation von Datenverarbeitungen durch Landesbehörden. Nach Art. 14 Data Act müssen Dateninhaber bei einer „außergewöhnlichen Notwendigkeit“ entsprechend Art. 15 Data Act öffentlichen Stellen Daten bereitstellen, wenn diese einen entsprechend Art. 17 Data Act ordnungsgemäß begründeten Antrag stellen. Dieser Anspruch soll öffentlichen Stellen die notwendige Informationsgrundlage zur Bewältigung eines öffentlichen Notstands zur Verfügung stellen. Der Anspruch dürfte insbesondere von Behörden der Länder geltend gemacht werden, wenn sie Notstände verhindern oder bewältigen müssen. Dass eine Bundesbehörde (BNetzA) die detaillierten Voraussetzungen eines Informationsanspruchs von Landes- und Kommunalbehörden entsprechend Art. 15 und 17 Data Act überprüft oder untersucht, ob die Landes- und Kommunalbehörden hinreichende Maßnahmen ergriffen haben, um die Vertraulichkeit und Integrität der verlangten Daten zu sichern, widerspricht der föderalen Ordnung der Verwaltungskompetenzen nach Art. 83 ff. GG. Ebenso widerspricht es dieser Ordnung, wenn die BfDI kontrolliert, ob Länderbehörden in solchen Notfällen personenbezogene Daten verarbeiten dürfen. Nach Art. 1 Abs. 2 lit. d Data Act gilt das Kapitel V des Data Act zwar für alle Daten des Privatsektors mit Schwerpunkt auf nicht-personenbezogenen Daten, doch ist es bei Datenverarbeitungen entsprechend Kapitel V weder ausgeschlossen noch unwahrscheinlich, dass Verarbeitungen personenbezogener Daten stattfinden, wie auch z. B. die Anforderungen in Art. 17 Abs. 1 lit. c, g, Art. 17 Abs. 2 lit. e, Art. 18 Abs. 4, Art. 19 Abs. 1 lit. b Data Act zeigen.

3. Die Regelung in § 3 des Referentenentwurfs gewährleistet keine praktikable Aufsichtsstruktur.

a) Durch die Regelung in § 3 des Referentenentwurfs kann es in der Praxis zu Abgrenzungsproblemen bzw. zu Doppelstrukturen bei der Aufsicht kommen. Dies betrifft Fälle, in denen Dateninhaber, Nutzer, Dritte und andere Adressaten des Data Act für bestimmte Sachverhalte der Aufsicht der BfDI für andere Sachverhalte wiederum der Aufsicht der Landesdatenschutzbehörden unterliegen bzw. Fälle, in denen eine trennscharfe Abgrenzung dieser Sachverhalte und damit eine trennscharfe Abgrenzung zwischen dem, was innerhalb „des Rahmens" des Data Act i. S. d. § 3 Abs. 1 des Referentenentwurfs und was außerhalb dieses Rahmens liegt, kaum möglich ist. Damit ergibt sich für Unternehmen und Behörden das Gegenteil der beabsichtigten Zuständigkeitsvereinfachung, nämlich eine Doppelaufsicht durch eine Bundes- und eine Landesbehörde ggf. zum gleichen Lebenssachverhalt. Für die primäre Bewertung ihres Datennutzungsanliegens bzw. der Datenverarbeitungen „im Rahmen" des Data Act sind die BfDI und BNetzA zuständig und für die diesen vorausgehenden und nachfolgenden Datenverarbeitungen die Landesdatenschutzbehörden.

Um dies an einem Beispiel zu illustrieren: Ob der Hersteller eines vernetzten Geräts bestimmte Daten, die durch die Gerätenutzung entstehen, erheben, speichern und auswerten darf, wäre eine Frage, die die Landesdatenschutzbehörden zu entscheiden hätten. Ob der Nutzer einen Anspruch hat, dass der Hersteller ihm oder einem Dritten diese bereitstellt, hätte die BNetzA zu prüfen und die datenschutzrechtliche Seite mit der BfDI abzustimmen. Ob der Nutzer die Daten abfragen und für eigene Zwecke weiterverarbeiten darf oder ob der Dritte die Daten für andere Zwecke verarbeiten darf, würde je nach Auslegung des Begriffs „im Rahmen" in § 3 des Referentenentwurfs entweder in die Zuständigkeit der BfDI oder in die der Landesdatenschutzbehörden fallen. Hätte der Hersteller die Nutzungsdaten z. B. mit anderen Daten zusammen zu einem Nutzungsprofil verarbeitet, wären für diese Datenverarbeitung und die Verwendung des Ergebnisses ebenfalls die Landesdatenschutzbehörden zuständig. Für diese Daten gilt der Data Act nicht.

b) Für die Aufsicht und Beratung in Datenschutzfragen sind in den Ländern schon immer die Landesdatenschutzbehörden und gerade keine Bundesbehörden zuständig. Dies gilt auch für den nicht-öffentlichen Bereich.[1] Zu diesem gehören nicht nur große Unternehmen, sondern auch viele mittelständische, kleine und kleinste Unternehmen, Handwerksbetriebe, freie Berufe, Vereine, Verbände, Parteien, NGOs und viele weitere Akteure. Sie können alle von den Regelungen des Data Act in unterschiedlichen Rollen betroffen sein. Die Landesdatenschutzbehörden kennen diese Akteure in ihren Ländern, die wirtschaftlichen und gesellschaftlichen Besonderheiten der Region und haben über Jahre Beratungsnetzwerke bzw. spezifische Beratungsangebote aufgebaut und beraten ständig viele Akteure auf Nachfrage. Der Standortvorteil einer Datenschutzaufsicht vor Ort mit kurzen Wegen und bewährten Kommunikationszusammenhängen sollte nicht zugunsten einer vermeintlichen Verwaltungsvereinfachung aufgegeben werden.

---

[1] Eine Ausnahme hiervon stellt lediglich die historisch bedingte sektorspezifische Zuständigkeit der BfDI für die Kontrolle des Datenschutzes bei der Erbringung von Telekommunikations- und Postdienstleistungen dar.

c) Sowohl für die betroffenen Unternehmen als auch die betroffenen Personen führt die Regelung in § 3 des Referentenentwurfs – entgegen seiner Intention – zu mehr Unannehmlichkeiten und zu geringerer Rechtsicherheit. Betroffene Personen ebenso wie betroffene Unternehmen, die sich in ihren Rechten verletzt fühlen, müssen ihre Beschwerden bei der BNetzA oder der BfDI in Bonn einlegen – also bei einer entfernten, mit den regionalen Verhältnissen unvertrauten Behörde.

Wollen Unternehmen oder Bürgerinnen und Bürger gegen Entscheidungen der BNetzA oder der BfDI den Rechtsweg beschreiten, müssten sie statt beim heimischen Verwaltungsgericht vor dem VG Köln (§ 52 Nr. 2 VwGO) klagen.

Da die Datenschutzfragen „im Rahmen“ des Data Act wie gezeigt nicht trennscharf von anderen Datenschutzfragen zu Verarbeitungen derselben Adressaten abgegrenzt werden können, bewirkt der Referentenentwurf, dass häufig mindestens zwei Datenschutzbehörden für den gleichen Lebenssachverhalt zuständig sind. Mindestens zwei unterschiedliche Aufsichtsbehörden führen parallele Aufsichtsverfahren durch und sind für die Interpretation von Grundfragen des Datenschutzrechts sowie zur Bewertung eines verwobenen Sachverhalts zuständig. Dies ist immer mit dem Risiko divergierender Beurteilungen verbunden. Die dadurch entstehende Rechtsunsicherheit wird durch die Möglichkeit divergierender Entscheidungen unterschiedlicher Gerichte erheblich verstärkt. Zudem bedeutet dies einen unnötigen doppelten Ressourceneinsatz.

Aus den genannten unionsrechtlichen, verfassungsrechtlichen und letztlich auch übergeordneten digitalpolitischen Gründen bitten die Datenschutzaufsichtsbehörden der Länder darum, die Effektivität und Rechtssicherheit aufsichtlicher Entscheidungen als Grundbedingung digitaler Innovation in den Vordergrund zu stellen. Die Datenschutzaufsichtsbehörden der Länder empfehlen, die Regelung in § 3 Abs. 1 zu streichen und die Regelungen in den Absätzen 2 bis 7 an diese Grundentscheidung anzupassen.