**Hessisches Ministerium für Wirtschaft,
Energie, Verkehr, Wohnen und ländlichen Raum**

HESSEN

Stellungnahme zum RefE eines Gesetzes zur Durchführung der Verordnung (EU) 2023/2854 (Data Act-Durchführungsgesetz – DA-DG) des Bundesministeriums für Wirtschaft und Klimaschutz und des Bundesministeriums für Digitales und Verkehr

Anhörung (§ 47 GGO)

Der Gesetzesentwurf wird diesseits dem Grunde nach begrüßt und begegnet keinen durchschlagenden Bedenken. Jenseits der grundsätzlich positiven Einschätzung soll nachstehend indes auf verschiedene Punkte hingewiesen werden, die nach diesseitigem Dafürhalten einer Klarstellung oder Anpassung bedürfen.

a. Zum Erfüllungsaufwand der Verwaltung:

Der Referentenentwurf weist aktuell ausschließlich Mehrkosten der Bundesverwaltung aus. In Ansehung der Tatsache, dass mit dem Gesetzesentwurf auch ausschließlich Aufgaben einer Bundesbehörde geregelt werden sollen, erscheint dies folgerichtig. Auch im Hinblick auf die Zusammenarbeit mit anderen Behörden geht der Gesetzesentwurf in § 4 Abs. 2 DA DG-E von einer Kooperation mit ausschließlich Bundesbehörden aus. Klarstellend sollte daher im Vorblatt sowie der Begründung zum Gesetzesentwurf erwähnt werden, **dass den Ländern durch den Gesetzesentwurf keine Mehraufwände entstehen.**

b. Zu § 3 Abs. 1:

Gegen die Übertragung der Zuständigkeit für die Datenschutzaufsicht auf die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) bestehen sowohl verfassungsrechtliche als auch datenschutzpolitische Bedenken. Nach Art. 83 Grundgesetz führen die Länder die Bundesgesetze als eigene Angelegenheit aus. Für die Datenschutzaufsicht sind in Deutschland dementsprechend grundsätzlich die Datenschutzbeauftragten der Länder zuständig, sowohl für die Wirtschaft als auch für die öffentlichen Stellen der Länder. Deren Zuständigkeit für Wirtschaftsunternehmen bestimmt § 40 Abs. 1 Bundesdatenschutzgesetz (BDSG) in Verbindung mit dem jeweiligen Landesrecht (Hessen § 13 Abs. 1 HDSIG). Die Zuständigkeit für die öffentlichen Stellen der Länder regelt das Landesrecht (Hessen § 13 Abs. 1 HDSIG).

Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) ist nach § 9 Abs. 1 BDSG nur zuständig für „die Aufsicht über die öffentlichen Stellen des Bundes“ sowie, abweichend von der in § 40 Abs. 1 BDSG bestimmten Zuständigkeit der Landesdatenschutzbeauftragen, für „Unternehmen, soweit diese für die geschäftsmäßige Erbringung von Telekommunikationsdienstleistungen Daten von natürlichen oder juristischen Personen verarbeiten…“.

Art. 37 Abs. 3 Data Act bestimmt ausdrücklich, dass die für die Überwachung der DSGVO zuständigen Behörden auch für die Kontrolle des Datenschutzes im Anwendungsbereich des Data Act zuständig sind.

Für die im Referentenentwurf für das Data Act-Durchführungsgesetz vorgesehene Übertragung der Zuständigkeit der Datenschutzaufsicht (die Unternehmen und öffentliche Stellen betreffen würde) auf die BfDI besteht deshalb keine Notwendigkeit; sie bedeutet eine Abweichung von der im Grundgesetz festgelegten Zuständigkeitsverteilung zwischen Bund und Ländern und führt zur Schaffung von Doppelstrukturen.

Darüber hinaus ist das Eindringen der BfDI in den gewerblichen Bereich aus datenschutzpolitischen Gründen strikt abzulehnen. Der Amtsvorgänger der BfDI hat seit Jahren versucht, die Zuständigkeit auf die Wirtschaft zu erweitern. Durch die im Gesetzentwurf vorgesehene Erweiterung ihrer Zuständigkeit wäre die BfDI auch für hessische Unternehmen zuständig, würde ihr Gewicht unter den Datenschutzaufsichtsbehörden in Deutschland weiter erhöhen und ist dabei zugleich aufgrund der europarechtlichen Vorgabe in Art. 52 Abs. 1 DSGVO völlig unabhängig von jeder Verantwortung gegenüber dem bzw. Kontrolle durch den Deutschen Bundestag oder den Hessischen Landtag. Eine solche Entwicklung sollte nicht gefördert werden.

Ähnliche Bedenken schildert der Hessische Beauftragte für Datenschutz und Informationsfreiheit in einem Schreiben an den Hessischen Minister für Wirtschaft, Energie, Verkehr, Wohnen und ländlichen Raum (s. Anl.)

c. Zu § 4 Abs. 2 S. 1:

Der Refentenentwurf sieht in der oben genannten Regelung noch eine Benehmensherstellung zwischen der BNetzA und den sachlich betroffenen Bundesbehörden vor. Das Herstellen des Benehmens wird im folgenden Satz 2 konkretisiert, wonach die BNetzA die im Rahmen des Benehmens eingegangenen etwaigen Stellungnahmen anderer Bundesbehörden lediglich zu würdigen haben. Insoweit wird angeregt, zu überprüfen, ob vorliegend auf ein Einvernehmen abgestellt werden kann, um hierdurch eine faktische Verbindlichkeit der fachlich-sachlichen Stellungnahmen zu erwirken.

d. Zu § 5 Abs. 5 S. 1:

Der Referentenentwurf sieht aktuell die Möglichkeit eines ganz oder teilweisen Widerrufs oder den Erlass nachträglicher Auflagen vor. Im Hinblick auf das Instrument des Widerrufs wird angeregt, allenfalls im Rahmen der Begründung zu konkretisieren, ob die Rechtsfolge des Widerrufs ex tunc oder analog zu § 49 VwVfG sowohl ex tunc als auch ex nunc Wirkung entfaltet. Darüber hinaus wird in Anlehnung an allgemeine verwaltungsrechtliche Überlegungen angeregt zu überprüfen, ob zusätzlich zum Instrument des Widerrufs auch die Möglichkeit einer Rücknahme in den Gesetzesentwurf zu implementieren ist.

e. Zu § 7 Abs. 4 S. 1 Nr. 1:

Es wird angeregt zu überprüfen, ob die Vorlage einer Stellungnahme in der Praxis redundant ist, was zur Streichung der Bestimmung führen würde. Dem liegt folgende Überlegung zu Grunde. Das zusätzliche Erfordernis einer Stellungnahme dürfte in der Praxis vor allem bürokratischen Mehraufwand generieren. Da die reine Vorlage einer Stellungnahme im Hinblick auf die durchzusetzenden Verpflichtungen aber nicht maßgeblich und insoweit vor allem auf die Abhilfe gem. Nr. 2 abzustellen ist, dürfte der Mehrwert einer Stellungnahme in der Praxis eher gering ausfallen. Dies gilt naturgemäß nicht für den Fall, dass natürliche oder juristische Personen der Auffassung sind, nicht einer Verpflichtung des DA zu unterliegen. § 7 Abs. 4 S. 2 iVm Abs. 5 sieht hierfür allerdings ohnehin vor, dass dem Abhilfeverlangen gemeinsam mit der Maßnahmenanordnung widersprochen werden kann. Die Gefahr einer verfassungswidrigen Rechtswegsverwährung ist somit ausgeschlossen.

f. Zu § 8 Abs. 3 S. 3:

In Ansehung der zu protokollierenden Daten und der damit verbundenen eher geringen datenschutzrechtlichen Risiken wird angeregt, die Rechtsfolge hier als gebundene Entscheidung auszugestalten.

g. Zu § 13 Abs. 6:

Mit Blick auf den Bestimmtheitsgrundsatz wird angeregt, die Kostenauferlegung im Rahmen des Gesetzeswortlauts – allenfalls aber der Begründung – näher zu konkretisieren.

h. Zu § 15 Abs. 1 S. 1:

Im Rahmen der Rechtsklarheit wird angeregt, das Wort „ausschließlich“ zwischen den Worten „Übermittlung“ und „elektronisch“ einzufügen.

1 Anlage

DER HESSISCHE BEAUFTRAGTE
FÜR DATENSCHUTZ UND INFORMATIONSFREIHEIT

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

Stellungnahme im Rahmen der Länderanhörung

Die Länder haben die Möglichkeit, bis zum 14. März 2025 zu dem genannten Referentenentwurf der Bundesministerien für Wirtschaft und Klimaschutz sowie Digitales und Verkehr eine Stellungnahme abzugeben.

Aus der Sicht des Hessischen Beauftragten für Datenschutz und Informationsfreiheit ist der Referentenentwurf hinsichtlich der Regelung in § 3 unklar und widersprüchlich (1.), verstößt aus mehreren Gründen gegen Unionsrecht (2.) und die verfassungsrechtliche Verteilung der Verwaltungskompetenzen (3.) und führt entgegen seiner eigenen Zielsetzung zu mehr Bürokratie und einer Verkomplizierung der Aufsichtsstruktur (4.).

Ziel des Data Act ist es, die Verwendung von Daten, die bei der Nutzung von vernetzten Produkten und verbundenen 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 (also zum Beispiel bei Geräten, die klar einer Person zugeordnet werden können, wie zum Beispiel Haushaltsgeräte oder Autos), richtet sich deren Verarbeitung nach der DS-GVO.

Im Fall eines Widerspruchs zwischen Data Act und DS-GVO geht nach Art. 1 Abs. 5 Satz 3 Data Act die DS-GVO 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 Satz 1 Data Act ist ferner geregelt, dass die für die Überwachung der Anwendung der DS-GVO zuständigen Aufsichtsbehörden bezüglich des Schutzes personenbezogener Daten auch für die Überwachung der Anwendung der vorliegenden Verordnung zuständig sind. Diese Aufsicht über die Verarbeitung personenbezogener Daten durch Verantwortliche aus dem öffentlichen und nicht öffentlichen Bereich in Hessen haben § 40 Abs. 1

BDSG und § 13 Abs. 1 HDSIG dem Hessischen Beauftragten für Datenschutz und Informationsfreiheit übertragen.

Im Gegensatz dazu soll nach § 3 des Referentenentwurfs die Zuständigkeit für die Überwachung der Anwendung der DS-GVO im Rahmen des Data Act auf die Bundesbeauftragte für Datenschutz und Informationsfreiheit (BfDI) übertragen werden.

Dieser Regelungsentwurf stößt auf mehrfache Bedenken:

1. ist der Referentenentwurf hinsichtlich der Regelung in § 3 unklar und widersprüchlich.

Bei einem Abgleich zwischen dem Normtext in § 3 des Entwurfs mit der Begründung bleibt offen, was der Bundesgesetzgeber regeln soll. Der Wortlaut des § 3 Abs. 1 des Entwurfs und seine Begründung auf S. 26 können so verstanden werden, dass im Anwendungsbereich des Data-Act abweichend von Art. 83 GG, § 40 Abs. 1 BDSG und § 13 Abs. 1 HDSIG künftig die BfDI im Rahmen des Data Act alleinige Datenschutzaufsichtsbehörde für die Überwachung der DS-GVO, anderen EU-Rechts und nationalen Rechts über den Schutz personenbezogener Daten sein soll. Dagegen heißt es in der Begründung auf Seite 22 des Entwurfs aber, dass die für die Überwachung der Anwendung der DS-GVO zuständigen Aufsichtsbehörden bezüglich des Schutzes personenbezogener Daten auch für die Überwachung des Data Acts zuständig sind.

Nach § 3 Abs. 1 des Referentenentwurfs soll die BfDI „*im Rahmen der Verordnung (EU) 2023/2854*“ zuständige Datenschutzaufsichtsbehörde sein. Es bleibt aber unklar, welcher Aufsichtsbereich damit erfasst ist. Nach Art. 1 Abs. 1 Data Act regelt dieser

„*a) die Bereitstellung von Produktdaten und verbundenen Dienstdaten für den Nutzer des vernetzten Produkts oder verbundenen Dienstes,*

b) die Bereitstellung von Daten durch Dateninhaber für Datenempfänger,

c) die Bereitstellung von Daten durch Dateninhaber für öffentliche Stellen …“.

Nach Art. 2 Nr. 7 Data Act ist die Bereitstellung – wie in Art 4 Nr. 2 DS-GVO – das passive Anbieten von Daten zum Abruf durch einen Dritten. Sie ist nur ein Schritt im Rahmen von 19 in Art. 3 Nr. 7 Data Act beispielhaft genannten Schritten in der Verarbeitung von (personenbezogenen) Daten. Danach wäre die BfDI also für die Aufsicht über das Bereitstellen von Daten zuständig, für alle anderen Verarbeitungsformen und Schritte des Art. 3 Nr. 7 Data Act und Art. 4 Nr. 2 DS-GVO wären weiterhin die Landesdatenschutzbeauftragten zuständig. Ob der Referentenentwurf dies genau so meint, ist fraglich.

2. verstößt der Referentenentwurf aus drei Gründen gegen Unionsrecht

a) Art. 37 Abs. 3 Satz 1 Data Act bestimmt, dass die für die Überwachung der Anwendung der DS-GVO

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

Nach dem klaren Wortlaut der Verordnung will der europäische Gesetzgeber durch einen Gleichlauf der Zuständigkeiten nach Data Act und DS-GVO eine Zuständigkeitszersplitterung vermeiden und knüpft daher ausdrücklich an die bestehende Zuständigkeitsordnung nach der DS-GVO an. Danach ist der HBDI für den Schutz personenbezogener Daten auch im Rahmen des Data Act die zuständige Aufsichtsbehörde. (s. hierzu auch die Praktikabilitätserwägungen unter 4.)

b) Für eine Abweichung von dieser Regelung im Data Act fehlt Deutschland eine Öffnungsklausel. Die klare und abschließende Regelung in Art. 37 Abs. 3 Satz 1 Data Act bietet keinen Anhaltspunkt für die Zulässigkeit einer abweichenden Regelung. 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 DS-GVO möglich. Zwar geben diese Regelungen den Mitgliedsstaaten 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. Diese vorrangige Regelung geht – 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. Art. 57 Abs. 1 Buchst. f DS-GVO überträgt 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 mitgliedsstaatliche Abweichungsbefugnis, den Datenschutzaufsichtsbehörden. Art. 37 Abs. 3 Satz 2 Data Act erklärt diese Aufgabenzuweisung ausdrücklich für sinngemäß anwendbar. Diese Aufgabe kann daher nicht der BNetzA übertragen werden.

Eine zusammengefasste Entscheidung im Sinne von § 3 Abs. 6 des Referentenentwurfs, in der die datenschutzaufsichtliche Bewertung letztlich alleine als Beurteilungsbeitrag einer gesamtverantwortlichen Data Act-Aufsichtsbehörde erscheinen würde, verkürzt diese unionsrechtlich zugewiesene Aufgabe und erschwert jedenfalls den durch Art. 78 DSGVO gewährleisteten Rechtsschutz betroffener Personen, also auch der Bürgerinnen und Bürger in Hessen, gegen datenschutzaufsichtliche Entscheidungen.

3. verstößt § 3 des Referentenentwurfs aus drei Gründen 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 schmäleren 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 Landesbehörden entsprechend Art. 15 und 17 Data Act überprüft, 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 Buchst. 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.

4. gewährleistet die Regelung in § 3 des Referentenentwurfs keine praktikable Aufsichtsstruktur.

a) Nach § 3 des Referentenentwurfs sind für die Bereitstellung von Daten die BfDI und für alle anderen Formen der Datenverarbeitung die Landesaufsichtsbehörden zuständig. Für die der Bereitstellung vorangehende Erhebung und weitere Verarbeitung von Nutzungsdaten gilt die DS-GVO und sind nach wie vor die Landesdatenschutzaufsichtsbehörden zuständig.

Soweit es im Anwendungsbereich des Data Act um Nutzungsanliegen mit personenbezogenen Daten geht, sind zwangsläufig auf Seiten der Datenempfänger stets (Weiter-)Verarbeitungen verbunden, die ebenfalls in vollem Umfang der DS-GVO unterliegen. Damit ergibt sich für Unternehmen und Behörden das Gegenteil der beabsichtigten Zuständigkeitsvereinfachung, nämlich eine Doppelaufsicht durch eine Bundes- und eine Landesbehörde zum gleichen Lebenssachverhalt. Für die primäre Bewertung ihres Datennutzungsanliegens nach dem Data Act sind die BNetzA und BfDI zuständig und für vorausgehenden und nachfolgenden Datenverarbeitungen die Landesdatenschutzaufsichtsbehörden.

Um dies an einem Beispiel zu illustrieren: Ob der Hersteller eines vernetzten Gerätes bestimmte Daten, die durch die Gerätenutzung entstehen, erheben, speichern und auswerten darf, wäre eine Frage, die die Landesdatenschutzaufsichtsbehörden zu entscheiden hätten. Ob der Nutzer einen Anspruch hat, dass der Hersteller ihm oder einem Dritten diese bereitstellt, hätte die BfDI zu prüfen und ihr Ergebnis mit der BNetzA abzustimmen. Ob der der Nutzer die Daten abfragen und für eigene Zwecke weiterverarbeiten darf oder ob der Dritte die Daten für welche Zwecke auch immer verarbeiten darf, hätten wiederum die Landesdatenschutzaufsichtsbehörden zu prüfen. 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 Landesdatenschutzaufsichtsbehörden zuständig. Für diese Daten gilt der Data Act nicht.

b) Für die Aufsicht und Beratung in Datenschutzfragen ist in Hessen schon immer eine Landesbehörde und gerade keine Bundesbehörde zuständig. Dies gilt auch für den nicht öffentlichen Bereich. 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 Acts in unterschiedlichen Rollen betroffen sein. Der HBDI kennt diese Akteure in Hessen, die wirtschaftlichen und gesellschaftlichen Besonderheiten der Region und hat über Jahre Beratungsnetzwerke aufgebaut und berät 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.

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. Bei Entscheidungen des HBDI wäre das Verwaltungsgericht Wiesbaden zuständig.

Da die Datenschutzfragen im Rahmen des Data Act beinahe immer auch mit Datenschutzfragen zu den Datenverarbeitungen vor der Bereitstellung und zu Weiterverarbeitungen nach der Bereitstellung verbunden sind, bewirkt der Referentenentwurf, dass immer mindestens zwei Datenschutzaufsichtsbehörden 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.

d) Durch die Regelung in § 3 des Referentenentwurfs soll nach S. 26 der Begründung im Rahmen des Data Act

„sichergestellt (werden), 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 anspruchsvollen Bereich der Datenschutz-Compliance führt“.

Diese einheitliche Vollzugspraxis kann nicht dadurch erreicht werden, dass allein die BfDI im Rahmen der Data Act (zu dessen Begrenzung s. oben 1.) zuständig wäre. Denn es geht um Regeln und Begriffe der DS-GVO, die für alle Anwendungsbereiche gleich ausgelegt und praktiziert werden müssen. Die BfDI käme daher auch in diesem Fall nicht darum herum, sich mit den Aufsichtsbehörden der Länder in diesen Fragen abzustimmen. Eine einheitliche Auslegung des Datenschutzrechts in Deutschland wird durch die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) und in der Europäischen Union durch den Europäischen Datenschutzausschuss (EDSA) gewährleistet. Die Vereinheitlichung der Auslegung und Anwendung des Datenschutzrechts in Deutschland ist der DSK in den letzten Jahren sehr erfolgreich gelungen.

Aus den genannten unionsrechtlichen, verfassungsrechtlichen und letztlich auch übergeordneten digitalpolitischen Gründen sollte die Effektivität und Rechtssicherheit aufsichtlicher Entscheidungen als Grundbedingung digitaler Innovation im Vordergrund zu stehen. Die Zuständigkeitsregelung des § 3 des Referentenentwurfs kann daher nicht unterstützt werden. Vielmehr ist zu empfehlen, die Regelung in § 3 Abs. 1 zu streichen und die Regelungen in den Absätzen 2 bis 7 an diese Grundentscheidung anzupassen.