bitkom

Vorschläge zur nationalen Durchführung des Data Act

Aufsichtsregime, Sanktionen, Streitbeilegung

Inhalt

1 Einleitung

Der deutsche Gesetzgeber ist durch den Data Act verpflichtet, bis zum grundsätzlichen Anwendungsbeginn der Verordnung insb. entsprechende Aufsichtsstrukturen zur Rechtsdurchsetzung zu schaffen. Hierfür wird ein Durchführungsgesetz benötigt. Dies ist wichtig, denn die Benennung der Aufsichtsbehörde(n) für den Data Act (DA) ist Grundlage für seine erfolgreiche Umsetzung und die Beantwortung zahlreicher Fragen vor und nach seines grundsätzlichen Anwendungsbeginns. Darüber hinaus können auch ein verhältnismäßiges Sanktionsregime und ein funktionierender Streitbeilegungsmechanismus entscheidend zum Wachstum der europäischen Datenwirtschaft im Rahmen des Data Acts beitragen.

2 Aufsichtsregime

2.1 Welche Vorgaben enthält der Data Act in Bezug auf neue Zuständigkeiten?

Mitgliedsstaaten entscheiden frei, ob sie als zuständige Behörden für Anwendung und Durchsetzung des DA (**DA-Aufsichtsbehörde**) eine oder mehrere Behörden benennen und ggf. schaffen.[1] Wenn ein Mitgliedsstaat mehr als eine DA-Aufsichtsbehörde benennt, muss er aus diesen einen Datenkoordinator benennen.[2]

Die Aufsichtsbehörde für Kapitel 6 und 8 „muss über Erfahrungen auf dem Gebiet Daten und elektronische Kommunikationsdienste verfügen“.[3] Insofern kann es Abstimmungsbedarf etwa mit BNetzA/BSI geben.

Eine Aufgabe der DA-Aufsichtsbehörde(n) ist die Zusammenarbeit mit den zuständigen Behörden anderer Mitgliedsstaaten, ggf. der EU-Kommission und dem EU-Dateninnovationsrat (**EDIB**)[4].

Soweit EU-KOM, EZB oder EU-Einrichtungen vom DA betroffen sind, ist deren Aufsichtsbehörde der EDPS.[5]

Anders als etwa der DSA erfordert der DA keine „völlige Unabhängigkeit“ der zuständigen Aufsichtsbehörden. Bezüglich der Unabhängigkeit der DA-Aufsichtsbehörden stellt der DA jedoch klar: „Bei der Wahrnehmung ihrer Aufgaben und Befugnisse gemäß dieser Verordnung handeln die zuständigen Behörden unparteiisch und unterliegen keiner direkten oder indirekten Einflussnahme von außen und dürfen von anderen Behörden oder von privaten Parteien im Einzelfall keine Weisungen einholen oder entgegennehmen.“[6]

[1] Art. 37 (1)
[2] Art. 37 (2)
[3] Art. 37 (4) b)
[4] Art. 37 (5) f)
[5] Art. 37 (3) S. 2
[6] Art. 37 (8)

2.2 Welche Vorgaben enthält der Data Act in Bezug auf konkurrierende Zuständigkeiten?

Die Zuständigkeiten der DS-GVO lässt der DA unberührt. Die Aufsichtsbehörden i.S.d. DS-GVO sind auch für die Überwachung der Anwendung des DA zuständig (nur) insoweit es um personenbezogene Daten geht.[7] Dies ist relevant, da personenbezogene Daten i.S.d. DS-GVO im Anwendungsbereich des DA liegen.[8] Insofern kann es Abstimmungsbedarf mit DS-GVO Aufsichtsbehörden geben.

In besonderen sektoralen Angelegenheiten des Datenzugangs und der Datennutzung bleibt die Zuständigkeit sektoraler Behörden gewahrt.[9] Insofern kann es Abstimmungsbedarf mit sektoralen Behörden geben.

Vorschriften die besonderen Bedürfnissen einzelner Sektoren oder Bereichen von öffentlichem Interesse Rechnung tragen, bleiben durch DA unberührt.[10] Dazu gehören insb. Sicherheitsanforderungen inkl. Cybersicherheit.[11] Insofern kann es Abstimmungsbedarf mit dem Bundesamt für Sicherheit in der Informationstechnik geben.

Wettbewerbsvorschriften, insb. auch zu Kartellen (101 AEUV) und Marktmissbrauch (102 AEUV), bleiben durch DA unberührt.[12] Insofern kann es Abstimmungsbedarf mit dem Bundeskartellamt und der EU-KOM geben.

Artikel 5 und 6 referenzieren auf den DMA. Insofern kann es Abstimmungsbedarf vor allem mit der EU-KOM geben.

2.3 Welche Stellen kommen in Betracht?

Für obige Aufgaben kommen verschiedene existierende Behörden in Betracht. Alternativ zur Benennung einer oder mehrerer existierenden Behörden können auch eine oder mehrere neue Behörden geschaffen und als Aufsichtsbehörden benannt werden.[13]

Im föderalen System der Bundesrepublik Deutschland sind grundsätzlich die Länder für die Ausführung der Gesetze zuständig.[14]

Dabei stellt sich eine Kompetenzproblematik, wenn es um die DA-Aufsicht geht. Eine ausnahmsweise Kompetenz des Bundes für die Ausführung des DA, der nach Inkrafttreten den Rang eines Bundesgesetzes haben wird, könnte sich

- aus Art. 87 f Abs. 1 GG (Kompetenz des Bundes im Bereich des Postwesens und der Telekommunikation), oder
- kraft Natur der Sache (Datenpolitik als Querschnittsaufgabe und Datennutzung als Querschnittsziel, die alle Ressorts und ihre nachgeordneten Bereiche betreffen), oder
- ggf. ersatzweise in Verbindung mit einer zu schaffenden GG-Norm ergeben.

Dies ist vor dem Hintergrund Anerkennung der Zuständigkeit der Europäischen Union in Bezug auf die eigentlichen Regelungen des DA zu sehen:

> „Da die Ziele dieser Verordnung, nämlich die Gewährleistung einer fairen Aufteilung des Wertes von Daten auf die Akteure der Datenwirtschaft und Förderung eines fairen Zugangs zu Daten und ihrer Nutzung, um zur Schaffung eines echten Binnenmarktes für Daten beizutragen, von den Mitgliedstaaten nicht ausreichend verwirklicht werden können, sondern vielmehr wegen des Umfangs und

[7] Art. 37 (3)
[8] Insb. Kap. 2 & 5.
[9] Art. 37 (4) a)
[10] ErwG. 115 S. 1
[11] ErwG. 115 S. 3
[12] ErwG. 116 S. 1
[13] Art. 37 (1)
[14] Art. 83 GG

> der Wirkungen der Maßnahme und der grenzüberschreitenden Nutzung der Daten auf Unionsebene besser zu verwirklichen sind, kann die Union im Einklang mit dem in Artikel 5 des Vertrags über die Europäische Union verankerten Subsidiaritätsprinzip tätig werden. […]“[15]

Aufsichtsbehörde könnte die **Bundesnetzagentur (BNetzA)** werden, die im Geschäftsbereich des BMWK liegt. Sie spielt eine zentrale Rolle bei Anwendung und Durchsetzung des **Digital Services Act** sowie voraussichtlich des **Data Governance Act** (der Digitale-Dienste-Koordinator ist eine unabhängige Stelle innerhalb der Strukturen der BNetzA).

Daneben kommen auch die 18 deutschen **Datenschutzaufsichtsbehörden** als Aufsichtsbehörden in Betracht. Im Detail handelt es sich dabei um den **Bundesbeauftragten für Datenschutz und Informationssicherheit** (kommissarisch derzeit: Ulrich Kelber), der als unabhängige Datenschutzbehörde zuständig für die Überwachung des Datenschutzes und der Informationsfreiheit bei öffentlichen Stellen des Bundes und bei Unternehmen, die Telekommunikations- und Postdienstleistungen erbringen, zuständig ist sowie **17 Landesdatenschutzbehörden** (in Bayern 2, sonst 1 pro Land), die im jeweiligen Land für öffentliche Stellen des jeweiligen Landes und/oder ansässige Unternehmen mit entsprechendem Sitz nach DS-GVO zuständig sind.

Ebenso in Frage kommt das **Bundesamt für Sicherheit in der Informationstechnik**, zu dessen Aufgaben insb. Prüfung, Zertifizierung und Akkreditierung von IT-Produkten und Dienstleistungen gehört sowie die Entwicklung einheitlicher und verbindlicher IT-Sicherheitsstandards gehört. Ebenso in Frage kommt das **Bundeskartellamt**, zu dessen Aufgaben insb. die Zusammenschlusskontrolle, die Kartellverfolgung sowie die Missbrauchsaufsicht gehören.

Daneben kommen sektorale Aufsichtsbehörden in Betracht, schematisch etwa das **Kraftfahrtbundesamt** für Hersteller von Kraftfahrzeugen, das **Eisenbahnbundesamt** für Hersteller von Eisenbahnen, die **Bundesnetzagentur** (als sektorale Aufsichtsbehörde) für Hersteller von Kraftwerken, das **Luftfahrtbundesamt** für Hersteller von Flugzeugen, die **BaFin** für Versicherungsunternehmen, das **Bundesinstitut für Arzneimittel und Medizinprodukte** für Hersteller von Medizinprodukten, das **Bundesamt für Verbraucherschutz und Lebensmittelsicherheit** für Hersteller von Spielwaren, das **Deutsche Institut für Bautechnik** für Hersteller von Lüftungstechnik und Betontechnologie, oder das **Bundesamt für Seeschifffahrt und Hydrographie** für Hersteller bestimmter Navigationsausrüstungen.

2.4 Was spricht für welche Aufsichtskonstellation?

2.4.1 Eine oder viele?

In jedem Fall sollte für Unternehmen ein einheitlicher Ansprechpartner – sog. single point of contact – benannt werden, wie er auch im Data Act vorgesehen ist („Datenkoordinator“, vgl. 2.1).

Noch entscheidender als der einheitliche Ansprechpartner (im Außenverhältnis) ist jedoch die Verteilung bzw. Bündelung von Kompetenzen zwischen zuständigen Stellen (im Innenverhältnis).

In Anbetracht unterschiedlicher im DA vorgesehenen bzw. bestehenden Sonderzuständigkeiten würde eine einzelne DA-Aufsichtsbehörde die meisten Synergieeffekte schaffen.

Schon in einer gemeinsamen (Data Act Stellungnahme des EDSA und des EDSB, Rn. 98) wird auf das Risiko operativer Schwierigkeiten hingewiesen, die sich aus der Benennung von mehr als einer für die Anwendung und Durchsetzung des DA zuständigen Behörde ergeben könnten. Es bestünden ernsthafte Bedenken, dass eine solche Governance-Architektur zu Komplexität und Verwirrung sowohl für Organisationen als auch für betroffene

[15] ErwG 119

Personen sowie zu Divergenzen bei den Regulierungsansätzen in der Union und somit zu einer Beeinträchtigung der Kohärenz in Bezug auf die Überwachung und Durchsetzung führen würde.

2.4.2 Wer genau?

Als Aufsichtsbehörde käme wegen der Anforderung für Aufsicht von Kapitel 6 und 8 (insb. Interoperabilitätsanforderungen), „über Erfahrungen auf dem Gebiet Daten und elektronische Kommunikationsdienste [zu] verfügen“,[16] insbesondere die BNetzA in Betracht. Diese Kompetenzen werden durch jene der BNetzA unter dem DSA sowie voraussichtlich DGA ergänzt, was weitere Synergieeffekte bringt. Auch hinsichtlich des Aufgabenkataloges in Art. 37 Abs. 5, welcher unter anderem die Förderung der Datenkompetenz und Sensibilisierung der Nutzer in Bezug auf ihre Rechte aus dem DA umfasst, kann die BNetzA im Telekommunikationsmarkt auf Erfahrungen bei der Beratung von Bürgerinnen und Bürgern zurückgreifen. Gleiches gilt für die Beobachtung von technologischen und wirtschaftlichen Entwicklungen.

Analog zu den positiv ausfallenden Einschätzungen bzgl. der Umsetzbarkeit der BNetzA als DDK unter Berücksichtigung der Unabhängigkeitsanforderungen des DDG unter Schaffung bestimmter Voraussetzungen in den Rechtsgutachten von (Kühling 2022, S. 51 f.) und (Cornils et al. 2022, S. 66 ff.) erscheint die Einsetzung der BNetzA als selbstständige Bundesoberbehörde als DA-Aufsichtsbehörde unter Vornahme bestimmter Änderungen (welche wohl bereits im Zuge der Einrichtung der DSA-Zuständigkeit erledigt werden (müssen)) absolut denkbar.

Die bestehenden Mandate und Kompetenzbereiche von BKartA sowie BSI müssten für Aufsichtsbefugnisse unter dem Data Act recht umfassend erweitert werden, was nicht naheliegend erscheint. Auch zielt der DA eher auf die Förderung des Wettbewerbs durch Data-Sharing und einheitliche technische Standards ab, was unseres Erachtens eher in den Kompetenzbereich der BNetzA als in den des BKartA fällt. Das BSI kann zwar auf viel Erfahrung im Bereich der Informations- und Kommunikationstechnik zurückgreifen, hat hierbei jedoch zuvörderst die Sicherheit im Blick, was relevant aber nicht Hauptanliegen des DA ist.

In Anbetracht der Erfahrungen mit der DSK und der weiterhin Wünsche offenlassenden Harmonisierung der Datenschutzanwendung innerhalb Deutschlands raten wir von einer über die im DA vorgeschriebene (bzw. unangetastete) Kompetenz der DS-GVO Aufsichtsbehörden hinaus dringend ab.

Für eine effektive Durchsetzung von Datenschutzrecht sowie Datennutzungsnormen, welche sich aus unterschiedlichen Rechtsgütern ergeben können, benötigt es voneinander **unabhängige, sich gegenseitig balancierende Institutionen**. Nach Art. 38 Abs. 6 DSGVO sollen Interessenkonflikte beim Datenschutzbeauftragten vermieden werden. Diesen Grundsatz sollten auch Behörden anwenden. Der Data Act möchte Daten möglichst weitgehend nutzbar machen. Die DSGVO hingegen verfolgt den Grundsatz der Datenminimierung und setzt der Datennutzung Grenzen. Zudem zeichnen sich die Datenschutzbehörden vor allem in ihrer Funktion als *Schutz*behörden aus. Dem Data Act geht es aber darum, die Nutzbarkeit von Daten im Binnenmarkt zu fördern und die Wertschöpfung aus diesem Nutzen fairer zu verteilen. Diesen Zielen entsprechend sollte die für die Durchsetzung zuständige Behörde wettbewerbsorientiert und durchsetzungsstark sein.

2.4.3 Sektoral oder horizontal?

Der notwendige Kompetenzaufbau für Kapitel 2-5 in puncto Daten, Datenzugangstechnologien, Datenvertragsklauseln, für Kapitel 6 und 8 in puncto Datenverarbeitungsdienste, Interoperabilität, Standardisierung, für Kapitel 7 in puncto Schutz von Betriebs- und Geschäftsgeheimnissen durch Cloud-Provider vor EU-rechtswidrigen Handlungen von Drittstaaten, würde sektorale Behörden im Vergleich zu einer horizontalen Verantwortlichkeit vor recht große Herausforderungen stellen.

[16] Art. 37 (4) b)

Vor dem Hintergrund zunehmenden sektorübergreifenden Datenaustauschs zwischen unterschiedlichen IoT-Produkten in vernetzten Ökosystemen (Auto kommuniziert mit Ladesäule, Handy kommuniziert mit Medizinprodukt, Gebäude kommuniziert mit Stadtverwaltung) ist unstreitig,

- dass eine horizontal gesamtverantwortliche DA-Aufsichtsbehörde essentiell ist,
- dass insb. sektorale Besonderheiten durch die Einbindung (aber nicht notwendigerweise Benennung) weiterer relevanter Behörden berücksichtigt werden müssen,
- dass Zuständigkeitskonflikte vermieden werden müssen.

Streitig ist, ob und inwiefern neben einer gesamtverantwortlichen DA-Aufsichtsbehörde (die ggf. Datenkoordinator sein sollte) sektorale DA-Aufsichtsbehörden benannt werden sollten.

- Einerseits bestünde hier, wie allgemein bei der Zuständigkeit von mehreren Behörden, die Gefahr von Überschneidungen und Zuständigkeitskonflikten. Dies könnte zu einer Fragmentierung der Anwendung einer horizontalen Verordnung (hier dem Data Act) führen und auch Auswirkungen in die Anwendung anderer Gesetze haben. Die Klärung von z.B. Auslegungsfragen ist innerhalb einer einzelnen Aufsichtsbehörde effizienter und schneller möglich als zwischen mehreren Behörden.
- Andererseits würde eine Herauslösung einzelner Kapitel und deren Übertragung auf unterschiedliche sektorale Aufsichtsbehörden– über deren gesicherte Kompetenz durch Artikel 37 (4) hinaus – ggf. viele Domänenkenntnisse in die Aufsichtsstruktur bringen.

Unstreitig ist wiederum, dass die genaue Abgrenzung zwischen aufsichtsbehördlichen Kompetenzen (benannt unter Data Act und/oder anderen anwendbaren Regelungen) so weit wie möglich im Durchführungsgesetz klargestellt werden sollte.

Der Data Act sieht in Bezug auf sektorale Vorschriften insb. vor, dass:

> „[Der DA] Vorschriften unberührt lassen [sollte], die besonderen Bedürfnissen einzelner Sektoren oder Bereichen von öffentlichem Interesse Rechnung tragen. Solche Vorschriften können zusätzliche Anforderungen an die technischen Aspekte des Datenzugangs, wie Schnittstellen für den Datenzugang, oder an die Art und Weise umfassen, wie der Datenzugang gewährt werden könnte, z. B. direkt über das Produkt oder über Datenvermittlungsdienste. Ebenso können solche Vorschriften Beschränkungen der Rechte der Dateninhaber auf Zugang zu oder Nutzung von Nutzerdaten oder andere Aspekte betreffen, die über den Datenzugang und die Datennutzung hinausgehen, wie z. B. Governance-Aspekte oder Sicherheitsanforderungen, einschließlich Anforderungen an die Cybersicherheit […]“**(ErwG 115)**
>
> „Bei besonderen sektoralen Angelegenheiten des Datenzugangs und der Datennutzung im Zusammenhang mit der Anwendung dieser Verordnung […] die Zuständigkeit der sektoralen Behörden [gewahrt bleibt]“ **(Art. 37 4) a))**
>
> „[die zuständigen Behörden insb. diese Aufgaben und Befugnisse haben:] Zusammenarbeit mit den einschlägigen zuständigen Behörden, die für die Anwendung anderer Rechtsakte der Union oder nationaler Rechtsakte zuständig sind, einschließlich […] mit sektoralen Behörden, um sicherzustellen, dass diese Verordnung im Einklang mit anderem Unionsrecht und nationalem Recht durchgesetzt wird“ **(Art. 37 5) g))**

Es wäre zu prüfen, inwiefern die Vorschriften insb. aus Art. 37 4) a) und Art. 37 5) g) im Durchführungsgesetz EU-rechtskonform konkretisiert werden können, um etwa die Formulierung „“[b]ei besonderen sektoralen Angelegenheiten“ mit Bedeutung zu füllen.

2.4.4 Operative Umsetzung

In jedem Fall sollte das Augenmerkt darauf liegen, ein belastbares und effizientes digitales Fallmanagement-System zwischen der/den DA-Aufsichtsbehörde/n und für anderes zuständige Behörden (d.h. BSI, DPAs, BKartA, sektorale Behörden, etc., etc.) gesetzlich zu etablieren, technisch aufzusetzen und rechtzeitig in Betrieb zu nehmen.

Als Rechtsgrundlage hierfür sind das formelle Amtshilfeverfahren nach Art. 37 (16) sowie informelle Informationsaustausche auf Basis sog. Waiver der beteiligten Parteien heranzuziehen.

In bestimmten Rechtsbereichen sind Genehmigungsfiktionen der Regelfall, um die Parteien nicht mit einer überlangen Verfahrensdauer zu belasten. Ein Beispiel dafür sind europäische und deutsche Fusionskontrollverfahren, welche teilweise Genehmigungsfiktionen von wenigen Wochen (!) besitzen.

Verfahrensrechtlich sollte deshalb im Einklang mit DA eine Genehmigungsfiktion hinsichtlich der Amtshilfe der DA-Aufsichtsbehörde bei Anruf durch sektorale Aufsichtsbehörden geprüft werden.

2.5 Welche Rolle wird Deutschland in der Governance auf EU-Ebene spielen?

Auch stellt sich die Frage nach der Rolle Deutschlands in der Governance auf EU-Ebene. Hier gibt es zwei zentrale Institutionen: der EU-Dateninnovationsrat (EDIB) sowie die Expertengruppe für B2B Data Sharing Contracts und Cloud Computing Contracts. Die Expertengruppe unter dem Data Act tagt bereits. Ebenso das EDIB, das schon unter dem DGA ins Leben gerufen und mit Aufgaben bedacht wurde, und nun weitere Aufgaben aus dem DA erhält. Die Frage, wer Deutschland in diesem Zusammenhang vertreten wird, ist vor dem Hintergrund der Tatsache, dass die BNetzA derzeit im Kontext des DGA (vorbehaltlich DGA Zuständigkeit?) im EDIB sitzt, bedeutsam.

3 Sanktions- und Verfahrensregelungen

Die Sanktionsregelungen der DS-GVO bleiben durch den DA unangetastet. Die Grundrechtsrelevanz des DA im Vergleich zur DS-GVO ist weit weniger ausgeprägt. Derweil sind Data Governance Act und Data Act Bestandteil der Europäischen Datenstrategie und müssen zusammen gedacht und durchgesetzt werden. Während ersterer insb. die Vermittlung von Daten regelt, normiert zweiter insb. Datenzugangsrechte.

Sinn und Zweck von DGA und DA sind dabei die Schaffung und Stärkung einer europäischen Datenwirtschaft. Dafür ist es entscheidend, dass das Sanktionsregime europaweit möglichst einheitlich ausgestaltet wird, um Forum-Shopping oder ein Race-to-the-Bottom zu vermeiden. Andererseits ist es für deutsche Unternehmen und Verbraucher:innen entscheidend, dass Deutschland sich durch ein unverhältnismäßiges Sanktionsregime keine heimischen Standortnachteile schafft.

Dabei sind die Anforderungen an das Sanktionsregime aus DGA (Art. 34) und DA (Art. 40) in Anbetracht einer nicht-abschließenden Liste zu berücksichtigender Kriterien sehr vergleichbar.

Diese Kriterien sollten die Grundlage für eine angemessene und verhältnismäßige Bußgeldberechnung sein. Über diese Kriterien hinaus sollten weder weiteren Kriterien auf nationaler Ebene (nach)normiert werden noch sollte ein Stufenmodell o.ä. eingeführt werden, welches keine Einzelfallgerechtigkeit garantiert.

Substanziell abweichend von DGA Art. 34 ist dabei in den Sanktionsvorschriften des Data Act nur die Anforderung von Data Act Art. 40, den Jahresumsatz der verstoßenden Partei im vorangegangenen Geschäftsjahr in der Union zu berücksichtigen, was im Rahmen der Ermittlung der Höhe der Geldbuße im Rahmen eines Bußgeldkorridors möglich erscheint.

Fahrlässig und vorsätzlich begangene Ordnungswidrigkeiten könnten grundsätzlich in einem Bußgeldkorridor bis 50T€ bzw. bis 10T€ sanktioniert werden, während abweichend davon bestimmte vorsätzlich durch juristische

Personen oder Personenvereinigungen mit einem jährlichen Gesamtumsatz von mehr als 50TT€ begangene Ordnungswidrigkeiten in einem Bußgeldkorridor bis zu 2 Prozent des im vorangegangenen Geschäftsjahr erwirtschaften weltweiten Jahresumsatzes sanktioniert werden könnten.

4 Streitbeilegungsstelle

Es besteht keine Pflicht für die BReg, eine staatliche Streitbeilegungsstelle einzurichten.[17]

Entscheidungen von Streitbeilegungsstellen sind nur bindend, wenn sich alle Parteien vor dem Verfahren verpflichten, die Entscheidungen als bindend anzuerkennen.[18]

Da die Streitbeilegungsstelle EU-Recht und nationales Recht zu berücksichtigen hat,[19] wird wohl auch die DS-GVO eine Rolle in bestimmten Streitbeilegungsverfahren spielen, was die Komplexität der entsprechenden Verfahren erhöht.

Gleichzeitig liegt die Entscheidungsfrist für Streitbeilegungsstellen nach Antragseingang bei 90 Tagen,[20] was zeitlich sehr herausfordernd sein kann und Auswirkungen auf Anrufhäufigkeit und Entscheidungsqualität haben könnte.

Die Entgelte des Streitbeilegungsverfahrens werden durch die Streitbeilegungsstelle festgelegt.[21] Dabei könnte die Kostenregelung für Dateninhaber bei Anrufungen nach Art. 4 (3) kaum ungünstiger sein (der Dateninhaber zahlt grundsätzlich die Kosten unabhängig vom Ausgang), was wiederum Auswirkungen auf die Anrufhäufigkeit haben könnte.

Aus den vorigen Gründen geht die Bitkom-Geschäftsstelle derzeit tendenziell von a) eher begrenzter Anrufhäufigkeit (mit bindenden Entscheidungen) der Streitbeilegungsstelle bei komplizierten Sachverhalten und b) eher einem Fokus auf kleine Streitigkeiten oder Einzelfragen bei sonst funktionierenden Verträgen aus.

Deshalb sollte eine staatliche Streitbeilegungsstelle eingerichtet werden, die die benötigte Fach- und Sachkompetenz vorhält und dafür sorgt, dass die Finanzierung der Streitbeilegungsstelle sichergestellt werden. Hier könnte eine TGK-ähnliche Unterstelle innerhalb der BNetzA als Vorbild dienen. Darüber hinaus müssen und sollten Mitgliedsstaaten in ihrem Hoheitsgebiet ansässige (nicht-staatliche) Streitbeilegungsstellen auf Antrag zulassen,[22] wofür ein entsprechendes Verfahren benötigt wird.

In jedem Fall könnte die EU-KOM eine Musterverfahrungsordnung für solche Stellen entwickeln.

[17] ErwG. 52 S. 3.
[18] Art. 10 (12)
[19] ErwG. 55
[20] Art. 10 (9) S. 1
[21] Art. 10 (2)
[22] Art. 10 (5)

Bitkom vertritt mehr als 2.000 Mitgliedsunternehmen aus der digitalen Wirtschaft. Sie erzielen allein mit IT- und Telekommunikationsleistungen jährlich Umsätze von 190 Milliarden Euro, darunter Exporte in Höhe von 50 Milliarden Euro. Die Bitkom-Mitglieder beschäftigen in Deutschland mehr als 2 Millionen Mitarbeiterinnen und Mitarbeiter. Zu den Mitgliedern zählen mehr als 1.000 Mittelständler, über 500 Startups und nahezu alle Global Player. Sie bieten Software, IT-Services, Telekommunikations- oder Internetdienste an, stellen Geräte und Bauteile her, sind im Bereich der digitalen Medien tätig oder in anderer Weise Teil der digitalen Wirtschaft. 80 Prozent der Unternehmen haben ihren Hauptsitz in Deutschland, jeweils 8 Prozent kommen aus Europa und den USA, 4 Prozent aus anderen Regionen. Bitkom fördert und treibt die digitale Transformation der deutschen Wirtschaft und setzt sich für eine breite gesellschaftliche Teilhabe an den digitalen Entwicklungen ein. Ziel ist es, Deutschland zu einem weltweit führenden Digitalstandort zu machen.

Herausgeber
Bitkom e.V.
Albrechtstr. 10 | 10117 Berlin

Ansprechpartner
David Schönwerth | Bereichsleiter Data Economy
T 030 27576-179 | d.schoenwerth@bitkom.org

Verantwortliches Bitkom-Gremium
AK Datenpolitik & Datenräume

Version 1.1 vom 22.05.2024