HDE Handelsverband Deutschland

# Stellungnahme

zum EU-Verordnungsvorschlag für ein EU-Datengesetz (Data Act) COM(2022) 68 final

Stand: 26. August 2022
[EU-Transparenzregisternummer: 31200871765-41]

# 1. Hintergrund

Der Handelsverband Deutschland (HDE) ist seit über 100 Jahren die Spitzenorganisation des deutschen Einzelhandels – des drittgrößten Wirtschaftszweigs in Deutschland – mit insgesamt drei Millionen Beschäftigten und gut 535 Milliarden Euro Jahresumsatz. Er vertritt die Belange und Interessen von rund 300.000 Einzelhandelsunternehmen – aller Branchen, Standorte und Betriebsgrößen. Bei 50 Millionen Kundenkontakten täglich versorgt der Einzelhandel seine Kunden mit der kompletten Bandbreite an Produkten – über alle Vertriebskanäle.

Die EU-Kommission hat am 23. Februar 2022 einen umfassenden Vorschlag für ein Datengesetz (Data Act) vorgelegt. Ziel dieses Vorschlags ist es laut EU-Kommission, für Fairness im digitalen Umfeld sorgen, einen wettbewerbsfähigen Datenmarkt zu fördern, Chancen für datengesteuerte Innovationen eröffnen und Daten für alle zugänglicher machen. Das Datengesetz soll somit Maßnahmen zur Schaffung einer gerechten Datenwirtschaft implementieren, etwa indem geregelt wird, wer die in den Wirtschaftssektoren in der EU erzeugten Daten nutzen darf und Zugriff darauf hat. Es soll dadurch ein ausgewogenes Verhältnis zwischen dem Recht auf Zugang zu Daten und Anreizen für Investitionen in Daten erreicht werden, ohne die geltenden Datenschutzvorschriften zu ändern.

Dieser letzte horizontale Baustein der Datenstrategie der Kommission soll eine Schlüsselrolle beim digitalen Wandel und der Verwirklichung der digitalen Ziele für 2030 spielen.

# 2. Position des HDE

Der Vorschlag für das Datengesetz beinhaltet eine Vielzahl verschiedener Maßnahmen. So wird unter anderem der Zugang zu und die Nutzung von Daten geregelt und zwar auch zwischen Unternehmen untereinander sowie zwischen Unternehmen und Behörden. Ebenso sind Regelungen für den Datenzugang von Nutzern zu den von ihren vernetzten Geräten erzeugten Daten, sowie für deren Weitergabe an Dritte enthalten. Des Weiteren enthält das Datengesetz einen Fairnesstest für Vertragsklauseln zum Datenaustausch, durch welchen bestimmte Klauseln in diesem Bereich als unfair verboten werden. Ebenso sind in dem Vorschlag unverbindliche Mustervertragsbedingungen für den Zugang zu und die Nutzung von Daten vorgesehen.

Grundsätzlich unterstützt der HDE das Ziel einer gerechteren Datenwirtschaft. Jedoch sind einige geplante Vorschriften in dem Kommissionsvorschlag als zu weitreichend zu bewerten. Zwar betrifft das Datenzugangsrecht für Nutzer von Produkten primär die Herstellerseite, jedoch sehen wir daneben noch weitere Elemente, welche aus Sicht des Handels besonders kritisch sind. So enthält der Vorschlag etwa einige Ansätze, welche sehr weit in die unternehmerische Freiheit eingreifen.



**Handelsverband Deutschland (HDE) e. V.**

Isabelle Kobinger | Referentin | E-Mail: kobinger.europa@hde.de
Avenue des Nerviens 85 | B-1040 Brüssel | Telefon: +32 (0) 2 737 03 75

**www.einzelhandel.de**

## I. Anwendungsbereich und Definitionen (Art.1 & 2)

Der Anwendungsbereich und die Definitionen werden in Art. 1 und 2 des Vorschlags für ein Datengesetz geregelt.

Dabei ist der Anwendungsbereich in der jetzigen Form als zu weit gefasst zu bewerten. Dieser soll etwa nach Art. 1 sämtliche Branchen umfassen, ohne dass in dem Datengesetz branchenspezifische Unterschiede berücksichtigt werden sollen. Das Recht auf Datenzugang ist kein Selbstzweck - unabhängig vom betroffenen Sektor. Während es in einigen Sektoren wettbewerbsfördernd sein kann, kann es in anderen Sektoren andere (negative) Folgen für den Wettbewerb haben.

Die Definitionen in dem Kommissionsvorschlag sind vorliegend ebenso zu weit und zudem unklar formuliert. Im Einzelnen zeigt sich dies vor allem bei den folgenden Begriffen, welche grundsätzlich durch ihre weite und ungenaue Formulierung in ihre Anwendung einige Rechtsunsicherheiten mit sich bringen können.

### 1) Definition „Daten“

Unter Daten soll jede digitale Darstellung von Handlungen, Tatsachen oder Informationen und jede Zusammenstellung solcher Handlungen, Tatsachen oder Informationen, auch in Form von Ton-, Bild- oder audiovisuellen Aufzeichnungen fallen.

Diese Definition ist vorliegend viel zu weit und unklar gefasst. So ist nicht eindeutig klar welche Art von Daten betroffen ist, und wie bestimmte Daten, beispielweise nutzergenerierte und produkterzeugte Daten, voneinander unterschieden werden sollen. Dies führt mit dazu, dass es an anderen Stellen im Kommissionstext zu Unklarheiten und Widersprüchlichkeiten bei der Frage kommt, welche Daten von den Vorschriften umfasst sein sollen. So räumt der erste Teil des Vorschlags den Nutzern etwa das Recht auf Zugang zu den von angeschlossenen Geräten erzeugten IoT-Daten ein. Dies steht dabei im Widerspruch zu den Bestimmungen über Daten zwischen Unternehmen und Behörden und dem Kapitel über den internationalen Datentransfer und -zugang, wo alle Arten von Unternehmensdaten in den Anwendungsbereich des Vorschlags zu fallen scheinen.

### 2) Definition „Produkte“

Zudem ist auch die Definition des Begriffs „Produkt“ im Kommissionsvorschlag kritisch zu bewerten. Dieser definiert als Produkt sämtliche körperliche bewegliche Gegenstände, die auch in einem unbeweglichen Gegenstand enthalten sein können, welche Daten über ihre Nutzung oder Umgebung erlangen, erzeugen oder sammeln und Daten über einen öffentlich zugänglichen elektronischen Kommunikationsdienst übermitteln können und deren Hauptfunktion nicht die Speicherung und Verarbeitung von Daten ist. Mit dieser Formulierung will die Kommission sogenannte IoT-Produkte abdecken.



**Handelsverband Deutschland (HDE) e. V.**

Isabelle Kobinger | Referentin | E-Mail: kobinger.europa@hde.de
Avenue des Nerviens 85 | B-1040 Brüssel | Telefon: +32 (0) 2 737 03 75

**www.einzelhandel.de**

Diese sehr weit gefasste Definition birgt für die Anwendung in der Praxis einige Rechtsunsicherheiten. Es ist nicht klar erkennbar, welche Produkte und Dienstleistungen genau dadurch abgedeckt werden sollen. Dies birgt somit das Risiko, etwa Zahlungssysteme, welche beispielsweise durch ein Kundentreuesystem und eine App funktionieren, ebenfalls erfasst werden. Dies würde den Anwendungsbereich jedoch überproportional und unverhältnismäßig erweitern und es wäre mit dieser Situation für Betroffene der Verordnung gar nicht erkennbar, welche Produkte nun erfasst werden und welche nicht.

Um IoT-Produkte kohärent zu umfassen, sollte an dieser Stelle für die Definition des Begriffs „Produkt" vielmehr die Definition für intelligente Geräte von dem Bericht der EU-Kommission zu der Sektoruntersuchung zum Internet der Dinge (Internet of Things, IoT) für Verbraucher verwendet werden. Es sind auch diese Geräte, welche in der Praxis hauptsächlich Daten generieren, die etwa für Nutzer von Interesse sind. Diese Definition umfasst kabellose elektronische Geräte, wie zum Beispiel (am Körper) tragbare Geräte, intelligente Lautsprecher und andere intelligente Haushaltsgeräte, die mit anderen Geräten oder Netzen verbunden werden können, mit ihnen Daten austauschen können und in gewissem Umfang interaktiv und autonom arbeiten können. Diese Definition schließt intelligente Mobilgeräte (d. h. Smartphones und Tablets) nicht mit ein.[1]Die Verwendung dieser Definition, welche schließlich bereits von der EU-Kommission anerkannt und verwendet wurde, würde auch die Kohärenz im IoT- Bereich bestärken.

### 3) Definition „Nutzer"

Der Vorschlag der Kommission definiert einen Nutzer in Art. 2 Abs. 5 als eine natürliche oder juristische Person, die ein Produkt besitzt, mietet oder least oder eine Dienstleistung in Anspruch nimmt.

Wie bereits bei den zuvor genannten Definitionen ist auch bei dieser die Formulierung einiges an Unklarheiten enthalten. Hierdurch könnten in der Praxis weitreichende Rechtsunsicherheiten entstehen. So sind verschiedene Konstellationen denkbar, in welchen mehrere juristische wie natürliche Personen unter diese Definition als Nutzer fallen könnten, so dass es für einen Dateninhaber gar nicht absehbar wäre, wer alles als „Nutzer" Ansprüche nach dem Datengesetz geltend machen kann. Dies könnte im schlimmsten Fall dazu führen, dass die Dateninhaber einer hohen Anzahl an „Nutzern" die Daten unter den Voraussetzungen des Datengesetzes zur Verfügung stellen müssten, und diesen Anfragen in der Praxis kaum nachkommen könnten, obwohl sie verpflichtet wären, dies unverzüglich zu erledigen. Dies wäre aber in der Praxi dann sehr wahrscheinlich jedoch nicht umsetzbar.

An dieser Stelle braucht es eine klarere und engere Definition, welche den Begriff des Nutzers klar abgrenzt.

[1] https://ec.europa.eu/competition-policy/system/files/2022-01/internet-of-things_final_report_2022_de.pdf



**Handelsverband Deutschland (HDE) e. V.**

Isabelle Kobinger | Referentin | E-Mail: kobinger.europa@hde.de
Avenue des Nerviens 85 | B-1040 Brüssel | Telefon: +32 (0) 2 737 03 75

**www.einzelhandel.de**

## II. Datenzugangsrechte und Schutzmechanismen:

In Kapitel II, Art. 3 bis 7, wird die Datenweitergabe von Unternehmen an Verbraucher und zwischen Unternehmen geregelt. Dabei wird festgeschrieben, wann ein Dateninhaber Zugang zu Daten gewähren muss. Dabei sollen laut Art. 3 Produkte so konzipiert und hergestellt werden, dass Daten, die durch ihre Nutzung generiert werden, einfach zugänglich sind.

Von diesen Regelungen ist in Art. 7 allerdings eine Ausnahme für KMU festgeschrieben, welche an dieser Stelle zu begrüßen ist.

### 1) Datenzugang:

Auf Anfrage eines Nutzers soll jeder Dateninhaber diesem kostenlos und unverzüglich jene Daten zur Verfügung stellen, die durch seine Nutzung eines Produkts oder eines damit verbundenen Dienstes generiert wurden (Art. 4). Der Begriff des Produkts wird dabei wie folgt definiert: Sämtliche körperliche bewegliche Gegenstände, die auch in einem unbeweglichen Gegenstand enthalten sein können, welche Daten über ihre Nutzung oder Umgebung erlangen, erzeugen oder sammeln und Daten über einen öffentlich zugänglichen elektronischen Kommunikationsdienst übermitteln können und deren Hauptfunktion nicht die Speicherung und Verarbeitung von Daten ist.

Damit betrifft dieses Datenzugangsrecht sämtliche Daten, die mit einem solchen Produkt bzw. mit einem verwandten Dienst generiert wurden, ohne dabei Unterscheidungen zu treffen. Ein „Nutzer“ kann hierbei, wie bereits angemerkt, sowohl eine natürliche als auch eine juristische Person sein. Diese sollen nach Art. 5 auch verfügen können, dass ihre mit dem Produkt generierten Daten vom Dateninhaber kostenlos mit einem Dritten geteilt werden und dies ohne unangemessene Verzögerung, unentgeltlich und in der gleichen Qualität, wie sie dem Dateninhaber zur Verfügung stehen. So könnte ein Autobesitzer z.B. verlangen, dass die vom Wagen generierten Daten nicht nur dem Hersteller, sondern auch einem unabhängigen Reparaturdienst oder seiner Versicherung zur Verfügung stehen. Unternehmen, die zentrale Plattformdienste erbringen, für die einer oder mehrere dieser Dienste als Gatekeeper gemäß dem DMA benannt wurden, sollen allerdings nicht als geeignete Dritte im Sinne dieses Artikels gelten.

Es sollte ebenfalls geprüft werden, ob die Bestimmungen nicht indirekt auch die Wahlmöglichkeiten des Nutzers in Bezug auf die Nutzung von Daten und Diensten einschränken könnten, was zu Lock-in-Effekten führen könnte. Diese würden den Zielen des Datengesetzes und des Datenschutzgesetzes zuwiderlaufen. Letztlich könnte so die Gefahr bestehen, dass das Recht des Nutzers, ein Produkt oder einen Dienst seiner Wahl zu nutzen, eingeschränkt wird und in einigen Fällen Innovationen behindert werden.



**Handelsverband Deutschland (HDE) e. V.**

Isabelle Kobinger | Referentin | E-Mail: kobinger.europa@hde.de
Avenue des Nerviens 85 | B-1040 Brüssel | Telefon: +32 (0) 2 737 03 75

**www.einzelhandel.de**

In seiner jetzigen Form ist dieses Recht auf Zugang zu Daten zu weit gefasst. Ein solches Recht kann zwar in einigen Sektoren wettbewerbsfördernd sein, jedoch kann es ebenso in anderen Sektoren andere, gegebenenfalls negative, Folgen für den Wettbewerb haben. Wir lehnen ein in dieser Form ausgestaltete Verpflichtung für eine kostenlose Gewährung des Datenzugangs ab.

Vielmehr sollte anstelle einer Pflicht mehr Anreize geschaffen werden, welche die Unternehmen dazu ermutigen, Daten weiterhin freiwillig und verantwortungsvoll zu teilen. Zu diesem Zweck sollte das Datengesetz nach unserer Ansicht auf den bereits bestehenden bewährten Praktiken für die gemeinsame Nutzung von Daten aufbauen, um die Bedingungen festzulegen, unter denen Unternehmen beispielsweise freiwillig Daten mit anderen Unternehmen im Rahmen eines bestimmten Governance-Modells teilen können. Es ist von entscheidender Bedeutung, dass die Unternehmen die Freiheit behalten, das Governance-Modell und die Technologie zu wählen, die am besten zu ihnen passen. Unternehmen, die daran interessiert sind, ihre Daten zur Verfügung zu stellen und/oder auf die Daten anderer zuzugreifen, sollten zu praktischen Instrumenten ermutigt werden, z. B. zu freiwilligen Musterverträgen, die auf den einschlägigen EU-Rechtsvorschriften beruhen, darunter Vorschriften zum Datenschutz und zu Privatsphäre, Sicherheit, Rechten an geistigem Eigentum, Datenbankrechten und Geschäftsgeheimnissen. Sollte diese Pflicht zur Gewährung des Zugangs zu Daten, welche durch die Nutzung eines Produkts oder eines damit verbundenen Dienstes generiert wurden, dennoch bestehen bleiben, so müsste dieser Zugang genauer konkretisiert und enger umfasst werden. So sollten nicht die Daten von allen Produkten und der damit verbundenen Dienste unter dieses Zugangsrecht fallen. Der Begriff Produkt ist in dem Vorschlag, wie bereits ausgeführt, sehr weit gefasst. Vielmehr sollte an dieser Stelle für die Definition des Begriffs „Produkt“ die bereits erwähnte Definition für intelligente Geräte von dem Bericht der EU-Kommission zu der Sektoruntersuchung zum Internet der Dinge (Internet of Things, IoT) für Verbraucher verwendet werden. Denn es sind diese Geräte, welche in der Praxis in der Hauptsache Daten generieren die etwa für Nutzer interessant sind.[2]

## 2) Unterscheidung zwischen verschiedenen Daten:

Der Vorschlag der Kommission enthält auch Unklarheiten in Bezug auf die Art von Daten, zu welchen ein Zugangsrecht bestehen soll. So wurde bei dem Begriff der Daten keine Unterscheidung zwischen unverarbeiteten und verarbeiteten Daten getroffen. Verarbeitete Daten werden als ein Produkt betrachtet, das Unternehmen anbieten können. Sie stellen somit ein Produkt wie jedes andere dar, welches Zeit und Fähigkeiten erfordert und seine Kosten hat. Unverarbeitete Daten haben einen geringeren Wert (bis sie verarbeitet werden), während verarbeitete Daten Zeit und Mühe benötigen, um zu einem wertvollen Produkt zu werden, was mit sehr hohen Kosten verbunden ist.

Daher sollte hier eine klare Unterscheidung im Datengesetz getroffen werden. Bei einem Zugang zu verarbeiteten Daten sollte etwa der Preis mindestens so hoch sein wie die Kosten für die Verarbeitung

[2] https://ec.europa.eu/competition-policy/system/files/2022-01/internet-of-things_final_report_2022_de.pdf



**Handelsverband Deutschland (HDE) e. V.**

Isabelle Kobinger | Referentin | E-Mail: kobinger.europa@hde.de
Avenue des Nerviens 85 | B-1040 Brüssel | Telefon: +32 (0) 2 737 03 75

**www.einzelhandel.de**

der Daten; die Prozesskosten müssen gedeckt werden. Sie sind ein Produkt, das wie jedes andere auch einen Wert hat.

### 3) Schutzmechanismen für die Offenbarung von Geschäftsgeheimnissen:

Ebenfalls werden in Kapitel II die Mechanismen zum Schutz von Geschäftsgeheimnissen des Dateninhabers bei Gewährung eines Datenzugangs festgeschrieben. Nach Art. 4 Nr. 3 dürfen Geschäftsgeheimnisse nur offenbart werden, wenn alle erforderlichen spezifischen Maßnahmen zur Wahrung der Vertraulichkeit von diesen, insbesondere gegenüber Dritten, getroffen werden. Der Dateninhaber und der Nutzer können Maßnahmen zur Wahrung der Vertraulichkeit der gemeinsam genutzten Daten, insbesondere gegenüber Dritten, vereinbaren. Nach Art. 5 Nr. 8 dürfen Geschäftsgeheimnisse nur insoweit an Dritte weitergegeben werden, als dies zur Erfüllung des zwischen dem Nutzer und einem Dritten vereinbarten Zwecks unbedingt erforderlich ist und der Dritte alle zwischen dem Dateninhaber und dem Dritten vereinbarten spezifischen erforderlichen Maßnahmen zur Wahrung der Vertraulichkeit des Geschäftsgeheimnisses ergreift. In einem solchen Fall soll die Charakterisierung der Daten als Geschäftsgeheimnis und die Maßnahmen zur Wahrung der Vertraulichkeit in der Vereinbarung zwischen dem Dateninhaber und dem Dritten festgelegt werden.

Diese Vorgaben zum Schutz von Geschäftsgeheimnissen sind vorliegend unzureichend. Sie sind zu ungenau formuliert und bringen somit ein hohes Maß an Rechtsunsicherheit mit sich. Der Dateninhaber kann nicht überprüfen, ob ein Nutzer tatsächlich alle "spezifischen erforderlichen Maßnahmen zur Wahrung des Geschäftsgeheimnisses" ergriffen hat. Was von diesen Maßnahmen umfasst sein soll oder gar erfasst sein muss, wird in dem Vorschlag auch nicht ausgeführt oder definiert. Diese Schutzmechanismen sind nicht einheitlich im Text definiert und somit in der Praxis kaum nachprüfbar. An dieser Stelle bräuchte es jedoch vielmehr klare, strenge und durchsetzbare Schutzmaßnahmen, durch welche ein sorgfältiger Schutz von Geschäftsgeheimnissen gewährleistet werden kann und welche auch dafür Sorge tragen, dass das Recht an geistigem Eigentum respektiert wird.

Es sollte außerdem geklärt werden, wer alles genau Zugang zu den Daten als sogenannter Dritter erhalten kann. Dies ist vorliegend nicht ausreichend geregelt, da etwa unter den Begriff des Dritten theoretisch eine Vielzahl an juristischen und natürlichen Personen fallen könnte.

### 4) Schutzmechanismen für die Nutzung von Daten:

In Art. 4 Nr. 4 ist geregelt, dass der Nutzer die aufgrund eines Antrags nach Art. 4 Nr. 1 erhaltenen Daten nicht zur Entwicklung eines Produkts verwenden darf, das mit dem Produkt, von dem die Daten stammen, konkurriert. Gemäß Art. 5 & 6 dürfen Dritte keine Zwangsmittel einsetzen oder offensichtliche Lücken in der technischen Infrastruktur des Dateninhabers zum Schutz der Daten missbrauchen, um Zugang zu den Daten zu erhalten. Des Weiteren dürfen sie diese Daten auch nicht anderen in



**Handelsverband Deutschland (HDE) e. V.**

Isabelle Kobinger | Referentin | E-Mail: kobinger.europa@hde.de
Avenue des Nerviens 85 | B-1040 Brüssel | Telefon: +32 (0) 2 737 03 75

**www.einzelhandel.de**

dieser Form zur Verfügung stellen oder die erhaltenen Daten verwenden, um ein Produkt zu entwickeln, das mit dem Produkt konkurriert, von dem die abgerufenen Daten stammen, oder die Daten zu diesem Zweck mit einem anderen Dritten teilen.

Die hier vom Datengesetz vorgesehenen Mechanismen zum Schutz der Daten sind in ihrem Ansatz sinnvoll, jedoch, zu schwach ausgestaltet und zu ungenau formuliert. Wie bei den Schutzmechanismen für Geschäftsgeheimnisse bringen sie somit ein hohes Maß an Rechtsunsicherheit mit sich. Das Verbot, mit den abgerufenen Daten ein Konkurrenzprodukt zu entwickeln, ist ein Papiertiger, der in der Praxis nicht durchsetzbar ist.

Der Schutz von weitergegebenen oder verkauften Daten muss gewährleistet sein und durch effektive und strenge Schutzvorschriften abgesichert werden.

## III. Vorgaben für Vertragsklauseln zum Datenaustausch (Art. 13):

In dem Vorschlag für ein Datengesetz werden auch Regelungen für Klauseln bei Verträgen zum Austausch von Daten festgelegt. So soll bei vertraglichen Vereinbarungen über den Zugang zu und die Nutzung von Daten ein vermeintliches Ungleichgewicht der Verhandlungsmacht zwischen Vertragsparteien nicht ausgenutzt werden können. Daher werden in Art. 13 für Situationen, in denen eine datenbezogene Vertragsklausel einseitig von einer Partei einem KMU auferlegt wird, bestimmte Klauseln als unfair verboten. Eine Vertragsklausel gilt dabei als einseitig auferlegt, wenn sie von einer Vertragspartei eingebracht wurde und die andere Vertragspartei trotz eines Verhandlungsversuchs nicht in der Lage war, ihren Inhalt zu beeinflussen.

Dazu umfasst Art. 13 eine allgemeine Bestimmung der Missbräuchlichkeit einer mit der gemeinsamen Nutzung von Daten zusammenhängenden Vertragsklausel, welche besagt, dass eine Vertragsklausel missbräuchlich ist, wenn sie so beschaffen ist, dass ihre Verwendung in grober Weise von der guten Geschäftspraxis beim Zugang zu Daten und ihrer Nutzung abweicht und gegen Treu und Glauben sowie gegen die guten Geschäftsgebaren läuft. Diese Bestimmung wird zudem durch zwei Listen von Klauseln ergänzt: Bei der ersten Liste gelten die dort genannten Klauseln immer als missbräuchlich, bei der zweiten Liste besteht eine mutmaßliche Missbräuchlichkeit.

Wie bei letzterem diese „mutmaßliche Missbräuchlichkeit“ gehandhabt wird oder wann sie genau eintritt, erläutert der Entwurf dabei nicht. Da auch zwischen dieser Liste und der Liste, bei welcher die Klauseln immer als missbräuchlich gelten, keine weitere Unterscheidung getroffen wird stellt sich die Frage, ob es sich um eine graue Liste, neben einer schwarzen Liste handeln soll? Jedoch sind für diese Liste weder ihre Funktionsweise noch die Frage, wann genau diese Klauseln als missbräuchlich feststehen und dies nicht mehr nur vermutet wird, geregelt.

Diese Vorgabe würde somit zu erheblichen Problemen bei einer Umsetzung in der Praxis führen, da hier ein hohes Maß an Rechtsunsicherheit gegeben ist. Sollten diese Listen bestehen bleiben so muss



**Handelsverband Deutschland (HDE) e. V.**

Isabelle Kobinger | Referentin | E-Mail: kobinger.europa@hde.de
Avenue des Nerviens 85 | B-1040 Brüssel | Telefon: +32 (0) 2 737 03 75

**www.einzelhandel.de**

die Unterscheidung zwischen ihnen klar im Gesetzestext festgelegt werden, sowie auch die Frage eindeutig geklärt werden muss, wie bei mutmaßlich missbräuchlichen Klauseln verfahren werden soll.

Des Weiteren fehlt es bei der in Kapitel IV enthaltenen Regelung zu missbräuchlichen Klauseln in Bezug auf Datenzugang und -nutzung zwischen Unternehmen an für die Praxis wichtigen Differenzierungen. Dort werden sehr allgemeine Grundsätze zu Vertragsklauseln, welche KMUs im Zusammenhang mit dem Zugang zu und der Nutzung von Daten bzw. dem Datenaustausch auferlegt werden, geregelt. Wie schon angeführt wirkt dieses Kapitel somit direkt auf Verträge sowie Vertragsgestaltungen gegenüber KMUs, wenn ein Zugang zu Daten beinhaltet ist. Zudem tragen Vertragspartner der KMU die Beweislast dafür, dass ihre Klauseln nicht missbräuchlich sind und dass diese nicht einseitig auferlegt wurden. Dies schafft eine Vermutung, der Widerlegung sich in der Praxis sehr schwer und aufwendig gestalten könnte, selbst wenn sie nicht zutreffend ist. Gemeinsam mit den bereits beschriebenen Unklarheiten, welche bei dieser vorgeschlagenen Regelung für Vertragsklauseln herrschen, sorgt dies insgesamt für eine unverhältnismäßige Belastung von Unternehmen in diesem Bereich.

Diese Regelungen zu Vertragsklauseln könnten auch weitreichende Folgen für Verbundunternehmen haben, wenn etwa Daten selbständigen Einzelhändlern, sofern diese als KMU einzustufen sind, zur Verfügung gestellt werden. Die in Verbundunternehmen bestehenden Verträge und Abläufe scheinen jedoch nicht das intendierte Ziel dieser Vorgaben zu sein. Nach den Erwägungsgründen (Erwägungsgründe 51&52) soll hier wohl vielmehr die „klassische“ Situation in B2B-Beziehungen erfasst werden: Demnach sollen die Fälle umschlossen werden, in welchen KMUs mit anderen Unternehmen einen Vertrag aushandeln, welcher den Zugang von Daten beinhaltet, wobei bei der anderen Vertragspartei eine stärkere Verhandlungsposition vorliegend sei; somit also Verträge und Vertragsverhandlungen zwischen Unternehmen welche als eigenständige und vollkommen voneinander unabhängige Vertragsparteien zusammenkommen und damit unterschiedliche Voraussetzungen in die Verhandlungen mitbringen. Dadurch scheint die Konstellation der Verbundunternehmen hier nicht Ziel der Vorschrift zu sein, so dass diese folglich von dieser Vorgabe ausgenommen werden sollten, um deren Anwendungsbereich nicht unverhältnismäßig auszudehnen.

## IV. Datenzugangsrecht für öffentliche Stellen (Art. 14 & 15):

In Art. 14 wird geregelt, dass ein Dateninhaber auf Antrag einer öffentlichen Stelle oder einem Organ, einer Agentur oder einer Einrichtung der Union, die ein außergewöhnliches Bedürfnis für die Verwendung der angeforderten Daten nachweisen kann, seine Daten zur Verfügung stellen soll. Dabei kann ein außergewöhnliches Bedürfnis nach Art. 15 nicht nur vorliegen, wenn die angeforderten Daten erforderlich sind, um auf eine öffentliche Notlage zu reagieren oder wenn die angeforderten Daten zeitlich und vom Umfang her begrenzt sind und zur Verhinderung oder zur Unterstützung bei der Bewältigung eines öffentlichen Notstands erforderlich sind. Vielmehr kann gemäß Art. 15 (c) dieses Bedürfnis bereits bestehen, wenn das Fehlen verfügbarer Daten die vorgenannten Stellen daran hindert, eine bestimmte Aufgabe im öffentlichen Interesse zu erfüllen, welche ausdrücklich gesetzlich



**Handelsverband Deutschland (HDE) e. V.**

Isabelle Kobinger | Referentin | E-Mail: kobinger.europa@hde.de
Avenue des Nerviens 85 | B-1040 Brüssel | Telefon: +32 (0) 2 737 03 75

**www.einzelhandel.de**

vorgesehen ist und sie nicht in der Lage war, die Daten auf anderem Wege zu erhalten. Grundsätzlich sollen die Daten „unverzüglich“ (Art. 18) zur Verfügung gestellt werden. Bei Vorliegen einer öffentlichen Notlage (Art. 15 (a)) müssen die Daten der öffentlichen Stelle auch kostenlos (Art. 20) bereitgestellt werden. Ausgenohmen von diesen Vorgaben sind lediglich KMUs.

Die hier geschaffene Ausnahme für kleine und mittlere Unternehmen ist zwar zu begrüßen, dennoch ist dieses Zugangsrecht für öffentliche Stellen viel zu weit gefasst. Die hier beschriebenen Voraussetzungen für ein außergewöhnliches Bedürfnis sind zu ungenau und zu umfassend gehalten. Auf diesem Weg könnten eine Vielzahl von Situationen darunter definiert werden, die nichts mit einer öffentlichen Notlage zu tun haben. Dadurch sind die Voraussetzungen für den Zugang öffentlicher Stellen zu Daten viel zu niedrig angesetzt und bei weitem nicht auf Notlagen begrenzt.

Wir erkennen an, dass es sinnvoll ist, bestimmte Daten mit öffentlichen Stellen zu teilen, um öffentliche Interessen zu verfolgen, wenn dies angebracht ist. In den meisten Fällen, in denen es keine sektorspezifischen Rechtsvorschriften gibt, mag der Zugang öffentlicher Stellen zu Unternehmensdaten zwar praktisch sein, ist aber nicht notwendig, damit die Behörden ihre Arbeit erledigen können. Aus diesem Grund sind wir der Meinung, dass das Datengesetz freiwillige Partnerschaften fördern und keine obligatorischen Bestimmungen für den Datenaustausch zwischen Unternehmen und Behörden einführen sollte. So tauscht unser Sektor tauscht bereits Daten mit Behörden aus, um gesetzlichen Verpflichtungen (Rückverfolgbarkeit, Registrierung von chemischen Stoffen) oder staatlichen Anforderungen (Statistiken, Steuerzwecke) nachzukommen.

Die hier vorgeschlagene Verpflichtung für einen Datenzugang erinnert in dieser Form an das 2017 vorgeschlagene Binnenmarkt-Informationstool (Single Market Information Tool - SMIT). Dieses sollte es ermöglichen, Marktinformationen direkt von Unternehmen abzufordern. Viele Kritikpunkte sind zwischen dem SMIT und der hier geplanten Verpflichtung ähnlich. Der Vorschlag für ein Binnenmarkt-Informationstool wurde schlussendlich aus guten und immer noch validen Gründen zurückgenommen; es sollte daher vermieden werden durch den Vorschlag für ein Datengesetz einen neuen Versuch zu starten, einen so stark damit vergleichbaren Mechanismus einzuführen.

Sollte die Kommission dennoch die Einführung neuer Vorschriften für den obligatorischen Datenzugang in Erwägung ziehen, sollte das Datengesetz klare und umfassende Bedingungen festlegen, unter welchen öffentliche Stellen Zugang zu Daten beantragen können, die sich im Besitz von Unternehmen befinden und von diesen kontrolliert werden. Dabei müssen die "öffentlichen Interessen", für die Unternehmensdaten angefordert werden können, konkret und eindeutig definiert werden. Der Zugang öffentlicher Stellen zu Daten sollte zielgerichtet und verhältnismäßig ausgestaltet sein. Er sollte sich dabei an Unternehmen richten, die eine wirksame Kontrolle über die Daten haben und einem unabhängigen Überprüfungsverfahren unterliegen. Des Weiteren müssten für einen solchen Zugang angemessene und eindeutige Schutzmaßnahmen wie Zweckbindung, klare Aufbewahrungsrichtlinien sowie technische Maßnahmen zum Schutz der Datenintegrität, der Privatsphäre, des Datenschutzes und der Datensicherheit gelten.



**Handelsverband Deutschland (HDE) e. V.**

Isabelle Kobinger | Referentin | E-Mail: kobinger.europa@hde.de
Avenue des Nerviens 85 | B-1040 Brüssel | Telefon: +32 (0) 2 737 03 75

**www.einzelhandel.de**

### V. Durchsetzung (Art. 31)

Gemäß Art. 31 des Kommissionsvorschlags soll jeder Mitgliedstaat eine oder mehrere zuständige Behörden benennen, die für die Anwendung und Durchsetzung dieser Verordnung verantwortlich sind. Die Mitgliedstaaten können eine oder mehrere neue Behörden einrichten oder auf bestehende Behörden zurückgreifen.

Warum die Durchsetzung des Datenschutzgesetzes, auf verschiedene Regulierungsbehörden aufgeteilt und den einzelnen Mitgliedstaaten überlassen wird ist vorliegend nicht nachvollziehbar. Die Durchsetzung schließt hier auch die Verhängung von Geldbußen bei Nichteinhaltung ein. Durch dieses dezentralisierte System, welches es den Mitgliedstaaten überlässt, die Vorschriften durchzusetzen, besteht ein sehr hohes Risiko, dass dies zu unterschiedlichen Praktiken in der EU führen. Es ist nicht klar, wie dies mit dem Ziel der Schaffung eines harmonisierten Rechtsrahmens auf der Grundlage von Artikel 114 des AEU-Vertrags vereinbar ist.

## 3. Fazit

Der HDE unterstützt Ziele wie die Förderung eines wettbewerbsfähigen Datenmarkts und mehr Fairness im digitalen Umfeld. Die in dem Vorschlag der Kommission getroffenen Ausnahmen für KMU sind ebenfalls zu begrüßen. Insgesamt lässt sich jedoch feststellen, dass der Vorschlag mit einigen seiner Vorgaben zu weit in die unternehmerische Freiheit eingreift. Datenzugangs- und Informationspflichten, Einschränkungen der Vertragsfreiheit, Anforderungen an die technische Ausgestaltung: Solche gesetzgeberischen Eingriffe sind nur dann zu rechtfertigen, wenn es ohne diese Maßnahmen zu Marktverzerrungen käme. Dies ist im Einzelhandel jedoch nicht der Fall. Hier hat die bisherige Praxis deutlich gezeigt, dass die beteiligten Parteien im Rahmen der Vertragsfreiheit ein für alle Seiten faires und wirtschaftlich sinnvolles Verhandlungsergebnis finden können. Die vorgeschlagenen Regelungen sind daher für unsere Branche weder notwendig noch zielführend. Hier ist zu befürchten, dass Regelungsansätze zu sehr in gut funktionierende Datenbeziehungen eingreifen und zu Unsicherheiten und Belastungen für innovative Unternehmen führen. So könnten etwa neue Zwänge, die vorschreiben, wann und wie Unternehmen Daten weitergeben oder wiederverwenden sollten, Markttrends in Richtung gemeinsamer Datennutzung und datengesteuerter Innovation im Keim ersticken. Dies könnte der Fall sein, wenn bestimmte einseitige Vertragsklauseln verboten würden, unabhängig davon, ob die Daten für den Markteintritt oder den Wettbewerb auf dem Markt unerlässlich sind oder ob Wettbewerbsinstrumente bereits Abhilfe schaffen können. Vor allem sollten neue Regeln für die gemeinsame Nutzung von Daten immer pragmatisch sein, sich an dem orientieren, was technisch machbar und wirtschaftlich tragfähig ist, und mit sich überschneidenden Rechtsvorschriften, insbesondere der allgemeinen Datenschutzverordnung, im Einklang stehen.



**Handelsverband Deutschland (HDE) e. V.**

Isabelle Kobinger | Referentin | E-Mail: kobinger.europa@hde.de
Avenue des Nerviens 85 | B-1040 Brüssel | Telefon: +32 (0) 2 737 03 75

**www.einzelhandel.de**