STELLUNGNAHME

Berlin, 13. Mai 2022

Deutscher Industrie- und Handelskammertag

Stellungnahme zum Vorschlag für eine Verordnung über harmonisierte Vorschriften für einen fairen Datenzugang und eine faire Datennutzung (Datengesetz)

Wir bedanken uns für die Gelegenheit zur Stellungnahme zu dem Entwurf für eine Verordnung über harmonisierte Vorschriften für einen fairen Datenzugang und eine faire Datennutzung (nachfolgend Data Act-E) der Europäischen Kommission.

Grundlage dieser Stellungnahme sind die dem DIHK bis zur Abgabe der Stellungnahme zugegangenen Äußerungen der IHKs sowie die wirtschaftspolitischen/europapolitischen Positionen des DIHK. Sollten dem DIHK noch weitere in dieser Stellungnahme noch nicht berücksichtigte relevante Äußerungen zugehen, wird der DIHK diese Stellungnahme entsprechend ergänzen.

A. Das Wichtigste in Kürze

Das Ziel der EU-Kommission, eine breitere Datennutzung industrieller Daten zu ermöglichen und das Potential für die langfristige Stärkung von Innovation und Wachstum zu nutzen, ist grundsätzlich zu unterstützen. Dafür benötigen Unternehmen verlässliche Rahmenbedingungen. Besonders mit Blick die Nutzung von Daten, an deren Entstehung mehrere Parteien mitgewirkt haben, bedarf es klarer und verständlicher Regeln, die es Unternehmen ermöglichen, rechtssicher ihre Geschäftsmodelle darauf aufzubauen. Daneben dürfen Unternehmen nicht durch Bürokratie und komplexe rechtliche Vorgaben überlastet werden.

Bei der Entscheidung über Zugangs- bzw. Nutzungsansprüche ist zu berücksichtigen, dass Daten ein wichtiger Wettbewerbsvorteil von vielen Unternehmen sind. Der Anreiz für Dateninhaber und Hersteller, datengetriebene Produkte, Dienstleistungen und Geschäftsmodelle zu entwickeln, muss erhalten bleiben. Ansonsten droht eine Abwanderung von IT- und Industriebetrieben und damit von Know-how ins Ausland. Gleichermaßen sollten Daten als Grundlage für die Entwicklung neuer Technologien und Dienstleistung in ausreichendem Maße zur Verfügung stehen. Insgesamt muss die Innovationsfähigkeit aller an der Datenwertschöpfungskette Beteiligten und der Schutz von sensiblen, wettbewerbsrelevante Informationen ausreichend gesichert werden. Dies gilt auch im Kontext mit weiteren im Data Act-E vorgesehene Regelungen, wie die Weiterverwendung von Daten des Privatsektors durch den öffentlichen Sektor, sowie den geplanten Vorschriften für Anbieter von Datenverarbeitungsdiensten.

DIHK | Deutscher Industrie- und Handelskammertag e.V.
Besucheranschrift: Breite Straße 29 | 10178 Berlin-Mitte | Postanschrift: DIHK | 11052 Berlin
Tel. 030-20308-0 | Fax 030-20308-1000 | Internet: www.dihk.de

Besonders wichtig ist aus Sicht der deutschen Wirtschaft daher:

- Klare, abgrenzbare Definitionen und Voraussetzungen für die Heraus- und Weitergabe zu schaffen, um Rechts- und Planungssicherheit zu erreichen.

- Zugangs- und Nutzungsrechte nicht exklusiv auf den Nutzer zu beschränken, um die berechtigten Interessen und die Innovationsfähigkeit aller Beteiligten zu gewährleisten.

- Ein hohes Schutzniveau für Geschäftsgeheimnisse und geistiges Eigentum sicherzustellen.

B. Relevanz für die deutsche Wirtschaft

Daten sind ein wichtiges Wirtschaftsgut und ein entscheidender Wettbewerbsfaktor für Unternehmen. Sie können nicht nur genutzt werden, um bestehende Prozesse im Betrieb zu optimieren, sondern dienen zunehmend dem reinen Geschäftsmodell von Unternehmen. Die Betriebe möchten die Potentiale aus Daten nutzen; stoßen dabei jedoch häufig auf Hindernisse. Eine Sonderauswertung der DIHK-Digitalisierungsumfrage (Februar 2022) unter ca. 4.300 Unternehmen zeigt, dass rechtliche Unsicherheiten für Deutschlands Unternehmen das größte Problem bei der stärkeren Nutzung von Daten sind. Danach fühlen sich 57 Prozent der Unternehmen durch datenschutzrechtliche Hemmnisse behindert, für weitere 38 Prozent der Unternehmen sind rechtliche Unklarheiten beispielsweise über Nutzungsansprüche ein Hindernis. Die Schaffung von Klarheit über Zugangs-, Nutzungs- und Weitergaberechte ist für die Unternehmen daher von großer Bedeutung.

Aus den Ergebnissen der Konsultation durch die IHKs und deren Mitgliedsunternehmen zu den Plänen eines Datengesetzes lässt sich ableiten, dass eine Vielzahl an Unternehmen Schwierigkeiten beim Zugang zu Daten hat. Dabei ergeben sich teilweise auch Ungleichgewichte bei den Vertragsverhandlungen zur Gewährung des Zugangs zu den Daten. Dies gilt insbesondere für kleinere Unternehmen, die aufgrund ihrer Marktstellung oftmals keine ander Wahl haben, als nicht verhandelbare Vertragspositionen zu akzeptieren. Vielmals wird schon auf technischer Ebene von großen Plattformen ein Zugang zu relevanten Daten vereitelt. Daraus lässt sich die Notwendigkeit der Schaffung eines ausgleichenden Ordnungsrahmens rechtfertigen.

Der Deutsche Industrie- und Handelskammertag (DIHK) vertritt die Interessen aller Unternehmen der deutschen gewerblichen Wirtschaft, einschließlich Hersteller, Produkt- und Softwareentwickler, Nutzer sowie Anbieter von Datenverarbeitungsdiensten. Um die Interessen aller an der Datenwertschöpfungskette beteiligten Akteure bestmöglich in Einklang zu bringen und die Innovationsfähigkeit der deutschen gewerblichen Wirtschaft insgesamt zu sichern, schlägt der DIHK folgende Nachbesserungen vor:

C. Im Einzelnen

Zu Kapitel I: Rollendefinition und Begriffsbestimmungen

Bei der Nutzung von vernetzten Geräten oder Maschinen fallen Daten an, die für unterschiedliche an der Datenwertschöpfungskette Beteiligte von Interesse sein können. Um klare und differenzierte

Regelungen für das Zusammenspiel der beteiligten Akteure zu schaffen und eine rechtssichere Ausgestaltung und Umsetzung einer Regulierung zu gewährleisten, sind zunächst trennscharfe Begriffsbestimmungen notwendig. Außerdem ist zu klären, wann und für welche Produkte der Data Act gelten soll. Da das geplante Gesetz die Breite der Wirtschaft betrifft, ist eine klare Ersichtlichkeit des Anwendungsbereich und eine eindeutige Zuordenbarkeit zu den beteiligten Akteuren von besonderer Bedeutung.

1. Anwendungsbereich/Produktbegriff

Nachgeschärft werden sollte zunächst am Anwendungsbereich der Verordnung. Sinnvoll ist es dabei, wie im vorliegenden Entwurf bereits vorgenommen, Geräte auszunehmen, die lediglich Inhalte anzeigen oder abspielen bzw. aufzeichnen und übertagen. Inkonsequent ist es jedoch, Smartphones und Tablets als solche Geräte zu verstehen und auszuschließen (vgl. Erwägungsgrund, nachfolgend ErwG 15). Diese und vergleichbare Geräte zeichnen sich gerade durch die Eigenschaft aus, Daten über ihre Umgebung zu erlangen und zu sammeln (vgl. ErwG 14), weshalb eine Bevorteilung gegenüber anderen vernetzen Produkten nicht verständlich ist. Die derzeit in ErwG 14 und ErwG 15 enthaltenen Positiv- und Negativbespiele sind grundsätzlich als Orientierungshilfe nützlich, in ihrer aktuellen Form allerdings nicht nachvollziehbar. Zweckmäßig könnte es sein, eine solche, nicht abschließende Liste als Hilfe für Unternehmen bei der Gestaltung von Dienstleistungen und Produkten in einem Annex zur Verordnung einzuführen und so auch deren Aktualität zu gewährleisten.

2. Nutzerbegriff

Der Data Act-E definiert einen Nutzer als *„eine natürliche oder juristische Person, die ein Produkt besitzt, mietet oder least oder eine Dienstleistung in Anspruch nimmt“* (Art. 2 Abs. 5). Daraus ergeben sich insbesondere in Konstellationen mit mittelbaren Besitzverhältnissen und längeren Besitz- bzw. Wertschöpfungsketten (z. B. Komponentenhersteller – Zulieferer – Hersteller – Nutzer) Unklarheiten bei der Nutzeridentifizierung. So ist es denkbar, dass eine Vielzahl von Nutzern existiert, was nachfolgend zu großem Aufwand und erheblicher Rechtsunsicherheit führen kann.

Es sollte daher präzisiert werden, in welchem Verhältnis die unterschiedlichen Nutzer stehen. Klar ist lediglich, dass seitens der Hersteller oder Entwickler entsprechende Strukturen geschaffen werden sollen, die den Zugang zu den Daten ermöglichen (vgl. ErwG 20). Unklar bleibt dabei, wie weit die Zugangsrechte jedes einzelnen Nutzers gehen sollen. Der Grundgedanke, der aus ErwG 18 hervorgeht, sieht vor, dass der Nutzer stets berechtigt sein sollte, den Nutzen aus allen Daten zu ziehen, die in dem von ihm genutzten Produkt oder der Dienstleistung entstehen.

Um eine Konkretisierung zu erreichen, ist es wichtig herauszuarbeiten, inwieweit durch das Nutzerverhalten ein Mehrwert bzw. eine Wertschöpfung erreicht wird. Dies wird in der Regel immer dann der Fall sein, wenn dabei ein Verhalten erfasst wird, auf dessen Grundlage Folgeannahmen getroffen werden können. Daneben wird ebenso eine Wertschöpfung durch Aggregation, Auswertung und Verarbeitung der Daten erreicht. Die dahinterstehenden technischen Prozesse wiederum funktionieren immer wieder identisch, unabhängig vom Nutzer.

3. Begriff des Dateninhabers

Der Data Act-E definiert den Dateninhaber in Art. 2 Abs. 6 als eine juristische oder natürliche Person, die durch die Kontrolle über die technische Gestaltung des Produkts und der damit verbundenen Dienste dazu in der Lage ist, bestimmte Daten bereitzustellen.

Daten werden häufig in einer Cloud gespeichert, die von einem Dritten als Dienstleister betrieben wird. Unklar ist, inwieweit – bei technischer Möglichkeit – auch dieser Dritter zur Herausgabe verpflichtet sein soll. In dieser Rolle müsste der Dritte dann auch die Wahrung von Geschäftsgeheimnissen sicherstellen, wozu er unter Umständen mangels Kenntnis nicht in der Lage ist. Nützlich wäre insoweit eine Klarstellung, dass bei der Einbindung von Dritten die Datenherausgabe nur auf Anweisung des Herstellers erfolgen kann.

4. Verhältnis Nutzer zu Dateninhaber

Ausgehend von der Definition des Dateninhabers in Art. 2 Abs. 6 des Data Act-E ist unklar, was passiert, sobald ein Nutzer die Daten vom Dateninhaber bereitgestellt bekommen hat. Ab diesem Zeitpunkt hat der Nutzer auch die Kontrolle über die Daten. Es wäre insofern denkbar, dass er seinerseits zum Dateninhaber wird (Rückschluss aus ErwG 30 letzter Satz). Damit unterläge er seinerseits den Pflichten zur Bereitstellung von Daten im Rahmen dieser Verordnung. Der Nutzer, der Daten vom Dateninhaber erhalten hat, könnte folglich von weiteren Nutzern in Anspruch genommen werden auf Zugang zu Daten. Sollte dies der Fall sein, so ist fraglich, ob Weitergabebeschränkungen, die in einem vorgelagerten Dateninhaber – Nutzer – Verhältnis vereinbart wurden, der Herausgabe der Daten entgegengehalten werden können. Eine Klärung dieses Konflikts ist unbedingt notwendig, um die gezielten Rechtsmissbrauch und die Umgehung von Geschäftsgeheimnissen zu vermeiden.

Zu Kapitel II-IV: B2B- und B2C-Datenaustausch

1. Allgemeines

Der vorliegende Entwurf zielt darauf ab Daten und die damit verbundene Wertschöpfung gerechter über die verschiedenen Akteure, wie Hersteller, Nutzer, Dienstleister und sonstige Dritte, zu verteilen. Damit soll verhindert werden, dass Unternehmen ihre Marktmacht nutzen, um die Datennutzung durch Andere zu verhindern. Die neuen Regelungen sollen dazu beitragen, Potentiale für digitale Technologien, Innovationen und Wachstum besser ausschöpfen zu können. Eine ausreichende Datenverfügbarkeit ist nicht zuletzt auch vor dem Hintergrund des geplanten EU-Gesetzes über Künstliche Intelligenz (AI-Act), welches Anforderungen an die Datengrundlage von Anwendungen Künstlicher Intelligenz stellt, von hoher Bedeutung.

2. Definition Datenbegriff

Damit das Ziel einer besseren Nutzung vorhandener Daten erreicht werden kann, ist als Grundvoraussetzung zu klären, um welche Daten in welcher Form es gehen soll. Die in Art. 2 Abs. 1 Nr.1 formulierte Definition ist diesbezüglich sehr unklar und weit gefasst. ErwG 17 konkretisiert lediglich dahingehend, dass „Daten, die sich aus einem Softwareprozess ergeben“ und „abgeleitete

Daten“ nicht erfasst sein sollen. Was genau darunter zu verstehen ist und wo es Grenzen gibt, ist nicht ersichtlich. Aus Sicht der gewerblichen Wirtschaft ist es daher dringend erforderlich, klar und unmissverständlich zu definieren, in welcher Form welche Daten vom Data Act erfasst sind und herausgegeben werden müssen. Dies ist unerlässlich, um den praktischen Umgang mit der Verordnung in Unternehmen zu ermöglichen. Eine gerichtliche Klärung der Rechtspraxis ist dabei insbesondere für KMU keine Option, da hohe Kosten und lange Prozesse eine hohe Abschreckungswirkung haben.

Um den Zweck des Data Act nicht zu unterlaufen, dürfen Daten nicht zur Last für Unternehmen werden. Insofern sollten Daten im Sinne des Gesetzes maximal Daten in der Verarbeitungsform meinen, die im Unternehmen verwendet werden oder zumindest vorhanden sind. Eine Weiterverarbeitung oder Aufbereitung, die zusätzlichen Aufwand erzeugt, ist nicht zumutbar, zumal dies neue Fragen der Kompensation aufwerfen würde. Konsequenterweise bedeutet dies, dass vorhandene Daten, die bislang noch gar nicht genutzt werden, nur bei technischer Möglichkeit und dann als Rohdaten zur Verfügung gestellt werden müssen. Zudem ist zu beachten, dass die Aufbereitung von Daten für sich betrachtet bereits ein Geschäftsmodell darstellt, für das es keine Anreize mehr gäbe, wenn Daten in dieser Form kostenlos oder zu Selbstkosten herausgegeben werden müssten.

Zu berücksichtigen ist dabei, dass besonders viele industrielle Anwendungen und Prozesse stark automatisiert stattfinden und nicht darauf ausgelegt sind, ein einzelnes Datum herauszugeben. Dadurch würden in diesen Prozessen unverhältnismäßig hohe Mehrkosten entstehen. Dies ist oftmals auch wenig sinnvoll, da der Aussagegehalt des einzelnen Datum ohne den Kontext vieler anderer Daten nur sehr gering oder sogar nicht gegeben ist. Es ist daher zu klären, dass der Verursachungsbeitrag zu einem einzelnen Datum nicht dazu führt, dass damit zusammenhängende Daten, die erst durch den Kontext mit anderen Daten entstanden sind, herausgegeben werden müssen.

3. Verteilung der Datenzugangsrechte zwischen Nutzern und Dateninhabern

Um die Entwicklung neuer innovativer Produkte zu fördern und Innovationen auf nachgelagerten Märkten voranzutreiben, sieht der Data Act-E vor, dem Nutzer alleine die Entscheidung zu überlassen, wie die Daten, an deren Entstehung er mitgewirkt hat, genutzt werden sollen. Dem Nutzer steht ein Rechtsanspruch auf Zugang zu diesen Daten zu. Damit verbunden wird ihm ein alleiniges Zuweisungsrecht über die Datennutzung durch andere Beteiligte eingeräumt. Dies bedeutet eine grundsätzliche Änderung im Vergleich zum bisherigen Umgang mit Daten und deren Nutzung. Bislang war es vom Gesetzgeber nicht geklärt, wer über die Nutzung von co-generiereten Daten entscheiden darf. In der Praxis handelten die Parteien dies daher in vertraglichen Verhandlungen aus.

Das vorgesehene Zugangsrecht für Nutzer könnte insbesondere kleineren Unternehmen die Teilnahme an der Datenökonomie ermöglichen bzw. erleichtern. Sie könnten die Daten beispielsweise verwenden, um Reparaturen oder Wartungen von Geräten durchzuführen oder Aufträge an Dritte zu vergeben. Allerdings darf eine verbesserte Rechtsposition von Nutzern und Dritten nicht zu Lasten der Innovationsfähigkeit von Dateninhabern bzw. deren Dienstleister geschehen, deren Geschäftsmodelle in vielen Fällen auf der Interaktion zwischen Geräte- und

Nutzerdaten basieren. Neben dem Mehrwert, der durch das Verhalten der Nutzer ensteht, resultiert ein großer Teil der Wertschöpfung der Daten auch aus dem Know-how des Dateninhabers. Die Zusammenführung, Auswertung oder Ableitung der Daten generiert ebenso einen erheblichen Wert. Dies bedarf erheblicher Investitionen und Know-how des betroffenen Unternehmens und ist daher schützenswert.

Die für den Dateninhaber vorgesehenen eingeschränkten Möglichkeiten selbst an die Nutzerdaten zu gelangen könnten für diesen, wenn er gleichzeitig auch Hersteller ist, nicht nur einen Wertschöpfungsverlust bedeuten, sondern auch die Weiterentwicklung der Produkte und Dienstleistungen erschweren und Investitionsanreize untergraben. Daneben stellt sich die Frage, inwiefern vor dem Hintergrund, Daten als nicht-rivales Gut zu verstehen (vgl. ErwG 6), der allgemeine Ansatz der Kommission, der dem Nutzer die alleinige Entscheidung über die Verwendung von Daten überlässt, gelungen ist. In der Praxis bestehen Bedenken, ob die alleinige Verlagerung des Nutzungs- und Zuweisungsrechts auf den Nutzer, zu Rivalitäten und Fehlanreizen führen wird.

Damit Investitionsanreize für den Produkttyp, von dem die Daten erlangt werden, erhalten bleiben und die Innovationsfähigkeit aller an der Wertschöpfungkette beteiligten Akteure sichergestellt wird, schlagen wir vor Zugangs- und Nutzungsrechte nicht exkusiv dem Nutzer zu gewähren, sondern auch anderen Teilnehmern in der Wertschöpfungskette. So können die berechtigten Interessen aller gewahrt werden ohne dabei ein Hemmnis für Innovation insbesondere auf nachgelagerten Märkten zu verhindern.

4. Weitergabe der Daten an Dritte

Neben dem Hersteller und Nutzer selbst können die Daten auch für Dritte interessant sein, die Produkte oder Dienstleistungen auf Anschlussmärkten anbieten, beispielsweise eine Versicherung. Der Data Act-E sieht vor, dass Nutzer unter bestimmten Bedingungen die Daten an Dritte weitergeben dürfen. Dies kann sich vorteilhaft auf die Innovationsfähigkeit von Unternehmen auf nachgelagerten Märkten auswirken. Jedoch kann die Weitergabe von Daten neben verschiedenen Arten von Effizenzgewinnen auch zu Wettbewerbsbeschränkungen führen. Dies gilt vor allem, wenn der Austausch von Daten nicht erfolgen kann, ohne dabei sensible, wettbewerbsrelevante Informationen offenzulegen. Dies ist vor allem dann zu befürchten, wenn zusätzlich zu den Rohdaten weitere Informationen geliefert werden müssen, die Auskunft über die Datenverarbeitung und damit auch über das Geschäftsmodell und die Marktstrategie von Unternehmen liefert. Dadurch könnte der Wettbewerbsvorteil des Unternehmens, das die Daten generiert und aufbereitet hat, beeinträchtigt werden.

Offen bleibt in der Ausgestaltung des Data Act-E, wie sensible Daten und Geschäftsgeheimnisse geschützt werden können und welche Anforderungen der Dateninhaber stellen darf, um die Vertraulichkeit als ausreichend gewahrt anzusehen. Aktuell werden neben Zugangs- und Nutzungsrechten von Daten auch Verwendungsrechte, also für welche konkreten Zwecke die herauszugebenden Daten genutzt werden dürfen, in Datennutzungsvereinbarungen (Data Use Agreements) vereinbart. Diese können gegebenenfalls mit Vertraulichkeitsvereinbarungen (Non-Disclosure Agreements (NDAs)) verknüpft werden. Sollten für ein Konkurrenzprodukt gewisse Daten benötigt werden, bei der Veröffentlichung des Produkts aber klar sein, dass das Produkt nur aufgrund der „geheimen“ Daten entwickelt werden konnte, verhindert das NDA, dass das Produkt

den Markt betreten darf. In dieser etablierten Form ist zumindest eine vertraglich Absicherung heute schon möglich. Eine erhebliche Rechtsunsicherheit könnte in diesem Kontext durch die in Art. 13 Data Act-E formulierten Anforderungen an Verträge über die Datennutzung entstehen.

Art. 4 Abs. 4 und Art. 6 Abs. 2 lit. e) des Data Act-E sehen vor, dass der Nutzer und Dritte die „erlangten Daten nicht zur Entwicklung eines Produkts nutzen [dürfen], das mit dem Produkt, von dem die Daten stammen, im Wettbewerb steht." Hier fehlt es an der nötigen Trennschärfe, in welchen Fällen ein konkurrierendes Produkt vorliegt. Unklar ist beispielsweise, ob es sich um ein identisches Produkt handeln muss, oder ob Produktähnlichkeiten ebenfalls erfasst sind. Abgrenzungsschwierigkeiten könnten sich auch bei Produkten mit mehreren Funktionen ergeben – etwa, wenn eine Funktion „konkurrierend" ist, andere Funktionen wiederum nicht.

Ebenso könnte hier ein gewisser Systembruch zur allgemeinen Wettbewerbsfreiheit vorliegen, wenn konkurrierende Produkte nicht entwickelt werden dürfen. So ist es nach geltender Rechtslage nicht urheberrechtswidrig, wenn Konkurrenzprodukte entwickelt werden. Im Rahmen der geltenden Schutzvorschriften dürfen nicht das Design eines Produkts oder der Quellcode einer Software kopiert werden. Allerdings drürfen Apps und Software entwickelt werden, welche die gleichen Funktionen haben, wie schon am Markt bestehende Produkte.

Desweiteren ist unklar, inwiefern sich durch Art. 4 Abs. 4 ein Widerspruch zu ErwG 28 ergibt, der besagt, dass der Nutzer ausdrücklich berechtigt ist, Daten an Dritte weiterzugeben, damit diese einen „anschließenden Dienst […] der möglicherweise mit einem vom Dateninhaber bereitgestellten Dienst im Wettbewerb steht" anbieten kann. Zwar ist es sinnvoll, in bestimmten Fällen nachgelagerten Märkten und Dienstleistungen einen Zugang zu relevanten Daten zu ermöglichen. Es erscheint jedoch zweifelthaft, ob eine trennscharfe Unterscheidung zwischen „Produkten" und „Dienstleistungen" und den daraus resultierenden Daten immer möglich ist und ob dies in der Praxis nicht zu erheblicher Rechtsunsicherheit und zu großem Streitpotential führt.

Aus diesem Grund spricht sich ein Teil der Unternehmen dafür aus, dass Art. 4 Abs. 4 nicht nur für Produkte, sondern auch für damit verbundene „anschließende Dienste" gelten sollte. Es gibt keinen offensichtlichen Grund, den Geltungsbereich eines solchen Verbots in Art. 6 Abs. 2 e) auf Produkte zu beschränken und Dienstleistungen gänzlich davon auszunehmen, obwohl diese ebenso eine Konkurrenz darstellen können. Dementgegen ist ein Teil der Unternehmen der Auffassung, dass konkurrierende Dienstleistungen insbesondere auf nachgelagerten Märkten möglich sein müssen, um dem Zweck des Data Acts, Daten besser zu nutzen, nicht zuwiderzulaufen.

Nicht zuletzt stellt sich die Frage, welche Möglichkeiten im Falle von Verstößen gegen das Verbot, die Daten für die Entwicklung von konkurrierenden Produkten einzusetzen, bestehen. Hier haben Unternehmen in der Praxis kaum eine Möglichkeit sich zu schützen, sofern die Rahmenbedingungen, wie zuvor beschrieben, unklar sind.

5. Produktgestaltung und technische Anforderungen

Damit der Zugang und die Weitergabe von Daten auch technisch möglich ist, müssen Hersteller nach Art. 3 ihre Produkte und Dienstleistungen so gestalten, dass ein Datenzugang „unverzüglich", wenn möglich sogar in „Echtzeit" stattfinden kann. Diese Anforderungen dürften die Hersteller in der Praxis vor erhebliche Herausforderungen stellen. Eine besonders hohe Komplexität könnte

entstehen, wenn mehrere Personen oder Beteiligte eines Leasing- oder Mietvertrags Zugang zu eine verbundenen Dienst haben. In diesem Fall sollten laut Data Act-E „*angemessene Anstrengungen bei der bei der Konzeption des Produkts oder verbundenen Dienstes oder der entsprechenden Schnittstelle unternommen werden, damit alle Personen Zugang zu den erzeugten Daten haben*“ (ErwG 20). Dies geht mit einem hohen Aufwand sowie finanziellen und adiminstrativen Kosten einher, die je nach Unternehmengsröße zu großen Belastungen führen können. Diese Verpflichtungen könnten insbesondere auch kleine Unternehmen treffen, die von den Pflichten des Data Act eigentlich ausgenommen sind, jedoch - um marktfähige Produkte anbieten zu können - alle Pflichten erfüllen müssen. Fraglich ist dabei, ob dieser Mehraufwand sich in Preisen für Dienstleistungen wird realisieren lassen, da für KMU der Konkurrenzdruck oft hoch ist.

Auf der anderen Seite bietet ein technisch einfacher Zugang zu Daten vielen Unternehmen Erleichterungen bei der Datennutzung und somit Chancen, die Potentiale besser zu nutzen. Es ist daher wichtig, Herstellern von Produkten und Anbietern von Diensten möglichst viel Spielraum bei der Umsetzung des Datenzugangs zu belassen. Entscheidend ist vor allem, dass im Ergebnis sichergestellt ist, dass für Nutzer und Dritte notwendige Daten zugänglich sind und genutzt werden können.

In diesem Zusammenhang definiert Art. 5 Abs. 1 zwar die Qualität der Datenbereitstellung an Dritte, jedoch bleibt die Form der Bereitstellung offen. Positiv an einer solchen offenen Regelung ist, dass diese Unternehmen eine sehr individuelle Ausgestaltung der Datenbereitstellung und eine angemessene Gegenleistung (vgl. Art. 9 Data Act-E) gegenüber Dritten ermöglicht. Diese Flexibilität bei der Form der Bereitstellung birgt jedoch das Risiko, dass in Zweifelsfällen eine gerichtliche Klärung der Auslegungsvarianten erforderlich wird. Derartige Probleme könnten sich beispielsweise bei der Bereitstellung von Daten an Dritte ergeben, die technisch über einen Portal-Account/Zugang möglich sind. Ein Zugang zu den Daten wäre damit zwar gegeben, jedoch eine massenhafte Datenverarbeitung, die Grundlage für viele digitale Geschäftsmodelle ist, häufig nicht, da dafür eine technische Schnittstelle notwendig ist. Um für Unternehmen keine Unsicherheit zu schaffen, ist einheitlich zu klären, wann welche Daten wie an Dritte zur Verfügung gestellt werden müssen.

Nach Inkrafttreten der Verordnung ist nach Art. 42 eine Übergangsfrist von zwölf Monaten bis zum Geltungsbeginn vorgesehen. Fraglich ist diesbezüglich, ob die Vorschriften des Data Act nach Geltungsbeginn für alle auf dem Markt befindelichen Produkte unabhängig vom Zeitpunkt des Inverkehrbringens gelten werden. Besonders mit Blick auf Dienstleistungen, die immer wieder neu mit Erbringung angeboten werden, ist unklar, ob ein ausreichender Bestandsschutz von Systemen, die vor dem Data Act konzipiert wurden, gewährleistet ist. Es sollte daher entweder in Betracht gezogen werden, die Übergangsfristen ensprechend auf beispielsweise 24 Monate zu verlängern oder abzustufen je nach Unternehmensgröße, damit gerade KMU, die keine eigene rechtliche Expertise haben, die Vorschriften umsetzen können. In jedem Fall sollten die in Art. 34 vorgesehenen Mustervertagsbedingungen und etwaige weitere Guidelines, die Hilfestellung besonders für KMU darstellen, spätestens bis zum Beginn der Umsetzungsfrist vorliegen, damit diese von Anfang an brücksichtigt werden können.

6. Informationspflichten

Neben technischen Anforderungen sieht der Entwurf in Art. 3 Abs. 2 vor, dass vor Abschluss eines Kauf-, Miet- oder Leasingvertrags für ein Produkt oder einen verbundenen Dienst dem Nutzer eine Reihe von Information bereitgestellt werden müssen. Die Informationspflicht würde in dieser Form insbesondere für Hersteller, jedoch auch für Händler und andere Beteiligte in der Lieferkette einen erheblichen administrativen Aufwand erzeugen. Dieser Aufwand käme zu den vielfältigen bereits heute bestehenden und zukünftigen Informationspflichten aus anderen Bereichen (z. B. Umwelt, Produktsicherheit) hinzu, die bislang wenig vereinheitlicht sind. Es sollte daher konkretisiert werden, in welcher Form die Informationen bereitgestellt werden müssen. Dies könnte z. B. in Form eines QR-Codes mit Link auf eine dauerhafte Website des für die Datenerzeugung verantwortlichen Wirtschaftsakteurs erfolgen. Dies würde zudem Abmahnrisiken für Händler vermeiden und infolge eines geeigneten Kontrollinstruments (URL/QR-Code auf der Verpackung) auch die Marktüberwachung und damit faire Wettbewerbsbedingungen unterstützen. Darüber hinaus könnte diese Form der Informationsbereitstellung Ressourcen einsparen, da Informationen nicht mehr zwingend in Papierform bereitgestellt werden müssen. Dieser Effekt würde verstärkt, wenn auch andere Informationen im digitalen Format bereitgestellt werden können.

Darüber hinaus sollte die Verpflichtung zur Bereitstellung der Informationen so an den jeweiligen Wirtschaftsakteuren orientiert werden, dass diese ihre jeweiligen Pflichten nachvollziehen können. Sofern die Einführung einer „für die Datenerzeugung verantwortlichen Person“ in Frage kommt, könnte die Verpflichtung auch dieser Person zugeordnet werden, während z. B. Händler verpflichtet wären, die Verfügbarkeit dieser Informationen zu überprüfen und u.a. einen Link auf die Informationen zusammen mit dem Kaufangebot im Online-Shop bereitzustellen.

7. Eingriffe in die Vertragsfreiheit

Die Vertragsfreiheit sollte so weit wie möglich erhalten bleiben, um das Innovationsklima im unternehmerischen Verkehr zu sichern und zu stärken. Nur dort, wo ein erwiesenes Marktversagen vorliegt, sind Abweichungen von diesem Grundsatz zu rechtfertigen. Der Data Act-E sieht ein solches Marktversagen in Fällen von Vertragsverhandlungen zwischen KMU und großen Unternehmen, die den Zugang zu Daten des großen Unternehmens zum Gegenstand haben. Ausweislich ErwG 46 *„ist ein Eingreifen nicht erforderlich, wenn Daten zwischen großen Unternehmen ausgetauscht werden oder wenn es sich beim Dateninhaber um ein kleines oder mittleres Unternehmen und beim Datenempfänger um ein großes Unternehmen handelt.“*

Dem liegt die Annahme zugrunde, dass nur Kleinstunternehmen oder KMU, die Datenzugang begehren, schutzwürdig sind. Um die vorgenannten Unternehmen zu schützen, enthält Art. 13 des Data Act-E daher bestimmte Klauseln, die immer missbräuchlich sind und zusätzlich solche, die als missbräuchlich gelten, also deren Missbräuchlichkeit nur widerleglich vermutet wird.

Grundsätzlich ist der an der Unternehmensgröße messende Ansatz zur Bewertung der Schutzbedürftigkeit geeignet, um die Stellung von KMU in Vertragsverhandlungen zu verbessern. Fraglich ist allerdings, ob die vorgesehen Differenzierungen geeignet sind, die jeweils im Einzelfall vorliegende Verhandlungsmacht in allen Fällen zutreffend abzubilden. Wie bereits zuvor ausgeführt, werden unbestimmte Rechtsbegriffe, wie die „Angemessenheit“ einer vereinbarten Vergütung zu weiteren Unsicherheiten in diesem Kontext führen. Die zusätzlichen Transparenz- und

Informationspflichten, die zur Beurteilungsmöglichkeit der Angemessenheit verpflichtend sind, stellen einerseits eine zusätzlich Belastung für Unternehmen dar und können andererseits dazu führen, dass sensible Informationen über die Kostenstrukturen und die Preisgestaltung eigener Dienste offengelegt werden müssen.

Die Präzisierung des sehr unbestimmten Begriffs der „fairen" Bedingungen, also unter welchen Voraussetzungen ein „fairer" Datenaustausch stattfinden kann, ist besonders wichtig. Schwierigkeiten diesbezüglich ergeben sich aus der Bestimmung eines fairen und gleichermaßen marktgerechten Preises für Daten. Nach dem Data Act-E sind bei der Aushandlung einer angemessen Gegenleistung „*Faktoren wie Menge, Format, Art, Angebot und Nachfrage sowie die Kosten für die Sammlung und Bereitstellung der Daten für den Datenempfänger*" zu berücksichtigen (ErwG 46). Damit der Datenempfänger die Angemessenheit prüfen kann, muss der Dateninhaber ihm ausreichend detaillierte Informationen für die Berechnung der Gegenleistung zur Verfügung stellen (vgl. ErwG 47). Allerdings kann die Auslegung der o.g. Faktoren sehr unterschiedlich ausfallen und ist angesichts der Vielfältigkeit der Daten und der Unterschiedlichkeit der Märkte und Rollen der Marktteilnehmer nur schwer zu beurteilen. Dies birgt eine hohe Rechtsunsicherheit.

Ausgenommen von dieser Möglichkeit sind KMU, von denen nur die unmittelbaren Kosten der Verursachung und nicht wie sonst eine angemessene Gegenleistung verlangt werden darf (vgl. ErwG 42, 44f.). Positiv daran ist, dass es KMU so erleichtert wird, datengetriebene Geschäftsmodelle zu entwickeln und zu betreiben, da Kosten begrenzt werden. Dementgegen steht, dass durch die Herausgabe der Daten unterhalb des Marktpreises - ohne die Möglichkeit alle Kosten, die bei der Entstehung der Daten verursacht werden, zu berücksichtigen - Anreize für Hersteller verloren gehen, in die Sammlung von Daten zu investieren. Aus Sicht der gewerblichen Wirtschaft ist es wichtig einen ausgewogenen Ansatz zu finden, der es allen Wirtschaftsakteuren ermöglicht, an der Datenökonomie teilzunehmen, ohne dass wettbewerbsverzerrende Bedingungen bei der Herausgabe der Daten entstehen. Sofern strukturelle Nachteile bei einzelnen Marktteilnehmern bestehen, sollten diese über Förderinstrumente wie beispielsweise der Innovationsförderung kompensiert werden.

8. Angemessener Schutz des geistigen Eigentums

Der Entwurf des Data-Acts sieht eine erhebliche Stärkung der Zugangsrechte zu Daten von Nutzern vernetzter Produkte und Geräten sowie Dritten vor, auch wenn Daten Geschäftsgeheimnisse beinhalten. Dabei kann das berechtigte Interesse von Unternehmen am Schutz der eigenen Geschäftsgeheimnisse dem Zugangsanspruch zu den Daten grundsätzlich nicht entgegengehalten werden. Die einzige vorgesehene Möglichkeit, um sich vor der Weitergabe und der Offenlegung von Geschäftsgeheimnissen wirksam zu schützen, ist es, vertraglich Nutzungs-, Verschwiegenheitsvereinbarungen zu schließen. Gegenüber KMU sind dabei allerdings die strengen Anforderungen an Vertragsklauseln in Art. 13 Data Act-E zu beachten, damit diese nicht unwirksam sind. Deshalb ist es besonders wichtig zu klären, was alles als Geschäftsgeheimnisse im Sinne des Data Acts zu verstehen ist.

Für Unternehmen ist es von besonderem Interesse den Austausch von Daten in einer Weise zu gestalten, die die Kontrolle darüber gewährleistet, wer die Daten für welche Zwecke nutzt. Um dies abzusichern, sind Rechte des geistigen Eigentums (einschließlich des Sui-generis-Rechts in Bezug

auf Datenbanken) und Geschäftsgeheimnisse bei der gemeinsamen Nutzung von Daten zwischen Unternehmen relevant. Da diese Regelungen zu Schutz durch den Data Act-E erheblich eingeschränkt werden, ist es wichtig, Unternehmen auch weiterhin ausreichend Spielraum zu verschaffen ihre schutzwürdigen Interessen hinreichend zu schützen. Die zusätzlichen Anforderungen durch die verpflichtende Missbrauchskontrolle in einigen Fällen stellt dabei eine weitere Einschränkung dar. Es daher wichtig, Dateninhabern die Möglichkeit einzuräumen die rechtmäßige Verwendung und Weitergabe der Daten nachvollziehen zu können. Zusätzlich sind klare Haftungsregeln notwendig für den Fall des Missbrauchs oder des Vertragsbruchs hinsichtlich der übermittelten Daten. Das derzeitige Schutzniveau für Daten im Rahmen der Datenbankrichtlinie und der Know-how-Richtlinie sollte grundsätzlich beibehalten, ggf. überprüft und weiterentwickelt werden, dass sowohl die mit der Generierung, wie auch die mit der Aufbereitung von Daten verbundenen Investitionen angemessen geschützt werden. Ebenso ist es zu berücksichtigen, dass durch sogenanntes reverse engineering mit Hilfe bestimmter Daten Details zu Produkten und Dienstleistungen rekonstruiert werden können. Davon betroffen könnten vor allem Unternehmen sein, die sehr spezialisierte und individuelle Produkte herstellen.

9. Zusammenspiel mit der DSGVO

Der Data Act-E sieht zwar vor, dass die DSGVO unberührt bleibt und daher die Regelungen weiterhin vollumfänglich gelten, wenn es sich um personenbezogene Daten handelt. Viele Unternehmen teilen bisher unter anderem keine Daten, da die DSGVO dem entweder entgegensteht oder zumindest Rechtsunsicherheit herrscht, inwieweit die Teilung der Daten datenschutzkonform möglich ist. Der Data Act-E sieht hierfür keine Lösung vor. Ob sich personenbezogene Daten und nichtpersonenbezogene Daten in der Praxis so einfach trennen lassen, ist zweifelhaft. In ErwG 30 heißt es, dass die DSGVO gelten soll, wenn personenbezogene und nicht personenbezogene Daten in einem Datensatz untrennbar miteinander verbunden sind. Weiterhin schweigt der Entwurf auch zur Frage, wann personenbezogene Daten sicher als anonymisiert gelten. Dies ist aber essentiell für die Frage, ob die DSGVO Anwendung findet oder nicht. Eine rechtssichere Anonymisierung wäre ein wichtiger Baustein, um die Datenteilung zu fördern. Grundlegende datenschutzrechtliche Bedenken, die bisher einer Datenteilung im Weg standen, werden demnach durch den Entwurf nicht aufgelöst. Die „volle Ausschöpfung des Potenzials der datengesteuerten Innovation“ kann nicht erreicht werden, wenn nicht auch datenschutzrechtliche Unsicherheiten gelöst werden.

Zu Kapitel V: B2G

Neben der Regelung des Zugangs zu Daten durch private Akteure sieht der Data Act-E zudem erweiterte Zugangsrechte durch öffentliche Einrichtungen vor. So muss ein Dateninhaber einer öffentlichen Einrichtung auf Antrag Daten zur Verfügung stellen, wenn ein „außergewöhnlicher Bedarf“ an der Nutzung der Daten besteht. Dieser liegt vor, wenn die Daten zur Bewältigung einer öffentlichen Notlage benötigt werden (vgl. Art. 15a), eine Notlage verhindert bzw. die Erholung von einer Notlage unterstützt werden muss (vgl. Art. 15b), oder die öffentliche Stelle oder Einrichtung ohne die angeforderten Daten nicht ihren rechtlichen Verpflichtungen nachkommen kann (vgl. Art. 15c).

Grundsätzlich ist eine Datenteilung auf freiwilliger Basis zu bevorzugen. Anreize für eine freiwillige Bereitstellung sieht der Data Act-E nicht vor. Diese könnten sich in Form von Steueranreizen, mehr Know-how und Investitionen öffentlicher Mittel zur Unterstützung der Entwicklung vertrauenswürdiger technischer Instrumente für die gemeinsame Nutzung von B2G-Daten darstellen. Der erzielte Mehrwert muss dabei stets in einem angemessenen Verhältnis zu dem Aufwand, der für die Unternehmen entsteht, stehen.

Im Falle eines hinreichend begründeten außergewöhnlichen Bedarfs trägt die Mehrheit der deutschen gewerblichen Wirtschaft eine Bereitstellung von Daten für staatliche Aufgaben jedoch mit. Dieses ist allerdings auf wenige, besonders begründete Ausnahmefälle zu reduzieren. Konkret sehen Unternehmen nach den Ergebnissen der Konsultation ein begründetes Interesse bei Daten für Notfall- und Krisenmanagement, Prävention und Resilienz. Die Erfahrungen der vergangenen Jahre haben aber auch gezeigt, dass Krisensituationen – etwa im Bereich der öffentlichen Gesundheit - lange anhalten können. Daraus resultiert ein Spielraum für die öffentlichen Stellen, den es einzugrenzen gilt. Im Ergebnis sollte es zu keinem Zustand des dauerhaften Datenzugangs kommen. Unternehmen und öffentliche Stellen benötigen diesbezüglich mehr Rechtssicherheit.

Damit dieses Ziel erreicht werden kann sollte es vermieden werden den in Art. 15 Data Act-E verwendeten unbestimmten Rechtsbegriff *„außergewöhnliche Notwendigkeit“* mit weiteren unbestimmten Rechtsbegriffen *„öffentliche Notlage“* und *„andere Ausnahmesituationen“* konkretisiert wird. Die vorgenannten Rechtsbegriffe eröffnen eine Breite an Szenarien, die in großen Teilen über die Bereitschaft der Unternehmen ihre Daten bereitzustellen hinausgehen. Aus diesem Grund bedarf es die klarer festlegen in welchem zeitlichen und inhaltlichen Umfang Unternehmen Daten an öffentliche Stellen herausgeben müssen. Öffentliche Stellen sollten dabei besonders hinsichtlich der in Art 15 lit. c) genannten, sehr weit interpretierbaren, im öffentlichen Interesse zu erfüllenden Aufgaben klarere Vorgaben bekommen. Unklar ist außerdem, wie Daten weitergegeben bzw. verwendet werden dürfen und inwiefern ein ausreichender Schutz sensibler Daten gewährleistet werden soll. Schutzmaßnahmen für die Unternehmen sind daher dringend erforderlich.

In jedem Fall benötigen die Unternehmen eine angemessene Kompensation und geeignete Voraussetzungen für eine effiziente Bereitstellung. Die Erhebung und Übermittlung von Daten ist für die Unternehmen mit einem hohen Verwaltungsaufwand und Kosten verbunden, die im vorgesehenen Entwurf nicht bzw. nur zum Teil entschädigt wird. Während die Daten im Falle einer Bewältigung einer Notstandssituation nach Art. 15a unentgeltlich bereitgestellt werden müssen, kann der Dateninhaber in den Fällen Art. 15b und 15c einen finanziellen Ausgleich für die Herausgabe verlangen. Dieser Ausgleich darf *„die technischen und organisatorischen Kosten, die durch die Erfüllung des Verlangens entstehen, erforderlichenfalls einschließlich der Kosten einer Anonymisierung und technischen Anpassung, zuzüglich einer angemessenen Marge, nicht übersteigen“* (Art. 20). Die Bereitstellung ist jedoch nicht nur ein Kostenfaktor, sondern gewährt aus Sicht vieler KMU auch Externen unerwünschte Einblicke in sensible Betriebszusammenhänge. So fehlt es insbesondere vielen KMU an eigenen Kompetenzen im Unternehmen, um dem Datenbereitstellungsverlangen einer öffentlichen Stelle nachkommen zu können. Gibt es im Unternehmen keine Kompetenzen zur Datenanalyse, so müssen externe Dienstleister herangezogen werden. Öffentliche Einrichtungen, die Zugang zu Unternehmensdaten benötigen, müssen daher die technischen Voraussetzungen sowie geeignete Tools dafür schaffen, dass Unternehmen Daten einfach, möglichst automatisiert und ohne externe Hilfe liefern können. Für die

Nutzung der Daten sind außerdem Maßnahmen zur Datensicherheit, einschließlich Schutz vertraulicher Geschäftsinformationen und transparente Berichterstattung über die Verwendung der Daten durch Behörden erforderlich.

Zu Kapitel VI-VIII: Datenverarbeitungsdienste

Der vorliegenden Gesetzesentwurf sieht auch für Anbieter von Datenverarbeitungsdiensten, z. B. Cloud- oder Edgedienste neue Regelungen vor. Davon profitieren sollen die Nutzer dieser Dienste, indem es ihnen erleichtert werden soll, ihren Anbieter zu wechseln. Datenverarbeitungsdienste müssen den Umstellungsprozess unterstützen und jegliche kommerzielle, technische, vertragliche und organisatorische Hindernisse beseitigen.

Ein Hauptvorteil von Cloud-Diensten liegt - neben der Flexibilität und Skalierbarkeit - in der Benutzerfreundlichkeit für Entwickler und Betreiber, die es einfach machen, Dienste und Anwendungen zu erstellen und zu betreiben. Der Nachteil dieser Einfachheit ist, dass die Anwendungen der Kunden oft tief in das proprietäre Ökosystem des Cloud-Anbieters integriert sind, was es den Kunden erschweren kann, den Anbieter zu wechseln, ohne den Zugang zu Daten, Anwendungen und anderen digitalen Assets zu verlieren. Da immer mehr Verbraucher, Regierungen und Unternehmen auf Cloud-Dienste angewiesen sind, wird es umso wichtiger, einen offenen und dynamischen Cloud-Markt zu schaffen.

Die mehrheitliche Zahl der Unternehmen unterstützt daher den Ansatz, die Verhandlungsposition der Cloud-Nutzer zu verbessern und den Wechsel zu erleichtern. Laut den Ergebnissen der Konsultation wird in diesem Kontext ein Recht auf Übertragbarkeit für gewerbliche Nutzer von Cloud-Computing-Diensten als erforderlich erachtet. Die Funktionsäquivalenz des Dienstes (Aufrechterhaltung eines Mindestfunktionsumfangs eines Dienstes nach dem Wechsel) wird als technisch machbar angesehen, wenn sowohl der vorherige Dienst als auch der übernehmende Dienst (teilweise oder vollständig) dieselbe Dienstart abdeckt (vgl. ErwG 72).

Es ist zu erwarten, dass die neuen Regelungen erhebliche Auswirkungen auf heute bestehende Geschäftsmodelle von Datenverarbeitungsdiensten haben wird. Diese dürfen jedoch nicht dazu führen, dass Entwicklungen auf diesen Märkten gehemmt werden. Diensteanbieter benötigen eine verlässliche Basis, auf der sie kalkulieren können. Die in Art. 23 vorgesehene Kündigungsfrist für Kunden von höchstens 30 Kalendertagen könnte das Geschäftsmodell vieler Anbieter beeinflussen, da Umsatzprognosen basierend auf Vertragslaufzeiten unmöglich werden. Gleichzeitig sollte im Sinne der Vermeidung von „lock-in Effekten“ sichergestellt werden, dass die Kunden nicht durch unverhältnismäßig lange Kündigungsfristen oder die Erhebung von unverhältnismäßig hohen Gebühren an einem Anbieter-Wechsel gehindert werden.

Zu Kapitel IX: Anwendung und Durchsetzung

Der Ansatz eines europaweit einheitlichen Vorgehens ist zu unterstützten. Dies verbessert die Bedingungen für einen funktionierenden europäischen Binnenmarkt für Daten und stärkt somit die europäische Datenwirtschaft. Es bedarf dringend einem einheitlichen und abgestimmten Vorgehen unter den Mitgliedsstaaten, unter anderem was Governance und Überwachung betrifft.

D. Ansprechpartner mit Kontaktdaten

Steffen von Eicke
Referatsleiter Digitaler Binnenmarkt, EU-Verkehrspolitik, Regionalpolitik
Deutscher Industrie- und Handelskammertag e. V.
Avenue des Arts 19 A-D / 1000 Brüssel / Belgien
Telefon: + 32 2286-1639
vonEicke.steffen@dihk.de | www.dihk.de

Alena Kühlein
Bereich Digitale Wirtschaft, Infrastruktur, Regionalpolitik
Referatsleiterin Wirtschaft digital
Deutscher Industrie- und Handelskammertag e. V.
Breite Straße 29 | 10178 Berlin
Telefon: +49 30 20308-2107
Kuehlein.Alena@dihk.de | www.dihk.de

Wer wir sind:

Unter dem Dach des Deutschen Industrie- und Handelskammertags (DIHK) haben sich die 79 Industrie- und Handelskammern (IHKs) zusammengeschlossen. Unser gemeinsames Ziel: Beste Bedingungen für erfolgreiches Wirtschaften.

Auf Bundes- und Europaebene setzt sich der DIHK für die Interessen der gesamten gewerblichen Wirtschaft gegenüber Politik, Verwaltung und Öffentlichkeit ein.

Denn mehrere Millionen Unternehmen aus Handel, Industrie und Dienstleistung sind gesetzliche Mitglieder einer IHK - vom Kiosk-Besitzer bis zum Dax-Konzern. So sind DIHK und IHKs eine Plattform für die vielfältigen Belange der Unternehmen. Diese bündeln wir in einem verfassten Verfahren auf gesetzlicher Grundlage zu gemeinsamen Positionen der Wirtschaft und tragen so zum wirtschaftspolitischen Meinungsbildungsprozess bei.

Darüber hinaus koordiniert der DIHK das Netzwerk der 140 Auslandshandelskammern, Delegationen und Repräsentanzen der Deutschen Wirtschaft in 92 Ländern.

Er ist im Register der Interessenvertreter der Europäischen Kommission registriert (Nr. 22400601191-42).