Stellungnahme

zum Konsultationsprozess der EU-Kommission zum „Data Act“-Entwurf

13. Mai 2022

Vorbemerkung

Die Europäische Kommission hat am 23.02.2022 den Data Act Entwurf (DA-E) verabschiedet. Ziel des Legislativvorhabens ist es, den Zugang und die Nutzung nicht-personenbezogener Daten in der EU zu verbessern und somit die datenbasierter Wertschöpfung in der EU zu unterstützen sowie den Wechsel von Clouddienst-Anbietern zu vereinfachen.

Der ZVEI setzt sich schon seit Jahren dafür ein, den unternehmens- und sektorübergreifenden fairen Austausch industrieller, nicht-personenbezogener Daten zu fördern und somit datengetriebene Geschäftsmodelle zu erleichtern. Aus Sicht des ZVEI eröffnet die Nutzung sowie der Zugang zu industriellen Daten und deren multilateraler Austausch enormes wirtschaftliches und gesellschaftliches Wertschöpfungspotential. Digitale und datengetriebene Geschäftsmodelle helfen industrielle Prozesse in allen Leitmärkten der Elektro- und Digitalindustrie (industrielle Produktion, Energie, Mobilität, Gebäude, Gesundheit, Components und Consumer) effizienter und verlässlicher und damit letztlich ressourcenschonender zu gestalten.

Der ZVEI unterstützt grundsätzlich die in dem DA-E beschriebenen Ziele einer verbesserten Datenallokation sowie den Datenerzeuger verstärkt in die Datenökonomie einzubinden. Um das Wertschöpfungspotenzial von Industrie- und Maschinendaten vollständig heben zu können, müssen Daten zu den Akteuren in der Wertschöpfungskette fließen können, die den größten Mehrwert aus den Daten generieren. Es ist jedoch zu befürchten, dass der vorliegende Kommissionsentwurf an der industriellen Praxis vorbei reguliert und daher zu mehr Rechtsunsicherheiten, Aufwand und Kosten für viele Unternehmen führen und somit im Ergebnis weniger Innovation und digitale Wertschöpfung erzielen wird.

ZVEI e. V. • Charlottenstraße 35/36 • 10117 Berlin
Innovationspolitik
Telefon: +49 30 306960 19 • Fax: • E-Mail: Dominic.Doll@zvei.org • www.zvei.org

Präsident: Dr. Gunther Kegel • Vorsitzender der Geschäftsführung: Dr. Wolfgang Weber

Kernforderungen der Elektro- und Digitalindustrie

- Um das volle Potential datenbasierter Wertschöpfung im industriellen Kontext auszuschöpfen, müssen Daten in den Sektoren, in denen es sinnvoll ist, in alle Richtungen der multilateralen Wertschöpfungsnetzwerke fließen können.

- Eine getrennte Betrachtung im DA-E der Regulierungsbereiche B2B und B2C Datenteilung (Kapitel 2 DA-E) ist dringend notwendig, da die in ihren jeweiligen Kontexten generierten Daten verschieden sind. Der DA-E sollte sich ausschließlich auf den Regelungsbereich der nicht personenbezogene Daten fokussieren. Der Data Act muss mit anderen EU-Rechtsakten wie dem Data Governance Act und der Datenschutzgrundverordnung abgestimmt bzw. zur DS-GVO klar abgegrenzt werden.

- Die Definitionen des DA-E sind nicht praktikabel im Sinne der industriellen Anwendung und bergen die Gefahr eher zu mehr Rechtsunsicherheit und somit weniger Wertschöpfung zu führen. Auch die Gefahr der unbeabsichtigten Offenlegung von Betriebsgeheimnissen durch zu ungenaue Definitionen ist zu befürchten.

- Zusätzliche Produktanforderungen können erhebliche finanzielle und administrative Mehraufwände mit sich bringen, die vermeidbare Hürden auf dem Weg zur Digitalisierung der Industrie sowie der Umsetzung von marktfähigen Produkten darstellen.

- Hersteller sollen zukünftig verpflichtet werden, nutzergenerierte Daten an Nutzer oder auch an Dritte weiterzugeben. Dadurch sind ggf. enthaltene IP-Rechte und Geschäftsgeheimnisse in Gefahr. Die vorgeschlagenen Schutzmaßnahmen sind jedoch rechtlich nicht durchsetzbar oder unzureichend für alle Szenarien (B2B, B2C, B2G) definiert. Sollten IP-Rechte und Geschäftsgeheimnisse nicht technisch und rechtssicher geschützt werden, gehen Investitionsanreize verloren. Dies würde sich negativ auf die Digitalisierung der Industrie und den Nachhaltigkeitsbestrebungen auswirken. Die Elektro- und Digitalindustrie bietet etwa mit der Verwaltungsschale in der Industrie 4.0 Lösungsbausteine für ein technisch sicheres und vertrauensvolles Datenteilen.

Definitionen und Terminologie

Die in Art. 2 DA-E formulierten Definitionen legen die Grundlage für eine technisch und rechtlich sichere Umsetzung des DA-E. Daher müssen die Definitionen den heterogenen Anforderungen unterschiedlicher Sektoren genügen.

1. **„Daten“**: zu ungenaue und weit gefasste Definition. Maschinen generierte Daten können sich in Bezug auf die Verarbeitung (Rohdaten vs. analysierte oder verarbeitete Daten), die Offenlegung von Geschäftsgeheimnissen und Know-how sowie die kommerzielle und technische Durchführbarkeit ihrer Bereitstellung unterscheiden. Es ist ebenso unklar, wann die Schwelle der "aus solchen Daten abgeleiteten („derived“) oder gefolgerten („inferred“) Informationen" (Erwägungsgrund 14) erreicht ist.

Weiterhin bedarf es einer konkreten Abgrenzung zwischen nutzergenerierten vs. produkterzeugten Daten (kommt es allein auf die Nutzung des Produktes oder auf die Nutzung durch einen User an?) sowie gegenüber Daten mit Personenbezug.

2. **„Produkt“**: Für eine technisch und rechtlich sichere Anwendung ist der Begriff zu ungenau definiert. In diesem Kontext ist zudem zu präzisieren, was ein „“öffentlich zugänglicher elektronischer Kommunikationsdienst“ ist, da die meisten Komponenten im industriellen Kontext aus Sicherheitsgründen keine Schnittstellen zu öffentlich zugänglichen Netzwerken o.ä. besitzen. Zudem hängt die Fähigkeit, über einen öffentlich zugänglichen elektronischen Kommunikationsdienst zu kommunizieren, im industriellen Umfeld nicht allein vom Produktdesign ab. Notwendige Voraussetzungen müssen erfüllt sein, einschließlich standardisierter Kommunikationsprotokolle und Netzinfrastruktur auf Seiten des Kunden.

3. **„verbundene Dienste**“: Die Definition ist für die rechtssichere Anwendung zu weit und unspezifisch. Um mehr Klarheit zu schaffen, sollte sich die Definition ausschließlich auf „Grundfunktionen“ („basic function“) beschränken und nicht nur unspezifisch auf „eine seiner Funktionen“ (ein unbestimmtes Subset der Funktionen) abzielen.

4. **„Datenverarbeitungsdienst“:** Es sollte konkret definiert werden, welche Dienstleistungen hierunter fallen.

5. **„Nutzer“ & „Dateninhaber“:** Der Data Act Entwurf vermittelt den Eindruck eines sehr vereinfachten, dichotomen und nicht praxisnahen Verständnisses von Hersteller – Kunden (Nutzer)–Beziehungen. Der Entwurf berücksichtigt nicht die Möglichkeit, dass in multilateralen und -direktionalen Wertschöpfungsnetzwerken auch der Nutzer („user“) eines physischen Assets der Datenhalter sein kann. Hier muss eine Nachschärfung der Begriffe Nutzer („user“) und Dateninhaber („data holder“) entsprechend der industriellen Praxis erfolgen.

Zudem erfasst der DA-E die Rolle des Komponentenproviders überhaupt nicht bzw. scheint diese unter den Asset Provider („Datenhalter“) zu subsumieren. In der industriellen Praxis verfügt der Komponentenprovider jedoch vielfach nicht über die Daten - hat aber ein Interesse an den Nutzungsdaten seiner Komponente.

6. **„Öffentlicher Notstand“:** Die Definition des "öffentlichen Notstands" ist zu weit gefasst und offen für Interpretationen (z. B. statistische Zwecke, Forschung); sie muss überarbeitet werden, um sie auf bestimmte Fälle zu beschränken, die nicht über den öffentlichen Notstand hinausgehen. Das Gleiche gilt für weiterführende Begriffe, z. B. "öffentliches Interesse", "Vorbeugung/Wiederherstellung" und "außergewöhnlicher Bedarf". Entsprechend sollten Schutzmaßnahmen eingeführt werden, um einen Missbrauch von Artikel 15 c) Absatz 1 zu verhindern. Da es keinen Marktpreis für Industriedaten gibt, könnten öffentliche Stellen unabhängig von der Angemessenheit des Preises exzessiven Gebrauch von Datenzugangsanfragen machen.

7. Die in Art. 28 (1) DA-E genannten **“Betreiber von Datenräume”** (“Operators of data spaces”) müssen, um Rechtsunsicherheiten zu vermeiden, in Art. 2 DA-E definiert werden.

8. Der DA-E verzichtet auf eigene Definitionen der Begriffe **„Hersteller“** („manufacturer“) bzw. **„Diensteanbieter“** („service provider“), obgleich Hersteller und Diensteanbieter gleichermaßen von dem Anwendungsbereich gemäß Art. 1 Nr. 2 (a) DA-E betroffen sind.

Zusätzliche Produktanforderungen

Damit der Data Act zu mehr datengetriebener Wertschöpfung führt, müssen Rechtsunsicherheiten, die sich aus zusätzlichen Produktanforderungen ergeben, verhindert werden. Dazu muss der Data Act mit anderen EU-Rechtsakten wie dem Data Governance Act und der Datenschutzgrundverordnung abgestimmt werden. Es muss deutlich mehr Klarheit geschaffen werden, wie bspw. Daten trotz geänderten Nutzungszwecks DS-GVO-konform weitergenutzt werden können (siehe auch Abschnitt Rechtsunsicherheiten & Einschränkung der Vertragsfreiheit).

Durch die ungenaue Definition des Begriffs „Produkt“ bleibt unklar, welche Komponenten von physischen Assets (z. B. Sensoren) unter die Definition eines Produkts fallen, insbesondere in Anbetracht der Erwägungsgründe 14 und 15. Im industriellen Umfeld können einzelne Komponenten normalerweise nicht eigenständig Daten erzeugen. Sie erfordern vielmehr eine spezifische und maßgeschneiderte Konfiguration durch den Nutzer oder den von ihm beauftragten Ingenieurdienstleister. Somit können industrielle Komponenten ihre Funktionen nur auf der Grundlage bestimmter Konfigurationen durch den Benutzer ausführen. In Erwägungsgrund 15 werden nun Produkte ausgenommen, die relevante Daten nur auf der Grundlage „menschlicher Eingaben“ generieren können. Vor diesem Hintergrund sind daher auch industrielle Anwendungen (wie z.B. industrielle Steuerungen, "PLCs", sowie Industrie-PCs, "IPCs"), die das Erfordernis der „menschlichen Eingabe“ erfüllen in die Beispiele des Erwägungsgrundes 15 mit aufzunehmen.

Darüber hinaus wäre es wünschenswert zu klären, ob das einzelne Bauteil aufgrund seiner Konstruktion die technischen Anforderungen bereits eigenständig erfüllen muss oder ob es nur erforderlich ist, dass die technischen Anforderungen im Zusammenspiel mit anderen unabhängigen Modulen erfüllt werden. Industrielle Steuerungen stellen bspw. standardmäßig keine Netzwerkverbindungen her, sondern können dies nur tun, wenn der Benutzer ein zusätzliches Netzwerkmodul auf der Grundlage individueller Einstellungen und unter Berücksichtigung seiner spezifischen Anforderungen mit den Steuerungsmodulen kombiniert.

Gemäß Art. 3 DA-E müssen Hersteller ihre Produkte „by default“ so gestalten, dass der Zugang zu den nutzergenerierten Daten unverzüglich und in Echtzeit ermöglicht werden kann. Viele Unternehmen der Elektro- und Digitalindustrie stellen auch ohne regulatorische Verpflichtung ihren Kunden nutzergenerierte Daten zur Verfügung. Aus Art. 3 DA-E ergeben sich nun jedoch erhebliche Anforderungen an die Hersteller, die nicht nur das Produkt, sondern auch Transparenz- und Informationspflichten etwa über die Art und den Umfang der Datenerhebung betreffen. Diese Informationspflichten erfordern einen erheblichen Mehraufwand, da diese für jedes Produkt individuell und marktspezifisch (EU vs. nicht-EU Märkte) erstellt werden müssten. Es ist zu befürchten, dass dieser Aufwand in keinem Verhältnis zum zusätzlichen Nutzen für den Kunden steht. Einem Gerätehersteller, der ein Gerät so designt, dass dem jeweiligen Nutzer die nutzungsgenerierten Daten im Gerät selbst zur Verfügung gestellt werden und der den Nutzer nicht vertraglich in der Nutzung dieser nutzungsgenerierten Daten einschränkt oder nur in einer ein gewisses Mindestnutzungsmaß erlaubenden Weise, sollte der Data Act keine weiteren Verpflichtungen auferlegen. Liegen die Nutzungsdaten des IoT Devices ohnehin beim Nutzer des Devices, sollte der DA-E keine zusätzlichen Produktanforderungen definieren.

Aus den Produktinformationspflichten gemäß Art. 3 (2) DA-E ergeben sich für die Hersteller zudem Dokumentationspflichten, die für alle Nutzer des Produkts entlang des gesamtem Produktlebenszyklus nachvollziehbar sind. Hier gilt es Konsistenz und Kohärenz mit anderen Regulierungen sicherzustellen, die dazu ebenfalls Vorgaben machen (z.B. Digitaler Produktpass im Rahmen des Entwurfs einer Ecodesign for Sustainable Products Regulation).

Das Konzept „digitale Produktpass“ ist eine Möglichkeit gesetzlich vorgeschriebenen Informationsanforderungen zu begegnen aber auch privatwirtschaftliche Informationsanforderungen zu erfüllen. Er sollte technisch genormt, aber flexibel in seiner Anwendung und für neue Anwendungsfälle einfach erweiterbar sein.

Der ZVEI hat für industrielle Anwendungen (B2B-Bereich) einen dezentralen Lösungsansatz für einen digitalen Produktpass auf Basis sog. Teilmodelle der Verwaltungsschale (IEC

63278-1) entwickelt und die Anwendbarkeit im Rahmen eines Pilotprojektes zum digitalen Typenschild erfolgreich demonstriert.

Um nicht die IT-Sicherheit der Produkte zu kompromittieren, sollte ausdrücklich die indirekte Bereitstellung von Daten über Internet-Plattformen erlaubt sein. Art. 3 (1) und Art. 3 (2) DA-E sind entsprechend anzupassen.

Industrielle Rohdaten (meist Sensordaten) enthalten für den Nutzer meist keinen direkt erkennbaren Mehrwert. Erst durch die Zusammenstellung und Verarbeitung verschiedener Parameter lassen sich relevante Aussagen über IoT-Assets erzielen. Es kann von dem Hersteller nicht verlangt werden zu antizipieren, welche Rohdaten vom Kunden möglicherweise zukünftig abgefragt werden und entsprechende Produktmodifikationen vorzuhalten. Ferner muss eindeutig geklärt werden, welche Art von „Daten" unter den Regulierungsanspruch des DA-E fallen. Fraglich ist, ob Art. 4 und Art.5 DA-E den Hersteller dazu verpflichten, jedes generierte Datum zu speichern und für welche Dauer. Hierunter fielen somit auch temporäre Daten, die, gemäß ihrer Definition, in regelmäßigen Abständen überschrieben werden. Sollte der DA-E keine diesbezügliche Einschränkung vornehmen, würden große Mengen an nicht wiederverwertbaren Daten anfallen, die jedoch on-device oder auf Clouds gespeichert werden müssten.

Auch die in Art 24 (1) b) DA-E geforderten Bereitstellung von allen Metadaten beim Wechsel von Datenverarbeitungsdiensten ist im industriellen Kontext nicht sinnvoll. Der technische und bürokratische Aufwand zur Bereitstellung der in Art. 24 (b) genannten Informationen steht in keinem Verhältnis zum Mehrwert für den Nutzer, da weder der Nutzer diese Informationen verwerten kann noch können diese Informationen in einer anderen Plattformumgebung (sinnvoll) genutzt oder technisch implementiert werden.

In Art. 25 (4) räumt die EU-Kommission die Möglichkeit ein, per delegiertem Rechtsakt „Überwachungsmechanismen" einzuführen, um die auf dem Markt verlangten Wechselentgelte überwachen zu können. Der DA-E lässt völlig offen, wie diese Mechanismen aussehen könnten. Sollten diese softwareseitig implementiert werden, würde dies weitere Produktanforderungen mit sich bringen sowie durch mögliche, zusätzliche Schnittstellen Bestrebungen im Sicherheitsdesign der Produkte erschweren.

Die Übergangsfrist von 12 Monaten gemäß Art. 42 DA-E ist zu kurz, insbesondere wenn man mögliche Anpassungen in der Produktgestaltung berücksichtigt und in Anbetracht der Tatsache, dass die technischen Anforderungen für die Interoperabilität von Datenräumen in Art. 28 DA-E (Datenstruktur, Formate usw.) noch veröffentlicht werden müssen. Für den Fall, dass Datenformate technisch nicht realisierbar sind oder Definitionen erst sehr viel später erfolgen, wird eine längere Übergangsfrist erforderlich sein. 36 Monate wären angemessen.

Geschäftsgeheimnisschutz

Mehr datenbasierte Wertschöpfung kann nur erreicht werden, wenn Vertrauen in Datenteilung und -zugang geschaffen wird. Weil Hersteller durch den DA-E zukünftig verpflichtet werden sollen, Daten an Nutzer oder auch an Dritte weiterzugeben, besteht die reelle Gefahr, dass in Daten enthaltene IP-Rechte und Geschäftsgeheimnisse offengelegt und somit nicht nur Wertschöpfung vermindert, sondern auch Vertrauen beschädigt wird. Um Missbrauch zu verhindern, sieht der DA-E zwar zahlreiche Nutzungsbeschränkungen für Weiterverwender vor, etwa das Verbot, die Daten für andere Zwecke oder für die Entwicklung von Konkurrenzprodukten zu nutzen (Art. 4 (4) DA-E). Der Hersteller muss jedoch selbst tätig werden und mit dem Nutzer oder den Dritten angemessene Schutzmaßnahmen vereinbaren. Wie deren Einhaltung kontrolliert, nachgewiesen und durchgesetzt werden soll, bleibt aber völlig offen, da es den Herstellern an hinreichenden Kontrollmöglichkeiten fehlt und zusätzlich durch Art. 4 (2) mögliche Kontrollmechanismen

entzogen werden. Es ist zu befürchten, dass Art. 4 (4) DA-E zu einer „leeren Vorschrift“ verkommt.

In industriellen Märkten mit wenigen Anbietern und ähnlichen, mit unter baugleichen Produkten, können Daten über Nutzung, Zustand und Performance des Produktes wettbewerbsrelevante Informationen enthalten. Das Ergebnis dieser Daten beruht meist auf kostenintensiven und langjährigen F&E-Aktivitäten des Herstellers. Werden diese Daten an Dritte weitergegeben, erleidet der Hersteller einen Wettbewerbsnachteil. Sollte den Herstellern in Aussicht gestellt werden, dass Wettbewerbsvorteile aus F&E-Aktivitäten durch den Data Act torpediert werden, könnte dies zu einem Rückgang der Innovationsleistung im gesamten Sektor führen.

Der DA-E sollte dahingehend konkretisiert werden, dass Dritte keinerlei Sicherheitslücken in weitergegebenen Datensätze nutzen dürfen. In Art. 5 (4) DA-E ist „offensichtlich“ somit zu streichen.

Die wirksame Durchsetzung vertraglicher Geheimhaltungsverpflichtungen ist praktisch unmöglich, insbesondere im Falle der Weitergabe an Dritte. Einmal unrechtmäßig weitergegebene Geschäftsgeheimnisse sind nicht mehr geheim, egal wie ein Gericht entscheiden mag. Eine solche unbefugte Weitergabe von Geschäftsgeheimnissen kann im schlimmsten Fall die Existenz des Unternehmens gefährden.

Die verpflichtende Weitergabe von Geschäftsgeheimnissen, ganz gleich ob im B2B, B2C -Bereich (Art. 4 (3)), gegenüber Dritten (Art. 5 (8)) oder im B2G -Bereich (Art. 19 (2)) ist strikt abzulehnen. Nur im Rahmen der Vertragsfreiheit sollten Daten, die Geschäftsgeheimnisse enthalten, geteilt oder der Zugang zu diesen ermöglicht werden. Es bedarf einer Konkretisierung des DA-E wer im Falle eines Verstoßes bei Datenweitergabe an Dritte haftet sowie welche Gerichte für solche Klagen zuständig sein werden.

Die theoretische Möglichkeit, eine finanzielle Entschädigung bei Vertragsverstoß zu verlangen reicht nicht aus, um die Rechte der Dateninhaber zu wahren, da ein Schadensersatzanspruch sich in diesen Fällen vor Gericht kaum beziffern lässt.

Für einen vertrauensvollen und technisch sicheren Austausch und Zugang zu Daten bietet die Elektro- und Digitalindustrie etwa mit der Verwaltungsschale in der Industrie 4.0 bereits Lösungsbausteine an. Sie schafft herstellerübergreifende und branchenneutrale Interoperabilität für Kommunikation, Dienste und Semantik entlang des gesamten Lebenszyklus und ermöglicht den kontrollierbaren Zugriff auf alle freigegebenen Informationen eines physischen Assets.

Laut Art. 35 DA-E würden ganze Datenbanken (unabhängig von der Menge der Daten, die möglicherweise nicht mit Art. 4 oder 5 in Verbindung stehen) ungeschützt bleiben. Eine derart weitreichende Einschränkung des sui generis-Rechts scheint weder notwendig noch verhältnismäßig zu sein, um das erklärte Ziel des Schutzes der Rechte aus Art. 4 und Art. 5 DA-E zu erreichen. Anstatt den Datenbankschutz gänzlich abzuschaffen, sollte das Datenbankschutzrecht nur dort eingeschränkt werden, wo der Datenzugriff oder die Datennutzung nach dem Data Act zulässig ist.

Rechtsunsicherheiten & Einschränkungen der Vertragsfreiheit

Grundsätzlich sollten Geschäftsbeziehungen auf Grundlage der Vertragsfreiheit basieren. Wo es nachweislich zu Marktasymmetrien und Wettbewerbsnachteilen kommt, soll der Gesetzgeber maßvoll eingreifen können, um eine verbesserte Datenallokation zu fördern.

Ein Eingriff in die Vertragsfreiheit der Hersteller durch den Data Act erscheint nur in Marktsegmenten verhältnismäßig, in denen aufgrund von Monopolen oder Oligopolen eine starke Macht- und Informationsasymmetrie zwischen Anbietern und Nachfragern besteht.

Vielfach ergeben sich Rechtsunsicherheiten durch ungenaue oder nicht praxistaugliche Definitionen. Es ist nicht eindeutig, welche (nicht-)personenbezogenen Daten beispielsweise unter die Datenzugangsansprüche des Kapitels 2 fallen. Art. 4 (1) klärt nicht eindeutig, welchen konkreten Beitrag der Nutzer eines Produktes zur Datengenerierung geleistet haben muss. Reicht die bloße Nutzung des Produktes oder muss die Nutzung durch einen zuordbaren/ identifizierbaren Nutzer passieren. Damit die von der EU-Kommission beabsichtigten positiven Effekte für eine faire Datennutzung zum Tragen kommen, bedarf es daher klarer Definitionen, die zu mehr Rechtssicherheit beitragen. Daher gilt es eine rechtssichere Abgrenzung zur DS-GVO und Daten mit Personenbezug zu schaffen. Das betrifft eine Vielzahl an Punkten wie den soeben angesprochenen Personenbezug durch Nutzerzuweisung, Inkohärenzen mit DS-GVO-Pflichten oder der Anonymisierung von zur Verfügung gestellten Daten. Unternehmen bedürfen einer klaren Orientierungshilfe hinsichtlich der Anforderungen für eine datenschutzkonforme Anonymisierung personenbezogener Daten. Mit Blick auf die legislativen Vorgaben ist zu konstatieren, dass die DS-GVO keine konkreten Vorgaben zur Anonymisierung personenbezogener Daten enthält und der Data Act die bereits bestehenden Unsicherheiten in der Praxis weiter verschärfen wird.

Überdies steht auch die Zuordnungsnotwendigkeit von nutzungsgenerierten Daten zu einem „user“ massiv im Widerspruch zu den Anliegen des Datenschutzes. Entsprechend dem DA-E müssten allgemeine Maßnahmen zur Erhebung auch für nutzergenerierte Daten mit Personenbezug ergriffen und dem Nutzer zugänglich gemacht werden. Insofern ergibt sich eine Zuordnungsnotwendigkeit, die auf die Ermöglichung der Zugänglichmachung unter einfachen Bedingungen abzielt. Dabei wird in Art. 1 Abs. 3 des DA-E zugleich ausdrücklich klargestellt, dass die DS-GVO in ihrer Anwendbarkeit und ihren Verpflichtungen uneingeschränkt auch für nutzungsgenerierte, personenbezogene Daten gilt. Entsprechende „technisch organisatorische Maßnahmen“ (TOM) aus Art. 25 und 32 DS-GVO – und die Prinzipien der Datensparsamkeit und Datenminimierung, welche insbesondere bei der Ausgestaltung der TOM berücksichtigt werden müssen, sollen laut EU-Kommission auch im Data Act Anwendung finden. Die TOM als allgemeine Voreinstellungen und Sicherheitsvorkehrungen für Datenverarbeitungen (u. a. Speicherung und Zurverfügungstellung) zielen jedoch darauf ab, vor einer beabsichtigten oder unbeabsichtigten Zugänglichmachung von Daten ab dem Zeitpunkt der Speicherung grundsätzlich zu verhindern und zu erschweren. Hieraus ergibt sich ein massiver Widerspruch zum DA-E, der den Zugang für den Nutzer so einfach wie möglich gestalten soll.

Ferner bedarf es einer Präzisierung wie die Anforderung, dass die bei ihrer Nutzung erzeugten Daten standardmäßig für den Nutzer einfach, sicher und direkt zugänglich sind („data access by design“ bzw. „by default“) in Einklang mit den von der EU-Kommission forcierten Produktregulierungen wie der Funkanlagenrichtlinie (RED) und der technischen Standardisierung zu mehr Daten- und Cybersicherheit gebrachten werden sollen.

Im Ergebnis ist zu befürchten, dass der Industrie die Aufgabe zufallen wird, die präzise Unterscheidung zwischen personenbezogenen Daten und nicht personenbezogenen Daten herzustellen. Im Umfeld von Maschinen- oder Prozessdaten existiert hier derzeit ein Bereich der Unsicherheit, da z.B. Prozessdaten, je nach Kontext, personenbezogen sein können –

aber nicht müssen. Die bisherige Unternehmenspraxis hat deshalb im Sinne der Risikovorsorge darauf abgezielt, im Zweifel die Vorgaben der DS-GVO einzuhalten, um keinen (mit empfindlichen Bußgeldern bewehrten) Datenschutzvorfall zu erzeugen.

Mit der derzeitigen Konstellation des DA-E wird dieses Verhalten nicht mehr möglich sein: Werden Daten nach bestem Wissen und Gewissen entsprechend den Vorgaben aus der DS-GVO nicht verfügbar gemacht, könnte ein Verstoß gegen den Data Act gegeben sein, der nach Art. 33 Abs. 3 DA-E in mit der DS-GVO identischem Bußgeld bewehrt ist. Würde hingegen ein Datum zu Unrecht als nicht-personenbezogen gewertet, läge ein ebenfalls bußgeldbewehrter Datenschutzverstoß aus der DS-GVO vor.

Unternehmen haben so keine Handlungsvariante, die „stets auf die sichere Seite" führen würde. Es ist nicht akzeptabel, dieses Risiko dem Unternehmer aufzubürden. Die eindeutige Bestimmung, was ein personenbezogenes Datum ist, ist Aufgabe des Verordnungsgebers, nicht der Industrie.

Die Informationspflichten vor Vertragsabschluss, die sich aus Art. 3 (2) DA-E ergeben, scheinen die Vorgaben aus Art. 13 und 14 DS-GVO zu spiegeln. Dies ist für den industriellen Kontext jedoch nur sehr schwer umsetzbar, da die anzugebenen Informationen stark vom Nutzerverhalten abhängig sind. Außerdem ist zu befürchten, dass sich die Informationspflichten aus Art. 3 (2) in Verbindung mit Art. 4 (6) DA-E, dass der Dateninhaber nicht personenbezogene Daten nur auf Grundlage einer vertraglichen Vereinbarung mit dem Nutzer des Produktes nutzen darf, stark innovationshemmend auswirken. Art. 4 (6) DA-E manifestiert faktische Eigentumsrechte an industriellen Daten, indem ausschließlich der „Nutzer" über die weitere Verfügbarkeit der Daten bestimmt. Durch den Ausschluss des „re-use" gemäß Art. 4(6) DA-E werden Produkt- und Prozessoptimierungen (und somit Nachhaltigkeit), Innovationen und digitale Wertschöpfung verhindert.

Ferner ist der in Art. 4 (6) DA-E manifestierten Zustimmungserfordernis in der Praxis nicht oder nur mit erheblichem Aufwand nachzukommen. Dies gilt bspw. bei indirekten Vertriebsmodellen, komplexen Lieferketten oder im Fall des Zweiterwerbs.

Sensoren im industriellen Kontext generieren große Mengen an Rohdaten, die keinen direkten Mehrwert für den Nutzer bieten. Es muss sichergestellt werden, dass aufgrund ihrer Beschaffenheit (Daten "as it is") keine Gewährleistungs- und/oder Haftungs-Ansprüche entstehen.

Es muss sichergestellt werden, dass die konzerninterne Weitergabe von Daten (z. B. von einer lokalen Vertriebseinheit an eine zentrale Verarbeitungseinheit oder Dateneinheit) nicht als Weitergabe an einen anderen Datenempfänger im Sinne der Nichtdiskriminierung (Art. 8 (3)) angesehen wird, da der Zweck einer solchen Weitergabe (konzerninterne Auslagerung bestimmter Verarbeitungsschritte, z. B. aufgrund zentraler F&E-Kapazitäten zur Verbesserung des Dienstleistungsniveaus für den Nutzer) den Markt nicht mehr beeinträchtigt, als wenn die Daten bei der ursprünglichen Konzerneinheit des Dateninhabers liegen.

Die Bereitstellung von Daten in industriellen Umgebungen, insbesondere von Rohdaten aus Sensoren und ähnlichen Geräten, erfordert eine Vielzahl von Voraussetzungen, die insbesondere aufgrund unterschiedlicher Topologien, Umgebungen, Kommunikationsprotokolle, Art der erfassten Daten usw. erfüllt werden müssen. Einzelfälle sind gemäß Art. 8 (3) DA-E daher nicht vergleichbar. Der geforderte Nachweis des Dateninhabers, dass die Umstände nicht vergleichbar sind und daher eine abweichende Datenfreigabe nicht diskriminierend ist, würde voraussetzen, dass der Dateninhaber

vertrauliche Geschäftsinformationen des anderen Datenempfängers, der für den Vergleich herangezogen wird, offen legt. Ferner erfordert Art. 9 (2) und (4) DA-E, dass dem Datenempfänger detaillierte Informationen zur Verfügung gestellt werden, die die Berechnung der Gegenleistung ermöglicht. Dies bedarf möglicherweise unverhältnismäßige und rechtswidrige Einblicke in budgetäre Geschäftsgeheimnisse und Kostenkalkulationen.

Die in Art. 8 (3) und Art. 9 (2) und (4) DA-E dargelegten Erfordernisse stehen somit im Widerspruch zu Art. 101 AEUV, der Wettbewerbern den Austausch wettbewerblich sensibler Daten im Grundsatz untersagt.

Sollten Daten gemäß Art. 11 (2) DA-E unsachgemäß genutzt oder weitergegeben worden sein, ist dies ein Straftatbestand und sollte entsprechend geahndet werden. Ferner hat, unabhängig davon, ob hieraus dem Datenbesitzer ein Schaden entstanden ist oder nicht, der Datenempfänger die Daten zu löschen. Entsprechend ist Art. 11 (3) DA-E zu streichen.

In Art. 13 (2) DA-E sind für eine Rechtssichere Anwendung die Beschreibungen „gröblich von der guten Geschäftspraxis abweicht“ sowie „redlichen Geschäftsverkehr“ genau zu definieren.

Ebenso bedarf es einer Konkretisierung von Art. 13 (4) DA-E, der eine Vielzahl unbestimmter Rechtsbegriffe enthält und offenbar dem deutschen AGB-Recht nachgebildet ist, ohne jedoch auf eine vergleichbare handelsrechtliche Regelungsdichte oder eine auch nur annähernd vergleichbare Entscheidungspraxis zurückgreifen zu können, die diese Begriffe mit Sinn füllen. Es ist mit einer enormen Zunahme von Vorabentscheidungsverfahren zu rechnen, deren Bearbeitung die europäischen Gerichte zeitlich stark beanspruchen, die Verfahrensdauer extrem verlängern und damit den Rechtsschutz in einschlägigen Fällen konterkarieren wird. Die Erfahrung aus dem deutschen Recht zeigt, dass es sehr schwierig ist, individuelle Vereinbarungen gemäß Art. 13 (5) zu treffen. In der Praxis werden deutsche Unternehmen dadurch massiv benachteiligt. Diese Fehlentwicklung gilt es im europäischen Recht nicht zu wiederholen.

Art. 13 (4) a) DA-E schließt „unangemessenen Beschränkungen“ in Verträgen aus. Hiervon ausgenommen werden sollten der Ausschluss des Rechtswegs bei nachweislich technischen Defekten.

In den in Art. 17 (1) DA-E dargelegten Anforderungen an öffentliche Stellen, sollte berücksichtig werden, dass die öffentliche Stelle klar definieren muss, wann diese beabsichtigt die Daten wieder zu löschen und ob die Technik der Pseudonymisierung ausreichend ist. Ferner muss Art. 19 (a) DA-E nachgeschärft werden, dass die Daten „ausschließlich zu dem bestimmten Zweck genutzt werden dürfen“.

Art. 24 (2) DA-E sieht vor, dass, sollte der in Art. 24 1 a und c vorgesehene verbindliche Zeitraum technisch nicht machbar sein, müsse dies in einem ausführlichen Bericht begründet werden. Der DA-E lässt hier notwendige Spezifikationen hinsichtlich “der technischen Machbarkeit” sowie des Inhalts des Berichts offen.

Der DA-E sieht in Kapitel 7 DA-E „Schutzvorkehrungen für nicht-personenbezogene Daten im internationalen Umfeld“ vor. Diese Vorschriften sind nicht zureichend ausgearbeitet und scheinen die Ansprüche der DS-GVO zu spiegeln. Damit wird dem Schutz von industriellen Daten ein Schutzniveau auferlegt, das normalerweise nur zum Schutz personenbezogener Daten und somit von Grundrechten erforderlich ist.

Dies birgt die Gefahr, unverhältnismäßigen bürokratischen Aufwands für die Unternehmen und das ungeklärte Fragen des Drittstaatentransfers von personenbezogenen Daten, die

sich aus dem Schrems II Urteil ergeben, auch auf den Bereich der nicht-personenbezogenen Daten übertragen werden. Damit wird das Risiko, die Bewertung von (stark politisch beeinflussten) Faktoren vorzunehmen, auf private Unternehmer verlagert. Es ist notwendig, den Unternehmer von dieser Verantwortung zu entlasten. Mehr Klarheit ist auch in Bezug auf die Anforderung erforderlich, "alle angemessenen technischen, rechtlichen und organisatorischen Maßnahmen" zu ergreifen, um einen unrechtmäßigen Zugang oder eine unrechtmäßige Übertragung von Daten außerhalb der EU zu verhindern. In Erwägungsgrund 78 wird eine Reihe von Maßnahmen genannt, darunter die Verschlüsselung von Daten. Die genaue Art der Schutzmaßnahmen, die umgesetzt werden müssen, sollte jedoch genauer definiert werden und bestehende Standards und Rahmenwerke berücksichtigen, die von Industrie-Initiativen wie Gaia-X entwickelt werden.

Es sollte auch sichergestellt werden, dass die Bestimmungen des DA-E mit anderen Governance-Modellen vereinbar sind und insbesondere genügend Raum für Data-Governance-Modelle lassen, die in europäischen Dateninitiativen wie Gaia-X oder den europäischen Datenräumen entwickelt werden. Insbesondere für kleinere Akteure in der Datenwirtschaft werden Modelle für Data Governance sehr wichtig sein, um Transaktionskosten zu senken und Rechtssicherheit zu erhöhen.

Auswirkung auf Geschäftsmodelle / Praxisbeispiele

Der DA-E zielt darauf ab durch eine verbesserte Datenallokation die digitale Wertschöpfung zu steigern. Dies sollte jedoch nicht auf Kosten bestehender Geschäftsmodelle geschehen. Im Folgenden wird anhand von Praxisbeispielen demonstriert, wie durch ungenaue Begriffsdefinitionen sowie ein sehr vereinfachtes Verständnis von industriellen Wertschöpfungsketten negative Auswirkungen auf bestehende Geschäftsmodelle zu erwarten sind.

Praxisbeispiel 1: Sensorhersteller im ZVEI-Leitmarkt Gebäude

Ein Unternehmen verkauft im B2B-Bereich Sensoren, die vielfältige Umweltdaten erfassen, wie z.B. Lufttemperatur, Luftfeuchtigkeit, Tür- oder Fensterkontakte, etc. Die so gesammelten Daten werden vom Unternehmen über Gateways einer Daten- und Prozessplattform zugeführt, die der Kunde entweder selber betreibt oder über den Sensorhersteller als SaaS mieten kann. Der Kunde kann dann die so erfassten Daten überwachen, auswerten, automatische Alarme konfigurieren, etc.

Zunächst einmal wäre im vereinfachten Sinne des DA-E dieses Unternehmen Hersteller und somit auch Dateninhaber. Tatsächlich hat der Sensorhersteller jedoch keinerlei Zugriff auf die von ihren Sensoren gelieferten Daten. Die Datenhoheit für die so generierten Daten liegt stets bei den Kunden.

Sollte das Unternehmen nun die Anforderungen aus dem DA-E erfüllen müssen, die bei der Nutzung erzeugten Daten direkt (Art. 3 (1) DA-E) zu einer angemessenen Gegenleistung (Art. 9 DA-E) und/oder einem Dritten unverzüglich, für den Kunden kostenlos (Art. 5 DA-E) bereitzustellen, wäre das gegenwärtige Geschäftsmodell nicht mehr tragfähig. Die Kosten für den Betrieb eines Rechenzentrums auf die erwartete Lebensdauer der Sensoren umzulegen, wäre so teuer, dass das Geschäft implodieren würde.

Die Anforderung, dass der Kunde problemlos zwischen verschiedenen „Auswertediensten“ wechseln können soll (Art. 28 DA-E), hätte auch Auswirkungen auf den Sensor-Hersteller, da

die Anforderungen an die Datenstruktur sich je nach Auswertesystem erheblich unterscheiden. Insbesondere die sektorübergreifende Interoperabilität wird durch die vorhandenen, sehr unterschiedlichen Datenstandards des jeweiligen Sektors und ggf. der verschiedenen Domains innerhalb eines Sektors, zu erheblichen Aufwendungen einer übergreifenden Standardisierung führen.

Bislang war es möglich, gemeinsam mit einem Kunden im B2B – Bereich die Datenstruktur für die Migration zu optimieren. Die üblicherweise durch eine Standardisierung erreichten Skaleneffekte sind im B2B – Bereich nicht zu erwarten, da die Migrationsinhalte vollkommen individuell sind und ggf. auch über Patente o.Ä. geschützt sein können. Solche Services sind heutzutage Teil des Geschäftsmodells im B2B – Segment, was nicht mehr zulässig wäre oder nach Art. 5 Abs. 1 DA-E umgangen werden könnte

Auch für Anbieter von Datenverarbeitungsdienste muss der DA-E deutlicher definieren, was genau mit den Begriffen „“dieselbe Dienstart“ (Art. 26 (2) DA-E) und „offene Schnittstelle“ (Art. 26 (1) DA-E) gemeint ist. Eine solche API kann gerade bei datenintensiven Services enorme Kosten verursachen und somit neue Geschäftsmodelle schnell unwirtschaftlich werden lassen. Aus Wettbewerbsgründen sind die in Art. 26 aufgeführten technischen Aspekte den Wettbewerbern zudem nicht bekannt. Diese öffentlich zu machen, würde Wettbewerbsverluste nach sich ziehen. Datenverarbeitungsdienste insbesondere aus dem KMU-Bereich können die „Gleichwertigkeit der Funktionen“ beim Wechsel zu einem Konkurrenzprodukt finanziell nicht abbilden. Durch diese Anforderung werden insbesondere kleine Anbieter aus dem Markt gedrängt, da diesen unverhältnismäßig großen bürokratischen und finanziellen Aufwänden auferlegt werden.

Praxisbeispiel 2 aus dem ZVEI-Leitmarkt Industrie

Der Einsatz einer kollaborativem Zustandsüberwachung soll eine möglichst störungsfreie, effektive und effiziente Produktion ermöglichen. Dazu werden Daten aus der Maschine, der Maschinenkomponente oder dem Maschinenumfeld benötigt. Diese Daten sind vielschichtig und unorganisiert. Zudem fehlen dem Produktbetreiber die notwendigen Meta-informationen, um die Daten korrekt interpretieren zu können.

Bei einer einfachen Zustandsüberwachung kann aufgezeigt werden, dass eine Störung eingetreten ist oder eine Störung möglichweise eintreten wird. Weitere Verbesserungen sind schwer möglich und die damit bereitgestellte Lösung nicht ausreichend. Beispielsweise kann ein Füllstandsensor dem Maschinenbetreiber signalisieren, dass der Schmiermittelfüllstand zu gering ist und nachgefüllt werden muss. Tritt die Meldung während der Produktion über das Wochenende auf, ist die Produktion unterbrochen und der Produktionsausfall hoch. Eine zeitlich basierte Vorhersage des Ausfalls ist ungenau. Wird nun versucht die XYZ-Verfahrwege (entsprechend xyz-Achsen im dreidimensionalen kartesischen Koordinatensystem)zu erfassen, um die Leerung des Behälters exakter prognostizieren zu können zeigt sich, dass sich aus diesen Daten die Geometrien der produzierten Teile rekonstruieren lassen. Möglicherweise handelt es sich dabei bereits um geschäftskritische Informationen oder um schützenswerte Informationen zu denen auch meist vertragliche Verpflichtungen bestehen.

Zudem ist die Benutzerinteraktion ein wichtiges Element zur Störungsbeseitigung. Einfache Ein/Aus Schaltvorgänge die zum falschen Zeitpunkt ausgelöst wurden, stehen im Zusammenhang mit Wartungsintervallen oder Gewährleistungsansprüchen. Ist der Nutzer bekannt, wird die Grenze zu personenbezogenen Daten im IoT Umfeld unscharf.

Der Aufwand in Erhebung, Auswertung und Ableitung sowie den Datenschutz zu gewährleisten ist enorm und bedarf organisatorischer und prozessualer Veränderung bei den Datenverwertern. Die Investition zahlt sich durch zielgerichtete Produkte aus, die nach der Nutzung ausgelegt werden können. Das führt zu einer besseren Nutzung und Wiederverwertbarkeit und trägt zur Schonung der Ressourcen bei.

Viele Beratungsprodukte und Services beruhen darauf, die Produktionsabläufe von Kunden zu analysieren und Verbesserungspotentiale aufzuzeigen. Art. 4 (6) DA-E würde einen großen Graubereich schaffen, weil a priori schwer nachweisbar ist, dass die Informationen zur Entwicklung von Services genutzt werden und nicht zum Nachteil des Betroffenen eingesetzt werden.

Praxisbeispiel 3 aus dem ZVEI Leitmarkt Consumer

Konformität mit DS-GVO

Wenn Unternehmen ihre Produkte nicht selbst an Endkunden vertreiben, sondern in der Zwischenebene Händler einsetzen, dann kennen die Unternehmen als Dateninhaber ihre Endkunden als Nutzer nicht. Sofern eine Bereitstellung der Daten, die der Nutzer beim Dateninhaber generiert, nicht wie in Art. 3 gefordert, direkt mit dem Produkt zur Verfügung stellen kann (z.B. vernetzte Elektrowerkzeuge, deren Daten aber nur via Kopplung App oder beim Auslesen des Chips im Reparaturfall möglich ist), dann muss diese Bereitstellung der Daten nach Art. 4 auf elektronischem Wege erfolgen. Wie kann hier sichergestellt werden, dass die Daten der rechtmäßige Nutzer erhält und der Dateninhaber, weil auch personenbezogene Daten bereitgestellt werden können, keinen Datenschutzverstoß begeht? Da das Werkzeug in einem Betrieb mehrere Mitarbeiter verwenden können, müsste sichergestellt werden, dass nur diejenigen personenbezogenen Maschinendaten zur Verfügung gestellt werden, die der konkrete Nutzer generiert hat. Dies ist de facto nicht möglich. Dasselbe gilt auch für den in EG 20 genannten Vorschlag der Einrichtung eines Nutzerkontos; wie kann hier sichergestellt werden, dass der rechtmäßige Nutzer das Gerät mit dem Nutzerkonto koppelt und damit seine Daten erhält und nicht diejenigen eines Dritten?

Wenn mehrere die Produkte in Gebrauch haben (z.B. weil die Schreinerei Werkzeuge als Arbeitsmittel beschafft für seine Mitarbeiter und alle diese Zugriff auf die Werkzeuge haben), dann generieren sie allesamt Daten beim Dateninhaber. Nach dem aktuellen Wortlaut müssen dem „Nutzer“ die generierten Daten zur Verfügung gestellt werden, was demzufolge alle Mitarbeiter der Schreinerei sind. Wenn die Unternehmensleitung selbst die Produkte nutzt und, wie bereits in den vorherigen Beispielen angemerkt, eine Trennung zwischen den Daten unterschiedlicher Nutzer nicht möglich ist und dies auch vom Dateninhaber nicht kontrolliert werden kann, dann erhält sie möglicherweise personenbezogene Informationen über die Mitarbeiter, die sie voraussichtlich nicht haben dürfte. Begehen der Dateninhaber und/oder die Unternehmensleitung dann einen Datenschutzverstoß? Liegt es im Verantwortungsbereich des Dateninhabers, dass der Unternehmensleitung durch die Datenbereitstellung Möglichkeiten zur Leistungs- und Verhaltenskontrolle der Mitarbeiter an die Hand gegeben werden? Darüber hinaus findet sich auch hier wieder die Problemstellung, dass man (a) anderen (auch Mitarbeitern, nicht nur der Unternehmensleitung) Informationen über andere zur Verfügung stellt und (b) als Dateninhaber die Rechtmäßigkeit nicht überprüfen kann, z.B. wenn ein Mitarbeiter kündigt oder de facto das Gerät nicht nutzt, die

Datenbereitstellung aber einfordert. Hier bleibt dasselbe Authentifizierungsthema wie in den vorgenannten Beispielen.

Rechtssicherheit bei Weiterverkäufen oder Diebstahl

Bei Weiterverkäufen von Produkten, bei denen eine Bereitstellung der Daten nicht direkt per Design zur Verfügung gestellt werden kann, erhält der Hersteller als Dateninhaber keinerlei Info über den Weiterverkauf. Wie kann der Dateninhaber bei einem Nutzerkonto sicherstellen, dass der Nutzer rechtmäßig im Besitz dieser Maschine ist und somit rechtmäßig die Daten anfordert? Müssen hier Kaufvertrag o.Ä. Dokumente als Nachweis erbracht werden? Wie wird darüber hinaus sichergestellt, dass dem ursprünglichen Eigentümer nicht weiterhin die Daten (des Neuen) zur Verfügung stehen? Demselben Problem sieht man sich ausgesetzt im Falle des Diebstahls von Produkten.

Herausgeber:

ZVEI e.V.
Abteilung Digital- & Innovationspolitik

Lyoner Str. 9
60528 Frankfurt am Main

Verantwortlich:
Dominic Doll
Manager Digitalisierung und Innovationspolitik

Telefon: +49 30 306960-19
E-Mail: dominic.doll@zvei.org

www.zvei.org

12. Mai 2022

Über den ZVEI

Der ZVEI vertritt die gemeinsamen Interessen der Elektro- und Digitalindustrie und der zugehörigen Dienstleistungsunternehmen in Deutschland und auf internationaler Ebene.

Die Branche beschäftigt rund 877.000 Arbeitnehmerinnen und Arbeitnehmer im Inland. 2021 lag ihr Umsatz bei rund 200 Milliarden Euro.

Fast ein Viertel aller privaten F+E-Aufwendungen in Deutschland kommen von der Elektroindustrie. Jährlich wendet die Branche rund 20 Milliarden Euro für F+E auf und mehr als sechs Milliarden Euro für Investitionen. Ein Drittel des Branchenumsatzes entfallen auf Produktneuheiten. Jede dritte Neuerung im verarbeitenden Gewerbe insgesamt erfährt ihren originären Anstoß aus der Elektroindustrie.

ZVEI e. V.