Compliance Handbuch EU Data Act

Rechtssichere Implementierung des neuen EU-Datengesetzes in der Praxis

Herausgegeben von

Sebastian Rockstroh
Rechtsanwalt (Syndikusrechtsanwalt), Ingolstadt

Dr. Peter Katko
Rechtsanwalt und Digital Law Leader bei EY Law

Eric Meyer
Senior Associate bei EY Law

Carl Heymanns Verlag 2025

Bibliografische Information der Deutschen Nationalbibliothek
Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.d-nb.de abrufbar.

ISBN 978-3-452-30432-2

www.wolterskluwer.com

Die Ausführungen in diesem Buch dienen lediglich als Anregungen und Arbeitshilfen. Die Verantwortung bei Anwendung und Umsetzung des Data Act liegt beim Benutzer. Herausgeber, Autoren und Verlag übernehmen keine Haftung für die Richtigkeit und Vollständigkeit der enthaltenen Ratschläge und Positionen.

Zur erleichterten Lesbarkeit wird im Text auf die gleichzeitige Nennung weiblicher, männlicher und diverser Sprachformen verzichtet und nur die männliche Form verwendet. Sämtliche Nennungen gelten jedoch selbstverständlich gleichermaßen für alle Geschlechtsformen.

Verlag, Herausgeber und Autoren übernehmen keine Haftung für inhaltliche oder drucktechnische Fehler.

Umschlagkonzeption: Martina Busch, Grafikdesign, Homburg-Kirrberg
Satz: Datagroup-Int SRL, Timisoara, Romania
Druck und Weiterverarbeitung: Sowa Sp. z o.o., Piaseczno, Polen

Gedruckt auf säurefreiem, alterungsbeständigem und chlorfreiem Papier.

Vorwort

Willkommen zu unserem Handbuch Data Act.

Von manchen als Meilenstein der europäischen Datenregulierung betrachtet ist zentraler Inhalt des Data Act der Anspruch der Nutzer von vernetzten (IoT) Geräten auf Zugang sowie Bereitstellung der im Rahmen des Betriebs generierten Daten. Die technische Umsetzung bedeutet für die Hersteller jedoch erheblichen Aufwand, weshalb auch viel Kritik am Data Act laut wurde. Tatsächlich stellt sich die Frage, ob so viele brachliegende und gleichzeitig werthaltige Datensilos bei Herstellern und Dateninhabern vorhanden sind, die diese regulatorischen Eingriffe rechtfertigten. Können also mit implementierungsintensiver Regulatorik Geschäftsmodelle befördert werden oder lässt wie schon bei der DSGVO dieser Ansatz Innovation aus der EU abwandern? Andererseits ist der Data Act nun erst einmal bindend Gesetz geworden; als Herausgeber dieses Handbuchs möchten wir die relevanten Stakeholder aufseiten von Herstellern, Dateninhabern und Anbietern bei der Umsetzung des Data Act unterstützen. Dies mit Erfahrung aus der Umsetzungspraxis; und über juristische Interpretation hinaus auch mit Schemata und optischen Darstellungen.

Im Teil 1 geht es um Datenzugang und Datennutzung. Also einerseits die Gestaltung des Datenzugangs (»Access by Design«) und andererseits der Workflow im Hinblick auf die Datenbereitstellung mit dem Fokus auf Authentifizierung, Bestimmung der Daten, Datenschutz sowie Schutz von Geschäftsgeheimnissen. Darüber hinaus werden mögliche Leitplanken für die Gestaltung von Verträgen zwischen einerseits Dateninhabern und anderseits Nutzern und Dritten dargestellt. Die Vielzahl der Themen macht jedoch auch hier augenfällig, dass operative Aufwände für IoT-Hersteller und Betreiber beträchtlich sein werden.

Im Teil 2 geht es dann um die Bereitstellung von Daten der Privatwirtschaft an den öffentlichen Sektor (Business to Government – B2G). Zwar hat die Corona-Pandemie gezeigt, dass in bestimmten Notlagen der öffentliche Sektor mit einer größeren Datengrundlage punktgenauer agieren kann. Aber auch hier stellt sich die Frage, ob nicht sektoral schon ausreichend Berichtspflichten und Zugriffsmöglichkeit bestehen. Die Praxis wird weisen, inwieweit Unternehmen durch die Vorbereitung auf diese Bereitstellungspflichten wie schon bei Access-by-Design erhebliche Kosten entstehen.

Im Teil 3 wird durch Möglichkeiten zum Wechsel des IT-Cloudproviders sowie Interoperabilität versucht, Lock-In-Effekte im IT Betrieb aufzulösen. Kunden von IT-Services soll es erleichtert werden, zu anderen Anbietern zu wechseln. Nachdem das Universum von IT-Dienstleistungen sich immer mehr in die Cloud bewegt, dürfte die Basis für leichteren Anbieterwechsel in der IT geschaffen werden. In der Praxis werden die starke Verzahnung in der Welt des jeweiligen IT-Serviceprovider nebst Migrationsaufwand weiterhin hohe faktische Hürden darstellen. Mit den Transparenzpflichten bei Drittstaatentransfers knüpft der Data Act an Regelungen der DSGVO an – wie schon beim Datenzugang mit der Datenportabilität.

Abschließend möchten wir als Herausgeber betonen, dass uns jedenfalls daran gelegen ist, ein möglichst praxisnahes Werk zum Data Act mit vielen Anwendungshinweisen zu schaffen – unabhängig von der rechtspolitischen Kritik. Insofern gilt unser besonderer Dank den kompetenten Mitautoren sowie Julie Tiltmann und Silvana Redfearn für ihre geduldige Unterstützung.

Wir wünschen viel Spaß beim Lesen.

Ihre Herausgeber

Sebastian Rockstroh, Dr. Peter Katko und Eric Meyer

Autorinnen und Autoren

Birnbauer, Daniela, (LL.M.), MA (Wien) Rechtsanwältin, Wien	Abschnitt 1, Kapitel 2, F.
Bürckel, Lorena (LL.M.) Rechtsanwältin (Syndikusrechtsanwältin), Stuttgart	Abschnitt 1, Kapitel 2, H.
Mag. Dannhausen, Estella, Bsc. LL.M. (Uni Wien) Rechtsanwältin, Wien	Abschnitt 1, Kapitel 2, D.
Foerster, Martin Projectmanager Data & AI Porsche AG, Berlin	Abschnitt 1, Kapitel 2, F.
Frison, Laura, LL.M. Eur. (München) Rechtsanwältin (Syndikusrechtsanwältin), Ingolstadt	Abschnitt 1, Kapitel 2, E. Abschnitt 1, Kapitel 2, I.
Dr. Katko, Peter EY Digital Law Leader, München	Abschnitt 1, Kapitel 1 Abschnitt 1, Kapitel 2, A. I Abschnitt 1, Kapitel 2, A. II. 1. Abschnitt 1, Kapitel 2, E.
Krug, Nicole, LL.M. (London) Rechtsanwältin (Syndikusrechtsanwältin), Kassel	Abschnitt 1, Kapitel 2, H.
Leuthner, Christian Rechtsanwalt, Partner, Frankfurt	Abschnitt 1, Kapitel 2, H.
Meyer, Eric Senior Associate EY Law, München	Abschnitt 1, Kapitel 1 Abschnitt 1, Kapitel 2, A. II. 2. Abschnitt 1, Kapitel 2, A. II. 5 Abschnitt 1, Kapitel 2, C. Abschnitt 1, Kapitel 2, F.
Peschel, Christopher Rechtsanwalt (Syndikusrechtsanwalt), Erlangen	Abschnitt 1, Kapitel 2, G. Abschnitt 1, Kapitel 2, I. Abschnitt 1, Kapitel 3
Reich, Lennart Rechtsanwalt, Baker McKenzie, Stadtbergen	Abschnitt 2, Kapitel 4 Abschnitt 2, Kapitel 5 Abschnitt 2, Kapitel 6 Abschnitt 2, Kapitel 7
Rockstroh, Sebastian Rechtsanwalt (Syndikusrechtsanwalt), Ingolstadt	Abschnitt 1, Kapitel 2, D.
Schall, Tobias Rechtsanwalt EY Law, München	Abschnitt 1, Kapitel 2, B. Abschnitt 3, Kapitel 8 Abschnitt 3, Kapitel 9
Schels, Stefan Rechtsanwalt (Syndikusrechtsanwalt), Ingolstadt	Abschnitt 1, Kapitel 2, A. II. 3. Abschnitt 1, Kapitel 2, E. Abschnitt 1, Kapitel 2, G.

Schultz, Marion Rechtsanwältin, Geschäftsführende Gesellschafterin Trenchant Rechtsanwalts-GmbH, Nürnberg	Abschnitt 3, Kapitel 8 Abschnitt 3, Kapitel 9
Dr. iur. Schwinger, Florian Rechtsanwalt (Syndikusrechtsanwalt), Ingolstadt	Abschnitt 1, Kapitel 2, A. II. 4. Abschnitt 1, Kapitel 2, A. II. 6. Abschnitt 1, Kapitel 3
Schwarz, Alexander Rechtsanwalt und Partner Shepherd & Black PartGmbB, Nürnberg	Abschnitt 1, Kapitel 2, A. II. 2. Abschnitt 1, Kapitel 2, C. Abschnitt 1, Kapitel 2, G.
Tannen, Florian Rechtsanwalt, Partner bei Baker McKenzie, München	Abschnitt 2, Kapitel 4 Abschnitt 2, Kapitel 5 Abschnitt 2, Kapitel 6 Abschnitt 2, Kapitel 7
Weiß, Rebekka, LL.M. (Glasgow) Leiterin Regulierungspolitik, Microsoft Deutschland GmbH, Berlin	Abschnitt 3, Kapitel 8 Abschnitt 3, Kapitel 9
Dr. Wiesemann, Hans Peter Rechtsanwalt, München	Abschnitt 1, Kapitel 2, B. Abschnitt 1, Kapitel 3
Zimmermann, Robert Rechtsanwalt (Syndikusrechtsanwalt), Wolfsburg	Abschnitt 1, Kapitel 3

Inhaltsübersicht

Inhaltsverzeichnis

sollten unternehmensintern Prozesse definiert werden, um die in der Datenbank enthaltenen Informationen aktuell zu halten.

Im **Online-Handel** sollten die **Produktbeschreibungen** frühzeitig um die entsprechenden Informationen **ergänzt** werden. 129

Im **Offline-Handel** sollten – soweit möglich – **Produktverpackungen** um die entsprechenden Informationen bzw. eine **Link** oder einen **QR-Code** auf diese Informationen ergänzt werden. Falls dies nicht möglich ist, sollten frühzeitig die entsprechenden **Aufsteller** oder **Aufkleber** bereitgehalten werden. 130

C. Access by Design (Art. 3 DA)

I. Einführung

Der Data Act etabliert in Art. 3 Abs. 1 die Verpflichtung für Hersteller von **vernetzten Produkten** und Anbietern von **verbundenen Diensten**, Nutzern standardmäßig Zugang zu ihren **Produktdaten** und **verbundenen Dienstdaten** zu verschaffen. Diese Verpflichtung stellt dabei keinen Anspruch des Nutzers gegenüber dem Hersteller oder Anbieter dar, sondern ist eine *ex lege* Verpflichtung, die der Hersteller oder Anbieter bei der Entwicklung seiner vernetzten Produkte oder verbunden Dienste berücksichtigen muss. Sie gilt für derartige Produkte und Dienste, die nach dem 12. September 2026 in Verkehr gebracht werden (vgl. Art. 50 UAbs. 3 DA). Im Ergebnis etabliert der Gesetzgeber hier eine »**Access by Design**«-**Anforderung** an derartige Produkte und Dienste. 131

Insbesondere die Design-Anforderung der direkten Zugriffsmöglichkeit auf Produktdaten hat naturgemäß weitreichende Konsequenzen für die technischen wie organisatorischen Gegebenheiten und Prozesse beim Hersteller. Denn anders als die **ohne Weiteres verfügbaren Daten**, welche nach Art. 4 bzw. Art. 5 DA bereitzustellen sind (im Detail hierzu unter Rdn. 44 ff.; sowie Abschnitt 1, Kapitel 2, Titel D. und E.), bezieht sich Art. 3 auf alle Produktdaten bzw. verbundenen Dienstdaten, die das vernetzte Produkt bzw. der verbundene Dienst bei seiner Nutzung generiert und die zur Ausleitung konzipiert sind. Diese Datenkategorien müssen daher nicht bereits beim Dateninhaber/Hersteller in dessen Servern/Backends vorliegen, um vom Anwendungsbereich des DA umfasst zu sein. 132

So schlussfolgert auch *Bomhard* richtigerweise, dass »*[a]ngesichts der sehr weiten Datendefinition in Art. 2 Abs. 1 DA als auch der Tatsache, dass personenbezogene Daten und nicht-personenbezogene Daten aufgeführt werden, […] jedes denkbare Datum von Art. 1 Abs. 2 DA und damit vom Data Act umfasst sein [dürfte]*«[46], was auch die Produkt- und verbundenen Dienstdaten nach Art. 2 Nr. 15 und 16 DA praktisch sehr umfassend macht. 133

46 *Bomhard*, »Der Anwendungsbereich des Data Act – Offene Fragen rund um Art. 1 DA«, MMR-Beil. 01/2024, S. 72.

134 So fallen beispielsweise bei einem modernen Fahrzeug mit rund 20.000 Datenpunkten, die sich in Zeitabständen von Zehntelsekunden bis Sekunden aktualisieren und potenziell ausleitbar sind, Datenmengen an, die rasch in die Terabyte gehen.[47] Von diesen Daten wird aktuell nur ein Bruchteil tatsächlich aus dem Fahrzeug ausgeleitet, da jedes übertragene Kilobyte mit **Kosten** verbunden ist, etwa für den Datentransport (d.h., Kosten des Mobilfunkanbieters), das Speichern (d.h., Kosten für die Server) und die Verarbeitung durch Mensch und Computer. Die Kosten einer jeden Datenausleitung sind daher gegen den wirtschaftlichen Vorteil des Nutzbarmachens dieser Daten abzuwägen. Davon abgesehen ist eine kontinuierliche **Echtzeit-Übertragung** von den anfallenden Datenmengen mit der derzeitig verfügbaren LTE/5G-Technologie technisch unmöglich. Die häufig beschworenen Datenmonopole sind in der Automobil-Branchen vor diesem Hintergrund daher bloß beschränkt vorhanden, da Hersteller auf die im Fahrzeug generierten Daten zwar theoretisch zugreifen könnten, dies aus Kostengründen jedoch nur sehr eigeschränkt tun bzw. die technischen Möglichkeiten eine umfassende Ausleitung derzeit auch gar nicht erlauben. So werden von den Automobilherstellern selbst nur selektiv und in vorab definierten Umfängen bestimmte Daten aus zuvor festgelegten Fahrzeugen im Rahmen der rechtlichen Zulässigkeit für einen vorab determinierten Zeitraum ausgeleitet. Die so erhobenen Daten unterscheiden sich somit von Fall zu Fall und stellen in keiner Weise eine kontinuierliche und in Echtzeit nutzbare Zugriffsmöglichkeit dar. Vielmehr dürfte es sich bei derart ausgeleiteten Daten, die der Hersteller zu eigenen konkreten Zwecken nutzt, um ohne Weiteres verfügbare Daten handeln, die Nutzer vom Hersteller als Dateninhaber nach Art. 4 DA verlangen können.

135 Die Verpflichtung des Art. 3 Abs. 1 DA stellt Hersteller daher vor unerwarteten technischen, organisatorischen und letztlich auch finanziellen Herausforderungen. Dabei hat der Gesetzgeber es leider verpasst, die unterschiedliche Komplexität von vernetzten Produkten zu berücksichtigen und für eine entsprechende praktische **Verhältnismäßigkeit** der verschiedenen Hersteller zu sorgen. Denn praktisch dürften Hersteller von etwa Smartwatches, Fitness-IoT Geräten oder etwa »smarten« Staubsaugern vor weniger komplexen Herausforderungen nach Art. 3 DA stehen, wie Automobilhersteller oder Herstellern großer, komplexer IoT-Produktionsanlagen. Hersteller der vorherigen Produktkategorien haben bereits heute etablierte Zugriffsmöglichkeiten der Nutzer auf die Gerätedaten, sei es am dem jeweiligen Produkt selbst oder mittelbar über damit verbundene Applikationen, wie »Health Apps«. Viel entscheidender dürfte aber der Fakt sein, dass eine Smartwatch eine viel geringere Datenmenge bei der Nutzung produziert als etwa das moderne Fahrzeug.

136 Unabhängig von dieser Verhältnismäßigkeitsdiskussion, sind im Ergebnis Entwickler und Hersteller von vernetzten Produkten angehalten, ihre **Entwicklungsprozesse**

47 *»Connected cars are forecast to make up 95% of all vehicles on the road by 2030, with each one generating an estimated 25 gigabytes of data per hour, which is the same amount of data as it would take someone to stream 578 hours of music.«* Quelle: https://www.zdnet.com/article/connected-cars-powered-by-ai-will-make-up-95-of-all-vehicles-on-the-road-by-2030/; https://www.comparitech.com/blog/information-security/how-much-data-does-your-car-log/.

um die Anforderung »**Access by Design**« zu erweitern. Dies kann mit mal mehr, mal weniger Aufwand einhergehen und ist abhängig von der Komplexität des herzustellenden vernetzten Produkts.

Um bei dem Beispiel der Automobilindustrie zu bleiben, so muss das vernetzte Produkt »Fahrzeug« so konzipiert und hergestellt werden, dass auch dem Nutzer Produktdaten zugänglich sind. Wie dieser Zugang im Detail erfolgen muss, ob er etwa direkt oder »mittelbar direkt« erfolgen kann (sprich direkt im Fahrzeug mittels Schnittstelle oder via remote Server-Lösung), bleibt bis zur abschließenden Klärung durch den EuGH abzuwarten. Es spricht einiges dafür, dass Hersteller von vernetzen Produkten hier eine **Abwägung** treffen können, wie sie die Anforderung aus Art. 3 DA erfüllen möchten. Die **EU Kommission** spricht sogar von einem **Wahlrecht**, ob der Zugriff direkt oder indirekt (nach Art. 4 Abs. 1 DA) erfolgen soll (ausführlich dazu unten im Abschnitt II.).[48] In jedem Fall muss der Zugang für den Nutzer zu seinen Produktdaten aber *einfach, sicher und unentgeltlich* sein. Dies stellt die Automobilhersteller wie die gesamte Branche mit ihren produktbedingten langen Entwicklungszyklen, die eher als Jahrzehnt als Jahre gedacht werden vor erhebliche Hürden, gesetzliche Anforderungen mit fundamentalen Auswirkungen auf die fahrzeuginterne Dateninfrastruktur bei relativ kurzen Umsetzungsfristen zur erfüllen. Eine solche Schnittstelle kann daher realistisch erst in zukünftigen Fahrzeuggenerationen vernünftig eingeplant, entwickelt und umgesetzt werden. Bis dahin stehen Fahrzeughersteller vor der Herausforderung, eine Beurteilung für jene Modelle vorzunehmen, die noch lange nach dem Geltungsbeginn des Art. 3 Abs. 1 DA am 12.09.2026 vom Fertigungsband laufen werden, ob eine Anpassung für eine direkte Schnittstelle im Fahrzeug relevant und technisch durchführbar ist. Über diese direkte oder indirekte Schnittstelle müssen in weiterer Folge Datenmengen zugänglich gemacht werden, die in dem nach dem DA geforderten Ausmaß bislang nicht vorgesehen waren. Entsprechend gering fallen die aktuellen (und für kommende Fahrzeuggenerationen bereits geplanten) Kapazitäten aus. 137

Dabei darf nicht außer Acht gelassen werden, dass der DA gleichzeitig verhindern soll, dass Anreize für Investitionen in vernetzte Produkte, von denen die Daten erlangt werden, verloren gehen.[49] In diesem Sinne sieht Art. 9 DA vor, dass Dateninhaber von Dritten, denen sie die Daten bereitstellen, eine **angemessene Gegenleistung** fordern können, um unverhältnismäßige Belastungen bei Datenzugang und Datennutzung zu vermei- 138

48 EU Kommission, »Frequently Asked Questions« (v. 1.2), S. 17 (abrufbar unter: https://digital-strategy.ec.europa.eu/en/library/commission-publishes-frequently-asked-questions-about-data-act [letzter Abruf: 3. Februar 2025]) (Hervorhebung durch den Autor): *»By the date of entry into application of the Data Act (12 September 2025), products already on the market and new products (when placed on the market) must allow for data to be accessed by the user.* ***By this date, manufacturers have to decide whether such access will be made directly or indirectly (cf. Article 4[1]).*** *Companies will find practical ways to incentivize the use of the solution that works best for them. Sectoral legislation can be more specific.«.*

49 Vgl. Erwgr. 32 DA.

den. Andernfalls wäre die Datenweitergabe wirtschaftlich nicht mehr tragfähig.[50] Eine solche Entschädigung soll insbesondere jene Kosten umfassen, die mit der Bereitstellung der Daten verbunden sind, wie beispielsweise Kosten, die für die Wiedergabe, die elektronische Verbreitung, die Speicherung und die Formatierung der Daten anfallen.[51]

139 Der europäische Gesetzgeber hat damit im Kontext des Art. 5 DA klargestellt, dass jede Datenbereitstellung mit entsprechenden Kosten verbunden ist. Nichts anderes kann für die Datenzugangsansprüche des Nutzers gelten. Zwar hat sich der europäische Gesetzgeber in dieser Konstellation dazu entschieden, dem **Nutzer** ein **kostenfreies Zugangsrecht** einzuräumen. Dennoch darf die grundsätzliche **Interessensabwägung** auch hier nicht außer Acht gelassen werden: eine unverhältnismäßige Belastung der Normadressaten (Hersteller und Anbieter) muss verhindert werden, andernfalls kein Anreiz mehr besteht, überhaupt noch Daten zu generieren und zu erheben.

140 Neben der Schaffung eines Zugangs für Nutzer durch die Hersteller und Anbieter, treffen die Verkäufer, Vermieter oder Leasinggeber von diesen vernetzten Produkten oder verbunden Diensten – bei dem es sich auch um den Hersteller oder Anbieter handeln kann – **Transparenzanforderungen** gegenüber dem Nutzer.[52] Der Gesetzgeber möchte damit den Nutzer als »Herr seiner Daten« etablieren, und die Information nach Art. 3 Abs. 2 und 3 DA ist dabei die Voraussetzung, den Nutzer über die Datenfähigkeiten der vernetzten Produkts als auch über die entsprechenden Datenempfänger, als mögliche Adressaten seiner Datenbereitstellungsansprüche nach Art. 4 und 5 DA, bestmöglich und umfänglich in Kenntnis zu setzen.

II. Rechtliche Inhalte – Die einzelnen Elemente und Anforderungen von Art. 3 DA

1. Die konkreten Designanforderungen an vernetzte Produkte oder verbundene Dienste aus Art. 3 Abs. 1 DA (»Access by Design«)

141 Nach der Vorstellung des EU Gesetzgebers herrscht »*in vielen Sektoren*« eine Situation, nach der »*die Hersteller, da sie die Kontrolle über die technische Konzeption der vernetzten Produkte oder verbundener Dienste haben, bestimmen, welche Daten generiert werden und wie darauf zugegriffen werden kann, obwohl sie keinen Rechtsanspruch auf diese Daten haben. Daher muss sichergestellt werden, dass vernetzte Produkte so konzipiert und hergestellt sowie damit verbundene Dienste so konzipiert und erbracht werden, dass die Produktdaten und die verbundenen Dienstdaten, einschließlich der entsprechenden Metadaten, die zur Auslegung und Nutzung dieser Daten erforderlich sind, und zwar auch, um die Daten abrufen, nutzen oder weitergeben zu können, für einen Nutzer stets leicht und sicher zugänglich sind, und dies kostenlos, in einem umfassenden, strukturierten, gängigen und maschinenlesbaren Format*«[53].

50 Vgl. Erwgr. 46 DA.
51 Vgl. Erwgr. 47 DA.
52 Vgl. Art. 3 Abs. 2 und 3 DA.
53 Vgl. Erwägungsgrund 20 S. 3 ff. DA.

Deshalb verlangt Art. 3 Abs. 1 DA, dass vernetze Produkte und verbundene Dienste so konzipiert bzw. erbracht werden, dass »*die Produktdaten und verbundenen Dienstdaten – einschließlich der für die Auslegung und Nutzung dieser Daten erforderlichen relevanten Metadaten – standardmäßig für den Nutzer einfach, sicher, unentgeltlich in einem umfassenden, strukturierten, gängigen und maschinenlesbaren Format und, soweit relevant und technisch durchführbar, direkt zugänglich sind.*«[54] 142

Ausgangspunkt ist damit das vernetzte Produkt bzw. der verbundene Dienst. Diese müssen so konzipiert bzw. erbracht werden, dass Nutzer Zugang zu den von ihnen mit diesen Produkten bzw. Diensten erzeugten Produktdaten und verbundenen Dienstdaten haben. Wenngleich der Gesetzgeber es unterlassen hat, den konkreten Adressaten in Art. 3 Abs. 1 DA zu nennen, so ist denklogisch nur richtig, dass sich die Anforderungen aus Art. 3 Abs. 1 DA zur Konzeptionierung und Herstellung bzw. Erbringung an den jeweiligen Hersteller eines vernetzten Produkts bzw. den Anbieter eines verbundenen Dienstes richten. Sie sind es, die das Produkt bzw. Dienst »*konzipieren und herstellen/erbringen*«. 143

Wie in der Einführung beschrieben, etabliert der Gesetzgeber damit eine *ex lege* Verpflichtung für Hersteller und Anbieter in Form von »**Access by Design**«. 144

Der »Access by Design« nach Art. 3 Abs. 1 DA verlangt dabei nicht die »*Bereitstellung*« der Daten, sondern lediglich deren **Zugänglichmachung**. Begrifflich ist die Bereitstellung ein mehr gegenüber der Zugänglichmachung aus operativer Aufwandssicht. Die Bereitstellung setzt generell eine aktive Komponente des Dateninhabers voraus, indem die Daten dem Nutzer derart verfügbar gemacht werden müssen, dass diese vom Speichermedium extrahiert und in einem gängigen Format so zur Verfügung gestellt werden, dass der Nutzer die bereitstehenden Daten abrufen kann, ohne auf den Speicherort selbst zugreifen zu müssen, um die Daten zu extrahieren. Die Zugänglichmachung hingegen setzt allein die Ermöglichung eines Zugangs des Nutzers auf den Speicherort mit den dort gespeicherten Daten voraus, sodass der Nutzer die Daten ohne weiteres Zutun des Herstellers selbst extrahieren kann – beispielsweise mittels eines Kabels. Ob der Datenzugang tatsächlich realisiert wird, liegt in der Entscheidung des Nutzers, den insoweit die Aktionslast trifft.[55] 145

Beim Zugang wird also der Nutzer selbst aktiv und greift auf den Datenspeicher mit den Daten zu, wohingegen bei der Bereitstellung dem Nutzer die Daten als bereits durch den Dateninhaber extrahiert zur Abrufung zur Verfügung stehen. In Erwägungsgrund 24 DA wird entsprechend differenziert zwischen der Information des Nutzers darüber, wie die Daten durch den Nutzer »***abgerufen***« oder »*wie auf sie **zugegriffen** werden kann*«. 146

Diese Ansicht wird insbesondere weiter durch den Gedanken in Art. 3 Abs. 2 lit. d) DA untermauert, der verlangt, dass der Verkäufer, Vermieter oder Leasinggeber – wobei es sich auch um den Hersteller handeln kann – den Nutzer über die »*techni-* 147

54 Art. 3 Abs. 1 DA.

55 Vgl. *Specht-Riemenschneider*: Der Entwurf des Data Act, MMR 2022, 809 (815).

schen Mittel« informiert, die für den Zugriff bzw. den Abruf der Daten notwendig sind (ausführlicher hierzu im Abschnitt 1, Kapitel 2, Titel B.).

148 Die Differenzierung wird besonders in der in Art. 4 Abs. 1 DA angelegten Abgrenzung zu Art. 3 Abs. 1 DA deutlich: »*soweit der Nutzer **nicht** direkt vom vernetzten Produkt oder verbundenen Dienst aus **auf die Daten zugreifen** kann, stellen die Dateninhaber dem Nutzer ohne Weiteres verfügbare Daten […] **bereit**.*«[56]

149 Ein Abrufen von Daten scheint also mit der Bereitstellung von Daten und ein Zugreifen auf Daten mit einer Zugänglichmachung von Daten zu korrespondieren.

▶ Hinweis

150 In ihren veröffentlichten »*Frequently Asked Questions*«[57] geht die EU Kommission bei Frage 22 davon aus, dass der direkte Zugang erfüllt ist, wenn der Nutzer ohne Eingreifen einer anderen Partei, insbesondere des Dateninhabers, auf etwa die Produktdaten zugreifen kann (Hervorherbungen durch den Autor):

»*Data are ›**directly accessible**‹ when:*
- *The **user is able to access the data without the intervention of any other party, notably the data holder** (this is an alternative to making requests under Articles 4 and 5, which do require data holder intervention).*
- ***The user has the technical means to stream or download the data as a result of the design of the connected product**[.] **Recital 22 explains that the location where the data are stored is irrelevant: data can be ›directly accessible‹ from a storage point on the device itself or from a remote server under the control of the manufacturer or a data holder.***

*Put simply, for data to be ›**directly accessible**‹, the user must therefore be able to access it without the involvement of the data holder, regardless of where the data are stored. Even if there is direct access and a remote server, the data holder is obliged to provide the means (i.e. appropriate interfaces, such as an API) to allow the user to easily access the relevant data (cf. recital 35, which compares Article 3[1] of the Data Act with Article 20 of the GDPR).*«[58]

151 Im Ergebnis reicht es für den »Access by Design« nach Art. 3 Abs. 1 DA aus, wenn der Hersteller oder Anbieter dem Nutzer den Zugang zu den Daten gewährt. Eine aktive Bereitstellung bedarf es durch sie nicht, sondern der Nutzer muss selbst aktiv den Zugang nutzen.

56 So beispielsweise auch Erwägungsgrund 40 DA: »*[…] **Dritte, denen Daten** auf Verlangen des Nutzers **bereitgestellt werden** […]*«; in Art. 5 Abs. 1 DA geht es ebenso um bereitstellen und nicht zugänglich machen von Daten.

57 Abrufbar unter: https://digital-strategy.ec.europa.eu/en/library/commission-publishes-frequently-asked-questions-about-data-act (letzter Abruf: 3. Februar 2025).

58 Ibid., S. 16 f.

a) Das vernetzte Produkt und der verbundene Dienst

Ein **vernetztes Produkt** ist im Sinne des Data Acts ein (physischer[59]) Gegenstand, der Daten über seine Nutzung oder Umgebung mittels seiner Komponenten oder seines Betriebssystems erlangt, generiert oder erhebt und nach außen übermitteln kann, wobei dessen Hauptfunktion nicht in der Speicherung, Verarbeitung oder Übermittlung von Daten im Auftrag Dritter besteht.[60] Erfasst sein sollen damit insbesondere solche Produkte, die auch als »**Internet der Dinge**« bezeichnet werden, mit Ausnahme von Prototypen.[61] 152

Als Beispiele für **elektronischen Kommunikationsdienste** zählt der Gesetzgeber in Erwägungsgrund 14 insbesondere *»terrestrische Telefonnetze, Fernsehkabelnetze, Satellitennetze und Nahfeldkommunikationsnetze«* auf. 153

Der Gesetzgeber hat ebenfalls erkannt, dass **vernetzte Produkte** (engl. »Connected Product«) 154

> *»in allen Bereichen der Wirtschaft und Gesellschaft vor[kommen], einschließlich in privaten, zivilen oder gewerblichen Infrastrukturen, Fahrzeugen, medizinischer Ausrüstung, Lifestyle-Ausrüstung, Schiffen, Luftfahrzeugen, Haushaltsgeräten und Konsumgütern, Medizin- und Gesundheitsprodukten oder landwirtschaftlichen und industriellen Maschinen und Anlagen«.*[62] 155

Bei dem **verbundenen Dienst** (engl. »Related Service«) handelt es sich um 156

> *»einen digitalen Dienst, bei dem es sich nicht um einen elektronischen Kommunikationsdienst handelt, – einschließlich Software –, der zum Zeitpunkt des Kaufs, der Miete oder des Leasings so mit dem Produkt verbunden ist, dass das vernetzte Produkt ohne ihn eine oder mehrere seiner Funktionen nicht ausführen könnte oder der anschließend vom Hersteller oder einem Dritten mit dem Produkt verbunden wird, um die Funktionen des vernetzten Produkts zu ergänzen, zu aktualisieren oder anzupassen«.*[63] 157

Als verbundener Dienst bzw. »**virtueller Assistent**« gilt zum Beispiel die Software »Alexa« nach Art. 1 Abs. 4 DA, die auf der gleichnamigen Sprachbox (= vernetztes Produkt) von Amazon läuft bzw. mit dieser verbunden ist. Ebenso können etwa zusätzliche Dienste, etwa Stau- und zusätzliche Ladeinfrastrukturelemente in Navigationsangeboten von Fahrzeugen, die nachträglich durch den Nutzer gebucht werden können, als verbundene Dienste gelten. 158

b) Die Produktdaten und verbundene Dienstdaten

Der Nutzer soll bei diesen vernetzten Produkten und verbundenen Diensten Zugang zu seinen generierten Produktdaten bzw. verbundenen Dienstdaten erhalten. 159

59 Vgl. Erwgr. 14 DA erster Satz.
60 Vgl. Art. 2 Abs. 5; Erwgr. 14, 15 DA.
61 Vgl. Erwgr. 14.
62 Vgl. Erwgr. 14.
63 Vgl. Art. 2 Nr. 6 DA.