Vorschlag COM(2022) 68 vom 23. Februar 2022 für eine **Verordnung über harmonisierte Vorschriften für einen fairen Datenzugang und eine faire Datennutzung (Datengesetz)**

EU-DATA ACT

cep**Analyse** Nr. 11/2022

LANGFASSUNG

A. WESENTLICHE INHALTE DES EU-VORHABENS 2
1 Hintergrund und Ziele 2
2 Verbesserung des Zugangs zu Daten, die bei der Nutzung vernetzter Produkte und verbundener Dienste erzeugt werden (B2C und B2B) [Kapitel II und X Data Act] 3
2.1 Spezifische Ziele 3
2.2 Zentrale Begrifflichkeiten 3
2.3 Datenzugangsgewährung (Access by design) und Informationspflichten 3
2.4 Datenbereitstellung an Nutzer 4
2.5 Datenbereitstellung an Dritte 4
2.6 Zusammenspiel des Data Act mit der DSGVO 5
2.7 Pflichten Dritter, die Daten auf Verlangen des Nutzers erhalten 6
2.8 Ausnahmen für kleine und Kleinstunternehmen 6
2.9 Sui-Generis-Datenbankschutzrecht 7
3 Grundregeln für die Erfüllung gesetzlicher Datenbereitstellungspflichten [Kapitel III Data Act] 7
4 Missbräuchliche Vertragsklauseln gegenüber KMU [Kapitel IV Data Act] 8
5 Aufsicht und Rechtsdurchsetzung [Kapitel IX Data Act] 9
6 Sektorspezifische Rechtsakte, Inkrafttreten und Geltungsbeginn [Kapitel XI Data Act] 9
B. JURISTISCHER UND POLITISCHER KONTEXT 10
1 Stand der Gesetzgebung 10
2 Politische Einflussmöglichkeiten 10
3 Formalien 10
C. BEWERTUNG 11
1 Ökonomische Folgenabschätzung 11
2 Juristische Bewertung 21
2.1 Kompetenz 21
2.2 Subsidiarität 21
2.3 Verhältnismäßigkeit gegenüber den Mitgliedstaaten 22
2.4 Sonstige Vereinbarkeit mit EU-Recht 24
D. FAZIT 39

Autoren: Dr. Anja Hoffmann und Philipp Eckhardt | hoffmann@cep.eu
cep | Kaiser-Joseph-Straße 266 | 79098 Freiburg | Telefon 0761 38693-0 | www.cep.eu

A. Wesentliche Inhalte des EU-Vorhabens

1 Hintergrund und Ziele

- Laut Kommission hat die Menge an erzeugten Daten in den letzten Jahren exponentiell zugenommen. Viele Daten verbleiben jedoch in den Händen weniger Unternehmen und werden nur unzureichend als „Ressource für die Sicherung des ökologischen und des digitalen Wandels“ genutzt. Dies gilt, obgleich Daten „potenziell unbegrenzt für verschiedene Zwecke verwendet und weiterverwendet werden [können], ohne dass dadurch [ihre] Qualität oder Quantität beeinträchtigt wird“. [S. 1, Erwägungsgrund 1]
- Zahlreiche Hindernisse hemmen jedoch die volle Ausschöpfung des „enormen“ Potenzials von Daten. Zu ihnen zählen u.a. [S. 1, Erwägungsgrund 2]
  - fehlende Anreize für Dateninhaber, Daten zu teilen,
  - ein geringes Vertrauen in den Austausch von Daten mit Dritten,
  - bestehende Unsicherheiten bezüglich Datenrechten und -pflichten,
  - Hindernisse technischer Art, wie etwa das Fehlen technischer Schnittstellen,
  - fehlende Normen zur „semantischen und technischen“ Interoperabilität, sowie
  - vertragliche Ungleichgewichte beim Datenzugang und bei der Datennutzung.
- Um diesen Hindernissen zu begegnen, hat die Kommission einen Vorschlag für eine Verordnung über harmonisierte Vorschriften für einen fairen Datenzugang und eine faire Datennutzung (Data Act) vorgelegt. Ziel des Vorschlags ist es, [S. 3]
  - den Datenzugang und die Datennutzung zu fördern und
  - die Wertschöpfung aus Daten „gerechter“ unter den Akteuren der Datenwirtschaft zu verteilen.
- Der Data Act ist der vierte horizontale, sektorübergreifend geltende Rechtsakt unter der EU-Datenstrategie [COM(2020) 66, s. cep**Analysen** Nr. 2020-7 und 2020-8], die den Austausch und die Weiterverwendung von Daten in der EU fördern soll. Er gilt neben
  - der PSI-Richtlinie (EU) 2019/1024, die die Weiterverwendung von Daten im Besitz der öffentlichen Hand fördert [näher zu dieser Richtlinie cep**Study** "European Leadership in the Digital Economy, S. 25ff.],
  - dem Daten-Governance-Rechtsakt (DGA), der u.a. neue Regeln für neutrale Datenvermittlungsdienste einführt [Verordnung (EU) 2022/868 über europäische Daten-Governance und zur Änderung der Verordnung (EU) 2018/1724, s. cep**Analyse** Nr. 6/2021 zum Kommissionsvorschlag COM(2020) 767], und
  - dem Digital Markets Act [DMA, COM(2020) 842, cep**Analysen** Nr. 14 u. 15/2021], der Datenkombinierungsverbote und Portabilitätspflichten für besonders marktmächtige „Gatekeeper“-Plattformen vorsieht.
- Der Data Act soll einen einheitlichen, sektorübergreifenden Rahmen für den Datenzugang und die Datennutzung schaffen [S. 1] und insbesondere
  - den Zugang zu Daten verbessern, die bei der Nutzung vernetzter Produkte und verbundener Dienste erzeugt und von einem Unternehmen kontrolliert werden, und zwar sowohl für Verbraucher (Business to Consumer, B2C) als auch für andere Unternehmen (Business to Business, B2B; s. Abschnitt 2);
  - Grundregeln für die Erfüllung gesetzlicher Datenbereitstellungspflichten festlegen (s. Abschnitt 3);
  - KMU vor missbräuchlichen Vertragsklauseln schützen (s. Abschnitt 4);
  - öffentliche Stellen ermächtigen, private Unternehmensdaten für eigene Zwecke zu nutzen, wenn hierfür eine „außergewöhnlicher Notwendigkeit“ besteht (nicht Gegenstand dieser cep**Analyse**);
  - Anbieter von Datenverarbeitungsdiensten wie Cloud-Computing verpflichten, ihren Kunden den Wechsel zu anderen Anbietern zu ermöglichen (nicht Gegenstand dieser cep**Analyse**);
  - vertrauliche nicht-personenbezogene Daten gegen unautorisierte Zugriffe aus Drittstaaten schützen (nicht Gegenstand dieser cep**Analyse**); und
  - die Interoperabilität von Datenräumen, Datenverarbeitungsdiensten und intelligenten Verträgen verbessern (nicht Gegenstand dieser cep**Analyse**).
- Die Mitgliedstaaten „sollten“ für in den Anwendungsbereich des Data Act fallende Sachverhalte keine zusätzlichen nationalen Anforderungen regeln oder aufrechterhalten, sofern der Data Act dies nicht ausdrücklich vorsieht [Erwägungsgrund 4].

2 Verbesserung des Zugangs zu Daten, die bei der Nutzung vernetzter Produkte und verbundener Dienste erzeugt werden (B2C und B2B) [Kapitel II und X Data Act]

2.1 Spezifische Ziele

- Der Data Act soll den Datenzugang und die Datennutzung für Verbraucher und Unternehmen, insbesondere für KMU, erleichtern und die Entwicklung innovativer vernetzter Produkte und Dienste fördern, gleichzeitig aber Anreize für Investitionen der Dateninhaber in die Wertschöpfung durch Daten aufrechterhalten [S. 3f., Erwägungsgrund 19]. U.a. soll er
  - Verbrauchern mehr Kontrolle über und Kompetenzen in Bezug auf ihre Daten verschaffen [S. 3, 10, 16],
  - die Rechtssicherheit bei der „gemeinsamen Nutzung" von Daten erhöhen [S. 3] und
  - „Fairness" bei Verträgen über die gemeinsame Datennutzung gewährleisten [S. 3].

2.2 Zentrale Begrifflichkeiten

- Als „Produkte" [im Folgenden „vernetzte Produkte"] gelten körperliche bewegliche Gegenstände, die [Erwägungsgründe 14 und 16, Art. 2 Ziff. 2]
  - Daten über ihre Nutzung oder ihre Umgebung „erlangen, erzeugen oder sammeln",
  - Daten über öffentlich zugängliche elektronische Kommunikationsdienste – z.B. Telefon- oder Satellitennetze – übermitteln können, und
  - auch in unbeweglichen Gegenständen enthalten, z.B. in ein Gebäude eingebaut sein können.

  Vernetzte Produkte, häufig auch als „intelligente Geräte", Produkte des „Internets der Dinge" (Internet of Things, IoT) bzw. „IoT-Produkte" geläufig, können damit u.a. Fahrzeuge, Haushaltsgeräte, Konsumgüter, Medizinprodukte und landwirtschaftliche sowie industrielle Maschinen sein.

- Nicht als „vernetzte Produkte" gelten Gegenstände, deren Hauptfunktion darin besteht, Daten zu speichern und zu verarbeiten, d.h. von Menschen erzeugte Inhalte wie Texte, Ton-, Video- und sonstige Dateien anzuzeigen, abzuspielen oder z.B. für die Nutzung durch Online-Dienste aufzuzeichnen und zu übertragen. Dazu zählen u.a. PCs, Server, Tablets, Smartphones und Webcams. [Erwägungsgrund 15, Art. 2 Ziff. 2]

- „Verbundene Dienste" sind digitale Dienste, die mit einem vernetzten Produkt verbunden oder in dieses integriert sind und ohne die das Produkt nicht funktioniert, z.B. eine von einem E-Bike-Hersteller angebotene mobile Anwendung (App), bei deren Nutzung ein E-Bike erst seine volle Funktionalität entfaltet [Art. 2 Ziff. 3, Erwägungsgrund 16].

- „Virtuelle Assistenten" sind Software, die Aufträge, Aufgaben oder Fragen von Nutzern verarbeiten und so als Schnittstelle fungieren können, die Nutzern den Zugang zu eigenen oder fremden Diensten oder die Steuerung eigener oder fremder „Geräte" (vernetzter Produkte) ermöglichen [Art. 2 Ziff. 4, Erwägungsgrund 22], wie etwa Siri von Apple, Alexa von Amazon oder Google Assistant von Google. Alle Regelungen des Data Act, die auf „vernetzte Produkte" oder „verbundene Dienste" Bezug nehmen, gelten daher auch für virtuelle Assistenten, die dazu genutzt werden, um auf vernetzte Produkte zuzugreifen oder diese zu steuern. Sie gelten jedoch nicht, soweit die Assistenten auch Daten erzeugen, die nicht aus einer Interaktion zwischen dem Nutzer und einem vernetzten Produkt stammen, also z.B. eine Pizzabestellung über Siri. [Erwägungsgrund 22, Art. 7 Abs. 2]

- „Nutzer" sind natürliche oder juristische Personen, die ein vernetztes Produkt besitzen, etwa gekauft, gemietet oder geleast haben, bzw. einen verbundenen Dienst nutzen [Art. 2 Ziff. 5, Erwägungsgrund 18].

- „Dateninhaber" sind natürliche oder juristische Personen, die [Art. 2 Abs. 6, Erwägungsgrund 5]
  - nach dem Data Act, nach anderem EU- oder nationalem Recht berechtigt oder verpflichtet sind, Daten bereitzustellen (d.h. eine rechtliche Kontrolle über Daten ausüben), oder
  - bei nicht-personenbezogenen Daten dazu in der Lage sind, da sie die technische Gestaltung des Produkts bzw. Dienstes kontrollieren (d.h. eine faktische Kontrolle über diese Daten ausüben).

  Dateninhaber sind regelmäßig die Hersteller eines vernetzten Produkts oder Erbringer eines verbundenen Dienstes [S. 16, Erwägungsgründe 4 und 19].

2.3 Datenzugangsgewährung (Access by design) und Informationspflichten

- Die Hersteller und Entwickler von vernetzten Produkten und die Erbringer von verbundenen Diensten (im Folgenden: IoT-Produktanbieter) müssen in der EU angebotene vernetzte Produkte bzw. erbrachte

verbundene Dienste so ausgestalten, dass die durch ihre Nutzung erzeugten Daten für den Nutzer standardmäßig „einfach, sicher und – soweit relevant und angemessen – direkt zugänglich“ sind [Art. 1 Abs. 2 lit. a, Art. 3 Abs. 1, S. 18].

- Nutzer müssen bereits vor dem Kauf, der Anmietung oder des Leasings eines vernetzten Produkts bzw. verbundenen Dienstes auf verständliche Weise u.a. darüber informiert werden [Art. 3 Abs. 2],
  - welche Daten das Produkt bzw. der Dienst voraussichtlich erzeugen wird und ob dies kontinuierlich und in Echtzeit geschehen wird,
  - wie der Nutzer auf die Daten zugreifen kann,
  - wie der Nutzer die Datenweitergabe an Dritte veranlassen kann, und
  - ob und zu welchem Zweck die IoT-Produktanbieter die Daten selbst nutzen oder Dritten deren Nutzung gestatten will.

2.4 Datenbereitstellung an Nutzer

- Können Nutzer nicht direkt vom vernetzten Produkt aus auf Daten zugreifen, müssen die Dateninhaber ihnen die Daten, die bei der Nutzung des Produkts bzw. des verbundenen Dienstes erzeugt werden, auf Verlangen der Nutzer „unverzüglich, kostenlos und ggf. kontinuierlich und in Echtzeit“ bereitstellen [Art. 4 Abs. 1].
- Als bei der Nutzung von vernetzten Produkten oder verbundenen Diensten „erzeugte“ Daten gelten u.a. Daten, die [Erwägungsgrund 14 und 17]
  - von Nutzern absichtlich aufgezeichnet werden,
  - als Nebenprodukt von Nutzeraktionen aufgezeichnet werden, z.B. Diagnosedaten, sowie
  - ohne jegliche Nutzeraktion generiert werden, z.B. wenn sich das vernetzte Produkt im Bereitschaftsmodus befindet.

  Nicht erfasst sind hingegen aus den erzeugten Daten „abgeleitete Daten oder gefolgerte Informationen“, die z.B. von einer Software aus den Daten berechnet werden.
- IoT-Produktanbieter sollten sicherstellen, dass, falls mehrere Nutzer ein bestimmtes Produkt bzw. einen bestimmten Dienst nutzen, alle Nutzer auf die erzeugten Daten zugreifen können, etwa über getrennte Nutzerkonten oder den Zugriff mehrerer Nutzer auf ein gemeinsames Nutzerkonto [Erwägungsgrund 20].
- Die Datenbereitstellung kann erfolgen [Erwägungsgrund 21]
  - direkt vom Datenspeicher des Geräts über kabelgebundene oder drahtlose lokale Funknetze, oder
  - von einem entfernten Server; dies kann ein Server des Herstellers, oder eines als Dateninhaber fungierenden Dritten oder eines Cloud-Diensteanbieters sein.
- Die Bereitstellung der Daten setzt jedoch nicht zwingend deren Übertragung voraus. Es genügt, dass Nutzer die Daten direkt auf dem Produkt oder auf dem entfernten Server verarbeiten können, indem sie Algorithmen am Ort der Datenerzeugung einsetzen [Erwägungsgründe 8, 21].
- Dateninhaber müssen Nutzern Geschäftsgeheimnisse nur offenlegen, wenn diese die erforderlichen Schutzvorkehrungen getroffen haben, um deren Vertraulichkeit – insbesondere gegenüber Dritten – zu wahren. Dateninhaber können mit Nutzern Maßnahmen zur Wahrung der Vertraulichkeit der Daten vereinbaren [Art. 4 Abs. 3], etwa in einem Non-Disclosure-Agreement (NDA).
- Nutzer dürfen erlangte Daten nicht zur Entwicklung von Produkten nutzen, die mit dem vernetzten Produkt im Wettbewerb stehen [Art. 4 Abs. 4].
- Dateninhaber dürfen nicht-personenbezogene Daten, die bei der Nutzung eines vernetzten Produkts bzw. eines verbundenen Dienstes erzeugt werden, nur „auf der Grundlage“ eines Vertrags mit dem Nutzer verwenden. Sie dürfen die Daten nicht dazu verwenden, um Wissen zu erlangen über [Art. 4 Abs. 6, Erwägungsgrund 25]
  - die „wirtschaftliche Lage, Vermögenswerte und Produktionsmethoden“ des Nutzers, oder
  - die Nutzung des vernetzten Produkts bzw. des verbundenen Dienstes durch den Nutzer.

  Dies gilt nur, wenn das Erlangen des Wissens die „gewerbliche Position“ des Nutzers „untergraben“ könnte.

2.5 Datenbereitstellung an Dritte

- Dateninhaber müssen bei der Nutzung eines vernetzten Produkts bzw. verbundenen Dienstes erzeugte Daten direkt einem Dritten bereitstellen, wenn der Nutzer oder eine in seinem Namen handelnde Partei dies

verlangt [Art. 5 Abs. 1]. Der Nutzer kann das Produkt z.B. von einem Dritten reparieren lassen und ist so nicht mehr allein von Diensten des Herstellers abhängig [S. 16].

- Dateninhaber müssen Dritten die Daten unverzüglich, ohne Qualitätsverlust und ggf. kontinuierlich und in Echtzeit bereitstellen. Sie können dafür von den Dritten – nicht aber von den Nutzern – eine „angemessene Gegenleistung für etwaige Kosten" verlangen, die ihnen durch die Bereitstellung des Direktzugangs für den Dritten entstehen [Erwägungsgrund 31].

- Dateninhaber dürfen Daten jedoch nicht an sogenannte „Gatekeeper" weitergeben. Gatekeeper sind Unternehmen, die von der Kommission als solche benannt wurden, weil sie kumulativ [Art. 5 Abs. 2, 4 i.V.m. Art. 3, Art. 2 Abs. 1, 2 Gesetz für digitale Märkte]
  - mindestens einen sogenannten „zentralen Plattformdienst" erbringen, der gewerblichen Nutzern als „wichtiges Zugangstor" zu Endkunden dient:
    - Zentrale Plattformdienste sind u.a. Marktplätze und Stores für Software-Anwendungen, Suchmaschinen, soziale Netzwerke, Cloud-Dienste, Werbedienste, Sprachassistenzdienste und Browser;
    - Es wird vermutet, dass ein zentraler Plattformdienst als wichtiges Zugangstor dient, wenn er im letzten Geschäftsjahr in der EU durchschnittlich mindestens
      - 45 Mio. monatlich aktive Endnutzer und
      - 10.000 jährlich aktive gewerbliche Nutzer hatte;
  - erhebliche Auswirkungen auf den Binnenmarkt haben, dies wird vermutet, wenn sie
    - den zentralen Plattformdienst in mindestens drei Mitgliedstaaten anbieten und
    - in den letzten drei Jahren in der EU jeweils mindestens 7,5 Mrd. Euro Jahresumsatz erzielt haben oder im letzten Geschäftsjahr einen durchschnittlichen Marktwert von mindestens 75 Mrd. Euro hatten; und
  - in ihrer Tätigkeit eine gefestigte und dauerhafte Position innehaben oder voraussichtlich in naher Zukunft innehaben werden; dies wird vermutet, wenn sie in jedem der letzten drei Geschäftsjahre in der EU durchschnittlich mindestens
    - 45 Mio. monatlich aktive Endnutzer und
    - 10.000 jährlich aktive gewerbliche Nutzer hatten.

- Gatekeeper dürfen [Art. 5 Abs. 2]
  - keine Daten annehmen, die Nutzer von Dateninhabern erhalten haben, und
  - Nutzer nicht dazu auffordern oder z.B. durch Versprechen einer Gegenleistung dazu anreizen, vom Dateninhaber erhaltene Daten für einen Gatekeeper-Dienst bereitzustellen oder vom Dateninhaber zu verlangen, dass er dem Gatekeeper Daten bereitstellt.

- Dateninhaber sollten ihre Position nicht missbrauchen, um einen Wettbewerbsvorteil auf Märkten zu erlangen, auf denen sie mit dem Dritten in Wettbewerb stehen. Sie dürfen daher nicht-personenbezogene Daten, die bei der Nutzung des vernetzten Produkts bzw. des verbundenen Dienstes erzeugt werden, nicht verwenden, um Wissen zu erlangen über [Art. 5 Abs. 5, Erwägungsgrund 29]
  - die „wirtschaftliche Lage, Vermögenswerte und Produktionsmethoden" des Dritten, oder
  - die Nutzung der Daten durch den Dritten.

  Dies gilt nur, wenn das Erlangen des Wissens die „gewerbliche Position" des Dritten „untergraben" könnte. Dritte können einer solchen Nutzung der Daten durch Dateninhaber jedoch widerruflich zustimmen.

- Dateninhaber müssen gegenüber Dritten ggf. auch Geschäftsgeheimnisse offenlegen, soweit [Art. 5 Abs. 8]
  - dies unbedingt erforderlich ist, um den zwischen Nutzern und Dritten vereinbarten Zweck zu erfüllen, und
  - Dritte alle mit Dateninhabern (vertraglich) – z.B. in einem NDA – vereinbarten und erforderlichen Maßnahmen zur Wahrung ihrer Vertraulichkeit getroffen haben.

2.6 Zusammenspiel des Data Act mit der DSGVO

- Alle Rechte und Pflichten aus der Datenschutzgrundverordnung [DSGVO, (EU) 2016/679] und der E-Privacy-Richtlinie 2002/58/EC bleiben bestehen und müssen neben dem Data Act eingehalten werden [Art. 1 Abs. 3].

- Das Recht der Nutzer auf Datenzugang ergänzt das in Art. 20 DSGVO verankerte Recht auf Datenübertragbarkeit (Portabilität). Dieses berechtigt betroffene natürliche Personen („Betroffene") dazu, sie betreffende personenbezogene Daten von dem für die Datenverarbeitung Verantwortlichen, also z.B. dem Dateninhaber, in einem „strukturierten, gängigen, maschinenlesbaren und interoperablen Format" zu erhalten und an einen anderen Verantwortlichen zu übertragen oder direkt an diesen übermitteln zu lassen. [Erwägungsgrund 31]

- Der Data Act schafft jedoch keine neue Rechtsgrundlage für Dateninhaber [Erwägungsgründe 24, 5],
  - personenbezogene Daten, die das vernetzte Produkt oder der verbundene Dienst erzeugt, dem Nutzer oder einem Dritten bereitzustellen, soweit der Nutzer nicht selbst Betroffener i.S.d. DSGVO ist;
  - Daten, die das vernetzte Produkt oder der verbundene Dienst erzeugt, zu besitzen oder selbst zu nutzen.
- Erzeugt das vernetzte Produkt oder der verbundene Dienst personenbezogene Daten und verlangt ein Nutzer von einem Dateninhaber, ihm oder einem Dritten Zugang zu diesen Daten zu gewähren, gilt Folgendes:
  - Ist der Nutzer eine natürliche Person und damit zugleich von der Datenverarbeitung „Betroffener" i.S.d. DSGVO, ist der Dateninhaber verpflichtet [Erwägungsgründe 24, 30]
    - dem Nutzer oder dem Dritten nach den Regeln der DSGVO (Art. 20) Zugang zu seinen personenbezogenen Daten zu geben und ergänzend
    - dem Nutzer nach Art. 4 Data Act oder dem Dritten nach Art. 5 Data Act Zugang zu allen durch das vernetzte Produkt oder den verbundenen Dienst erzeugten personenbezogenen und nicht-personenbezogenen Daten zu gewähren.
  - Ist der Nutzer kein „Betroffener", sondern ein Unternehmen, und erzeugt das vernetzte Produkt bzw. der verbundene Dienst personenbezogene Daten anderer Betroffener (z.B. Mitarbeiter), die das Produkt nutzen, ist der Nutzer zugleich „Verantwortlicher" i.S.d. DSGVO und es gilt [Art. 4 Abs. 5, Art. 5 Abs. 6 i.V.m Art. 6 Abs. 1, Art. 9 DSGVO, Erwägungsgrund 30]:
    - Der Dateninhaber darf dem Nutzer oder einem Dritten die personenbezogenen Daten der anderen Betroffenen nur bereitstellen, wenn es dafür eine gültige Rechtsgrundlage in der DSGVO gibt.
    - Nutzer, die Zugang zu solchen Daten verlangen, benötigen für die Verarbeitung der Daten ebenfalls eine Rechtsgrundlage in der DSGVO, etwa eine Einwilligung der Betroffenen oder ein berechtigtes Interesse.

2.7 Pflichten Dritter, die Daten auf Verlangen des Nutzers erhalten

- Dritte, denen auf Verlangen eines Nutzers Daten bereitgestellt wurden, dürfen die Daten nur wie folgt nutzen:
  - für die mit dem Nutzer vereinbarten Zwecke – z.B. zur Erbringung einer Reparaturdienstleistung – und unter den mit dem Nutzer vereinbarten Bedingungen [Art. 6 Abs. 1];
  - für die Entwicklung neuer und innovativer Produkte oder verbundener Dienste, nicht aber für die Entwicklung von Produkten, die mit dem vernetzten Produkt „im Wettbewerb stehen" [Art. 6 Abs. 2 lit. e, Erwägungsgrund 35].
- Dritte dürfen Nutzer nicht [Art. 6 Abs. 2 lit. a und f, Erwägungsgrund 34]
  - in irgendeiner Weise zwingen, täuschen oder manipulieren, etwa indem sie – z.B. bei der Gestaltung ihrer digitalen Schnittstellen zum Nutzer – Techniken wie „Dark Patterns" verwenden, die dazu dienen, die Autonomie, Entscheidungsfähigkeit oder Wahlmöglichkeiten des Nutzers zu untergraben, um ihn zur unerwünschten Offenlegung von Daten zu bewegen;
  - an der Weitergabe der Daten an weitere Dritte hindern, etwa durch Vertragsklauseln.
- Dritten ist es ferner verboten, erhaltene Daten [Art. 6 Abs. 2, Erwägungsgrund 35]
  - für ein Profiling, d.h. für die Erstellung eines Profils des Nutzers zu verwenden, außer dies ist zur Erbringung des vom Nutzer gewünschten Dienstes erforderlich,
  - an Gatekeeper (s.o.) weiterzugeben,
  - an andere Dritte weiterzugeben, außer dies ist zur Erbringung des vom Nutzer gewünschten Dienstes erforderlich,
  - zur Entwicklung eines Produkts an andere Dritte weiterzugeben, das mit dem vernetzten Produkt „im Wettbewerb steht".

2.8 Ausnahmen für kleine und Kleinstunternehmen

- Die vorgenannten, in Kapitel II des Data Act geregelten Pflichten zum Design bzw. zur Zugangsgewährung und zur Bereitstellung von Informationen und von Daten gelten nicht für IoT-Produktanbieter, die kleine oder Kleinstunternehmen sind, d.h. weniger als 50 Mitarbeiter und einen Jahresumsatz bzw. eine Jahresbilanz von maximal 10. Mio. Euro haben [Art. 7 Abs. 1 i.V.m. Art. 2 der Empfehlung 2003/361/EG]. Dies gilt nicht, sofern sie [Art. 7 Abs. 1, Erwägungsgrund 37]
  - größere Partnerunternehmen oder verbundene Unternehmen haben, oder
  - von größeren Unternehmen mit der Herstellung oder dem Design des Produkts beauftragt werden.

- Für kleine oder Kleinstunternehmen gelten jedoch die Pflichten des Data Act für Dateninhaber, wenn sie nicht IoT-Produktanbieter, aber dennoch Dateninhaber sind [Erwägungsgrund 37].

2.9 Sui-Generis-Datenbankschutzrecht

- „Datenbanken" sind u.a. Sammlungen von Daten, die systematisch oder methodisch angeordnet und einzeln zugänglich sind. Sie unterliegen nach der Datenbankrichtlinie einem besonderen Schutz. Insbesondere können Datenbanken unter den Schutz des sogenannten „Sui-Generis-Rechts" fallen. Der Schutz dieses speziellen, vom Urheberrecht unabhängigen geistigen Eigentumsrechts entsteht, wenn die Investitionen für die Beschaffung, Überprüfung und Darstellung der in der Datenbank enthaltenen Daten wesentlich waren. Datenbankhersteller können Nutzern dann u.a. die Entnahme oder Weiterverwendung „wesentlicher" Teile des Inhalts der Datenbank untersagen. [Art. 1, 7 Datenbankrichtlinie 96/9/EG]
- Der Data Act „stellt klar", dass das Sui-Generis-Datenbankschutzrecht keine Anwendung auf Daten findet, die bei der Nutzung vernetzter Produkte oder verbundener Dienste erlangt oder erzeugt wurden, z.B. durch Sensoren. Dateninhaber dürfen die Bereitstellung von Daten an Nutzer oder Dritte daher nicht unter Berufung auf das Sui-Generis-Datenbankschutzrecht verweigern. [Art. 35, Erwägungsgrund 84, S. 15]

3 Grundregeln für die Erfüllung gesetzlicher Datenbereitstellungspflichten [Kapitel III Data Act]

- Der Data Act legt einheitliche Bedingungen für Fälle fest, in denen Dateninhaber rechtlich verpflichtet sind, Datenempfängern – das sind geschäftlich handelnde Personen in der EU, die nicht Nutzer vernetzter Produkte oder verbundener Dienste sind – Daten bereitzustellen [Art. 1 Abs. 2 lit. c, Art. 2 Nr. 7, Art. 8-12].
  - Diese Bedingungen gelten, wenn ein Dateninhaber entweder [Art. 12]
    - nach Art. 5 Data Act verpflichtet ist, einem Dritten Daten bereitzustellen, die bei der Nutzung eines Produkts oder verbundenen Dienstes erzeugt werden [s.o. Ziffer 2.5], oder
    - nach einer anderen EU-Rechtsnorm oder nationalen Umsetzungsvorschrift, die nach dem Geltungsbeginn des Data Act in Kraft getreten ist, verpflichtet ist, einem Datenempfänger Daten bereitzustellen.
  - Dagegen gelten diese Bedingungen nicht [Erwägungsgrund 38],
    - soweit der Dateninhaber verpflichtet ist, einem Nutzer Daten bereitzustellen,
    - für Datenbereitstellungspflichten nach der DSGVO, insbesondere die Portabilitätspflichten des Art. 20,
    - für Datenbereitstellungspflichten nach EU-Recht, das vor Geltung des Data Act in Kraft getreten ist,
    - bei der Bereitstellung von Daten auf freiwilliger Basis.
- Um ihre Datenbereitstellungspflichten zu erfüllen, müssen die Dateninhaber mit den Datenempfängern Datennutzungsverträge abschließen [Art. 8 Abs. 2]. Diese sind frei verhandelbar, müssen aber einige Anforderungen erfüllen:
  - Die Datenbereitstellung muss zu „fairen, angemessenen und nichtdiskriminierenden Bedingungen" (englisch abgekürzt: FRAND) und „in transparenter Weise" erfolgen [Art. 8 Abs. 1].
  - Vertragsklauseln sind nicht bindend, wenn sie [Art. 8 Abs. 2 i.Vm. Art. 13 und Kapitel 2]
    - einem Kleinstunternehmen, kleinen oder mittleren Unternehmen (KMU) – d.h. Unternehmen mit weniger als 250 Mitarbeitern und maximal 50 Mio. Euro Jahresumsatz oder 43 Mio. Euro Jahresbilanzsumme – einseitig auferlegt wurden und missbräuchlich sind (s. dazu Abschnitt 4), oder
    - die Rechte der Nutzer auf Datenzugang nach Kapitel II beschränken.
  - Daten dürfen, außer auf Verlangen des Nutzers, einem Datenempfänger nicht auf exklusiver Basis bereitgestellt werden [Art. 8 Abs. 4].
  - Wird für die Datenbereitstellung eine Vergütung vereinbart, muss diese „angemessen" sein und es gilt:
    - Bei Datenbereitstellung an ein KMU darf die Vergütung die unmittelbaren Bereitstellungskosten nicht übersteigen und muss nichtdiskriminierend sein [Art. 9 Abs. 1 und 2, Art. 8 Abs. 3].
    - Damit der Datenempfänger die Angemessenheit prüfen kann, muss der Dateninhaber ihm detaillierte Informationen zur Berechnung der Vergütung zur Verfügung stellen [Art. 9 Abs. 4].
  - Der Dateninhaber trägt die Beweislast, dafür, dass eine Vertragsklausel oder die vereinbarte Vergütung nichtdiskriminierend ist; sieht er für „vergleichbare Kategorien" von Datenempfängern unterschiedliche Bedingungen vor, muss dies objektiv gerechtfertigt sein [Art. 8 Abs. 3, Art. 9 Abs. 2, Erwägungsgrund 41].
- Dateninhaber dürfen technische Schutzmaßnahmen ergreifen, um [Art. 11 Abs. 1]
  - einen unbefugten Zugang zu Daten und deren Weitergabe zu verhindern,
  - die Einhaltung der im Data Act geregelten Pflichten für den Datenempfänger zu gewährleisten, und

– sicherzustellen, dass der Datenempfänger die im Datennutzungsvertrag geregelten Bedingungen einhält.

Dabei können Dateninhaber auch auf „intelligente Verträge“ (smart contracts) zurückgreifen. Smart Contracts sind Computerprogramme, die in einem elektronischen Vorgangsregister fälschungssicher gespeichert sind, auf Basis vorab festgelegter Bedingungen Transaktionen ausführen und das Ergebnis der Ausführung in dem Register aufzeichnen [Art. 2 Abs. 16, S. 4].

- Datenempfänger, die sich durch Falschangaben, Täuschung, Zwang oder Ausnutzung von Lücken in technischen Schutzmaßnahmen Zugang zu Daten erschleichen, Daten für nicht genehmigte Zwecke nutzen oder ohne Zustimmung des Dateninhabers weitergeben, müssen [Art. 11 Abs. 2]
  – die erhaltenen Daten unverzüglich vernichten,
  – die Herstellung, das Angebot oder die Nutzung von Waren, abgeleiteten Daten oder Diensten einstellen, die auf Basis des durch die Daten erlangten Wissens erzeugt wurden, und
  – die Ein- und Ausfuhr oder die Lagerung von rechtsverletzenden Waren stoppen und die Waren vernichten.

  Die genannten Konsequenzen für Waren, abgeleitete Daten oder Dienste gelten nicht, wenn [Art. 11 Abs. 3]
  – der Dateninhaber oder der Nutzer etwas anderes anweist,
  – sie unverhältnismäßig mit Blick auf die Interessen des Dateninhabers wären, oder
  – dem Dateninhaber kein „erheblichen Schaden“ durch die Datennutzung entstanden ist.

- Die Mitgliedstaaten müssen es Dateninhabern und Datenempfängern ermöglichen, Streitigkeiten darüber, ob die Vertragsbedingungen fair, angemessen und nichtdiskriminierend sind und die Bereitstellung der Daten in transparenter Weise erfolgt, alternativ zu gerichtlichen Verfahren vor staatlich zugelassenen Streitbeilegungsstellen beizulegen [Art. 10].

4 Missbräuchliche Vertragsklauseln gegenüber KMU [Kapitel IV Data Act]

- Der Data Act macht Vorgaben zum Schutz von KMU, die Daten von Vertragspartnern nutzen wollen, welche eine stärkere Verhandlungsposition innehaben und den KMU daher „unfaire“ Vertragsbedingungen aufzwingen könnten [S. 2, Erwägungsgründe 5, 51]. Die Regeln gelten nur für diejenigen Teile eines Vertrags, die mit der Bereitstellung von Daten zusammenhängen, d.h. für Vertragsklauseln in Bezug auf [Art. 13 Abs. 1]
  – den Datenzugang und die Datennutzung oder
  – die Haftung und Rechtsbehelfe bei Verletzung oder Beendigung datenbezogener Pflichten.

- Solche Vertragsklauseln sind für KMU nicht bindend, wenn sie [Erwägungsgrund 51 und 52, Art. 13 Abs 1, 5]
  – ihnen einseitig auferlegt wurden und
  – missbräuchlich sind.

- Eine Vertragsklausel gilt als einem KMU einseitig auferlegt, wenn sie [Art. 13 Abs. 5, Erwägungsgrund 52]
  – von der anderen Vertragspartei („Verwender“) eingebracht wurde und
  – das KMU versucht hat, über ihren Inhalt zu verhandeln,
  – ihren Inhalt aber mangels Verhandlungsspielraums nicht beeinflussen konnte.

  Nicht einseitig auferlegt sind Klauseln, die
  – von den Vertragsparteien ausgehandelt wurden oder
  – vom Verwender eingebracht und vom KMU ohne weiteres akzeptiert wurden.

  Beanstandet ein KMU eine Klausel, muss der Verwender beweisen, dass diese nicht als einseitig auferlegt gilt.

- Eine Vertragsklausel ist erstens stets missbräuchlich (schwarze Liste), wenn sie [Art. 13 Abs. 3]
  – die Haftung des Verwenders für Vorsatz oder grobe Fahrlässigkeit ausschließt oder beschränkt,
  – die Haftung des Verwenders oder die Gewährleistungsrechte des KMU bei der Verletzung von Vertragspflichten ausschließt, oder
  – dem Verwender das alleinige Recht zur Bestimmung der Vertragsmäßigkeit bereitgestellter Daten oder zur Auslegung einer Vertragsklausel vorbehält.

- Die Missbräuchlichkeit einer Vertragsklausel wird zweitens vermutet (graue Liste), wenn sie u.a. [Art. 13 Abs. 4]
  – die Haftung des Verwenders oder die Gewährleistungsrechte des KMU bei der Verletzung von Vertragspflichten unangemessen beschränkt,
  – dem Verwender ein Recht auf Zugang zu Daten des KMU und auf deren Nutzung in einer Weise eröffnet, die den berechtigten Interessen des KMU erheblich schadet,

  - ein KMU daran hindert oder in seinem Recht beschränkt, von ihm bereitgestellte oder erzeugte Daten selbst in verhältnismäßiger Weise zu nutzen, zu erfassen oder zu verwerten oder eine Kopie dieser Daten zu erhalten, oder
  - dem Verwender eine unangemessen kurze Kündigungsfrist einräumt.
- Vertragsklauseln sind drittens auch dann missbräuchlich, wenn ihre Verwendung [Art. 13 Abs. 2]
  - „gröblich von der guten Geschäftspraxis beim Datenzugang und der Datennutzung“ abweicht und
  - gegen „Treu und Glauben“ und den „redlichen Geschäftsverkehr“ verstößt.
- Ist eine Klausel unwirksam, gilt der Vertrag im Übrigen weiter, es sei denn, die missbräuchliche Klausel ist vom Rest des Vertrags nicht trennbar [Art. 13 Abs. 6].
- Die Vorgaben gelten nicht für Vertragsklauseln über [Art. 13 Abs. 7]
  - den Hauptgegenstand des Vertrags, und
  - den zu zahlenden Preis.
- Die Kommission will nicht-bindende Mustervertragsklauseln für den Datenzugang und die Datennutzung entwickeln, um ausgewogene Verträge zu unterstützen [Art. 34].

5 Aufsicht und Rechtsdurchsetzung [Kapitel IX Data Act]

- Die Mitgliedstaaten müssen eine oder mehrere – neue oder bestehende – Behörden benennen, die für die Durchsetzung des Data Act zuständig sind, und mit den nötigen Mitteln zur Wahrung ihrer Aufgaben ausstatten. Betrauen die Mitgliedstaaten mehrere Behörden, müssen sie auch eine koordinierende Behörde benennen. [Art. 31 Abs. 1, 4, 7]
- Die für die Durchsetzung der DSGVO jeweils zuständige Datenschutzaufsichtsbehörde ist jedoch auch für den Schutz personenbezogener Daten im Rahmen des Data Act zuständig [Art. 31 Abs. 2 lit. a].
- Behörden, die nach sektorspezifischen Vorschriften benannt wurden, sind in ihrem Zuständigkeitsbereich – d.h. bei sektorspezifischen Problemen des Datenaustauschs – auch für die Durchsetzung des Data Act zuständig [Art. 31 Abs. 2 lit. b].
- Natürliche und juristische Personen können wegen Verletzung ihrer Rechte nach dem Data Act Beschwerde bei der zuständigen Behörde des Mitgliedstaats einlegen, in dem sie ihren gewöhnlichen Aufenthalt, Arbeitsplatz oder ihre Niederlassung haben; verwaltungsrechtliche oder gerichtliche Rechtsbehelfe bleiben unberührt [Art. 32].
- Zuständige Behörden arbeiten untereinander und mit den zuständigen Behörden anderer Mitgliedstaaten zusammen, um die einheitliche Anwendung des Data Act zu gewährleisten und um Beschwerden zu bearbeiten und zu lösen [Art. 31 Abs. 3, 4, Art. 32 Abs. 3, Erwägungsgrund 81].
- Die Mitgliedstaaten müssen Vorschriften über Sanktionen bei Verstößen gegen die Verordnung erlassen. Vorgesehene Sanktionen müssen „wirksam, verhältnismäßig und abschreckend“ sein. [Art. 33]
- Soweit die Datenschutzaufsichtsbehörden zuständig sind, können sie bei Verstößen gegen die oben unter Ziffer 2 und 3 dargestellten Pflichten in Kapitel II und III des Data Act Geldbußen nach den Bedingungen der DSGVO verhängen, und zwar in Höhe von bis zu 20 Millionen Euro oder 4% des gesamten weltweit erzielten Jahresumsatzes im vorangegangenen Geschäftsjahr, je nachdem, welcher Betrag höher ist [Art. 33 Abs. 3].

6 Sektorspezifische Rechtsakte, Inkrafttreten und Geltungsbeginn [Kapitel XI Data Act]

- Der Data Act lässt bestehende sektorspezifische Rechtsvorschriften in Bezug auf den Datenzugang und die Datennutzung unberührt, legt aber einen Rahmen für künftige vertikale, sektorspezifische Vorschriften fest [S. 6 und 10], die zusätzliche Anforderungen regeln können, um den Bedürfnissen einzelner Sektoren, der geplanten gemeinsamen europäischen Datenräume oder eines Gebiets von öffentlichem Interesse gerecht zu werden [Art. 40 Abs. 2, Erwägungsgrund 87, S. 10].
- Der Data Act tritt 20 Tage nach Veröffentlichung im EU-Amtsblatt in Kraft und gilt 12 Monate später [Art. 42].

B. Juristischer und politischer Kontext

1 Stand der Gesetzgebung

23.02.22 Annahme durch Kommission

Offen Annahme durch Europäisches Parlament und Rat, Veröffentlichung im Amtsblatt, Inkrafttreten

2 Politische Einflussmöglichkeiten

Generaldirektionen:	GD Kommunikationsnetze, Inhalte und Technologien
Ausschüsse des Europäischen Parlaments:	Industrie, Forschung und Energie (ITRE, federführend), Berichterstatterin: Pilar del Castillo Vera (EVP-Fraktion, ES); Bürgerliche Freiheiten, Justiz und Inneres (LIBE, assoziiert), Berichterstatter: Dr. Sergey Lagodinsky (Fraktion der Grünen / Freie Europäische Allianz, D); Recht (JURI, assoziiert), Berichterstatter: Iban García del Blanco (S&D-Fraktion, ES); Verbraucherschutz (IMCO, assoziiert), Berichterstatter: Adam Bielan (ECR-Fraktion, PL)
Bundesministerien:	Digitales und Verkehr (federführend)
Ausschüsse des Deutschen Bundestags:	Digitales (federführend)
Entscheidungsmodus im Rat:	Qualifizierte Mehrheit (Annahme durch 55% der Mitgliedstaaten, die 65% der EU-Bevölkerung ausmachen)

3 Formalien

Kompetenznorm:	Art. 114 AEUV (Binnenmarkt)
Art der Gesetzgebungszuständigkeit:	Geteilte Zuständigkeit (Art. 4 Abs. 2 AEUV)
Verfahrensart:	Art. 294 AEUV (ordentliches Gesetzgebungsverfahren)

C. Bewertung

1 Ökonomische Folgenabschätzung

Einführung

Der Austausch und die gemeinsame Nutzung von Daten spielen in der digitalisierten Wirtschaft eine immer bedeutendere Rolle. Oft sind die Daten jedoch unter der Kontrolle weniger Akteure und ihr Potential wird nicht in ausreichendem Maße ausgeschöpft. Hier will die Kommission mit dem Data Act gegensteuern und Daten, die bei der Nutzung von vernetzten Produkten und verbundenen Diensten erzeugt werden (IoT-Daten), einem breiteren Kreis von Akteuren zugänglich machen. Dazu zählen neben den Nutzern der Produkte bzw. Dienste auch Dritte, die mit Hilfe der Daten eigene Produkte und Dienstleistungen herstellen bzw. erbringen können.

Der Wille, mehr Parteien den Zugang und die Nutzbarmachung von IoT-Daten zu ermöglichen, rührt insbesondere auf zwei Grundannahmen bezüglich der Eigenschaften von Daten. Zum einen der Hypothese, dass mit der intensiven Nutzung von Daten Skalenerträge verbunden sind, und zum anderen, dass Daten im Konsum nichtrivalisierend sind.

Skalenerträge entstehen auf Datenmärkten regelmäßig aufgrund von Größenvorteilen. Erstens sind die Kosten der Herstellung eines Informationsguts anfänglich regelmäßig hoch, sinken jedoch oft dann bei der Herstellung weiterer Informationsgüter. Die Datenproduktion geht also mit hohen Fixkosten aber niedrigen Grenzkosten einher. Zweitens steigt die Qualität datenbasierter Güter regelmäßig mit der Menge der zur Verfügung stehenden Daten. Skalenerträge können daher eine verstärkte Nutzbarmachung von Daten rechtfertigen und stützen, zugleich jedoch auch Marktmacht begründen.

Ferner können Daten, die von einem Akteur genutzt werden, häufig auch von einem anderen Akteur für andere Zwecke genutzt werden. Ihr Informationsgehalt geht durch eine Mehrfachnutzung nicht verloren und Daten „verbrauchen“ sich in diesem Sinne bei ihrer Verwendung nicht. Damit beschränkt der „Konsum“ des Gutes „Daten“ durch einen Nutzer nicht die Konsummöglichkeiten eines anderen Nutzers an demselben Gut. Es herrscht keine Rivalität diesbezüglich. Ist dies der Fall, können Daten regelmäßig als „öffentliche Güter“ eingestuft werden und dann kann es wohlfahrtsteigernd sein, die Nutzung von Daten nicht zu beschränken, sondern im Gegenteil deren Austausch und die Weiterverwendung aktiv zu fördern. Denn wenn Nutzer nicht vom Konsum ausgeschlossen werden können, haben sie einen Anreiz, nicht für die Kosten der Datenproduktion zu zahlen. In diesem Fall, und gegeben die Kosten der Datenproduktion sind positiv, wird das Niveau der Datenproduktion suboptimal niedrig sein. Maßnahmen zur Förderung des Datenaustauschs können dann zur Entwicklung neuer datengetriebener Produkte und Dienstleistungen beitragen und das Innovationspotential erhöhen.

Die Eigenschaft als öffentliches Gut haben Daten jedoch nur, wenn neben der Nicht-Rivalität auch Nicht-Ausschließbarkeit im Konsum der Daten besteht, der Dateninhaber also nicht in der Lage ist, den Zugang und die Nutzung durch Dritte aktiv zu beschränken. Kann er dies jedoch, etwa indem er technische Maßnahmen ergreift, um die Daten unter seiner „Kontrolle“ zu halten[1]– und dies ist in der Praxis häufig der Fall – weisen Daten oft eher den Charakter eines „Clubgutes“ auf. Die grundsätzliche Fähigkeit eines Dateninhabers, Dritte von der Datennutzung auszuklammern, führt dazu, dass Daten zu einem handelbaren Gut werden. Nun ist bei Clubs – man denke an ein Fitnessstudio – häufig zu beobachten, dass eine steigende Zahl von Clubmitgliedern dazu führt, dass die Preise für einzelne Clubmitgliedern zwar sinken und die Attraktivität des Clubs damit steigt, jedes zusätzliche Mitglied den Nutzen des Clubs jedoch für andere wegen potenzieller Überlastung (zumindest ab einer bestimmten Schwelle) reduziert. Der Clubbesitzer hat somit ein Interesse daran, die Mitgliederzahl (etwa über den Preis) zu begrenzen, um den Wert seines Clubs zu erhalten. Ähnlich verhält es sich bei Daten. Hier kann es zwar nicht zu einer „Übernutzung“ von Daten bei steigender Nutzerzahl kommen. Jeder zusätzliche Nutzer eines Datensatzes reduziert jedoch deren Wert für andere Nutzer, da man in der Regel – auch bei hoher Innovationsfreunde – von einer begrenzten Anzahl von Anwendungsmöglichkeiten ausgehen muss. Daher kann es für einen Dateninhaber, der als De-facto-Dateneigentümer fungiert, sinnvoll sein, den Zugang zu Daten zu beschränken, um sie wertvoll zu halten, zumal er regelmäßig selbst Datennutzer ist und er somit sowohl als Clubbesitzer als auch als Clubmitglied angesehen werden kann.

[1] Ein formelles Eigentumsrecht an Daten existiert nicht. Die Fähigkeit, Daten dennoch unter Kontrolle zu halten, begründet jedoch oftmals eine „de-facto“ Eigentümerschaft.

Aus dieser Gemengelage entstehen Zielkonflikte, deren regulatorische Handhabung alles andere als trivial erscheint. Skalenerträge und der Charakter als öffentliches Gut unterstützen die Forderung, Daten möglichst breit zu streuen, vielfältigen Nutzungsmöglichkeiten zugänglich zu machen und damit Innovationen zu unterstützen und den Wettbewerb zu beflügeln. Dem gegenüber steht der Charakter von Daten als Clubgut, wo ein großflächiges Teilen eines „Datenschatzes" Anreize beim De-facto Dateninhaber senken kann, in dessen Produktion zu investieren, da er den Nutzen aus der Produktion ggfs. mit Dritten teilen muss und etwaige Wettbewerbsvorteile, die er mit den Daten erzielen kann, durch die Gewährung von Datenzugang zu verlieren droht.[2]

Der Data Act ist der Versuch der Kommission, einen Mittelweg zwischen einem „konsequent proprietären Ansatz" zu finden, der „das Risiko einer ineffizienten Unternutzung von Daten birgt" und einem „radikalen Open-Access-Ansatz", der „zu einer Tragödie der Allmende" führt, und damit mit einer „Unterinvestition in die Erstellung von Daten" – und somit einer zu geringen Generierung von Daten – einhergehen würde.[3] Im Vergleich zum Status quo, in dem zumeist Verträge über die Datennutzung entscheiden, wagt die Kommission nun einen großen Schritt hin zu mehr „Open-Access", um bestehende Datensilos aufzubrechen, den Wettbewerb, insbesondere auf nachgelagerten Märkten, zu fördern und Nutzern von vernetzten Produkten und verbundenen Diensten sowie Dritten an der durch die Datennutzung generierten Wertschöpfung teilhaben zu lassen.

In diesem Lichte sollen im Folgenden die zentralen regulatorischen Vorgaben des Data Act einer genaueren Prüfung unterzogen werden:

Die Kommission will künftig alle IoT-Produktanbieter dazu verpflichten, ihre Produkte bzw. Dienste so zu gestalten, dass Nutzer grundsätzlich auf die bei deren Nutzung erzeugten Daten zugreifen können. Nutzern soll es ihrerseits ermöglicht werden, die gemeinsam mit dem faktischen Dateninhaber – oft der IoT-Produktanbieter – generierten Daten mit Dritten zu teilen. Die Kommission begründet diese Vorgaben insbesondere mit dem Argument der „Fairness in der digitalen Wirtschaft". Zum einen trügen die Nutzer der vernetzten Produkte durch deren Verwendung zu dessen Wertschöpfung bei, sodass sie quasi ein Recht an der Teilhabe an den Wertschöpfungsgewinnen hätten. Zum anderen seien die bei der Nutzung der Produkte erzeugten Daten ein zentraler Inputfaktor zur Entwicklung von „Anschluss-, Neben- und sonstige Diensten", etwa Reparaturdienstleistungen, sodass mit der Datenweitergabe an Dritte Innovationen ausgelöst, Markteintritte begünstigt sowie Lock-in-Effekten vorgebeugt werden können.

Nun könnte man in – von wirksamem Wettbewerb geprägten – Märkten für vernetzte Produkte erwarten, dass verschiedene IoT-Produktanbieter unterschiedliche Datenzugangsmodelle anbieten (müssen), um Kunden gewinnen zu können. IoT-Produktanbieter, die es Nutzern nicht ermöglichen, Daten selbst zu nutzen oder sie an Dritte weiterzugeben, würden rasch aus dem Markt ausscheiden, sofern für diese Daten(mit)nutzung eine Präferenz bei den Nutzern besteht. Die Kommission scheint nun jedoch davon auszugehen, dass ein solcher wirksamer Wettbewerb nicht besteht und es – über alle IoT-Produktkategorien und alle Nutzergruppen hinweg – eine „Unterbereitstellung" datenzugangsgewährender vernetzter Produkte gibt, bzw., dass auch eine „Unterversorgung" Dritter mit IoT-Nutzungsdaten besteht und daher insbesondere der Wettbewerb auf nachgelagerten Märkten sowie die Innovationsfreudigkeit eingeschränkt ist. Der freie Markt liefere somit nicht die wohlfahrtsoptimale „Verteilung der Daten zum Nutzen der Gesellschaft".

Dieses Urteil ist in seiner Pauschalität nicht überzeugend. Es suggeriert (1), dass ein solches Marktversagen auf allen Märkten für vernetzte Produkte vorliegt, egal ob es sich dabei etwa um den Markt für vernetzte Fahrzeuge oder den für eine spezielle vernetzte Industriemaschine handelt, und (2), dass das Versagen unabhängig von der Art der Nutzer des vernetzten Produktes besteht, also etwa egal ob es sich bei diesem typischerweise um einen Verbraucher oder aber ein Unternehmen handelt. Davon kann jedoch nicht per se ausgegangen werden.[4]

Nicht auf all diesen verschiedenartigen Märkten für vernetzte Produkte herrscht Marktversagen. Nicht überall gibt es Problematiken, wie etwa

---

[2] Vgl. dazu auch Van Roosebeke, B./Anzini, M./Eckhardt, P./Pierrat, A., cepStudie "European Leadership in the Digital Economy, 2020.

[3] Schweitzer, H., & Welker, R. (2020). A legal framework for access to data–A competition policy perspective. Data access, consumer interests and public interest, Forthcoming, S. 5.

[4] Drexl et al. weisen zudem darauf hin, dass IoT-Produktanbieter im Gegensatz zu Gatekeepern regelmäßig nicht von Netzwerkeffekten profitieren, sodass ihre Marktposition leichter anfechtbar ist und davon auszugehen ist, dass die Märkte für vernetzte Produkte „eher wettbewerbsorientiert sind". [Drexl et al. (2022), Position Statement of the Max Planck Institute for Innovation and Competition of 25 May 2022 on the Commission's Proposal of 23 February 2022 for a Regulation on harmonised rules on fair access to and use of data (Data Act), Ziffer 33].

1. eine unangreifbare Marktmacht auf Seiten des IoT-Produktanbieters bzw. des Dateninhabers, die es Nutzern erschweren bzw. unmöglich machen würde, sich Datenzugangsrechte und Datenweitergaberechte auszubedingen,
2. unüberbrückbare Informationsasymmetrien zwischen IoT-Produktanbietern bzw. Dateninhabern und Nutzern, die es Nutzern erschweren, eine fundierte und (langfristig) präferenzkompatible Entscheidung beim Kauf, beim Mieten bzw. beim Leasen eines vernetzten Produkts zu treffen, oder
3. eine ungleich verteilte Verhandlungsposition, die es dem IoT-Produktanbieter bzw. Dateninhaber erlauben würde, Nutzern „unfaire" Vertragskonditionen aufzudrängen.

Die Gewährung von Datenzugangs- bzw. Datenweitergaberechten lässt sich am ehesten noch begründen, wenn Verbraucher Nutzer eines vernetzten Produktes sind. Denn hier ist, insbesondere aufgrund eines Defizits an Informationen bei der Entscheidung über den Erwerb, des Mietens bzw. des Leasens eines vernetzten Produkts, regelmäßig zu erwarten, dass diese nicht hinreichend auf die Datenzugänglichkeit achten, etwa weil sie den Nutzen der eigenen Verfügung über die Daten oder der Weitergabe der Daten an Dritte (noch) nicht vollständig erfassen (können).[5] In der Folge fragen sie eher vernetzte Produkte nach, die, entgegen ihren Interessen, Daten beim IoT-Produktanbieter bzw. Dateninhaber belassen.

Mit Blick auf Unternehmen als Nutzer der vernetzten Produkte kann aber in weit größerem Maße erwartet werden, dass diese etwaige Informationsdefizite zu reduzieren versuchen und sich mit den Anbietern vertraglich auf „ausgewogene" Datenzugangs- bzw. Datenweitergaberechte verständigen können. Auch ist hier anzunehmen, dass nicht in jedem Fall der IoT-Produktanbieter über eine stärkere Verhandlungsmacht verfügt. Im Gegenteil sind auch regelmäßig Szenarien wahrscheinlich, bei denen Großunternehmen von kleinen IoT-Produktanbietern verlangen (können), dass nur sie als Nutzer auf gemeinsam erzeugte Daten zugreifen und sie verwerten dürfen. Ein „Versagen" des Marktes ist also in B2B-Szenarien ungleich unwahrscheinlicher und der regulatorische Eingriff über den Data Act damit nicht in jedem Fall angemessen. Er kann in einigen Fällen auch kontraproduktiv sein, insbesondere dann, wenn bereits vertragliche Regelungen bestehen, die von allen beteiligten Akteuren als zufriedenstellend betrachtet werden.

Ein marktversagensunabhängiges, pauschales Datenzugangs- und Datenweitergaberecht ist zudem insbesondere problematisch, da es nun alle Hersteller bzw. Entwickler verpflichtet, vernetzte Produkte so zu produzieren bzw. zu entwerfen, dass sie Datenzugang ermöglichen („Access by design"). Dieser Eingriff in die unternehmerische Freiheit schränkt sie in ihren Produktgestaltungsmöglichkeiten ein, erhöht den Aufwand und die Kosten bei der Produktentwicklung/-herstellung und kann damit zu höheren Produktpreisen führen. Gleichzeitig ist jedoch nicht sicher, dass access by design ein Produktfeature ist, das in jedem Fall auf Nachfrage stößt und für das es eine Zahlungsbereitschaft auf Seiten potenzieller Nutzer gibt. Tut es das nicht, ist access by design schlicht unnötig. Er könnte bei Herstellern bzw. Entwicklern und bei den Nutzern den Anreiz schaffen, wieder vermehrt „nicht-vernetzte" Produkte anzubieten bzw. auf diese umzusteigen. Dies wäre dann jedoch nicht mit den intendierten Zielen, die sich die Kommission mit dem Data Act gesetzt hat, kompatibel.

Erstes Zwischenfazit:

Der Ansatz der Kommission, über alle vernetzten Produkte und Nutzergruppen hinweg einheitliche „horizontale" Vorschriften zur Datennutzung und Datenweitergabe festzulegen, geht fehl. Ein großflächiges Marktversagen besteht nicht. Allenfalls in B2C-Szenarien ließe sich ein solches aufgrund von inhärenten Informationsasymmetrien feststellen. Die EU-Gesetzgeber sollten sich daher für einen deutlich spezifischeren und differenzierenden Regulierungsansatz stark machen.

Unabhängig von der Beurteilung des grundsätzlichen Regulierungsansatzes bietet der Data Act viel Raum für weitere Diskussionen:

Zunächst ist hier der Anwendungsbereich des Data Act zu nennen, dem es an hinreichender Rechtsklarheit und Rechtssicherheit mangelt. Es fehlt insbesondere an Eindeutigkeit bei den Fragen

(1) welche Produkte und Dienste der Data Act erfasst, d.h. bei welchen Produkten und Diensten der Datenzugang ermöglicht werden soll,
(2) wer die Adressaten der Regeln zum Datenzugang und zur Datenweitergabe sind und wer tatsächlich Dateninhaber und wer Datennutzer ist, und

[5] Zum Zeitpunkt des Erwerbs eines vernetzten Fahrzeugs macht sich ein Verbraucher ggfs. noch keine Gedanken darüber, dass ein Reparaturdienst eines Dritten etwaige Daten nach mehreren Jahren der Nutzung benötigen könnte.

(3) zu welchen Daten konkret Zugang gewährt werden muss.

Zu (1) Erfasste Produkte und Dienste: Der Data Act erfasst vernetzte Produkte und damit Produkte, die Daten über ihre Nutzung oder ihre Umgebung erlangen, erzeugen oder sammeln (z.B. vernetzte Maschinen), nicht aber solche, deren Hauptfunktion darin besteht, Daten zu speichern und zu verarbeiten, Inhalte anzuzeigen, abzuspielen, aufzuzeichnen oder zu übertragen (z.B. Webcams, Tablets). Diese Abgrenzung von erfassten vs. nicht erfassten Produktkategorien bietet einen großen Interpretationsspielraum. So ist bspw. unklar, ob Smartphones oder Fitnesstracker in die eine oder die andere Kategorie fallen, da ihnen ggfs. die Produkteigenschaften beider Kategorien innewohnen. Da die Konsequenzen der regulatorischen (Nicht-)Einstufung bedeutend sind, ist hier zwingend eine weitere Konkretisierung vonnöten. Diese sollte in erster Linie im Rechtsakt selbst erfolgen. Jedoch sollte auch über eine weitere Präzisierung durch die Kommission etwa über delegierte Rechtsakte nachgedacht werden, wobei technologischen Entwicklungen und Innovationen im IoT-Sektor Rechnung getragen werden sollte.

Ungeachtet der regulatorischen Unschärfe bei den vom Anwendungsbereich der Verordnung erfassten vernetzten Produkten ist auch nicht ersichtlich, warum die Kommission die Abgrenzung überhaupt in dieser Form vornimmt. Mit der Abgrenzung geht letztlich die Vermutung einher, dass eine „Datenunternutzung" und Marktversagensproblematiken – z.B. Lock-in-Effekte, asymmetrische Informationsverteilung, Machtkonzentration auf Seiten der Produkthersteller bzw. Dateninhaber, mangelnder Wettbewerb auf Anschlussmärkten – in erster Linie auf den Märkten erfasster IoT-Produkte vorliegen, nicht aber auf den Märkten anderer, nicht erfasster datenerzeugender Produkte. Davon kann jedoch nicht pauschal die Rede sein. Die Abgrenzung ist damit letztlich willkürlich, kann Wettbewerbsverzerrungen bedingen und zu Regulierungsarbitrage einladen. Bei der Konkretisierung der erfassten Produktarten sollte die Kommission damit neben der Herstellung von Rechtsklarheit und -sicherheit auch darauf hinwirken, sich auf solche Produkte zu beschränken, bei denen faktisch Marktversagensentwicklungen zu beobachten sind.

Zu (2) Verhältnis Hersteller/Entwickler, Dateninhaber und Nutzer: Hauptadressaten des Data Act sind in erster Linie die Hersteller bzw. Entwickler von vernetzten Produkten sowie die faktischen Inhaber von Daten. Hier stellen sich mehrerlei Fragen, die der Data Act nur unzureichend beantwortet. Insbesondere bleibt unklar (nur eine Auswahl offener Fragen),

- wer nach Auffassung der Kommission tatsächlich der Hersteller bzw. Entwickler eines solchen Produkts ist; es mangelt an einer Definition dieser Akteure,
- was passiert, wenn Hersteller und Entwickler unterschiedliche Unternehmen sind und – wenn mehrere Akteure am Herstellungs- bzw. Entwicklungsprozess eines Produkts beteiligt sind – wen die Vorschriften zur Zugänglichmachung von Daten treffen,
- ob der/die Hersteller bzw. Entwickler auch gleichzeitig (immer) als der/die Dateninhaber angesehen wird bzw. werden kann, oder wie das Verhältnis dieser beiden Hauptadressaten zueinander ist,
- an welchen der beiden Hauptadressaten sich eine Vorschrift des Data Acts tatsächlich richtet; für wen bspw. die Transparenzpflichten[6] gelten, und
- welche Rechtsfolgen damit einhergehen, wenn der Nutzer eines vernetzten Produkts de facto die Kontrolle über die generierten Daten hat und damit als „Dateninhaber" angesehen werden könnte und nicht etwa der Hersteller bzw. Entwickler des Produkts.

Grundsätzlich scheint die Kommission in ihren Überlegungen von einfachen und wenige Akteure umfassenden Wirtschaftsbeziehungen auszugehen. Komplexere Wertschöpfungsketten, bei denen bspw. mehrere Hersteller einzelne Komponenten zur Produktion eines vernetzen Produkts beisteuern, scheinen nicht im Fokus zu stehen bzw. werden von den Vorschriften nicht adäquat und konsequent abgebildet. Auch die Tatsache, dass Personen die vernetzten Produkte nutzen könnten, die diese nicht direkt erworben, gemietet oder geleast haben, wird von den Vorgaben entweder ausgeblendet oder nicht spezifisch genug adressiert.[7]

---

[6] Der Data Act schreibt diese zwar vor, sagt aber nicht, ob sie vom Hersteller/Entwickler, vom Dateninhaber oder etwa direkt vom Verkäufer eines vernetzten Produkts erfüllt werden müssen.

[7] Muss bspw. ein Hersteller/Entwickler bzw. ein Dateninhaber mit allen Nutzern einer vernetzten Maschine bspw. einen Vertrag zur Nutzung nicht-personenbezogener Daten abschließen oder nur mit dem Eigentümer der Maschine, dem Mieter bzw. dem Leasingnehmer? Braucht ein Fahrer eines vernetzten Fahrzeugs, der nicht der Eigentümer des Fahrzeugs ist, ein separates Nutzerkonto?

All diese Unklar- und Uneindeutigkeiten sorgen für erhebliche Rechtsunsicherheit für alle betroffenen Parteien und müssen daher dringend angegangen werden. Bevor diese nicht beseitigt sind, lassen sich zahlreiche Folgen der Data Acts jedenfalls nur schwer abschätzen.

Zu (3) Zugänglichmachung von Daten: Der Data Act schreibt den Zugang zu bei der Nutzung eines vernetzten Produkts oder verbundenen Dienstes „erzeugten" Daten vor und zielt dabei insbesondere auf die dabei generierten „Rohdaten" ab, während aus den erzeugten Daten „abgeleitete Daten oder gefolgerte Informationen" außen vor bleiben sollen. Die Begrenzung auf Rohdaten ist grundsätzlich sachgerecht, da damit Investitionsanreize auf Seiten der Produkthersteller/-entwickler bzw. der Dateninhaber gesichert und deren Innovationspotenzial nicht unbotmäßig geschmälert wird. Dies wäre regelmäßig der Fall, wenn auch Zugang zu aufwendig aufbereiteten Daten gewährt werden müsste.[8] Zwar würde der Wettbewerb auf Sekundärmärkten durch den Zugriff auch zu aufbereiteten Daten intensiviert, er reduziert jedoch den Anreiz insbesondere der Dritten, selbst in die Datenaufbereitung zu investieren, und lädt diese daher zu Trittbrettfahrer-Verhalten ein. Die Begrenzung auf Rohdaten stellt damit auch sicher, dass Dritte, denen die Nutzer der vernetzten Produkte Daten zur Verfügung stellen, ihrerseits Anstrengungen unternehmen, Innovationen auf Basis der erhaltenen Daten zu generieren.

Gleichwohl bedarf es auch hier einiger Klarstellungen. Denn der Data Act lässt etwa die zur Datenbereitstellung verpflichteten Parteien im Unklaren darüber, ob sie auch solche „Rohdaten" zur Verfügung stellen müssen, die zwar bei der Nutzung erzeugt werden, aber (bisher) nicht explizit erhoben, (dauerhaft) gespeichert oder sonst gesteuert verarbeitet werden. Wären auch solche Daten erfasst, würde dies eine Zusatzerhebung, Speicherung und ggf. Aufbereitung bisher nicht gesammelter Daten nötig machen. Dies wäre in vielen Fällen unnötig, teuer und stünde auch im Widerspruch zum Grundsatz der Datenminimierung der DSGVO. Hersteller, Entwickler und Dateninhaber sollten daher nicht zu einer solchen weitergehenden Datensammlung verpflichtet werden.

Zweites Zwischenfazit:

Dem Geltungsbereich des Data Act mangelt es derzeit in mehrerlei Hinsicht an Rechtsklarheit. In seiner jetzigen Fassung wirft er mehr Fragen auf, als er Antworten liefert. Dies schafft veritable Rechtsunsicherheiten sowohl für jene Akteure, die Daten bereitstellen müssen als auch für jene, die sie nutzen dürfen. Diese Unklarheiten müssen beseitigt werden. Dazu gilt es die Definitionen des Data Acts eindeutiger zu formulieren, Verantwortlichkeiten zu klären und insbesondere die ganze Komplexität von Herstellungsprozessen, Lieferketten und Nutzungsverhalten abzubilden.

Access „by-design":

Der Data Act verpflichtet die IoT-Produktanbieter dazu, ihre Produkte bzw. Dienste so auszugestalten, dass die Nutzer direkten Zugang zu den Daten erhalten. Diese Access-by-design-Pflicht beschränkt die IoT-Produktanbieter zunächst aktiv in ihrer Produktgestaltung. Dies stellt einen weitgehenden Eingriff in deren unternehmerische Freiheit dar und bedarf deshalb einer hinreichenden Rechtfertigung. Gegeben es herrscht kein wirksamer Wettbewerb auf einem oder mehreren IoT-Märkten und die IoT-Produktanbieter haben etwa aufgrund ihrer Marktstellung die volle Kontrolle über die generierten Daten (s. dazu auch einleitende Erläuterungen der ökonomischen Bewertung), ließen sich Access-by-design-Pflichten, die Nutzern einen effektiven Datenzugang sichern, insbesondere damit begründen, dass die Nutzer durch die Verwendung vernetzter Produkte regelmäßig aktiv dazu beitragen, den Wert der Produkte zu steigern. Oft sind es nicht allein die IoT-Produktanbieter, die Daten „produzieren". Stattdessen sorgen sowohl sie als auch die Käufer, Mieter oder Leasingnehmer oder mittelbare Nutzer eines Produkts kollaborativ dafür. In diesen Fällen kann es daher angemessen sein, dass auch alle an der Datenerzeugung beteiligten Akteure an den mit der Datengenerierung einhergehenden Wertschöpfungszuwächsen partizipieren dürfen. Eine breite, allumfassende Access-by-Design-Pflicht unabhängig von der Wettbewerbssituation ist jedoch abzulehnen. Unabhängig davon muss klargestellt werden, ob die Access-by-design-Pflicht auch für vernetzte Produkte gelten soll, die bereits am Markt erhältlich sind, was unverhältnismäßig wäre, oder ob sie nur für neue Produkte greifen soll, was angemessen wäre. In jedem Fall sollte den IoT-Produktanbietern eine angemessene Frist für die Implementierung der neuen Vorgaben eingeräumt werden.

Transparenzpflichten:

Oft wissen Nutzer von vernetzten Produkten und verbundenen Diensten nicht, ob, zu welchen Zwecken und in welchem Ausmaß die bei der Nutzung der Produkte bzw. Dienste anfallenden Daten vom IoT-Produktanbieter

[8] Das Anreizargument greift jedoch umso weniger, je eher die Vernetztheit eines Produkts ein nicht wesentliches Zusatzelement des Produktes ist und je geringer der Aufwand bzw. die Kosten für die Bereitstellung der Datenkomponente des Produkts sind.

genutzt werden, welche Daten überhaupt erzeugt werden und welche Möglichkeiten sie als Nutzer zur Verwendung der Daten haben, obgleich sie häufig einen aktiven Beitrag an der Wertschöpfung leisten. Der von der Kommission anvisierte Abbau dieser Informationsasymmetrien mittels Transparenzvorgaben kann Nutzer in die Lage versetzen, eine informierte Entscheidung beim Erwerb, beim Mieten oder Leasen eines vernetzten Produkts zu treffen und fördert damit grundsätzlich das Zustandekommen eines effizienten Marktergebnisses. Die Reduktion des Informationsgefälles ist insbesondere in B2C-Kundenverhältnissen sachgerecht. Für B2B-Konstellationen gilt dies jedoch nur eingeschränkt. Hier können eigene Anstrengungen der Unternehmen erwartet werden, im Zuge von Vertragsverhandlungen an die für sie relevanten Informationen zu Datenaspekten zu gelangen. Eine gesetzgeberische Hilfestellung ist für sie unnötig.

Zu klären im Zuge der Verhandlungen zum Data Act ist zudem noch (1) wer eigentlich der Adressat bzw. die Adressaten der Transparenzpflichten sind, (2) in welcher Form die Informationen den Nutzern zur Verfügung gestellt werden müssen und (3) wie mit Änderungen der Datennutzung über die Zeit umgegangen werden soll:

Zu (1): Derzeit ist offen, ob die Transparenzpflichten direkt für den IoT-Produktanbieter oder den Dateninhaber (falls dieser nicht gleichzeitig der IoT-Produktanbieter ist) gelten, oder, ob sie ggfs. auch bzw. oder andere Akteure treffen, wie etwa den Händler, bei dem der Nutzer das IoT-Produkt erwirbt oder den Leasinggeber, bei dem er dieses least. Letztere sind zwar derzeit nicht explizit vom Data Act erfasst, sie sind jedoch regelmäßig diejenigen Akteure, die im direkten Kontakt mit den potenziellen Nutzern stehen und das Produkt in den Verkehr bringen, während dieser Nutzerkontakt bei den IoT-Produktanbietern bzw. Dateninhabern regelmäßig nicht besteht. Falls die Pflicht für die letzteren Akteure gelten soll, was aufgrund der Nähe zum Nutzer regelmäßig angemessen wäre, muss insbesondere sichergestellt sein, dass sie ihrerseits über die nötigen Informationen verfügen (dies kann nicht per se als gegeben angenommen werden). Falls die Transparenzpflicht direkt die IoT-Produktanbieter trifft, müsste etwa geklärt werden, wie die offenzulegenden Informationen dem Nutzer bereitgestellt werden können, wenn kein direkter Kontakt zwischen den beiden Parteien besteht.

Zu (2): Völlig offen ist ferner, in welcher Form – digital, auf Papier, auf der Produktverpackung, als QR Code – die Informationen dem Nutzer bereitgestellt werden sollen. Eine einheitliche Vorgehensweise, die für alle von der Verordnung erfassten, vernetzten Produkte und verbundenen Dienste sinnvoll ist, ist dabei zwar aufgrund der verschiedenen Märkte unrealistisch. Grundlegende Leitlinien oder die Nennung von Best-Practices-Beispielen sind dennoch angezeigt, um einen Wildwuchs an unterschiedlichen Umsetzungen seitens der Verpflichteten zu vermeiden.

Zu (3): Die vorvertraglichen Transparenzpflichten stellen auf die voraussichtliche Datenerzeugung des vernetzten Produkts bzw. verbundenen Dienstes ab und darauf, welche erzeugte Daten selbst genutzt und ggfs. an Dritte weitergegeben werden sollen. Damit wird aber implizit angenommen, dass dies in jedem Fall ex ante schon feststeht und nach Vertragsschluss hier kein Wunsch nach Veränderung besteht. Es ist daher zu klären, ob eine Anpassung der Datennutzung nach Vertragsschluss durch die zur Transparenz verpflichtete Partei bspw. neue Transparenzpflichten auslöst oder auch eine Vertragsanpassung nötig macht.

Recht auf Datenzugang:

Wie bereits oben ausgeführt, ist ein breites, marktversagensunabhängiges Recht auf Zugang zu Daten für die Nutzer abzulehnen und, wenn überhaupt, nur in B2C-Konstellationen zu rechtfertigen. Ungeachtet dessen sollen im Folgenden einige, mit dem Zugangsrecht einhergehende Aspekte diskutiert werden.

Laut Kommissionsvorschlag sollen Nutzer – auf Verlangen – Zugang zu bei der Produktnutzung erzeugten Daten „unverzüglich, kostenlos und ggfs. kontinuierlich und in Echtzeit“ erhalten, sofern sie auf die Daten nicht sowieso direkt vom Produkt aus zugreifen können. Gleichzeitig soll der Dateninhaber erzeugte nicht-personenbezogene Daten nunmehr nur dann noch nutzen dürfen, sofern er hierfür vertraglich die Erlaubnis des Nutzers erhalten hat. Durch die Kombination dieser beiden Vorschriften wird die Stellung des Nutzers im Verhältnis zum Dateninhaber deutlich gestärkt. Die regulatorisch gewünschte Stärkung der Rechtsposition des Nutzers, die naturgemäß die des Dateninhabers schwächt, birgt jedoch einige praktische Gefahren:

Erstens geht die Datenbereitstellung mit hohen Kosten für den Dateninhaber einher, insbesondere, wenn diese kontinuierlich und in Echtzeit erfolgen muss und wenn bei der Nutzung des vernetzten Produkts Daten in großen Umfang erzeugt werden. Da die Datenbereitstellung in jedem Fall kostenlos erfolgen muss, obgleich der Dateninhaber möglicherweise signifikante Investitionen in die Fähigkeit des Produkts zur Datenerzeugung getätigt hat – und der Wertschöpfungsbeitrag des Nutzers ggf. gering ist – ist damit zu rechnen, dass der IoT-Produktanbieter den Aufwand etwa über eine Anhebung des Produktpreises oder der Verringerung der Vernetztheit des Produkts

begegnen wird. Beides wäre, im Sinne des Ziels der Kommission die Datenteilung in der EU zu fördern, kontraproduktiv.[9]

Zweitens bleibt die Wirkung der Pflicht zum Abschluss eines Vertrags über die Nutzung nicht-personenbezogener Daten offen. Zwar geht damit eine faktische Verbesserung der Verhandlungsposition der Nutzer einher. Ob daraus eine tatsächliche Stärkung der Position erwächst, ist jedoch fraglich, insbesondere wenn der Nutzer ein Verbraucher ist und das nachgefragte Produkt ein Massenprodukt. Dann ist regelmäßig zu erwarten, dass der Verbraucher seine potenzielle Macht nicht nutzt, weil er, wie derzeit üblich, wenig Interesse daran zeigt, in welchem Umfang der Dateninhaber die Daten selbst nutzt, oder sie de facto nicht nutzen können wird, weil der Dateninhaber (sofern er auch gleichzeitig der IoT-Produktanbieter ist), den Erwerb des Produkts auch von für ihn vorteilhaften Datennutzungsvereinbarungen abhängig macht. Ist der Nutzer hingegen ein Unternehmen, und haben wir es daher mit einem B2B Szenario zu tun, sollte es den beteiligten Akteuren freistehen, ob und wie sie die Datennutzung regeln. Ein einseitiges Zustimmungsrecht des Nutzers zur Nutzung gemeinsam generierter Daten geht jedenfalls unsachgemäß zulasten des Dateninhabers und damit derjenigen (Vertrags-)Partei, die Investitionen in die Nutzbarmachung der erzeugten Daten getätigt hat. Letztlich sollten – in einem von Wettbewerb geprägten Markt für vernetzte Produkte – die im Data Act vorgesehenen Transparenzpflichten die Nutzer bereits hinreichend in die Lage versetzen, eine fundierte Entscheidung über den Erwerb, das Anmieten oder das Leasen eines vernetzten Produkts treffen zu können. Zusätzliche verpflichtende Vertragsregelungen, die einseitig den Nutzer eines Produkts bevorzugen, sind jedenfalls und insbesondere in B2B Szenarien unnötig und gehen schlussendlich nur mit vermeidbaren Transaktionskosten einher, die einem verstärkten Datenaustausch im Weg stehen dürften.

Drittens stellt sich die Frage, warum nur die Nutzer eines vernetzten Produkts einen Zugangsanspruch gewährt bekommen sollen, während andere Akteure, die (un-)mittelbar an der Datenerzeugung beteiligt sind, nicht hiervon „profitieren“ sollen. Dies gilt etwa für all jene Fälle, bei denen der IoT-Produktanbieter nicht selbst der Dateninhaber ist und er somit möglicherweise selbst keinen Zugriff auf die erzeugten Daten hat, aber seinerseits Interesse an den Daten hätte, z.B. mit dem Ziel, sein eigenes vernetzten Produkt zu verbessern.

Umgang mit Geschäftsgeheimnissen:

Mit ihren Vorschlägen zur Offenlegung von Geschäftsgeheimnissen gegenüber Nutzern und interessierten dritten Datenempfängern auf Basis entsprechender Schutzvorkehrungen öffnet die Kommission eine Büchse der Pandora. Sie will einerseits Nutzern und Dritten den Zugriff zu Daten ermöglichen, die für den Dateninhaber als Geschäftsgeheimnisse gelten, andererseits aber diese Geheimnisse zugleich schützen, etwa vor dem Zugriff unautorisierter weiterer Akteure. Dass dieses Ziel einer „kontrollierten Offenlegung“ mit den vorgesehenen Vorgaben erreicht werden kann, ist jedoch wenig realistisch, insbesondere da die Kontrollinstrumente schwach sind. So wird der Dateninhaber regelmäßig nicht in der Lage sein, zu überwachen, ob die Schutzvorkehrungen von Nutzern bzw. Datenempfängern auch tatsächlich eingehalten werden. Auch mangelt es ihm an Mitteln zur Durchsetzung der Schutzvorkehrungen. Muss er jedoch die jederzeitige Preisgabe der Geschäftsgeheimnisse fürchten, lähmen die damit einhergehenden Unsicherheiten seine Investitions- und Innovationsbereitschaft. Das gilt es zu vermeiden. Da die Offenlegung von Geschäftsgeheimnissen regelmäßig ein hohes Maß an Vertrauen zwischen den beteiligten Parteien voraussetzt, sollte sie in erster Linie nur auf freiwilliger Basis erfolgen. Sollte der Gesetzgeber dennoch auf eine kontrollierte Offenlegung bestehen, gilt es erstens genauer zu regeln, welche Schutzvorkehrungen als hinreichend angesehen werden können, und zweitens müssen Regeln geschaffen werden, die dem Dateninhaber eine effektive und wirksame Kontrolle ermöglichen.

Entwicklung eines Konkurrenzprodukts durch den Nutzer oder Dritte:

Die Kommission will Nutzern und Dritten verbieten, erlangte Daten zur Entwicklung von Produkten zu nutzen, die mit dem vernetzten Produkt des IoT-Produktanbieters im Wettbewerb stehen. Diese Schutzklausel soll verhindern, dass „Investitionsanreize für den Produkttyp, von dem die Daten erlangt werden […] untergraben werden“ und ist in diesem Sinne auch angemessen. Die Vorgabe muss jedoch noch konkretisiert werden. Es ist insbesondere näher zu spezifizieren, (1) was unter einem Wettbewerbsprodukt genau zu verstehen ist[10] und welche

[9] Es gibt zudem berechtigte Zweifel, ob eine kontinuierliche Echtzeit-Datenbereitstellung immer zu noch vertretbaren Kosten möglich ist oder ob hier nicht der damit einhergehende Aufwand den Nutzen deutlich übersteigt.

[10] Hier sollte insbesondere auf die bereits im Wettbewerbsrecht verankerten Verfahren abgestellt werden.

Kriterien hierfür herangezogen werden sollen[11], (2) welchen zeitlichen[12] und räumlichen[13] Rahmen die Beschränkung für die Nutzer hat, (3) wie diese Regelung kontrolliert wird,[14] und (4) welche Folgen ein potenzieller Verstoß seitens des Nutzers gegen das Verbot hat[15]. Auch sollte geklärt werden, ob die Schutzklausel auch die Entwicklung verbundener Dienste zu den vernetzten Produkten mit einbezieht. Dies wäre im Regelfall nur konsequent. Gleichzeitig sollten die Schutzklauseln nicht verhindern, dass Nutzer oder Dritte Konkurrenzprodukte entwickeln können, ohne sich dabei der erlangten Daten zu bedienen.

Ausnahmen für kleine Hersteller/Entwickler von vernetzten Produkten:

Die Kommission will bestimmte kleine und Kleinstunternehmen von den Access-by-design- bzw. Datenbereitstellungspflichten befreien. Dies ist aus mindestens zwei Gründen abzulehnen. Erstens geht diese Regelung von in der Pauschalität falschen Annahme aus, dass große IoT-Produktanbieter regelmäßig eher in der Lage sind, Datennutzungsmöglichkeiten für sich selbst auszubedingen. Es ist aber bspw. nicht per se anzunehmen, dass der Anbieter seine Größe immer aufgrund des vernetzten Charakters des Produkts gewonnen hat. Hierfür können andere Produkteigenschaften oder auch andere Produkte und Dienstleistungen des Unternehmens eine weitaus wichtigere Rolle gespielt haben. Im Gegenteil könnten auch gerade kleine, aber hoch spezialisierte Anbieter vernetzter Produkte, die auf ihrem jeweiligen Markt eine hervorgehobene Stellung haben, eine gute Verhandlungsposition bei der Frage der Verteilung von Datennutzungsrechten besitzen. Die simple Unterscheidung klein vs. groß ist daher nicht zielführend. Zweitens werden mit den Ausnahmen nicht zu rechtfertigende Wettbewerbsverzerrungen zwischen großen und kleinen IoT-Produktanbietern erzeugt.[16]

Datenweitergabe an Dritte:

Mit dem Data Act soll es den Nutzern vernetzter Produkte ermöglicht werden, die Daten, die bei der Nutzung des Produkts erzeugt werden, auch an Dritte weiterzugeben. Erklärtes Hauptziel ist es, dabei „Innovationen durch mehr Marktteilnehmer“ zu ermöglichen und insbesondere ein „wettbewerbsorientiertes Angebot von Anschlussdiensten“ wie Reparatur- und Wartungsdiensten zu schaffen. Auch soll die Entwicklung neuer Produkte und Dienste gefördert werden, die nicht mit dem vernetzten Produkt im Wettbewerb stehen [S. 16]. Wie eingangs der Bewertung beschrieben, ist eine marktversagensunabhängige Datenweitergabe an Dritte jedoch kritisch zu sehen (s. dazu ausführlich S. 12 und 13). Die Verfügbarmachung von Daten an Dritte kann zwar die Innovationsfähigkeit etwa von Anbietern von Anschlussdiensten verbessern, Effizienzgewinne erzeugen, den Wettbewerb auf den Sekundärmärkten stützen und Markteintritte auf diesen Märkten fördern. Liegt jedoch kein Marktversagen vor und sind die bereitgestellten Daten bspw. kein „wesentlicher Inputfaktor“ (im Sinne der Essential-Facilities-Doktrin)[17], kann die einfache Datenbereitstellung an Dritte die Eigenleistung des (potenziellen) Anbieters von Anschlussdiensten ausbremsen und ihn zu simplem Trittbrettfahrer-Verhalten einladen. Die verpflichtende Bereitstellung an Dritte schmälert zudem den Wert getätigter Investitionen in die Nutzbarmachung von IoT-Daten für den Dateninhaber und senkt damit den Anreiz für diesen, Kapital in die Vernetztheit seines Produkts zu stecken.[18]

---

11 Wie wird bestimmt, ob ein vom Nutzer entwickeltes vernetztes Produkt im Wettbewerb zum vernetzten Produkt des IoT-Produktanbieters steht?

12 Soll es einen Zeitpunkt in der Zukunft geben, zu dem der Nutzer auf Basis der erlangten Daten, ein Konkurrenzprodukt entwickeln darf, oder gilt das Verbot für immer?

13 Darf der Nutzer auf Basis der erlangten Daten überhaupt kein Konkurrenzprodukt entwickeln, unabhängig davon wo es angeboten wird (EU vs. Nicht-EU)?

14 Ist es die Aufgabe des IoT-Produktanbieters laufend zu prüfen, zu welchen Zwecken der Nutzer die bereitgestellten Daten nutzt und wie kann er dies praktisch tun? Was ist, wenn der Nutzer ein Konkurrenzprodukt entwickelt, aber ohne hierfür bereitgestellte Daten genutzt zu haben?

15 Rechtsfolgen einer unbefugten Nutzung treffen nach Art. 11 allenfalls den Datenempfänger, nicht aber den Nutzer.

16 Offen bleibt, ob die Verpflichtung für große IoT-Produktanbieter die kleineren Anbieter nicht letztlich zwingt, die Vorgaben der Verordnung ebenfalls zu erfüllen. Das wäre insbesondere dann der Fall, wenn die Nutzer eine Präferenz für Produkte entwickeln, die ihnen Datennutzungsmöglichkeiten gewähren.

17 Nach der Doktrin gilt eine Einrichtung nur dann als „wesentlich“, wenn der Zugang zu ihr (hier: der Zugang zu bestimmten Daten) „unerlässlich“ für die Ausübung einer nachgelagerten Tätigkeit ist. Das schließt ein, dass es sowohl faktisch als auch potenziell kein Substitut zu der als wesentlich betrachteten Einrichtung gibt. Ferner müssen „technische, rechtliche oder auch wirtschaftliche Hindernisse bestehen“, die es unmöglich machen, eine eigene solche Einrichtung (hier: eines eigenen vernetzten Produkts) zu entwickeln. Zudem muss die Verweigerung des Zugangs zu der Einrichtung dazu geeignet sein, den Wettbewerb auf dem nachgelagerten Markt de facto auszuschalten. [s. dazu auch Van Roosebeke et al. (2020) European Leadership in the Digital Economy, cepStudy]

18 Laut Haucap (2020) könnte dieser negative Effekt auf die Investitionsbereitschaft aufgrund des oft nicht-rivalisierenden Charakters von Daten und der Tatsache, dass Daten häufig einfach als Nebenprodukt ohne große Investitionskosten anfallen, geringer ausfallen wie

Verbot der Datenweitergabe an Gatekeeper:

Die Beschränkung des Zugriffs von Gatekeepern – also voraussichtlich u.a. Google, Meta, Apple –, zu den bei der Nutzung von vernetzten Produkten erzeugten Daten, um ihnen die Entwicklung weiterer Geschäftsmodelle auf Basis von IoT-Daten zu erschweren und insbesondere kleinen und mittelgroßen Unternehmen auf den Anschlussmärkten den Markteintritt zu erleichtern und ihnen eine Chance auf diesen Märkten zu geben, ist fragwürdig. Die dahinterstehende Intention der Kommission zu verhindern, dass Gatekeeper auch auf dem Markt für IoT-Daten Datenmonopole errichten können, ist zwar politisch nachvollziehbar. Die Beschränkung hat jedoch mehrere Defizite. Erstens schafft sie durch die Ungleichbehandlung potenzieller Datenempfänger Wettbewerbsverzerrungen zulasten der Gatekeeper. Zweitens limitiert sie damit künstlich das Angebot an Dienstleistungen auf den Anschlussdiensten für den Nutzer, sodass die Dienstleistungsvielfalt sinkt. Drittens ist auch fraglich, ob die Beschränkung tatsächlich ihre intendierte Wirkung entfaltet. Denn interessanterweise ist es zwar Nutzern verboten, vom Dateninhaber zu verlangen, Daten an Gatekeeper weiterzureichen. Dies schließt jedoch nicht aus, dass der Dateninhaber seinerseits (nicht-personenbezogene) Daten an Gatekeeper übermittelt, ohne dass ein solches explizites Nutzerverlangen vorliegt. Dies könnte die Intention der avisierten Beschränkung für Gatekeeper konterkarieren.

In diesem Zusammenhang ist ferner zu bedenken, dass die Kommission sich zwar anscheinend zum Ziel gesetzt hat, die datengetriebene Marktstellung von Gatekeepern im IoT-Markt nicht weiter – über ein (un)freiwilliges Mitwirken der Nutzer – fördern zu wollen, sie es aber dennoch implizit zulassen will, dass sich, abseits der Gatekeeper, auf den Anschlussmärkten Diensteanbieter etablieren können, die über exklusive Datennutzungsmöglichkeiten verfügen (Nutzer dürfen Dritten exklusive Nutzungsrechte einräumen). Das ist inkonsistent.

Gegenleistung für die Datenweitergabe:

Mit der Vorgabe, wonach Dateninhaber für die Datenweitergabe an Datenempfänger eine „angemessene" Gegenleistung erhalten dürfen und, dass diese bei KMU als Datenempfänger nicht über die Kosten hinausgehen darf, die mit der Bereitstellung der Daten unmittelbar einhergehen, soll verhindert werden, dass der Datenaustausch mit Dritten direkt an übermäßig hohen Vergütungen scheitert; gleichzeitig soll die geringere Verhandlungsmacht von KMU bei Datennutzungsvereinbarungen kompensiert werden. Die angestrebte Preisregulierung ist jedoch aus mehrerlei Hinsicht fragwürdig. Erstens sollte es in einer sozialen Marktwirtschaft in erster Linie Sache der Vertragsparteien sein, sich über etwaige Datenaustauschkonditionen zu einigen. Nur wenn der Dateninhaber hier bspw. über eine unangreifbare Marktmacht verfügt, wären staatliche Eingriffe erstrebenswert. Zweitens ist weitgehend unklar, was unter einer „angemessenen" Kompensation für die Datenbereitstellung bei der Datenweitergabe an große Datenempfänger zu verstehen ist, nicht zuletzt da die Bestimmung des Werts von Daten alles andere als trivial ist [s. dazu auch cep**Study**, S. 39-41). Sollte an der Vorgabe festgehalten werden, sollten, zur Förderung der Rechtsklarheit, zumindest grobe Leitlinien vorgegeben werden. Drittens birgt die preisgesteuerte Förderung von KMU, die nicht sicherstellt, dass der Dateninhaber die vollen Kosten erstattet bekommt, die Gefahr, dass die Datenweitergabe letztlich gänzlich unterbleibt, da die Anreize des Dateninhaber vernetzte Produkte bereitzustellen, sinken. Diese Gefahr besteht umso eher, wenn er sich mit einer Vielzahl von KMU als mögliche Datenempfänger konfrontiert sieht. Viertens weisen die Vorgaben eine gewisse Inkonsistenz auf, indem sie von der Grundannahme ausgehen, dass der Dateninhaber in jedem Fall die stärkere Verhandlungsposition innehat. Wieso jedoch ein mittelgroßes Unternehmen als Datenempfänger gegenüber einem Dateninhaber, der ggf. ein Kleinstunternehmen ist, einer spezifischen Schutzregelung bedarf, ist jedenfalls nicht ersichtlich und sollte daher korrigiert werden[19].

„Faire" Datennutzungsverträge:

Nach dem Data Act sollen KMU durch einige Regelungen vor „unfairen" Vertragsbedingungen geschützt werden, wenn sie Daten von Vertragspartnern nutzen wollen, die eine stärkere Verhandlungsposition innehaben. Damit sollen letztlich zwei Ziele erreicht werden. Einerseits sollen strukturelle Ungleichgewichte zwischen den Vertragsparteien ausgeglichen und andererseits die Teilnahme von KMU auf den Anschlussmärkten von vernetzten Produkten unterstützt werden. Die vorgeschlagenen Maßnahmen sind jedoch ein Eingriff in die Vertragsfreiheit und bedürfen daher einer hinreichenden Rechtfertigung. Denn wie auch die Datenethikkommission zutreffend analysiert, sorgen auf der Privatautonomie der beteiligten Akteure basierende Datennutzungsverträge in der Regel

---

etwa in „infrastrukturbasierten Sektoren […] wie etwa im Telekommunikationssektor" [Haucap, J. (2020). Plattformökonomie: Neue Wettbewerbsregeln—Renaissance der Missbrauchsaufsicht. Wirtschaftsdienst, 100(1), 20-29].

[19] s. zu diesem Aspekt auch Weizenbaum Institute for the Networked Society, Position Paper regarding Data Act, May 2022.

für „Fairness“, eine effiziente Ressourcenallokation und eine Steigerung der allgemeinen Wohlfahrt. Allenfalls bei Vorliegen eines Marktversagens sollte daher von der freien Verhandlung von Verträgen abgewichen werden können.[20] Die Kommission geht nun implizit davon aus, dass immer dann, wenn KMU Datenzugang begehren, ein solches Marktversagen gegeben ist. Das ist jedoch nicht der Fall. Zwar sind regelmäßig Situationen denkbar, bei denen KMU aufgrund einer eingeschränkten Verhandlungsmacht nicht oder nur schwer in der Lage sind, Vertragskonditionen aktiv mitzugestalten und der „stärkere“ Vertragspartner ihnen daher im Sinne eines Take-it-or-Leave-Diktums Konditionen quasi aufzwingen kann, was in der Folge Eintritte dieser KMU etwa im Bereich der Anschlussmärkte ausbremst und die Entwicklung von datengetriebenen Sekundärdiensten schadet. Eine ungleiche Verhandlungsposition wohnt jedoch quasi jedem Vertragsverhältnis inne und ist per se noch kein adressierungswürdiges Marktversagen. Die Kommission macht es sich hier zu einfach. Denn es spielt etwa keine Rolle, ob und in welchem Maße ein Datennachfrager auch auf andere Vertragspartner zur Bereitstellung gleicher oder ähnlicher Daten zurückgreifen kann („Substituierbarkeit“). Ist eine solche Substituierbarkeit jedoch gegeben, schmälert dies die Verhandlungsmacht des datenbereitstellenden Unternehmens, auch gegenüber KMU, und reduziert damit die Schutzwürdigkeit des Datennachfragers. Damit sind jedoch dann auch konkrete Fairnessregeln unnötig. Solche Fairnessregeln können demgegenüber dann eher angemessen sein, wenn das datennachfragende Unternehmen de facto nicht auf alternative Datenbereitsteller zurückgreifen kann. Zweitens ist die Fokussierung auf KMU als potenziell schwächere Vertragsparteien nicht zielgenau. Denn es ist nicht zwingend (allein) die Größe eines Unternehmens, die über die Verhandlungsmacht bestimmt.[21] Auch andere Aspekte, wie etwa die Existenz weiterer „Datenlieferanten“ oder die Höhe der Barriere für den Eintritt in den Markt des Datenbereitstellers können entscheidend sein. Fraglich ist ferner, warum die Fairnessregeln auch greifen sollen, wenn das datenbereitstellende Unternehmen ein kleines Unternehmen ist und dasjenige, welches Datenzugang begehrt, ein mittelgroßes Unternehmen. Dann müsste – nach der vorgebrachten Logik der Kommission – von einer umgekehrten Verteilung der Verhandlungsmacht ausgegangen werden. Dies gilt es zu korrigieren.

[20] Datenethikkommission, (2019). Gutachten der Datenethikkommission, S. 145.

[21] Siehe dazu auch Drexl et al. (2022), Rn. 125: Die Autor*innen weisen darauf hin, dass „ein Ungleichgewicht der Verhandlungsmacht“ […] „nicht von der Größe des Unternehmens abhängt, sondern […] vom Grad der Datenabhängigkeit“.

2 Juristische Bewertung

2.1 Kompetenz

Die Bestimmungen des Data Act zur Verbesserung des Zugangs zu Daten, die bei der Nutzung vernetzter Produkte und verbundener Dienste erzeugt werden, können auf die Kompetenz zur Harmonisierung des Binnenmarkts [Art. 114 AEUV] gestützt werden.[22] Dieser erlaubt – selbst wenn die Mitgliedstaaten bislang noch keine einschlägigen Regeln erlassen haben – auch präventive Harmonisierungsmaßnahmen. Voraussetzung ist aber, dass bei heterogener Entwicklung der nationalen Rechtsvorschriften wahrscheinlich neue Handelshindernisse entstehen und dass der Data Act deren Vermeidung bezweckt.[23] Der Data Act will Zugriffsrechte auf IoT-Daten festlegen und einen harmonisierten Rahmen für den Zugang und die Nutzung solcher Daten schaffen und so Hindernisse für einen gut funktionierenden Binnenmarkt für Daten beseitigen.[24] Zudem regelt er durch die Access-by-Design-Pflicht auch Anforderungen an vernetzte Produkte und beugt so Handelshindernissen innerhalb des EU-Binnenmarktes vor, die aus abweichenden nationalen Anforderungen an solche Produkte resultieren könnten. Aufgrund der zunehmenden Bedeutung des Datenaustauschs und der verbesserten Datennutzung in der digitalen Wirtschaft ist es wahrscheinlich, dass die Mitgliedstaaten unterschiedliche nationale Regelungen erlassen werden, um den Zugang zu Daten einschließlich IoT-Daten zu fördern. So hat etwa die deutsche Bundesregierung 2021 in ihrem Koalitionsvertrag[25] ein „Datengesetz" angekündigt, um den Zugang zu Daten für alle an ihrer Entstehung Beteiligten zu stärken. Andere Mitgliedstaaten haben bereits Regelungen zur Verbesserung der Datennutzung im B2G-Bereich erlassen.[26] Zudem laufen in einigen Mitgliedstaaten seit Jahren nicht-legislative Initiativen für die gemeinsame Datennutzung[27] wie etwa die Dutch Data Sharing Coalition[28] oder das Smart Data Technologie-Förderprogramm des BMWi aus dem Jahr 2017[29], denen eine Regulierung auch im B2B-Bereich nachfolgen könnte.

2.2 Subsidiarität

Unproblematisch. Generierung, Zugang und Nutzung von Daten erfolgen immer stärker grenzüberschreitend; vernetzte Produkte werden EU-weit gehandelt. Die Hindernisse für den Datenzugang und die verstärkte Datennutzung, die der Data Act beseitigen will, bestehen auf dem gesamten Binnenmarkt. Unterschiedliche nationale Regeln beseitigen die bestehende Rechtsunsicherheit nicht und könnten es zudem der Partei mit der stärksten Verhandlungsmacht ermöglichen, das anwendbare nationale Recht mit dem niedrigsten Schutzniveau zu wählen.[30] Regeln für den Datenzugang und die Datennutzung und Anforderungen an vernetzte Produkte können daher besser auf EU-Ebene verankert werden. Zudem ermöglicht nur eine Lösung auf EU-Ebene eine einheitliche Abstimmung mit den anderen für den Datenaustausch im Binnenmarkt relevanten EU-Rechtsakten, die mit dem Data Act zusammenspielen [u.a. DSGVO, E-Privacy-Richtlinie, Data Governance Act und Datenbankrichtlinie].

Die Wahl des Rechtsinstruments der Verordnung ist sachgerecht. Um IoT-Daten besser nutzbar zu machen, ist eine weitestmögliche Harmonisierung der Datenzugangs- und Datennutzungsrechte durch einheitliche und unmittelbar anwendbare Regeln sinnvoll. Diese sind auch angesichts der Komplexität der Materie und im Interesse einer zeitnahen Anwendbarkeit der neuen Vorschriften gegenüber einer umsetzungsbedürftigen Richtlinie vorzugswürdig; ferner können sie die einheitliche und effektive behördliche Durchsetzung erleichtern.[31]

---

22 Soweit der Data Act Art. 20 DSGVO erweitert, wäre eigentlich auch die EU-Kompetenz für Datenschutz und freien Datenverkehr [Art. 16 AEUV] als Rechtsgrundlage einschlägig. Da es sich hierbei nur um einen untergeordneten Regelungsteil handelt, kann Art. 16 nach der Schwerpunkttheorie des EuGH […] gegenüber Art. 114 AEUV vernachlässigt werden, zumal bei beiden Kompetenznormen das ordentliche Gesetzgebungsverfahren gilt.

23 EuGH, Rs. C-376/98 (Deutschland/Parlament und Rat), ECLI:EU:C:2000:544, Rn. 86.

24 Erwägungsgrund 5 sowie S. 1, 8 Data Act.

25 Koalitionsvertrag 2021 – 2025 zwischen der Sozialdemokratischen Partei Deutschlands (SPD), BÜNDNIS 90 / DIE GRÜNEN und den den Freien Demokraten (FDP), Mehr Fortschritt wagen – Bündnis für Freiheit, Gerechtigkeit und Nachhaltigkeit, S. 17, https://www.bundesregierung.de/resource/blob/974430/1990812/04221173eef9a6720059cc353d759a2b/2021-12-10-koav2021-data.pdf?download=1: „Für alle, die an der Entstehung von Daten mitgewirkt haben, stärken wir den standardisierten und maschinenlesbaren Zugang zu selbsterzeugten Daten. Mit einem Datengesetz schaffen wir für diese Maßnahmen die notwendigen rechtlichen Grundlagen:"

26 European Commission, Impact Assessment Report zum Data Act, SWD(2022) 34 final, S. 25 unter Verweis auf https://datasharingcoalition.eu.

27 European Commission, Impact Assessment Report zum Data Act, a.a.O., S. 25.

28 European Commission, Impact Assessment Report, a.a.O., S. 25 unter Verweis auf https://datasharingcoalition.eu.

29 https://www.bmwk.de/Redaktion/DE/Artikel/Digitale-Welt/smart-data.html.

30 Sog. „forum shopping"; vgl. auch Deutscher Bundesrat, Beschluss vom 10.06.2022, Drucks. 130/22, Rn. 2 (S. 2); Kommissionsvorschlag zum Data Act, S. 9.

31 Im Hinblick auf eine effektive Durchsetzung ist der Data Act allerdings noch verbesserungswürdig, vgl. unten Ziffer 2.3.

2.3 Verhältnismäßigkeit gegenüber den Mitgliedstaaten

Die Regelungen in Kapitel II zur Verbesserung des Datenzugangs B2C und B2B beschränken den legislativen Gestaltungsspielraum der Mitgliedstaaten, Datenteilungspflichten in Bezug auf IoT-Daten selbständig und ggf. abweichend zu regeln. Zudem knüpfen sie die Ausübung der Datenzugangs- und Nutzungsrechte an den Abschluss privatrechtlicher Verträge zwischen Dateninhabern, Nutzern und Dritten. Die Grundregeln für die Erfüllung gesetzlicher Datenteilungspflichten in Kapitel III und die Regeln über missbräuchliche Vertragsklauseln in Datennutzungsverträgen in Kapitel IV greifen in das nationale Vertragsrecht ein. Kapitel III unterwirft die Ausgestaltung bestimmter Datennutzungsverträge zwischen Dateninhabern und -empfängern sogenannten FRAND-Bedingungen. Kapitel IV erklärt missbräuchliche Klauseln in Verträgen mit KMU für nicht bindend, wobei die Missbräuchlichkeit durch Auslegung des Data Act – und nicht anhand des nationalen Rechts – festzustellen ist. Weil der Data Act offenbar vollharmonisierende Wirkung haben soll[32], dürfen die Mitgliedstaaten in seinem Anwendungsbereich keine zusätzlichen nationalen Anforderungen mehr regeln oder aufrechterhalten. Insbesondere können sie abweichende – auch strengere – nationale Klauselverbotskataloge und Generalklauseln im B2B-Bereich nicht mehr ohne weiteres anwenden. Dies gilt z.B. für nationales AGB-Recht, soweit es Vertragsklauseln in Bezug auf Datenzugang, Datennutzung, Haftung oder Rechtsbehelfe bei Verletzung oder Beendigung datenbezogener Pflichten betrifft und auch KMU und Kleinstunternehmen schützt.[33] Die Rechtslage würde sich dann insoweit von derjenigen bei der EU-Klauselrichtlinie unterscheiden, die für AGB gegenüber Verbrauchern gilt.[34] Unter dieser bleibt das nationale AGB-Recht formal anwendbar, insbesondere die nationale Klauselverbotskataloge. Denn die im Anhang der Klauselrichtlinie aufgeführte Liste von Klauseln mit missbräuchlichen Zielen und Folgen enthält nur Beispiele für missbräuchliche Klauseln[35]; zudem sieht die Richtlinie nur eine Mindestharmonisierung vor.[36]

Zugunsten einer Vollharmonisierung durch den Data Act lässt sich anführen, dass eine Beschränkung auf eine Mindestharmonisierung auch im B2B-Bereich, die es den Mitgliedstaaten ermöglichen würde, strengere Regeln zu erlassen oder beizubehalten, dem Ziel zuwiderliefe, einheitliche Regeln für Datenaustauschverträge zu schaffen. Zudem ist der Eingriff in das nationale Vertragsrecht dadurch in seiner Wirkung begrenzt, dass die Klauselkontrolle in Kapitel IV auf bestimmte – oben dargelegte – Klauselinhalte beschränkt ist. Dass die Generalklausel des Data Act aber offenbar völlig autonom unter bloßer Heranziehung der Klauseln der schwarzen und grauen Liste ausgelegt werden soll[37], die zudem nur wenige datenbezogene Regelungen enthalten, ist jedoch zu unbestimmt und daher unverhältnismäßig. Entspricht die zu prüfende Klausel im konkreten Fall keiner der gelisteten Klauseln, bliebe ihre Bewertung anhand der Generalklausel des Data Act völlig offen. Ein möglicher Rückgriff auf das europäische Vertragsrecht als hilfsweisem Beurteilungsmaßstab scheidet aus, da dieses nicht hinreichend harmonisiert ist. Um Schutzlücken zu vermeiden, muss der Data Act daher einen Referenzmaßstab für die Beurteilung festlegen und z.B. klarstellen, dass mitgliedstaatliche Gerichte auf das geltende nationale Vertragsrecht zurückgreifen dürfen, so wie es die Rechtsprechung des EuGH bei der EU-Klauselrichtlinie erlaubt.[38] Zudem sollte der EU-Gesetzgeber bedenken, dass es erstens zu Abgrenzungsschwierigkeiten und zweitens innerhalb eines Vertrags zu unterschiedlichen Wertungen kommen kann, wenn ein Teil der Klauseln dem Data Act unterfällt und die übrigen Klauseln nach nationalem Recht zu beurteilen sind.

Die Regeln zur Durchsetzung des Data Act sind noch unzureichend. Der Data Act sieht eine behördliche Durchsetzung seiner Regeln durch die Mitgliedstaaten vor. Die Verpflichtung, behördliche Strukturen für die Durchsetzung des Data Act einzurichten, greift in die Befugnis der Mitgliedstaaten ein, die Durchsetzung des EU-Rechts eigenständig zu organisieren. Sie ist gerechtfertigt, soweit die Regeln des Data Act durch Behörden besser und effektiver durchgesetzt werden können als (rein) privatrechtlich durch Zivilgerichte und Streitbeilegungsstellen. Die Gewährung der Datenzugangs- und Nutzungsrechte im Data Act wird jedoch durch zahlreiche vertragsrechtliche Regelungen flankiert. Daher kann es zu einem bislang unabgestimmten Nebeneinander von behördlicher

---

32 Vgl. Erwägungsgrund 4.

33 So etwa die §§ 305 ff. des deutschen Bürgerlichen Gesetzbuchs (BGB). In diesen Fällen wäre zu prüfen, inwieweit sich der Fall zumindest unter die Generalklausel des Art. 3 Abs. 2 Data Act subsumieren lässt.

34 Richtlinie 93/13/EWG vom 5. April 1993 über missbräuchliche Klauseln in Verbraucherverträgen, abrufbar unter https://eur-lex.europa.eu/legal-content/DE/ALL/?uri=CELEX%3A31993L0013.

35 EuGH, Urteil vom 14. März 2013, Rs. C-415/11 – Aziz, ECLI:EU:C:2013:164, Rn. 70 m.w.N. Laut Art. 3 Abs. 3 der EU-Klauselrichtlinie 93/13/EWG enthält der Anhang eine „als Hinweis dienende und nicht erschöpfende Liste der Klauseln, die für missbräuchlich erklärt werden können". Vgl. auch Leitlinien der EU-Kommission zur Auslegung und Anwendung der Richtlinie 93/13/EWG, ABl. (EU) Nr. C-323 vom 27.09.2019, S. 4ff., Ziffer 3.4.7.

36 Vgl. Art. 8 der EU-Klauselrichtlinie.

37 Erwägungsgrund 55.

38 EuGH, Urteil vom 14. März 2013, Rs. C-415/11 – Aziz, ECLI:EU:C:2013:164, Rn. 68.

Sanktionierung mit teils hohen Geldbußen und privatrechtlicher Durchsetzung kommen.[39] Soweit zusätzlich zu den mitgliedstaatlichen Gerichten die vorgeschlagenen privaten Streitbeilegungsstellen zuständig sind[40], bestehen damit sogar drei Durchsetzungsmöglichkeiten[41], die jeweils zu abweichenden Wertungen und damit Entscheidungen führen können. Sowohl Behörden als auch Gerichte müssen etwa die Generalklausel des Art. 13 Abs. 2 auslegen und darüber befinden, ob die Verwendung einer Klausel noch mit Treu und Glauben und der guten Geschäftspraxis zu vereinbaren ist. Schließt der Nutzer, der Zugang zu Daten begehrt, oder ein Dritter aufgrund des Data Act mit dem Dateninhaber einen Vertrag, können neben gesetzlichen Ansprüchen aus dem Data Act ggf. auch vertragsrechtliche Ansprüche aus diesen Verträgen bestehen. Dennoch lässt der Data Act das Verhältnis zur privatrechtlichen Durchsetzung offen. Ob die behördliche Durchsetzung bei allen Bestimmungen des Data Act erforderlich ist bzw. einen Mehrwert verspricht[42], sollte im weiteren Gesetzgebungsverfahren noch genauer geprüft werden. Zudem bedarf es einer näheren Abstimmung zwischen behördlicher und privater Durchsetzung.

Zudem ist bislang zu ungenau geregelt, welche nationale Behörde in welchen Fällen für die Durchsetzung der Regeln des Data Act zuständig ist. Der Data Act teilt die Zuständigkeit zwischen den Datenschutzaufsichtsbehörden (DPA), sektorspezifischen „Fachbehörden“ und den sonstigen von den Mitgliedstaaten zu benennenden Behörden auf. So sollen die DPAs „bezüglich des Schutzes personenbezogener Daten“ und die Fachbehörden „bei besonderen sektoralen Problemen des Datenaustauschs“ für die Durchsetzung zuständig sein. Diese Zuständigkeitszuweisungen sind unpräzise und müssen dringend konkretisiert werden[43], damit es nicht zu einem Zuständigkeitschaos und zu Überschneidungen kommt. Geklärt werden sollte auch, welche Behörde(n) welchen Mitgliedstaats bei grenzüberschreitenden Fällen zuständig ist/sind.[44] Abstimmungserfordernisse und -probleme zwischen den unterschiedlichen zuständigen Behörden können die Effektivität der Durchsetzung gefährden.

Zudem besteht aufgrund des weiten Regelungsbereichs des Data Act und der vielen verbliebenen Unklarheiten und Wertungsfragen bei seiner Anwendung[45] die Gefahr, dass es zu einer hohen Zahl an Beschwerden und sonstigen Rechtsstreitigkeiten kommen wird, welche Behörden und Gerichte überlasten könnten.[46] Die Einrichtung von Streitbeilegungsstellen[47] kann zeitnahe Entscheidungen ermöglichen, ob Vertragsbedingungen fair, angemessen und nichtdiskriminierend sind, und Gerichte entlasten. Sie ist daher im Allgemeininteresse sowie im Interesse der beteiligten Parteien sinnvoll. Dass der Data Act die Mitgliedstaaten verpflichtet, Streitbeilegungsstellen zu zertifizieren, ist daher sachgerecht. Deren Kompetenz sollte aber nicht auf Streitigkeiten über Transparenz und FRAND-Charakter der Vertragsbedingungen limitiert sein, sondern auch auf andere Streitigkeiten im Zusammenhang mit der Bereitstellung der Daten ausgeweitet werden[48], da sonst ggf. separate Verfahren angestrengt werden müssen. Zudem muss die Durchsetzbarkeit ihrer Entscheidungen sichergestellt werden.

---

39 Drexl et al., a.a.O., fordern insoweit eine Klarstellung im Data Act, dass die privatrechtliche Durchsetzung durch den Data Act vor den zuständigen Gerichten nicht eingeschränkt wird (Rn. 240 ff, 248).

40 Dies ist bei Streitigkeiten in Bezug auf die FRAND-Bedingungen (Kapitel III) der Fall.

41 Drexl et al., Rn. 253, halten dies für zu ausufernd und unnötig und halten daher bei bestimmten Vorschriften des Data Act –u.a. bei Kap. IV – eine ausschließlich privatrechtliche Durchsetzung für vorzugswürdig (Rn. 251f.).

42 Kritisch insoweit Drexl et al., Rn. 250, die für einen Ausschluss der behördlichen Vollstreckung plädieren, soweit die privatrechtliche Vollstreckung klar überlegen sei, was etwa bei der Fairnesskontrolle von Vertragsklauseln in B2B-Verhältnissen nach Kapitel IV der Fall sei.

43 Fraglich ist daher insbesondere, wann die DPA zuständig sind und welche Vorschriften des Data Act sie durchsetzen dürfen. Dürfen sie etwa nur Datenschutz im engeren Sinn durchsetzen und z.B. vorgehen, wenn Daten ohne datenschutzrechtliche Rechtsgrundlage ausgetauscht werden, oder müssen sie auch Datenzugangsansprüche zu personenbezogenen Daten durchsetzen, die Art. 20 DSGVO ergänzen? Ebenso muss geklärt werden, wann ein „besonderes sektorales Problem des Datenaustauschs“ vorliegt.

44 Siehe auch Drexl et al., Rn 247.

45 Vgl. etwa Ökonomische Bewertung S. 13f.

46 So bezüglich der Überforderung der Behörden auch Podszun, R./Pfeifer, C., Datenzugang nach dem EU Data Act: Der Entwurf der Europäischen Kommission, GRUR 2022, S. 953 ((961).

47 Art. 10 Data Act (vgl. oben A.3).

48 So z.B. die Frage, welche Daten bereitzustellen sind, vgl. Graef, I./Husovec, M., Seven Things to Improve in the Data Act, 07.03.2022, Ziff. 5, abrufbar unter https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4051793. Für die Ausweitung der Kompetenzen der Streitbeistellungsstellen auch Drexl et a., Rn. 108. Auch Gerpott, CR 2022, S. 271(279) hält die Beschränkung der Klärungskompetenz auf FRAND-Bedingungen für nicht nachvollziehbar. Kritisch zum Streitbeilegungsmechanismus auch Kerber, W., Governance of IoT Data: Why the EU Data Act will not fulfill its objectives, 08.05.2022, S. 12, abrufbar unter https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4080436.

2.4 Sonstige Vereinbarkeit mit EU-Recht

1. Einführung

IoT-Daten werden in komplexen Prozessen generiert, an denen mehrere Akteure mit individuellen Interessen beteiligt sind, die in unterschiedlichem Umfang zur Datenerzeugung beitragen.[49] Bei der Festlegung gesetzlicher Datenzugangs- und Nutzungsrechte und der inhaltlichen Regulierung der zu ihrer Ausübung abzuschließenden Verträge müssen die grundrechtlich geschützten Rechtspositionen erstens der Dateninhaber und zweitens der Nutzer und Dritten berücksichtigt werden, die Zugang zu den Daten begehren oder deren Daten betroffen sind. Drittens müssen die Grundrechte sonstiger Dritter wie das Recht auf Privatsphäre und auf den Schutz personenbezogener Daten berücksichtigt und alle Grundrechte in einen angemessenen Ausgleich gebracht werden.[50] Die im Data Act geregelten Pflichten für Dateninhaber, Hersteller, Nutzer und Dritte greifen in die Grundrechte der genannten Akteure ein, insbesondere in ihre unternehmerische Freiheit, einschließlich ihrer Vertragsfreiheit [Art. 16 GRCh], und ggf. ihr Recht auf Schutz ihres geistigen Eigentums [Art. 17 Abs. 2 GRCh].[51] Diese Grundrechte gelten jedoch nicht unbeschränkt: die o.g. Eingriffe sind EU-rechtlich gerechtfertigt, wenn der Data Act damit erstens ein legitimes Ziel verfolgt – hierzu muss die jeweilige Pflicht entweder einem von der EU anerkannten Interesse des Gemeinwohls oder dem Schutz kollidierender Grundrechte und Freiheiten anderer dienen – und die Pflicht zweitens hinreichend bestimmt und drittens verhältnismäßig, d.h. zur Erreichung des Ziels geeignet, erforderlich und angemessen ist [Art. 52 Abs. 1 GRCh].

Im Rahmen der Verhältnismäßigkeitsprüfung müssen die einzelnen widerstreitenden Rechtspositionen gegeneinander abgewogen werden.[52] Dabei sind neben der Frage, wie stark die eingreifende Pflicht anerkannten Gemeinwohlinteressen dient, unter anderem die Schwere des Eingriffs, das Gewicht der individuellen Interessen der beteiligten Akteure sowie der Umfang zu berücksichtigen, in dem diese zur Generierung der Daten beigetragen haben. Ferner ist zu prüfen, ob Ausgleichsmöglichkeiten wie Schutzmaßnahmen oder eine Vergütung den Eingriff abmildern. Schließlich spielt auch die Machtverteilung zwischen dem Dateninhaber und dem Nutzer oder Dritten eine Rolle.[53] All diese Faktoren stehen miteinander in einer Wechselwirkung. Daher kann ein starkes Interesse eines Akteurs am Datenzugang einen nur schwachen Beitrag desselben Akteurs zur Datengenerierung ausgleichen.[54] Auch lässt sich ein Datenzugangsanspruch umso eher rechtfertigen, je stärker er den genannten Gemeinwohlinteressen dient.[55] Ausgehend von diesem Prüfschema werden nachfolgend die wesentlichen grundrechtsrelevanten Pflichten des Data Act einer Rechtfertigungsprüfung unterzogen.

2. Datenbereitstellungspflichten an Nutzer und Dritte nach Art. 4 und 5 Data Act

Die Datenbereitstellungspflichten in Art. 4 und 5 Data Act greifen in die grundrechtlich geschützten Rechte der Dateninhaber auf Schutz ihrer unternehmerischen Freiheit [Art. 16 GRCh] und ggf. ihres geistigen Eigentums [Art. 17 Abs. 2 GRCh] ein. Die unternehmerische Freiheit schützt jegliche Art und Weise des Betriebs und umfasst insbesondere das Recht eines Unternehmens, frei über seine wirtschaftlichen, technischen und finanziellen

---

49 Allgemein – d.h. nicht auf IoT-Daten beschränkt – Gutachten der Datenethikkommission der deutschen Bundesregierung, Oktober 2019, S. 85, abrufbar unter https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/it-digitalpolitik/gutachten-datenethikkommission.pdf;jsessionid=2032194AE8CDE254DACD6FE603B6F9FB.1_cid295?__blob=publicationFile&v=6.

50 EuGH, Urteil vom 22.01.2013, Rs. C-283/11 - Sky Österreich, ECLI:EU:C:2013:28, Rn. 60; Jarass, Charta der Grundrechte der EU, 4. Aufl. 2021, Art. 52 Rn. 43. Vgl. auch, allerdings bezogen auf Datenzugangsrechte für Wissenschaft und Forschung, Specht-Riemenschneider, L., Studie zur Regulierung eines privilegierten Zugangs zu Daten für Wissenschaft und Forschung durch die regulatorische Verankerung von Forschungsklauseln in den Sektoren Gesundheit, Online-Wirtschaft, Energie und Mobilität im Auftrag des Bundesministeriums für Bildung und Forschung, S. 5, 21 143, abrufbar unter https://www.jura.uni-bonn.de/fileadmin/Fachbereich_Rechtswissenschaft/Einrichtungen/Lehrstuehle/Specht/Dateien/2021-08-25-LSR.pdf., S. 5, 21; siehe auch Specht-Riemenschneider, L., Stellungnahme zum Thema „Datenstrategie der Bundesregierung“ (BT-Drs. 19/26450) et al., Deutscher Bundestag, Ausschussdrucksache 19(23)109 vom 21.02.2021, S. 8, abrufbar unter https://www.bundestag.de/resource/blob/823800/6f11b79c8288a181eaec827c4361825b/Stellungnahme-Specht-Riemenschneider-data.pdf.

51 Siehe auch Bertschek, I./Bonin, H./Kühling, J./Thüsing, G./Wenzel, T., Entwicklung eines Konzepts zur Datenallmende, Forschungsbericht Nr. 581, Expertise im Auftrag des deutschen Bundesministeriums für Arbeit und Soziales, Juli 2021, S. 62, abrufbar unter https://ftp.zew.de/pub/zew-docs/gutachten/Kurzexpertise-Entwicklung-Konzept-zur-Datenallmende_2021.pdf.

52 Jarass, a.a.O., Rn. 43.

53 Gutachten der Datenethikkommission der deutschen Bundesregierung, a.a.O., S. 85f.

54 Gutachten der Datenethikkommission der deutschen Bundesregierung, a.a.O., S. 86.

55 Vgl., allerdings bezogen auf Datenzugangsrechte für Wissenschaft und Forschung – Specht-Riemenschneider, L., Studie zur Regulierung eines privilegierten Zugangs zu Daten für Wissenschaft und Forschung durch die regulatorische Verankerung von Forschungsklauseln in den Sektoren Gesundheit, Online-Wirtschaft, Energie und Mobilität im Auftrag des Bundesministeriums für Bildung und Forschung, S. 143, abrufbar unter https://www.jura.uni-bonn.de/fileadmin/Fachbereich_Rechtswissenschaft/Einrichtungen/Lehrstuehle/Specht/Dateien/2021-08-25-LSR.pdf.

Ressourcen zu verfügen.[56] Zu den Ressourcen des Dateninhabers lassen sich grundsätzlich auch die von ihm in rechtmäßiger Weise kontrollierten Daten zählen, auch wenn er diese Kontrolle nicht aus einer Rechtsposition heraus, sondern nur de facto innehat. Art. 16 GrCh stützt sich auch auf Artikel 119 Abs. 1 und 3 AEUV[57], der den freien Wettbewerb anerkennt und ihn als objektiv-rechtliches Prinzip der EU hervorhebt.[58] Diese Grundrechte gelten jedoch nicht schrankenlos.[59]

2.1 Unklarer Inhalt der Bereitstellungspflicht

Gemäß dem im EU-Recht anerkannten Grundsatz der Rechtsstaatlichkeit und Rechtssicherheit sowie dem Erfordernis einer gesetzlichen Grundlage in Art. 52 GrCh müssen Rechtsakte, die Grundrechte einschränken, hinreichend klar und bestimmt sein, damit der Betroffene die Folgen voraussehen und sich darauf einstellen kann.[60] Die Pflicht des Dateninhabers, Daten bereitstellen zu müssen, ist jedoch in ihrer derzeitigen Form zu vage und verstößt gegen das Bestimmtheitsgebot. Der Data Act lässt offen, wie die Bereitstellung von Daten im Einzelnen zu erfolgen hat. Hintergrund hierfür ist vermutlich, dass es sich um eine horizontale Regelung handelt, die möglichst einer Vielzahl unterschiedlicher Fälle gerecht werden will. Sie eröffnet den Dateninhabern einerseits viel Spielraum, da sowohl eine Bereitstellung der Daten „in situ“ - d.h. in der Sphäre des Dateninhabers, z.B. auf dem Gerät selbst bzw. auf dessen Server[61] – als auch eine Portierung und damit Übertragung der Daten in die Sphäre des Nutzers bzw. Dritten wie bei Art. 20 DSGVO[62] in Betracht kommt. Während ein Verbleib der Daten in der eigenen Sphäre den Dateninhabern eine bessere Kontrolle und damit einen besseren Schutz ermöglicht, kann ein solcher Zugriff für Nutzer und Dritte weniger attraktiv sein. Denn diese können die Daten in der fremden Umgebung ggf. nicht mit eigenen Datensätzen kombinieren[63] und somit nur eingeschränkt nutzen. Bleibt der Umfang der Pflicht derart unklar, können sich Dateninhaber und Nutzer bzw. Dritte aber nicht darauf einstellen. Dies schafft Rechtsunsicherheit, die zu Rechtsstreitigkeiten führen kann. Das Ziel des Data Act, Rechtssicherheit bei der gemeinsamen Nutzung von Daten zu erhöhen, würde so verfehlt.[64] Es muss daher spezifiziert werden, wie bzw. wo die Daten bereitzustellen sind. Statt einer zu unbestimmten horizontalen Bereitstellungspflicht könnte der Data Act hinsichtlich der Art und Weise der Bereitstellung zum einen danach differenzieren, an wen (Verbraucher oder gewerbliche Nutzer oder Dritte) die Daten bereitzustellen sind. Zum anderen könnte der EU-Gesetzgeber die Art und Weise der Bereitstellung in spezielleren Regelungen besser an Besonderheiten unterschiedlicher Datentypen und Sektoren anpassen (z.B. Zugriffe auf Geschäftsgeheimnisse oder Gesundheitsdaten grundsätzlich nur „in situ“ oder in der geschützten Umgebung eines Datenraums oder Datentreuhänders erlauben).

2.2 Verhältnismäßigkeit

2.2.1 Kein milderes Mittel

Die im Data Act geregelten Datenzugangs- und Nutzungsrechte wären nicht erforderlich, wenn das bestehende EU-Wettbewerbsrecht ausreichen würde oder eine Anpassung des Wettbewerbsrechts als „milderes Mittel“ in Betracht käme, um den Zugang zu IoT-Daten und deren Nutzung zu fördern und faire Datennutzungsverträge zu gewährleisten. Ansprüche nach bestehendem EU-Wettbewerbsrecht einschließlich der sog. „Essential-Facilities-

---

56 EuGH, Urteil vom 27. März 2014, C-314/12, ECLI:EU:C:2014:192, Rn. 49 – UPC Telekabel Wien; Bertschek et al., a.a.O., S. 62, Jarass, a.a.O., Art. 16 Rn. 10.

57 Vertrag über die Arbeitsweise der Europäischen Union, ABl. C-326 vom 06.10.2012, S. 47ff.

58 Vgl. die Erläuterungen zur Charta der Grundrechte (2007/C 303/02), ABl. C 303 vom 14.12.2007, S. 17ff., abrufbar unter https://eur-lex.europa.eu/legal-content/de/ALL/?uri=CELEX%3A32007X1214%2801%29, sowie Bertschek et al., a.a.O. (Fn. 235), S. 63. Noch ungeklärt ist dagegen, ob Art. 16 auch eine subjektiv-rechtliche Schutzdimension im Sinne eines Rechts für potenzielle Datennehmer hat, an einem unverfälschten Wettbewerb teilzunehmen (dafür Bertschek et al., a.a.O.). Der EuGH hat die Wettbewerbsfreiheit allerdings bislang noch nicht als subjektives Recht anerkannt, vgl. Bernsdorf, N., in Meyer/Hölscheidt, Charta der Grundrechte der Europäischen Union, 5. Auflage 2019, Rn. 15, Bertschek et al., a.a.O, S. 63 m.w.N. (dort Fn 110).

59 Siehe bereits oben 2.4, Ziffer 1.

60 Jarass, a.a.O., Einl. Rn. 37 und 46 sowie Art. 52 Rn. 27; EuGH, Urteil vom 1. Juli 2014, C-573/12 – Alands, ECLI:EU:C:2014:2037, Rn. 127f.

61 Dafür, dass eine solche Lösung möglich ist, sprechen etwa die Erwägungsgründe 8 und 21.

62 Nach Art. 20 DSGVO, der das Recht einer betroffenen Person auf Datenübertragbarkeit (Portabilität) personenbezogener Daten regelt, hat der Betroffene ein Recht, ihn betreffende personenbezogene Daten zu erhalten, d.h. in ihren eigenen Machtbereich übertragen zu bekommen (Abs. 1), oder direkt an einen anderen Verantwortlichen zu übermitteln (Abs. 2, vgl. auch Gola, P., DSGVO, 2. Aufl. 2018, Art. 20 Rn. 9 und 25 f.).

63 Vgl. auch Podszun, R./Pfeifer, C., GRUR 2022, S. 953 (961) sowie Kerber, W., Governance of IoT Data, a.a.O., S. 12, der sich gegen eine grundsätzliche Beschränkung auf einen bloßen „in situ“-Zugang ausspricht und eine tiefgreifende Analyse fordert, inwieweit ein solcher Zugang die Nutzbarkeit und den Wert der Daten einschränkt.

64 Kommissionsentwurf zum Data Act, S. 3.

Doktrin“ scheiden jedoch aus, wenn der Dateninhaber den Markt nicht beherrscht.[65] Insgesamt sind die Kriterien der Essential-Facilities-Doktrin eng auszulegen und schwierig nachzuweisen.[66] Etwaige Ungleichgewichte unterhalb der Schwelle der Marktbeherrschung werden vom EU-Wettbewerbsrecht nicht reguliert. Art. 3 Abs. 2 S. 2 der EU-Kartellverordnung Nr. 1/2003 erlaubt es den Mitgliedstaaten jedoch, über das europäische Recht hinauszugehen und Missbräuche auch unterhalb der Schwelle der echten Marktbeherrschung zu bekämpfen. Einige Mitgliedstaaten haben daher bereits Regeln erlassen, um den Zugang zu wettbewerbsrelevanten Daten auch unterhalb dieser Schwelle sicherzustellen.[67] So hat etwa Deutschland sein Gesetz gegen Wettbewerbsbeschränkungen (GWB) um Regelungen ergänzt, nach denen ein Missbrauch und damit ein Wettbewerbsverstoß schon bei relativer Marktmacht vorliegen kann, wenn ein Unternehmen von einem anderen Unternehmen abhängig ist.[68] Eine solche Abhängigkeit kann sich ausdrücklich auch daraus ergeben, dass ein Unternehmen für seine Tätigkeit auf den Zugang zu Daten angewiesen ist, die von dem relativ marktmächtigen Unternehmen kontrolliert werden.[69] Voraussetzung ist, dass es an zumutbaren Ausweichmöglichkeiten auf Drittunternehmen fehlt und zwischen den beteiligten Unternehmen ein „deutliches Ungleichgewicht“ in der Markt- bzw. Verhandlungsmacht besteht.[70] Die Verweigerung des Zugangs zu den Daten gegen angemessenes Entgelt kann dann eine unbillige Behinderung darstellen.[71] Die Voraussetzungen dieses Anspruchs sind jedoch im Einzelfall hoch.[72]

Die Entscheidung des EU-Gesetzgebers, auch im EU-Recht den Zugang zu Daten unterhalb der Schwelle der Marktbeherrschung zu erleichtern und hierzu Datenteilungspflichten einzuführen, ist aus juristischer Sicht im Grundsatz zu respektieren, da dem Gesetzgeber bei komplexen wirtschaftlichen Entscheidungen ein weiter Entscheidungsspielraum zusteht.[73] Denn es bestehen Anhaltspunkte dafür, dass der bestehende regulatorische Rahmen einschließlich des Wettbewerbsrechts nicht in allen Fällen ausreicht, um für einen ausreichenden Wettbewerb in der Datenwirtschaft zu sorgen und zukünftige Innovationen im Interesse der Gesellschaft zu ermöglichen.[74] Hiervon scheint auch die Kommission auszugehen.

Für den EU-Gesetzgeber ist es nicht unbedingt vorzugswürdig, rein wettbewerbsrechtliche Ansprüche auf Datenzugang vorzusehen. Solche Ansprüche haben den Nachteil, dass sie erst in einem u.U. langwierigen und kostspieligen Verfahren durchgesetzt werden müssen.[75] Zudem birgt ein kartellrechtliches Vorgehen auch praktische Schwierigkeiten, u.a. weil die Kartellbehörden bei Annahme eines Kontrahierungszwangs zugleich auch über die Konditionen (angemessene Vergütung) entscheiden müssten.[76] Bei personenbezogenen Daten kommt erschwerend hinzu, dass eine Anordnung der Wettbewerbsbehörde, die Daten bereitzustellen, nicht von einer Rechtsgrundlage in der DSGVO gedeckt wäre.[77] Die kartellrechtliche Durchsetzung von Datenteilungspflichten oder die

---

65 Näher zur Essential-Facilities-Doktrin (EFD) bereits Ökonomische Bewertung, S. 18. Dabei setzt die EFD eine genaue Definition der betroffenen Märkte voraus, die oft streitig und schwierig zu treffen ist. Je enger, also z.B. markenspezifischer die Märkte definiert werden, desto eher ist ein wettbewerbsrechtlicher Datenzugangsanspruch zu bejahen. Vgl. auch Specht-Riemenschneider, L., die ebenfalls davon ausgeht, dass wettbewerbsrechtliche Zugangsansprüche nur einen geringen Teil der erforderlichen Datenzugangsansprüche erfassen, vgl. Stellungnahme zum Thema „Datenstrategie der Bundesregierung“ (BT-Drs. 19/26450) et al., Deutscher Bundestag, Ausschussdrucksache 19(23)109 vom 21.02.2021, S. 7f., abrufbar unter https://www.bundestag.de/resource/blob/823800/6f11b79c8288a181eaec827c4361825b/Stellungnahme-Specht-Riemenschneider-data.pdf.

66 Vgl. Schweitzer, H./Haucap, J./Kerber, W./Welker, R., Modernisierung der Missbrauchsaufsicht für marktmächtige Unternehmen, Endbericht zu Projekt Nr. 66/17 im Auftrag des Bundesministeriums für Wirtschaft und Energie (BMWi), 29. August 2018, S. 133, abrufbar unter https://www.d-kart.de/wp-content/uploads/2021/06/modernisierung-der-missbrauchsaufsicht.pdf.

67 Vgl. auch Drexl et al, Rn. 36.

68 § 20 Abs. 1 i.V.m. § 19 Abs. 1, Abs. 2 Nr. 1 GWB.

69 § 20 Abs. 1a GWB. Danach kann eine Abhängigkeit von einem bei einem Unternehmen vorliegenden Datenbestand auch schon unterhalb der Marktbeherrschung bestehen.

70 § 20 Abs. 1 S. 1 GWB.

71 Gesetzentwurf der deutschen Bundesregierung zum GWB-Digitalisierungsgesetz, BT-Drucks. 19/23492 v. 19.10.2020, S. 80.

72 Oechsler, J., Skript zum Europäischen Kartellrecht, 2022, S. 232.

73 EuGH, Urteil vom 8. Juni 2010, Vodafone et al., ECLI:EU:C:2010:32, Rn. 52 m.w.N. Danach ist eine Maßnahme nicht schon deshalb rechtswidrig, wenn sie nicht die bestmögliche war, sondern nur dann, wenn sie zur Erreichung des angestrebten Ziels offensichtlich ungeeignet ist. Dies ist aber bei den Datenteilungspflichten nicht der Fall.

74 Bertschek et al., a.a.O., S. 26, 85 (insbesondere zu den kartellrechtlichen Hürden auf EU-Ebene S. 59ff).Vgl. auch Picht, P./Richter, H., GRUR Int, 2022, S. 398 (401).

75 Vgl. Schweitzer et al., a.a.O., S. 136.

76 Näher dazu van Roosebeke, B. et al., S. 77f.; vgl. zu den praktischen Folgeproblemen auch Podszun, R./Pfeifer, C., GRUR 2022, S. 953 (954).

77 Näher dazu van Roosebeke, B. et al., S. 77. Zwar erlaubt Art. 6 Abs. 1 lit. c) DSGVO Datenverarbeitungen, die zur Erfüllung einer rechtlichen Verpflichtung erforderlich sind; dies gilt jedoch nur dann, wenn die Rechtsgrundlage für die Verarbeitung durch Unionsrecht oder mitgliedstaatliches Recht festgelegt wird, nicht aber auf der Entscheidung einer Wettbewerbsbehörde beruht.

Einführung erweiterter wettbewerbsrechtlicher Ansprüche stellt somit kein milderes Mittel im Vergleich zu gesetzlichen Datenteilungspflichten im Data Act dar.

Freiwillige Regeln und Musterklauseln allein sind nicht vergleichbar wirksam wie Datenteilungspflichten und scheiden daher ebenso als milderes Mittel aus.

2.2.2 Interessenabwägung

(1) Als legitime öffentliche Zwecke für die im Data Act geregelten Datenbereitstellungspflichten kommen neben der verbesserten Nutzerkontrolle vor allem die Förderung von Wettbewerb und Innovation in Betracht. Dies gilt insbesondere im Hinblick auf Reparatur- und Wartungsdienste, aber auch für die Entwicklung völlig neuer Produkte und Dienste.[78] Bei der Abwägung der widerstreitenden Interessen ist Folgendes zu berücksichtigen:

(2) *Für* gesetzliche Datenteilungspflichten führt die Kommission zu Recht an, dass diese den fairen Wettbewerb stärken, Lock-in-Effekte vermeiden und die geteilten Daten als Inputfaktor zur Entwicklung von Anschluss-, Neben- und sonstigen Diensten dienen können.[79] Datenteilungspflichten können so die unternehmerische Freiheit der zugangsberechtigten Dritten und den freien Wettbewerb als anerkanntes Prinzip stärken, Innovationen fördern und Wohlfahrtssteigerungen erzeugen, die im Interesse der Allgemeinheit liegen. Ein generelles geistiges Eigentumsrecht des Dateninhabers an den von ihm kontrollierten Daten besteht zudem nicht. Auch sein berechtigtes Vertrauen auf Beibehaltung der bestehenden Situation (faktische Alleinkontrolle von Daten) genießt keinen eigentumsrechtlichen Schutz. Diese Situation kann durch Entscheidungen der Gemeinschaftsorgane im Rahmen ihres Ermessens verändert werden.[80] Der Nutzer wiederum, der Besitz und möglicherweise sogar Eigentum an dem vernetzten Produkt erworben hat, kann aufgrund des Rechts auf Nutzung und Weitergabe der Daten sein Produkt voll auskosten und ggf. mit verbesserten Funktionen nutzen oder es selbst reparieren oder von einem Dritten reparieren lassen.[81] Weniger schützenswert erscheint demgegenüber sein Interesse an einer bloßen Kommerzialisierung seiner Daten, d.h. daran, sich durch deren Weiterverkauf an einen Dritten einen rein finanziellen Vorteil zu verschaffen.

(3) *Gegen* Datenteilungspflichten spricht jedoch, dass es sich um einen schwerwiegenden Eingriff in die unternehmerische Freiheit des Dateninhabers handelt. Zum einen ist die Datenbereitstellung für den Dateninhaber i.d.R. kostspielig. Zum anderen hat er u.U. riskante Investitionen in die Fähigkeit seines vernetzten Produkts getätigt, Daten zu generieren, während der Nutzer ggf. einen geringen und der Dritte keinerlei Beitrag zur Erzeugung der Daten geleistet hat.[82] Zu weitgehende Datenteilungspflichten drohen daher die Innovationsbereitschaft der Dateninhaber sowie die Anreize für deren Investitionen in die Vernetztheit ihrer Produkte und damit in die Wertschöpfung durch Daten zu beseitigen, die die Kommission mit dem Data Act gerade aufrechterhalten will.[83] Der EuGH hat in anderem Zusammenhang anerkannt, dass es negative Auswirkungen auf die Schaffung neuer Werke haben kann, wenn die Vergütung des Herstellers trotz risikoreicher Investitionen in die Herstellung von Erzeugnissen nicht mehr angemessen gewährleistet werden kann.[84]

(4) Faktoren zur Abmilderung des Eingriffs

Der Eingriff wird zunächst dadurch abgemildert, dass kleine und Kleinstunternehmen (KKU) in Bezug auf Daten, die durch von ihnen hergestellte Produkte und verbundene Dienste erzeugt werden, von den Datenteilungspflichten befreit werden.[85] Dies entlastet KKU; andererseits sind damit eine große Anzahl von Unternehmen von der Pflicht ausgenommen, was deren Effektivität mindert. Auch die zahlreichen KKU in der EU können über wichtige Daten verfügen, für deren Teilung der Data Act Anreize vermissen lässt.

---

78 Siehe Ökonomische Bewertung, S. 14.

79 Zur Argumentation der Kommission siehe ök. BW S. 12. Ebenso Gutachten der Datenethikkommission der deutschen Bundesregierung, a.a.O., S. 82, 91.

80 EuGH, Urteil vom 5. 10. 1994, C-280/93, ECLI:EU:C:1994:367, Rn. 80; Deutschland/Rat der EU; Jarass, a.a.O., Art. 17 Rn. 13 (zum „entzogenen" Marktanteil eines Unternehmens).

81 Kommissionsvorschlag zum Data Act, S. 16: „Dadurch kommt der Eigentümer in den Genuss eines besseren Nutzerergebnisses und eines breiteren Spektrums von z-B. Reparatur- und Wartungsdiensten".

82 Siehe Ökonomische Bewertung, S. 16.

83 Data Act, S. 3.

84 EuGH, Urteil vom 28.04.1998, C-200/96, ECLI:EU:C:1998:172, Rn. 24 – Metronome Musik (zur freien Berufsausübung). In diesem Urteil hat der EuGH im Rahmen der Prüfung der Verhältnismäßigkeit eines ausschließlichen Rechts für den Hersteller von Tonträgern den Schutz hoher und risikoreicher Investitionen dieser Hersteller als schützenswertes Interesse erachtet, zumal Tonträger von Produktpiraten besonders leicht vervielfältigt werden könnten. Zur Relevanz dieses Urteils auch Bertschek et al., a.a.O., S. 75.

85 Art. 7 Abs. 1 Data Act, siehe oben A. 2.8. Dies gilt nicht, wenn sie von einem größeren Unternehmen mit der Herstellung beauftragt wurden.

Sind die Dateninhaber mittlere und große Unternehmen, bleibt es bei dem Eingriff in die unternehmerische Freiheit. Dass der Dateninhaber vom Dritten – nicht aber vom Nutzer, was angesichts des Nutzerbeitrags zur Generierung der Daten grundsätzlich angemessen erscheint – eine Vergütung für die Bereitstellung der Daten verlangen kann, mildert den Eingriff allerdings nicht wesentlich ab: Weil der Dateninhaber von KMU – die 99 % der Unternehmen in der EU ausmachen[86] – lediglich die unmittelbaren Bereitstellungskosten verlangen kann[87], kann er faktisch nur sehr eingeschränkt Gewinn mit der Weitergabe generierter Daten erzielen.[88] Zwar könnte der Dateninhaber den Eingriff auch durch eine Anhebung des Produktpreises abmildern; eine solche liefe aber wiederum dem Ziel zuwider, die Datenteilung in der EU zu fördern.[89]

Auch die im Data Act geregelten Nutzungsbeschränkungen[90] reichen in der vorgesehenen Form nicht aus, um die Wirkung des Eingriffs angemessen auszugleichen. Zwar darf der Dritte die Daten nur für die mit dem Nutzer vereinbarten Zwecke verarbeiten; auf diesen Vertrag hat der Dateninhaber aber keinen direkten Einfluss.[91] Das an sich sachgerechte Verbot für Nutzer und Dritte, Daten zur Entwicklung eines Konkurrenzprodukts zu nutzen, ist noch zu vage[92] und muss konkretisiert werden, um den Eingriff in die unternehmerische Freiheit der Dateninhaber verhältnismäßig auszugestalten. Dass es Dritten grundsätzlich verboten ist, die Daten an andere Dritte weiterzugeben – soweit dies nicht für die Erbringung des vom Nutzer gewünschten Dienstes erforderlich ist[93] – ist ebenfalls sachgerecht, aber gleichermaßen vage.[94] Zudem ist zweifelhaft, ob all diese Verbote und Beschränkungen einen hinreichenden Schutz bieten, da eine Kontrolle kaum möglich[95] ist. Der Nachweis einer unerlaubten Nutzung oder Weitergabe der Daten dürfte daher in der Praxis nur schwer zu führen sein – sofern der Dateninhaber diese überhaupt bemerkt. Keinen Schutz bietet der Data Act zudem im Hinblick auf die Nutzung durch Personen, an die Nutzer oder Dritte die Daten weitergeben dürfen. Es obliegt allein dem Dateninhaber, seine Vertragspartner auch zu einer Weitergabe der Verbote und Beschränkungen zu verpflichten.[96]

Der Eingriff wird allerdings dadurch abgemildert, dass der Dateninhaber gegenüber dem Dritten geeignete („appropriate“) technische Schutzmaßnahmen anwenden kann, um einen unbefugten Zugang zu den Daten zu verhindern.[97] Auch hier ist jedoch unklar, welche Schutzmaßnahmen der Dateninhaber nutzen darf und wann es sich um eine übermäßige Schutzmaßnahme handelt, die dem Dritten den Datenzugang unangemessen erschwert.[98] Der Dateninhaber ist insoweit in einem Dilemma: sind seine Schutzmaßnahmen zu locker, drohen unbefugte Datenzugriffe und eine Preisgabe seiner Geschäftsgeheimnisse; sind sie zu streng, riskiert er u.U. ein Bußgeld, weil er den Datenzugang unangemessen behindert. Um Rechtsunsicherheit zu vermeiden, sollte präzisiert werden, welche technischen Schutzmaßnahmen des Dateninhabers angemessen sind. Dabei sollte auch erläutert werden, wie intelligente Verträge als Schutzmaßnahmen helfen und eingesetzt werden können.

Dass der Data Act es Dritten verbietet, Nutzer mit Hilfe sogenannter „dark patterns“[99] – d.h. unlauterer Mittel – zur Datenweitergabe an sie zu bewegen[100], ist sachgerecht, um das Ziel zu erreichen, den Nutzern eine bessere Kontrolle über ihre Daten zu verschaffen: Weil das Datenzugangsrecht der Dritten stets von dem Willen eines

---

86 Europäische Kommission, vgl. https://ec.europa.eu/growth/smes_en.

87 Art. 9 Abs. 2 Data Act.

88 Gerpott, CR 2022, S. 271 (278).

89 Siehe ökonomische Bewertung, S. 16.

90 Siehe insbesondere oben A. Kapitel 2.7 und 2.4.

91 So jedenfalls in Bezug auf die Offenlegung von Geschäftsgeheimnissen auch Efroni, Z./von Hagen, P./Völzmann, L./Robert, P./Sattorov, M., Weizenbaum Institute for the Networked Society, Position Paper regarding Data Act, 2022, S. 17, abrufbar unter https://www.ssoar.info/ssoar/handle/document/79542.

92 Ebenso Efroni et al. (Weizenbaum Institute), a.a.O S. 15. Näher zu den Unklarheiten dieser Schutzklausel vgl. bereits ökonomische Bewertung, S. 17f.

93 Art. 6 Abs. 2 lit.c Data Act, vgl. oben A. 2.7.

94 Unklar ist, wann dieses Verbot nicht greift, was dann der Fall ist, wenn die Weitergabe „erforderlich“ ist, z.B. ob der Dritte die Daten an einen Datenaufbereitungs- oder -analysedienst weitergeben darf, wenn er für die Erbringung des Dienstes auf eine Aufbereitung der bereitgestellten Rohdaten angewiesen ist, aber nicht selbst über die erforderlichen Fähigkeiten verfügt.

95 Ebenso Rammos, T./Wilken, T., DB 2022, S. 1241 (1244); Hilgendorf, E./Vogel, P., JZ 2022, S. 380 (387).

96 Zudem ist unklar, wann es i.S.v. Art. 6 Abs. 2 Data Act für einen Dritten „erforderlich“ ist, die Daten an einen anderen Dritten weiterzugeben, um den vom Nutzer gewünschten Dienst zu erbringen. Darf der Dritte die Daten etwa einen anderen Dritten mit einer Datenanalyse o.ä. betrauen, die er selbst nicht leisten kann, aber für die Erbringung des Dienstes benötigt?

97 Art. 11 Abs. 1 Data Act.

98 Efroni et al. (Weizenbaum Institute), a.a.O., S. 17, 29 bezüglich des Schutzes von Geschäftsgeheimnissen.

99 „Dark patterns“ sind manipulative Gestaltungstechniken, die dazu dienen, Verbraucher zu täuschen bzw. durch unverhältnismäßige Beeinflussung zu für sie negativen Entscheidungen z.B. über die Offenlegung von Daten zu verleiten [vgl. EG 34].

100 Art. 6 Abs. 2 lit. a) Data Act.

Nutzers abhängig ist, besteht die Gefahr, dass Dritte versuchen werden, den Nutzer hierzu ggf. auch unlauter zu beeinflussen.

(5) Faktoren, die den Eingriff verstärken

(a) Eine Bereitstellung von Daten kontinuierlich und in Echtzeit erweitert die Nutzungsmöglichkeiten für Nutzer und Unternehmen, erhöht aber insbesondere bei großen Datenmengen den Aufwand und die Kosten für den Dateninhaber massiv.[101] Eine Pflicht zur kontinuierlichen Datenbereitstellung in Echtzeit erscheint deshalb nicht in jedem Fall gerechtfertigt. Vor allem wenn der damit verbundene Aufwand den Nutzen übersteigt, kann diese Pflicht unverhältnismäßig sein. Das Interesse des Nutzers an einer Nutzung kontinuierlicher Echtzeitdaten dürfte zumindest beim Durchschnittsverbraucher fraglich sein und auch bei Unternehmen verschiedener Sektoren variieren. Zu Recht sieht der Data Act insoweit auch ein Korrektiv vor, weil der Dateninhaber Daten nur „gegebenenfalls" kontinuierlich und in Echtzeit zur Verfügung stellen muss. Diese Einschränkung ist jedoch zu unbestimmt. Der Data Act muss näher präzisieren, unter welchen Voraussetzungen bzw. wem gegenüber ein kontinuierlicher Echtzeit-Zugang erforderlich ist. Dies kann am gezieltesten in sektorspezifischen Regelungen geschehen.

(b) Auch die Pflicht, ggf. auch Geschäftsgeheimnisse offenlegen zu müssen, vergrößert den Eingriff in die unternehmerische Freiheit der Dateninhaber, welche auch die für die Unternehmenstätigkeit bedeutsamen Geschäfts- und Betriebsgeheimnisse schützt.[102] Außerdem stellt der Schutz von Geschäftsgeheimnissen einen allgemeinen Grundsatz des Unionsrechts dar.[103] Geschäftsgeheimnisse werden daher unter bestimmten Voraussetzungen auch durch eine spezielle EU-Richtlinie[104] geschützt. Dass der Data Act die Offenlegung von Geschäftsgeheimnissen nicht grundsätzlich ausklammert, ist sachgerecht, da Dateninhaber die Bereitstellung der Daten sonst in vielen Fällen unter Berufung auf Geschäftsgeheimnisse verweigern könnten. Zu vage ist jedoch die vorgesehene Beschränkung, wonach Dateninhaber Geschäftsgeheimnisse gegenüber Dritten nur offenlegen müssen, soweit dies erstens für die Erfüllung des zwischen Nutzer und Drittem vereinbarten Zweck „unbedingt erforderlich" ist und der Dritte zweitens „alle zwischen ihm und dem Dateninhaber vereinbarten besonderen Maßnahmen getroffen hat, die erforderlich sind, um die Vertraulichkeit des Geschäftsgeheimnisses zu wahren".[105] Denn der Data Act lässt völlig offen, welche vom Dritten zu ergreifenden Schutzmaßnahmen angemessen sind[106], wann die entsprechenden Daten für die Erfüllung „unbedingt erforderlich" sind bzw. wer dies beurteilt.[107] Dies schafft Rechtsunsicherheit und könnte zu Rechtsstreitigkeiten führen, die die Datenbereitstellung verzögern.

Um das Risiko einer Offenlegung von Geschäftsgeheimnissen zu senken, kann der Dateninhaber mit dem Nutzer und dem Dritten ferner eine Geheimhaltungsvereinbarung (z.B. ein Non-Disclosure-Agreement, NDA) treffen und ggf. Vertragsstrafen für Verletzungen vorsehen.[108] Erwirbt jedoch eine große Vielzahl von Nutzern die Produkte des Dateninhabers, müsste er mit all diesen Nutzern NDAs schließen. Ungeachtet des hierfür erforderlichen Aufwands steigt mit der zunehmenden Anzahl von NDAs zugleich das Risiko, dass eine dieser Vereinbarungen verletzt wird.[109] Zum anderen versprechen NDAs nur dann einen effektiven Schutz, wenn sie wirksam durchgesetzt werden können. Wie die Durchsetzung erfolgt und welche Konsequenz ein Verstoß gegen das NDA hat, regelt der Data Act jedenfalls für das Verhältnis zwischen Dateninhaber und Nutzer nicht.

(6) Zur Unverhältnismäßigkeit einer horizontalen Datenteilungspflicht für alle Dateninhaber

Dass die Datenteilungspflichten im Data Act horizontal und einheitlich für alle vernetzten Produkte und verbundenen Dienste und ohne jede Differenzierung dahingehend gelten, ob es sich beim Nutzer um einen Verbraucher (B2C) oder um ein Unternehmen (B2B) handelt, ist unangemessen und daher unverhältnismäßig. Eine allgemeine

---

101 Siehe ökonomische Bewertung, S. 16.

102 EuGH, Urteil vom 23.09.2004, C-435/02, ECLI:EU:C:2004:552, Rn. 49 – Springer, Jarass, a.a.O., Rn. 10, so wohl auch Specht-Riemenschneider, a.a.O. (Studie), S. 5, 21.

103 EuGH, Urteil vom 14. 2. 2008, C-450/06, ECLI:EU:C:2008:91, Rn. 49 – Varec SA/Belgien, EuGH, Urteil vom 29.03.2012, C-1/11 (Interseroh Scrap), ECLI:EU:C:2012:194, Rn. 44 – Interseroh Scrap, Jarass, a.a.O., Rn. 16, Bertschek et al., a.a.O., S. 64.

104 Richtlinie (EU) 2016/943 des Europäischen Parlaments und des Rates vom 8. Juni 2016 über den Schutz vertraulichen Know-hows und vertraulicher Geschäftsinformationen (Geschäftsgeheimnisse) vor rechtswidrigem Erwerb sowie rechtswidriger Nutzung und Offenlegung, ABl. L 157 vom 15.06.2016, S. 1ff.

105 Art. 5 Abs. 8 Data Act, vgl. oben A. 2.5.

106 Siehe bereits Ökonomische Bewertung, S. 17.

107 Efroni et al. (Weizenbaum Institute), a.a.O., S. 12.

108 Art. 4 Abs. 3, Art. 5 Abs. 8 Data Act.

109 Vgl. auch Efroni et al. (Weizenbaum Institute), a.a.O., S. 13 („having numerous such agreements with numerous parties would render secrecy illusory").

Datenteilungspflicht wird den unterschiedlichen Datentypen (z.B. industrielle Produktionsdaten vs. personenbezogene Gesundheitsdaten), Gepflogenheiten, Erfordernissen und Geschäftsmodellen in den einzelnen Sektoren der Digitalwirtschaft und den insoweit stark divergierenden Interessen der einzelnen Akteure nicht hinreichend gerecht.[110] Angesichts sehr unterschiedlicher Probleme und Herausforderungen beim Austausch von Daten je nach Markt sollte die EU Datenteilungspflichten primär sektorspezifisch regeln. Anders als bei einer horizontalen Datenteilungspflicht lassen sich die Pflichten so an die spezifischen Besonderheiten des jeweiligen Sektors anpassen. Solche Pflichten sollten auch nur geregelt werden, soweit dies erforderlich erscheint, um den Datenaustausch im jeweiligen Sektor zu fördern.[111] Für die Bereitstellung sehr unterschiedlicher Datensätze wie Fahrzeugdaten, Mobilfunkdaten, Gesundheitsdaten oder Agrardaten sind spezifische, an die Besonderheiten des jeweiligen Sektors angepasste Datenteilungspflichten gegenüber einer einheitlichen horizontalen Datenteilungspflicht für alle IoT-Daten das bessere und mildere Mittel.

Für die Regelung einer allgemeinen Bereitstellungspflicht im Data Act spricht zwar, dass die Kommission auch das sektorübergreifende Teilen von Daten ermöglichen will. Eine Pflicht zum sektorübergreifenden Teilen von Daten sollte im Data Act aber aus den oben genannten Gründen allenfalls als Auffangtatbestand geregelt und ihre Voraussetzungen stärker zielorientiert ausgestaltet werden.

Darüber hinaus ist eine horizontale Datenteilungspflicht auch deshalb unangemessen, weil es an einem generellen Machtungleichgewicht zwischen Dateninhabern einerseits und Nutzern und Dritten andererseits fehlt. Denn im Rahmen der Prüfung, ob Datenteilungspflichten verhältnismäßig sind, ist auch die Machtverteilung zwischen den Parteien zu berücksichtigen. Ist der Nutzer ein Verbraucher, lässt sich ein Machtungleichgewicht noch am ehesten annehmen. Anders ist dies bei gewerblichen Nutzern und Dritten. Obwohl ein Zugangsrecht zu wettbewerbsrelevanten Daten bei ungleicher Machtverteilung auch unterhalb der Schwelle der Marktbeherrschung sinnvoll sein kann, erscheinen Datenteilungspflichten deshalb nicht generell, sondern allenfalls bei entsprechender Abhängigkeit von den Daten des Dateninhabers gerechtfertigt.[112] Eine solche Abhängigkeit der Nutzer und Dritten von den Daten des Dateninhabers besteht aber nicht pauschal in allen Sektoren und in allen Fällen.[113] Ist eine solche Abhängigkeit anzunehmen, kann ein Zugangsrecht zu wettbewerbsrelevanten Daten sinnvoll sein, sofern und soweit die Vorteile einer mehrfachen Nutzung der betreffenden Daten die Nachteile eines Verlustes der exklusiven Verfügung über diese Daten überwiegen.[114] Fehlt es im konkreten Fall an einer Abhängigkeit, kann es dem Nutzer und Dritten zugemutet werden, selbst entsprechende Rechte mit dem Dateninhaber auszuhandeln oder einen anderen Anbieter zu wählen. Gesetzliche Datenzugangs- und Nutzungsrechte sind dann nicht erforderlich. Dass die Kommission offenbar pauschal vom Bestehen eines Machtungleichgewichts ausgeht und Nutzern und Dritten ohne weitere Voraussetzungen Datenzugangs- und Nutzungsrechte einräumt, ist nicht sachgerecht. Der Eingriff in die unternehmerische Freiheit der Dateninhaber durch die generelle Datenteilungspflicht bei vernetzten Produkten und verbundenen Diensten ist insoweit auch aus diesem Grund unverhältnismäßig.[115] Vielmehr sollte der Data Act das Datenzugangs- und Nutzungsrecht an das tatsächliche Bestehen einer Abhängigkeit von den Daten knüpfen.[116] Er könnte das Bestehen einer Abhängigkeit in bestimmten Konstellationen ggf. auch vermuten und es dem Dateninhaber ermöglichen, diese Vermutung zu widerlegen und den Anspruch so abzuwehren.

---

[110] Vgl. auch Kerber, W., Governance of IoT Data, 08.05.2022, a.a.O., S. 25, abrufbar unter https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4080436. Auch im Commission Staff Working Document „Common European Data Spaces", SWD(2022) 45 final, S. 5, weist die Kommission auf die begrenzte Sinnhaftigkeit eines einheitlichen Ansatzes hin.

[111] Ebenso Specht-Riemenschneider, L., Stellungnahme zum Thema „Datenstrategie der Bundesregierung" (BT-Drs. 19/26450) et al., Deutscher Bundestag, Ausschussdrucksache 19(23)109 vom 21.02.2021, S. 3, 10, abrufbar unter https://www.bundestag.de/resource/blob/823800/6f11b79c8288a181eaec827c4361825b/Stellungnahme-Specht-Riemenschneider-data.pdf. Für sektorspezifische Datenteilungspflichten auch Kerber, W., Governance of IoT Data, a.a.O., S. 25, abrufbar unter https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4080436, „aus ökonomischer Perspektive", S. 25.

[112] Diese Argumentation lehnt sich an die oben unter C. 2.2.1 diskutierten Voraussetzungen der in Deutschland eingeführten wettbewerbsrechtlichen Ansprüche bei datenbedingter Abhängigkeit von Unternehmen mit relativer Marktmacht an.

[113] Zum Fehlen eines generellen Marktversagens siehe bereits Ökonomische Bewertung, S. 12 ff.

[114] Gesetzentwurf der deutschen Bundesregierung zum GWB-Digitalisierungsgesetz, BT-Drucks. 19/23492 v. 19.10.2020, S. 80.

[115] Dass der Data Act ein pauschales Datenzugangs- und Nutzungsrecht vorsieht, widerspricht auch der EU-Datenstrategie, wonach die Zugangsgewährung zu Daten nur bei Vorliegen besonderer Umstände und stets sektorspezifisch vorgeschrieben werden sollte, wenn in dem jeweiligen Sektor ein Marktversagen festgestellt wird oder vorhersehbar ist und durch das Wettbewerbsrecht allein nicht behoben werden kann, vgl. EU-Kommission, Mitteilung [COM(2020) 66] vom 19.02.2020 – Eine europäische Datenstrategie S. 16.

[116] Vgl. auch Picht, P./Richter, H., GRUR Int, 2022, S. 395 (401), die sich allgemein dafür aussprechen, den EU-Rechtsrahmen umfassender zu gestalten und – in Anlehnung an das u.a. in Deutschland kodifizierte Konzept der relativen Marktmacht (siehe dazu oben Kap. C. 2.2.1) – auch Unternehmen mit Marktmacht unterhalb der Marktbeherrschung zu erfassen.

2.2.3 Zwischenfazit

Die Datenteilungspflichten im Data Act greifen aufgrund ihrer Pauschalität ihrer aktuellen Form in unverhältnismäßiger Weise in die unternehmerische Freiheit der Dateninhaber ein. Zum einen muss – primär in sektorspezifischen Vorschriften – konkretisiert werden, wie die Datenbereitstellung genau zu erfolgen hat (wo genügt „in situ“, wo muss ggf. eine Übermittlung erfolgen). Um die Pflicht, Daten und Geschäftsgeheimnisse zu teilen, verhältnismäßig auszugestalten, sollte die Gewährung von Datenzugangs- und Nutzungsrechten zweitens an das tatsächliche Bestehen einer Abhängigkeit von den Daten geknüpft werden. Drittens müssen bessere und hinreichende Kontrollmöglichkeiten geschaffen werden, um das Risiko eines Missbrauchs der Daten und Geschäftsgeheimnisse auf ein vertretbares Maß zu senken. Ansonsten besteht die Gefahr, dass die Bereitschaft von Dateninhabern, in die Vernetzung ihrer Produkte zu investieren und diese auszubauen, abnimmt und das Ziel des Data Act, den Datenzugang und die Datennutzung für Verbraucher und Unternehmen zu erleichtern und gleichzeitig Anreize für Investitionen in die Wertschöpfung durch Daten aufrecht zu erhalten, daher nicht hinreichend gewährleistet werden kann.[117] Zur Ermöglichung einer besseren Kontrolle könnte es sinnvoll sein, den Data Act enger mit dem Data Governance Act[118] zu verknüpfen und vorzusehen, dass die Daten in geeigneten Fällen an einen neutralen Datentreuhänder bereitgestellt werden dürfen oder müssen, in dessen geschützter Umgebung Nutzer und Dritte die Daten sicher, datenschutzkonform und im Einklang mit den Vorgaben des Data Act – und ggf. vertraglicher Vereinbarungen zwischen den Parteien – verarbeiten können.[119]

3. Pflicht zum Vertragsschluss bei nicht-personenbezogenen Daten

Ferner greift die Pflicht des Dateninhabers, mit dem Nutzer einen Vertrag zu schließen, um „auf dessen Grundlage“ nicht-personenbezogene Daten selbst (weiter) nutzen zu dürfen[120], in unverhältnismäßiger Weise in seine unternehmerische Freiheit und seine Vertragsfreiheit ein.[121] Denn sie lässt sich so interpretieren, dass der Dateninhaber für die eigene Nutzung oder eine Weitergabe der Daten eine „vertragliche Nutzungserlaubnis“ durch den Nutzer benötigt. Der Nutzer hätte somit offenkundig die Möglichkeit, die Nutzung nicht-personenbezogener Daten durch den Dateninhaber zu verbieten.[122] Die Regelung zwingt somit Dateninhaber, die die Daten selbst weiter nutzen oder an Dritte verkaufen wollen, Verträge mit einer möglicherweise hohen Anzahl von Nutzern zu schließen und sich darin Weiterverkauf und Weiternutzung auszubedingen, was Aufwand und Kosten verursacht.[123] Dies ist unangemessen. Zwar besteht ein legitimes Ziel des Data Act darin, den Nutzern mehr „Kontrolle“ über „ihre“ Daten zu verschaffen. Dem Interesse der Nutzer an den Daten tut der Data Act aber bereits durch die Einräumung eines Datennutzungsrechts und die Transparenzpflichten dahingehend Genüge, wie der Dateninhaber die Daten selbst zu nutzen oder an Dritte weiterzugeben gedenkt. Ein überwiegendes Interesse des Nutzers, über die eigene Nutzungsmöglichkeit hinaus die Weiternutzung und Weitergabe nicht-personenbezogener Daten durch den Dateninhaber zu verbieten, ist dagegen nicht ersichtlich.[124] Dies gilt sowohl dann, wenn der Nutzer ein Verbraucher ist, als auch, wenn Unternehmen vernetzte Objekte nutzen und der Dateninhaber die generierten Daten de facto kontrolliert. Private Nutzer werden bei personenbezogenen Daten auch durch die DSGVO geschützt, weil der Dateninhaber zur Weiterverarbeitung der Daten eine Rechtsgrundlage benötigt. Gewerbliche Nutzer werden zumindest insoweit geschützt, als der Data Act es dem Dateninhaber verbietet, sich mit Hilfe der Daten Einblicke in die gewerbliche Position des Nutzers zu verschaffen und diese ggf. zu

---

117 I. Erg. ebenso Gerpott, T., Vorschlag für ein europäisches Datengesetz, CR 2022, S. 271 (276), im Hinblick auf die Zugangsrechte für die Nutzer.

118 Der Data Governance Act erfasst auch die Bereitstellung von Daten durch einen Dateninhaber an einen Datennutzer auf der Grundlage des Unionsrechts, vgl. Art. 2 Nr. 7 sowie EG 27, der davon ausgeht, dass Datenvermittlungsdienste zu Akteuren werden könnten, die auch die gemeinsame Datennutzung im Zusammenhang mit im EU-Recht festgelegten Verpflichtungen erleichtern dürften.

119 Grundlegend zur Rolle der Datentreuhänder Specht-Riemenschneider, L., Kerber, W., Datentreuhänder – Ein problemlösungsorientierter Ansatz, 16. Februar 2022, abrufbar unter https://www.kas.de/de/einzeltitel/-/content/datentreuhaender-ein-problemloesungsorientierter-ansatz.

120 Art. 4 Abs. 6 S. 1 Data Act, vgl. oben A. 2.4.

121 Siehe bereits ökonomische Bewertung, S. 17. Die Vertragsfreiheit ist zentraler Bestandteil des Grundrechts auf den Schutz der unternehmerischen Freiheit [siehe u.a. EuGH, Urteil vom 22. Januar 2013, C-283/11, ECLI:EU:C:2013:28, Rn. 42 – Sky Österreich; EuGH, Urteil vom 18.07.2013, Rs. C-426/11, ECLI:EU:C2013:521, Rn. 32 – Alemo-Herron] und umfasst u.a. (1) die Freiheit, den Vertragspartner zu wählen [vgl. EuGH, Urteil vom 05.10.1999, C-240/97, ECLI:EU:C:1999:479, Rn. 99 – Spanien/Kommission (bezogen auf das Recht, geschlossene Verträge zu ändern); siehe auch Bertschek et al., a.a.O., S. 63]; (2) Verträge inhaltlich auszugestalten [vgl. EuGH, Urteil vom C-426/11 ECLI:EU:C2013:521, Rn. 33f. – Alemo-Herron; siehe auch Bertschek et al., a.a.O., S. 63] und (3) Preise und sonstige Konditionen zu vereinbaren [Bertschek et al., a.a.O., S. 63].

122 Laut Drexl et al. lässt sich die Regelung sogar als „exklusives Datennutzungsrecht“ des Nutzers verstehen (Rn. 45ff.).

123 Vgl. bereits Ökonomische Bewertung, S. 17 („vermeidbare Transaktionskosten“).

124 Vgl. insoweit auch Drexl et al., Rn. 52. Zum fehlenden Interesse des Nutzers am Umfang der Datennutzung durch den Dateninhaber vgl. bereits ökonomische Bewertung, S. 16 f.

untergraben.[125] Gegen das Erfordernis einer vertraglichen Nutzungserlaubnis für nicht-personenbezogene Daten sprechen mehrere Gründe: Erstens wird so die Nutzung nicht-personenbezogener Daten durch den Dateninhaber und Dritte und damit zugleich der freie Fluss dieser Daten eingeschränkt.[126] Zweitens wären nicht-personenbezogene Daten damit letztlich sogar schwieriger nutzbar als personenbezogene Daten, deren Nutzung nicht zwingend eine Einwilligung erfordert, sondern auch auf eine der weiteren Rechtsgrundlagen in Art. 6 Abs. 1 DSGVO gestützt werden kann.[127] Drittens sind private Nutzer oder verhandlungsschwächere gewerbliche Nutzer auch bei einem Vertragszwang nicht ohne weiteres in der Lage, bestimmte Nutzungen und Weitergaben durch den Dateninhaber auszuschließen. Denn es ist zu erwarten, dass verhandlungsstärkere Dateninhaber den Verkauf des Produkts an den Vorbehalt eigener Nutzungsmöglichkeiten knüpfen werden.[128] Viertens schafft ein vertraglicher Erlaubnisvorbehalt Rechtsunsicherheit, die Dritte daran hindern könnte, Daten direkt vom Dateninhaber zu erwerben. Denn es ist unklar, ob der Dritte die Daten wie geplant nutzen kann, wenn ein Vertrag zwischen Dateninhaber und Nutzer fehlt oder unwirksam ist[129] oder die Nutzung der Daten durch den Dateninhaber oder einen Dritten von diesem Vertrag nicht gedeckt ist. Das Erfordernis einer vertraglichen Nutzungserlaubnis sollte daher gestrichen werden.[130]

4. Ausschluss von Gatekeepern vom Datenzugangsrecht

Der Ausschluss von Gatekeepern als „Dritte“ vom Datenzugangsrecht in Art. 5 greift zum einen in die unternehmerische Freiheit der Gatekeeper und zum anderen in die Vertragsfreiheit der Nutzer ein. Denn Nutzer dürfen die Daten nicht an einen Gatekeeper geben (lassen). Dies hindert die Nutzer zugleich daran, einen möglicherweise innovativen Dienst eines Gatekeepers in Bezug auf ihr vernetztes Produkt in Anspruch zu nehmen.[131] Mit diesem Weitergabeverbot will die Kommission verhindern, dass Gatekeeper auch auf den (künftigen) Märkten für IoT-Daten Datenmonopole errichten können. Dies stellt zwar ein grundsätzlich legitimes Ziel dar. Neben den ökonomischen Defiziten dieser Regelung[132] ist deren Verhältnismäßigkeit aber auch juristisch problematisch. Es ist bereits fraglich, ob das Weitergabeverbot geeignet ist, die Bildung von IoT-Datenmonopolen durch Gatekeeper tatsächlich zu erschweren. Denn der Data Act verbietet es – jedenfalls bei personenbezogenen Daten[133] – weder Dateninhabern, Daten ohne Zustimmung des Nutzers an einen Gatekeeper zu verkaufen[134], noch hindert er Gatekeeper daran, die Daten auf anderem Weg rechtmäßig zu erlangen.[135] Auch könnten Gatekeeper Hersteller von IoT-Produkten aufkaufen[136] oder eigene vernetzte Produkte auf den Markt bringen[137] und so auf diesem Weg selbst zum Dateninhaber werden. Zwar besteht ein nachvollziehbares politisches Interesse daran, Gatekeepern, die nach Ansicht der Kommission ohnehin „einzigartige Fähigkeiten“ zum Datenerwerb haben[138], die Erlangung von IoT-Daten zu erschweren, an deren Generierung sie keinen Anteil haben.[139] Auch der Dateninhaber hat – worauf wohl auch die Kommission abstellt[140] – ein Interesse daran, möglichst wenigen Dritten Daten bereitstellen zu müssen.[141] Ob der Ausschluss der Gatekeeper von den Daten gelingen wird, ist angesichts der fehlenden umfassenden Wirkung des Verbots aber zweifelhaft, so dass es jedenfalls unverhältnismäßig erscheint, das Gatekeeper-Verbot im Data Act einseitig zu Lasten der Vertragsfreiheit der Nutzer auszugestalten.[142] Insgesamt

---

125 Art. 4 Abs. 6 S. 2 Data Act.

126 Drexl et al., Rn. 46.

127 Zu diesem Widerspruch vgl. auch Drexl et al., Rn. 298.

128 Dies mildert zwar wiederum den Eingriff ab, führt aber zu weiteren Folgeproblemen und Rechtsunsicherheit.

129 Dies könnte z.B. der Fall sein, wenn die AGB, in denen der Dateninhaber sich die Nutzung der Daten vorbehält, der AGB-Kontrolle nicht standhalten.

130 Ebenso Drexl et al., Rn. 49, 52ff., die sich für eine Streichung des Art. 4 (6) S. 1 aussprechen.

131 Drexl et al., a.a.O., Rn. 92, Ökonomische Bewertung, S. 19..

132 Siehe ökonomische Bewertung, S. 19.

133 Vorbehaltlich einer gültigen Rechtsgrundlage nach der DSGVO.

134 Vgl. Drexl et al., a.a.O., Rn. 92.

135 Vgl. EG 36 am Ende.

136 Drexl et al., Rn. 92.

137 Gerpott, CR 2022, S. 271 (276).

138 Erwägungsgrund 36 Data Act.

139 Vgl. bereits Ökonomische Bewertung. S. 19.

140 Erwägungsgrund 36 Data Act.

141 Dies gilt allerdings am ehesten dann, wenn die Gefahr besteht, dass der Gatekeeper (potenziell) konkurrierende Produkte oder Dienste anbietet.

142 Vgl. Drexl et al., die den Ausschluss von Gatekeepern gegenüber den Nutzern daher als unfair betrachten. Die Vertragsfreiheit der Nutzer wird von der Kommission im Rahmen der Abwägung (EG 36) überhaupt nicht thematisiert. Vielmehr geht die Kommission allein davon aus, dass eine Pflicht der Dateninhaber, Daten auch Gatekeepern bereitstellen zu müssen, unverhältnismäßig wäre.

hat der EU-Gesetzgeber hier aber einen weiten Entscheidungsspielraum, da es sich um eine komplexe Thematik handelt.[143]

5. Interoperabilität

Schließlich setzt die Verhältnismäßigkeit von Datenteilungspflichten voraus, dass das Teilen von Daten in der Praxis auch funktioniert und nicht etwa an technischen Hürden scheitert. Deshalb sollte der Data Act auch in Bezug auf das Teilen von Daten grundlegende Anforderungen an die Interoperabilität festlegen.[144] Bislang sieht der Data Act Interoperabilitätsregeln nur für Datenräume, Datenverarbeitungsdienste und intelligente Verträge vor.[145] Auch Interoperabilitätsregeln sollten allerdings vorrangig sektorspezifisch festgelegt werden.

6. Besondere Aspekte des Datenzugangs „by design"

Auch die Verpflichtung für Hersteller, vernetzte Produkte so zu designen, dass Nutzer direkt auf die erzeugten Daten zugreifen können, greift in die unternehmerische Freiheit der Hersteller ein, da diese ihre Produkte technisch nicht frei gestalten dürfen [Art. 16 GRCh].[146] Diese Regelung dient ebenfalls maßgeblich dem legitimen Ziel, dem Nutzer mehr Kontrolle über seine Daten zu verschaffen, um ihm die Inanspruchnahme von Reparatur- und anderen Dienstleistungen Dritter und den Dritten das Angebot solcher Dienste zu ermöglichen. Im Rahmen der Abwägung spricht für eine Pflicht zur Gewährung direkten Datenzugangs für den Nutzer, dass dieser ggf. einen wesentlichen Beitrag zur Generierung der Daten geleistet hat. Zudem ist ein freier Direktzugang für den Zugangsberechtigten unkompliziert und effizient, weil der Nutzer die Daten nicht (wie bei den in Art. 4 und 5 Data Act geregelten Datenbereitstellungspflichten)[147] erst anfordern und der Dateninhaber diese bereitstellen muss.[148] Hierdurch wird auch der Dateninhaber, der oft der Hersteller des vernetzten Produkts ist, entlastet. Ein Direktzugang erfordert für den Hersteller jedoch einen hohen Aufwand und ist daher nicht in allen Fällen angemessen, insbesondere wenn der Aufwand das Interesse des Nutzers und dessen Bereitschaft, für Produkte mit Direktzugang einen höheren Preis zu zahlen, übersteigt. Zu Recht sieht der Data Act in Art. 3 Abs. 1 daher ein Korrektiv der Relevanz und Angemessenheit vor. Dieses ist allerdings zu unscharf und dürfte zu Rechtsunsicherheit und Rechtsstreitigkeiten führen. Um die Verhältnismäßigkeit zu wahren, muss daher näher konkretisiert werden, wann die Einrichtung eines Direktzugangs „relevant und angemessen" ist. Zudem muss für bereits auf dem Markt erhältliche vernetzte Produkte eine angemessene Übergangsfrist eingeräumt werden.[149]

7. Informationspflichten

Die Pflicht, den Nutzer über die erzeugten Daten, die Zugriffsmöglichkeiten, den Dateninhaber und die von diesem geplante Eigennutzung oder Weitergabe der Daten zu informieren, beschränkt die unternehmerische Freiheit der Anspruchsverpflichteten. Sie ermöglicht es dem Nutzer jedoch, den Umfang seines Datenzugangsrechts abzuschätzen, den Wert der Daten besser zu beurteilen und so eine informierte Entscheidung über den Erwerb des vernetzten Produkts zu treffen.[150] Die Informationspflicht bildet damit quasi die Vorstufe für eine mögliche Ausübung des Datenzugangsrechts des Nutzers und erleichtert dem Nutzer die Ausübung dieses Rechts. Dies ist insbesondere im B2C-Bereich sachgerecht, denn Verbraucher haben regelmäßig ein Informationsdefizit; ein solches kann aber auch im B2B-Bereich bestehen. Es muss jedoch präzisiert werden, wen die Pflicht trifft (Hersteller, Dateninhaber, Verkäufer), wer dem Nutzer welche Information zu liefern hat und wie der Informationsfluss in der Praxis erfolgen kann.[151] Dies ist auch deshalb wichtig, weil die Verletzung der Informationspflicht behördlich sanktioniert werden kann, was den Eingriff weiter verschärft. Der nötige Erfüllungsaufwand für den Hersteller erscheint jedenfalls dann angemessen, wenn es sich um Massenprodukte handelt, bei denen die bereitzustellenden Informationen nicht von Produkt zu Produkt abweichen, und die zudem eine ausreichend große Fläche für Aufdrucke haben, auf denen sich Informationen anbringen lassen.[152] Um die Verhältnismäßigkeit zu wahren, sollten die Transparenzpflichten aber nicht greifen oder der Verpflichtete die Bereitstellung der Informationen

---

143 Näher zur Kontrolldichte bei Grundrechtseinschränkungen Jarass, a.a.O., Art. 52 Rn. 45ff.

144 So auch Drexl et al., Rn. 67, 219.

145 Vgl. Art. 28-30 Data Act.

146 Ebenso Rammos, T./Wilken, T., Der Data Act- Chancen und Risiken für Unternehmen durch das geplante europäische Datengesetz, DB 2022, S. 1241 (1243).

147 Näher zu den Pflichten des Dateninhabers, dem Nutzer oder einem Dritten Daten bereitzustellen, oben Kap. A. 2.4 und 2.5.

148 Podszun, R./Pfeifer, C., GRUR 2022, S. 953 (956).

149 Siehe bereits ökonomische Bewertung, S. 15.

150 Siehe ökonomische Bewertung, S. 15f.

151 Siehe ökonomische Bewertung, S. 15.

152 Dadurch könnten Informationen den Nutzer auch stets dann erreichen, wenn der Hersteller keinen direkten Kontakt zum Nutzer (Käufer, Mieter, etc.) hat.

zumindest verweigern dürfen, wenn im Einzelfall keine Informationsasymmetrie besteht. Dies kann etwa der Fall sein, wenn der Nutzer – z.B. aufgrund vorangegangener Vertragsverhandlungen – über die Informationen bereits verfügt, oder wenn die ex ante-Bereitstellung der Informationen, etwa die Zusammenstellung aller von einem individuell konzipierten Gerät erzeugten Datenarten, im Einzelfall einen unverhältnismäßigen Aufwand bedeuten würde.

8. Änderungen in Bezug auf das Sui-Generis-Datenbankschutzrecht

Sammlungen von Daten, deren Beschaffung, Überprüfung oder Darstellung wesentliche Investitionen erfordert hat, können gemäß der EU-Datenbankrichtlinie[153] durch das „Sui-Generis"-Recht – ein besonderes geistiges Eigentumsrecht – geschützt sein. Die Regelung in Art. 35 Data Act, wonach dieses Schutzrecht nicht auf Datenbanken anwendbar ist, die bei der Nutzung vernetzter Produkte oder verbundener Dienste erzeugte Daten enthalten, beschränkt die Schutzfähigkeit entsprechender Datenbanken und greift dadurch – entgegen der Auffassung der Kommission[154] – in das geistige Eigentum [Art. 17 Abs. 2] und in die unternehmerische Freiheit [Art. 16 GRCh] der Datenbankhersteller (hier i.d.R. der Dateninhaber) ein. Die Freiheit des geistigen Eigentums umfasst neben einem etwaigen urheberrechtlichen Datenbankschutz auch das Sui-Generis-Recht des Dateninhaber.[155] Diese können ggf. getätigte wesentliche Investitionen nicht mehr amortisieren; zugleich werden Anreize gesenkt, in die Erstellung von IoT-Datenbanken zu investieren. Zwar hat der EuGH den Schutzbereich des Sui-Generis-Rechts für IoT-Daten zunehmend eingeengt[156]; er hat damit jedoch nicht alle Rechtsunsicherheiten beseitigt.[157] Denn die Unterscheidung zwischen einer nicht berücksichtigungsfähigen Investition in die *Erzeugung* von Daten und einer Investition in die *Beschaffung* (Sammlung) von Daten, die zum Datenbankschutz führt, ist schwierig. Unklar ist etwa, ob die Aufzeichnung bereits vorhandener Daten durch Sensoren als Beschaffung gewertet werden und so zum Datenbankschutz führen kann.[158] Die Regelung in Art. 35 Data Act beseitigt die bestehende Rechtsunsicherheit.[159] Die Entscheidung der Kommission, diesen Konflikt zu Lasten der Datenbankhersteller zu lösen und so dem legitimen Interesse der Nutzer und der Wettbewerber auf Zugang zu den IoT-Daten Vorrang vor den Interessen der Datenbankhersteller zu geben, erscheint grundsätzlich gerechtfertigt. Denn die Datenzugangs- und Datennutzungsansprüche des Data Act würden vollständig konterkariert, wenn der Datenbankhersteller deren Erfüllung stets unter Berufung auf sein Sui-Generis-Recht verweigern könnte. Dabei ist auch das Interesse der Allgemeinheit an der Nutzbarkeit der Daten zur Ermöglichung wohlfahrtssteigernder Innovationen in die Abwägung einzubeziehen. Um ein angemessenes Gleichgewicht[160] zu schaffen, würde es als milderes Mittel jedoch ausreichen, im Data Act zu regeln, dass das Sui-Generis-Schutzrecht – soweit es bei IoT-Daten überhaupt besteht – den im Data Act verankerten Ansprüchen auf Datenzugang und -nutzung nicht entgegengehalten werden kann (sog. Einwendungslösung). Nicht erforderlich ist es dagegen, Datenbanken, die IoT-Daten beinhalten, pauschal aus dem Schutzbereich des Sui-Generis-Rechts auszunehmen. Derartige Einschränkungen der Geltung sollten – falls überhaupt so gemeint und politisch erwünscht – im Interesse der Rechtsklarheit besser in der Datenbankrichtlinie selbst geregelt werden.

9. FRAND-Regeln (Kapitel III)

Die Regeln in Kapitel III des Data Act zur Ausgestaltung von Datennutzungsverträgen bei Datenteilungspflichten greifen in die Vertragsfreiheit der Dateninhaber[161] und Datenempfänger ein, weil sie ihren Vertrag im Einklang mit den FRAND-Bedingungen ausgestalten müssen und so bestimmte Bedingungen nicht mehr frei vereinbaren

---

153 Richtlinie 96/9/EG des Europäischen Parlaments und des Rates vom 11. März 1996 über den rechtlichen Schutz von Datenbanken, konsolidierte Fassung abrufbar unter https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:01996L0009-20190606&from=EN.

154 Siehe S. 17 des Kommissionsvorschlags („Die in Kapitel X vorgesehene Änderung des Datenbankrechts sui generis schränkt den darin enthaltenen Schutz des geistigen Eigentums nicht ein.")

155 Specht-Riemenschneider, L., a.a.O. (Studie), S. 5.

156 Hoffmann, A., cepInput Nr. 3/2022, S. 48f. m.w.N, abrufbar unter https://www.cep.eu/eu-themen/details/cep/eu-data-act-cepinput.html.

157 Siehe auch S. 5 des Kommissionsvorschlags zum Data Act.

158 Europäische Kommission, Evaluation of Directive 96/9/EC on the legal protection of databases, 25.04.2018 [SWD(2018) 146], S. 25 m.w.N. Anders als Erwägungsgrund 84 des Data Act suggeriert, geht Art. 35 Data Act damit über eine bloße „Klarstellung" hinaus, dass ein Sui-Generis-Schutz für Datenbanken, die IoT-Daten beinhalten, nicht besteht.

159 Vgl. auch Drexl et al., Rn. 257, die insoweit ebenfalls einen Ausschluss der Anwendbarkeit des Sui-Generis-Schutzrechts befürworten, soweit es mit dem Datenzugangs- und Nutzungsrecht des Data Act kollidiert.

160 Näher dazu EuGH, Urteil vom 3. Juni 2021, Rs. C-762/19, CV-Online Latvia ./. Melons, ECLI:EU:C:2021:434, Rn. 41.

161 Die Regelungen erfassen nur Dateninhaber, die z.B. nach Art. 5 Abs. 1 Data Act gesetzlich verpflichtet sind, einem Datenempfänger Daten bereitzustellen.

dürfen. Die Vertragsfreiheit ist ein zentraler Bestandteil des Grundrechts auf unternehmerische Freiheit.[162] Sie umfasst u.a. die Freiheit, den Vertragspartner zu wählen[163], Verträge inhaltlich auszugestalten[164] und Preise und sonstige Konditionen zu vereinbaren.[165] Der Data Act will durch diese Regeln Fairness bei Verträgen über die gemeinsame Datennutzung gewährleisten.[166]

Allgemeine Grundregeln im Data Act ermöglichen die einheitliche Ausübung solcher Pflichten und verhindern eine Fragmentierung der nationalen Rechtsvorschriften. Die FRAND-Regeln können einen Ausgleich zwischen dem Schutz der Interessen der Dateninhaber und den Interessen Dritter an einer Öffnung der Datensätze bieten und erlauben zudem eine flexible Beurteilung des Einzelfalls.[167] Sie sind daher angesichts der Vielzahl unterschiedlicher Sektoren und Konstellationen, in denen Datenteilungspflichten bestehen können, grundsätzlich sachgerecht.[168] Insbesondere die Regelung, wonach die Vergütung „angemessen" sein muss, ist jedoch noch zu unbestimmt[169] und kann zu einer länger anhaltenden Rechtsunsicherheit bis zu einer Klärung vor allem durch Gerichte und/oder Streitbeilegungsstellen führen. Einerseits kann und darf sie als Regel, die für eine Vielzahl von Datenteilungskonstellationen gelten soll, nicht zu konkret sein. Andererseits ist angesichts der Erfahrungen mit FRAND-Regeln im Zusammenhang mit der Gewährung von Zwangslizenzen für standardessenzielle Patente zu erwarten, dass es zu umfassenden Streitigkeiten über die Angemessenheit der Gegenleistung und damit zu Verzögerungen bei der Bereitstellung von Daten kommen wird.[170] Die Einrichtung alternativer Streitbeilegungsstellen im Data Act ist daher sachgerecht. Um längere Rechtsunsicherheit und eine hohe Auslastung der Streitbeilegungsstellen und Gerichte zu verhindern, sollten die Regelungen jedoch zeitnah präzisiert werden. Dies kann etwa im Rahmen sektorspezifischer Datenzugangsregelungen oder zumindest durch Leitlinien erfolgen.[171] Einen Anhaltspunkt für „faire" Regelungen können auch Mustervertragsklauseln bieten.[172] Dass die Kommission Mustervertragsklauseln für Datenaustauschverträge erarbeiten will[173], ist daher sachgerecht, denn solche Klauseln können Unternehmen, denen es an Erfahrung mangelt, eine praktische Hilfestellung geben, wie faire Datenaustauschvertrag gestaltet werden können. Zudem können sie helfen, die Kosten für den Abschluss solcher Verträge zu senken. Diese Musterklauselsätze sollten auch Ansätze zur Preisgestaltung enthalten.[174]

10. Missbräuchliche Vertragsklauseln gegenüber KMU (Kapitel IV)

Die Regeln in Kapitel IV zur Kontrolle missbräuchlicher Klauseln (auch als „Fairness Test" bezeichnet) greifen ebenfalls in die Vertragsfreiheit insbesondere der Dateninhaber ein, weil diese bestimmte Vertragsklauseln gegenüber KMU nicht mehr frei verwenden dürfen. Legitimer Zweck dieser Regelungen, die sowohl bei Bestehen einer Datenteilungspflicht[175] als auch bei freiwilligem Datenaustausch gelten[176], ist es zum einen, KMU den Zugang zu Daten zu erleichtern[177] und zum anderen, „Fairness" bei Verträgen über die gemeinsame Datennutzung

---

162 EuGH, Urteil vom 22. Januar 2013, C-283/11, ECLI:EU:C:2013:28, Rn. 42 – Sky Österreich, Rn. 80; EuGH, Urteil vom 18.07.2013, Rs. C-426/11, ECLI:EU:C2013:521, Rn. 32 – Alemo-Herron.

163 EuGH, Urteil vom 05.10.1999, C-240/97, ECLI:EU:C:1999:479, Rn. 99 – Spanien/Kommission (bezogen auf das Recht, geschlossene Verträge zu ändern). Siehe auch Bertschek et al., a.a.O., S. 63.

164 EuGH, Urteil vom C-426/11 ECLI:EU:C2013:521, Rn. 33f. – Alemo-Herron; siehe auch Bertschek et al., a.a.O., S. 63.

165 Bertschek et al., a.a.O., S. 63.

166 Kommissionsvorschlag zum Data Act, S. 3, 10.

167 Drexl et al., R. 99, 101.

168 Drexl et al. halten die Anwendung des FRAND-Standards bei horizontalen Regelungen, die auf eine Vielzahl möglicher Datenzugriffsregelungen anwendbar sein sollen, zumindest für „unvermeidbar".

169 Vgl. bereits Ökonomische Bewertung, S. 19. Vgl. auch Hilgendorf, E./Vogel, P., JZ 2022, S. 380 (388). Vgl. auch Gerpott, CR 2022, S. 271 (278), der die FRAND-Regelungen ebenfalls noch für zu abstrakt hält und sich u.a. für eine Einengung der Auslegungsspielräume in Art. 8 Abs. 1 sowie eine „fundamentale Überarbeitung" der Vergütungsregel in Art. 9 Data Act ausspricht.

170 Drexl et al, Rn. 99 ff., 101, 115.

171 S. bereits Ökonomische Bewertung, S. 19. Vgl. auch Drexl et al.Rn. 115 sowie Picht, P./Richter, H., GRUR Int. 2022, S. 395 (398), die in Bezug auf FRAND-Regelungen im EU-Gesetzespaket aus DSA, DMA und DGA eine zeitnahe „best practice guidance" vorschlagen sowie eine Einbeziehung von Interessenvertretern und Datenmittlern fordern, soweit der EU-Gesetzgeber noch nicht in der Lage ist, FRAND-Einzelheiten vorzugeben.

172 Picht, P./Richter, H., GRUR Int, 2022, S. 395 (397f.), bezogen auf das EU-Gesetzgebungspaket aus DSA, DMA und DGA; Hilgendorf, E./Vogel, P, a.a.O., S. 388.

173 Art. 34 Data Act, vgl. A. 4,

174 Picht, P./Richter, H., a.a.O., S. 398.

175 Die Regeln gelten damit über Art. 8 Abs. 2 auch für Verträge nach Kapitel III (unter Geltung der FRAND-Bestimmungen).

176 Drexl et al., Rn. 119.

177 Erwägungsgrund 36 Data Act.

zu gewährleisten.[178] Insbesondere will die Kommission verhindern, dass Vertragsparteien Ungleichgewichte in der Verhandlungsposition zum Nachteil der jeweils schwächeren Partei missbrauchen.[179]

Der Eingriff ist zum einen dahingehend begrenzt, dass der Klauselkontrolle nur solche Klauseln unterliegen, die gegenüber KMU verwendet werden. Größere Unternehmen – oder Verbraucher, für die allein die EU-Klauselrichtlinie gilt – können sich damit nicht auf die Regeln in Kapitel IV des Data Act berufen. Zum anderen erstreckt sich die Kontrolle nur auf Vertragsklauseln über den Zugang und die Nutzung von Daten und auf Klauseln, die die Haftung oder Rechtsbehelfe bei Verletzung oder Beendigung datenbezogener Pflichten betreffen. Sie gilt somit insbesondere nicht für Klauseln über den Hauptgegenstand des Vertrags oder den Preis, die frei verhandelbar bleiben. Auch ausgehandelte Klauseln werden nicht erfasst, d.h. die Möglichkeit, Klauseln frei auszuhandeln, bleibt bestehen. Schließlich bleibt bei Missbräuchlichkeit einer Klausel der Vertrag im Übrigen wirksam.

Um das Bestimmtheitsgebot zu wahren, müssen die Regelungen zur Klauselkontrolle und vor allem die Generalklausel des Art. 13 Abs. 2 Data Act jedoch konkretisiert werden. Dass der Data Act eine Generalklausel enthält, steht dem Bestimmtheitsgebot zwar nicht generell entgegen. Denn es ist unmöglich, alle potenziell missbräuchlichen Klauselfälle zu antizipieren und zu regeln. Die Generalklausel in Art. 13 Abs. 2 ermöglicht Flexibilität, weil sie auch vergleichbare Klauseln erfasst, die nicht in der schwarzen oder grauen Liste ausdrücklich geregelt sind. Ihr kommt somit eine Auffangfunktion zu; zugleich ermöglicht sie eine Fortbildung des Rechts. Generalklauseln werden aus diesen Gründen im EU-Recht bereits verwendet, etwa in der EU-Klauselrichtlinie[180] und in der Richtlinie 2005/29/EG über unlautere Geschäftspraktiken.[181] Der EuGH hat die Generalklauseln als solche in seinen zahlreichen Urteilen zu beiden Richtlinien nicht beanstandet. Die Verwendung einer Generalklausel als Auffangklausel neben einer schwarzen und grauen Liste mit näher geregelten missbräuchlichen Klauseln ist daher grundsätzlich geeignet, das Ziel, faire Verträge über Datenzugang und Datennutzung zu schaffen, zu erreichen und die Stellung von KMU in Vertragsverhandlungen zu verbessern. Jedoch werden die Kriterien für die Beurteilung der Missbräuchlichkeit im Data Act – anders als in der EU-Klauselrichtlinie – nicht hinreichend definiert. Zwar wird die allgemeine Generalklausel im Data Act in gewisser Weise dadurch konkretisiert, dass die aufgelisteten schwarzen und grauen Klauseln „als Maßstab für die Auslegung“ und Bestimmung der Missbräuchlichkeit nach der Generalklausel dienen sollen.[182] Aus der Formulierung in Art. 13 Abs. 3 und 4, wonach die gelisteten Klauseln in der Liste „im Sinne dieses Artikels“ (d.h. im Sinne der Generalklausel) missbräuchlich sind bzw. als missbräuchlich gelten, ergibt sich, dass die gelisteten Klauseln Beispiele für eine grobe Abweichung „von der guten Geschäftspraxis beim Datenzugang und der Datennutzung“ bzw. für einen Verstoß „gegen das Gebot von Treu und Glauben und den redlichen Geschäftsverkehr“ darstellen. Dies reicht jedoch nicht aus.[183] Die genannten unbestimmten Rechtsbegriffe sind zu vage und sollten soweit möglich konkretisiert werden. Insbesondere sollte – wie bei der EU-Klauselrichtlinie – näher geregelt werden, welche Aspekte bei der Beurteilung der Missbräuchlichkeit und von „Treu und Glauben“ und der Redlichkeit des Geschäftsverkehrs zu berücksichtigen sind.[184] Zudem muss der Data Act einen Referenzmaßstab für die Auslegung der Generalklausel festlegen.[185] Dies gilt auch für die Liste der „grauen“ Klauseln, die ebenfalls unbestimmte und damit auslegungsbedürftige Rechtsbegriffe enthält, die durch die Rechtsprechung der nationalen Gerichte und letztverbindlich durch den EuGH ausgelegt und so konkretisiert werden müssten. Aber selbst dann könnte es mehrere Jahre dauern, bis hinreichende Rechtssicherheit besteht, deren Schaffung zu den Zielen des Data Act gehört.[186]

Ferner sind die Regelungen zur Klauselkontrolle in der vorgeschlagenen Form auch unverhältnismäßig. Zwar ist das Ziel des EU-Gesetzgebers, KMU ähnlich wie Verbraucher zu schützen, legitim und wegen des weiten Entscheidungsspielraums des EU-Gesetzgebers zu akzeptieren. Zudem sind die Regelungen zwar grundsätzlich geeignet, KMU, die Daten nutzen wollen, zu faireren Verträgen zu verhelfen und ihre Teilnahme auf den Anschlussmärkten vernetzter Produkte zu unterstützen. Denn auch in B2B-Verhältnissen kann die Verhandlungsmacht

[178] Kommissionsvorschlag zum Data Act, S. 3, 10.
[179] Kommissionsvorschlag zum Data Act, S. 6.
[180] Richtlinie 93/13/EWG vom 5.4.1993 über missbräuchliche Klauseln in Verbraucherverträgen (s. Fußnote 34).
[181] Richtlinie 2005/29/EG über unlautere Geschäftspraktiken.
[182] Erwägungsgrund 55.
[183] Siehe bereits die Ausführungen zur Verhältnismäßigkeit gegenüber den Mitgliedstaaten (oben S. 21f.).
[184] Siehe Erwägungsgründe 15ff. sowie Art. 4 der EU-Klauselrichtlinie 93/13/EWG.
[185] Siehe bereits die Ausführungen zur Verhältnismäßigkeit gegenüber den Mitgliedstaaten (oben S. 21f.).
[186] Kommissionsvorschlag zum Data Act, S. 3.

ungleich verteilt sein, z.B. wenn eine Partei entscheidend von Daten abhängt, die von einer anderen kontrolliert werden.[187]

Die Regelungen sind jedoch erstens dann nicht erforderlich und sollten daher nicht gelten, soweit ein strukturelles Ungleichgewicht in der Verhandlungsmacht zwischen dem Verwender der Klauseln und dem KMU im Einzelfall nicht vorliegt.[188] An einem Ungleichgewicht und damit am Missbrauch einer stärkeren Verhandlungsposition dürfte es regelmäßig fehlen, wenn gleichrangige KMU untereinander Verträge schließen, formal gelten die Regelungen aber auch dann.[189] Zudem sollten Vertragsklauseln im B2B-Bereich nicht schon bei jeglicher Ungleichheit der Verhandlungsposition als missbräuchlich gelten, sondern – wie bei der EU-Klauselrichtlinie – nur dann, wenn die die Klausel ein erhebliches und ungerechtfertigtes Missverhältnis der vertraglichen Rechte und Pflichten zum Nachteil des Vertragspartners verursacht. Dies wäre der Fall, wenn der Verwender die rechtliche Stellung des Vertragspartners durch die Klausel hinreichend schwer beeinträchtigt[190] bzw. diesen unangemessen benachteiligt und seine ungleich stärkere Machtposition so „missbraucht". Dass der Data Act einen Missbrauch der Verhandlungsmacht zum Nachteil der schwächeren Partei voraussetzt, klingt auf Seite 6 und in Erwägungsgrund 54[191] an, sollte aber klarer gefasst und in den Gesetzestext aufgenommen werden.[192] Auch sollte ergänzt werden, dass das Maß der tatsächlichen Diskrepanz in der Verhandlungsmacht und der von beiden Seiten geleistete Beitrag an der Erzeugung der Daten im Rahmen des Merkmals „Treu und Glauben" berücksichtigt werden müssen. Auch wenn Art. 13 neutral formuliert ist, sollte zudem klargestellt werden, dass KMU auch als Dateninhaber Schutz genießen, wenn ihnen von einem verhandlungsstärkeren Dritten missbräuchliche Klauseln auferlegt werden.[193] Zudem erfassen die Regeln zur Klauselkontrolle nicht alle Fälle, in denen Vertragspartner Ungleichgewichte in der Verhandlungsposition zum Nachteil schwächerer Parteien missbrauchen. Die EU-Gesetzgeber sollten berücksichtigen, dass auch ein großes Unternehmen der Verhandlungsmacht eines kleinen Dateninhabers ausgeliefert und damit schutzbedürftig sein kann, wenn dieser z.B. wichtige Daten in einem Nischenmarkt kontrolliert.[194]

Zweitens ist auch das zusätzliche Erfordernis für die Anwendbarkeit der Klauselkontrolle unangemessen, wonach der Klauselnehmer (das KMU) einen gescheiterten Verhandlungsversuch unternommen haben muss. Die Klauselkontrolle ist anwendbar, wenn der Verwender einem KMU eine Klausel einseitig auferlegt hat, was dann vermutet wird, wenn das KMU die Klausel nicht beeinflussen konnte, obwohl es dies in einem Verhandlungsversuch versucht hatte.[195] Damit könnten KMU letztlich nur dann Schutz gegen missbräuchliche Klauseln nach Kapitel IV des Data Act genießen, wenn sie die Klauseln nicht ohne weiteres akzeptieren, sondern einen Versuch gestartet haben, die Klausel(n) im Wege der Verhandlung zu beeinflussen.[196] Dieses Erfordernis eines Verhandlungsversuchs ist nicht nur für KMU nachteilig, deren Schutz so eingeschränkt wird. Die Klauselkontrolle zugunsten von KMU wäre dann seltener anwendbar als die Klauselkontrolle zugunsten von Verbrauchern nach der EU-Klauselrichtlinie, welche dieses zusätzliche Erfordernis nicht enthält.[197] Das Erfordernis eines Verhandlungsversuchs erscheint für KMU zudem unpraktikabel, wenn der Verwender lediglich eine Vertragsschlussmöglichkeit per Klick-Button vorsieht.[198] Es belastet aber auch den Klauselverwender, dem eine Vielzahl von Verhandlungsanfragen

---

187 Drexl et al, Rn. 120.

188 Auch die Kommission rechtfertigt die Regelungen letztlich mit einem Missbrauch vertraglicher Ungleichgewichte, vgl. etwa Erwägungsgründe 2 und 5 Data Act.

189 Siehe bereits Ökonomische Bewertung, S. 20.

190 Leitlinien der EU-Kommission zur Auslegung und Anwendung der Richtlinie 93/13/EWG, ABl. (EU) Nr. C-323 vom 27.09.2019, S. 4ff., Ziffer 3.4.2. m.w.N. zur zugrundeliegenden Rechtsprechung des EuGH.

191 Nach EG 54 sollte die Klauselkontrolle nur auf überzogene Vertragsbedingungen angewandt werden, bei denen eine stärkere Verhandlungsposition missbraucht wird. Auch laut S. 6 des Kommissionsvorschlags zum Data Act will die Kommission das Vertragsrecht deshalb ändern, um den Missbrauch von Ungleichgewichten in der Verhandlungsposition zum Nachteil schwächerer Parteien zu verhindern.

192 Evtl. könnte die Annahme, dass ein KMU, dem Klauseln auferlegt werden, eine verhandlungsschwächere Position innehat, zumindest als bloße (widerlegbare) Vermutung ausgestaltet werden.

193 Ebenso Drexl et al., Rn. 54.

194 Ebenso Drexl et al., Rn. 125, der zu Recht darauf hinweist, dass wirtschaftliche Abhängigkeit nicht zwingend Größenunterschiede zwischen den Beteiligten voraussetzt. Aus diesem Grund hat Deutschland bei der Kartellrechtsreform 2021 mit dem GWB-Digitalisierungsgesetz das vergleichbare einschränkende KMU-Kriterium in § 20 Abs. 1 GWB abgeschafft, vgl. Gesetzentwurf der deutschen Bundesregierung zum GWB-Digitalisierungsgesetz, BT-Drucks. 19/23492 vom 19.10.2020, S. 78.

195 Art. 13 Abs. 5 Data Act und Erwägungsgrund 52. Näher zu den Regelungen siehe oben Kapitel A.4.

196 Davon gehen auch Drexl et al., Rn. 122f. aus.

197 Vgl. Auch Drexl et al., Rn. 122.

198 Drexl et al., Rn. 123, halten die höheren Anwendungsvoraussetzungen für die Klauselkontrolle daher für unangemessen und schlagen Drexl et daher eine Lösung wie bei der EU-Klauselrichtlinie 93/13/EWG vor.

von KMU drohen, die sich den durch die Klauselkontrolle verbürgten Schutz erhalten wollen.[199] Zudem ist unklar, wann ein hinreichender Verhandlungsversuch zu bejahen ist und wer die Beweislast für das Vorliegen bzw. Fehlen eines Verhandlungsversuches trägt.[200] Dies schafft zusätzliche Rechtsunsicherheit. Zwar ermöglicht der Data Act es dem Klauselverwender ausdrücklich, die gesetzliche Vermutung der einseitigen Auferlegung zu widerlegen und nachzuweisen, dass die Klausel nicht einseitig auferlegt wurde.[201] Hierzu könnte er entweder – wie auch bei der EU-Klauselrichtlinie – positiv nachweisen, dass die betreffende Klausel ausgehandelt wurde. Unklar ist aber, ob er alternativ auch das Fehlen eines Verhandlungsversuchs von Seiten des KMU nachweisen kann bzw. muss. Hierzu müsste er aber u.U. darlegen, dass das KMU die Klausel(n) hätte beeinflussen können, sie aber „akzeptiert" und z.B. gar nicht zu verhandeln versucht hat. Einen solchen Negativbeweis des fehlenden Verhandlungsversuchs für jede einzelne Klausel führen zu müssen, erscheint aber schwierig und ist daher unangemessen.[202] Anstatt zu versuchen, den Eingriff in die Rechte der Dateninhaber durch das vage Zusatzerfordernis eines gescheiterten Verhandlungsversuchs abzumildern, sollten die EU-Gesetzgeber die Klauselkontrolle lieber dadurch einschränken, dass sie für ihre Anwendung konsequent ein strukturelles Ungleichgewicht in der Verhandlungsmacht der Parteien verlangen (s.o.).

Dass die „grauen Klauseln" lediglich als missbräuchlich „gelten", impliziert, dass die dahintersteckende Vermutung der Missbräuchlichkeit bei „grauen" Klauseln vom Verwender widerlegt werden kann. Dies ist sachgerecht, da die grauen Klauseln allesamt unbestimmte, auslegungsfähige Rechtsbegriffe enthalten (z.B. „unangemessene Beschränkung", „erheblich schadet"); der Data Act sollte diese aber unbedingt präzisieren (s.o.).

11. Verhältnis zur DSGVO

Damit der Data Act seine Wirkung entfalten und die Datennutzung in der EU tatsächlich fördern kann, müssen bestehende Rechtsunsicherheiten im Zusammenhang mit der DSGVO beseitigt werden, die auch bei untrennbaren Mischdatensätzen aus personenbezogenen und nicht-personenbezogenen Daten Anwendung findet. Datenschutzrechtliche Bedenken und Grauzonen gehören zu den von Unternehmen am meisten genannten rechtlichen Hindernissen für den Handel mit Daten und die Entstehung nachgelagerter Datenmärkte.[203] Dass der Data Act der DSGVO Vorrang einräumt[204], ist sachgerecht, für die Beseitigung der Rechtsunsicherheit aber nur wenig hilfreich. Um den Datenaustausch tatsächlich zu erleichtern, muss erstens geklärt werden, ab wann Daten als anonymisiert[205] gelten und die Anwendbarkeit der DSGVO daher ausgeschlossen ist. Hier sollte die EU schnellstmöglich eine Lösung anstreben, etwa durch Unterstützung der Entwicklung von Standards, bei deren Einhaltung ein hinreichender Anonymisierungsgrad vermutet wird.[206] Findet die DSGVO Anwendung, sollte den Unternehmen zweitens zumindest durch Leitlinien Hilfestellung gegeben werden, auf welche Rechtsgrundlage das Teilen und Nutzen von Daten gestützt werden kann. Denn die DSGVO erlaubt eine zweckändernde Weiterverarbeitung von Daten nur unter engen Bedingungen, und die Einholung von Einwilligungen ist oft unpraktikabel und mit Unsicherheiten verbunden. So sollte z.B. ausdrücklich klargestellt werden, ob die Bereitstellung von Daten durch den Dateninhaber nach den Art. 3-5 Data Act durch Art. 6 Abs. 1 lit c DSGVO (Verarbeitung zur Erfüllung einer Rechtspflicht) gedeckt ist. Um das Teilen von Daten rechtssicher zu ermöglichen, könnten zudem punktuelle Anpassungen der DSGVO in engen Grenzen sinnvoll sein.[207] Weil die Datenzugangsansprüche nach DSGVO und Data Act nicht deckungsgleich sind – insbesondere erfolgt die Portierung an Dritte nach Art. 20 DSGVO stets kostenlos, während der Dritte nach dem Data Act eine Vergütung verlangen kann – entstehen zusätzliche

---

199 Drexl et al, Rn. 123.

200 Muss etwa der Verwender auch den fehlenden Verhandlungsversuch des KMU belegen, um nachzuweisen, dass die Klausel nicht einseitig auferlegt wurde? Oder greift die gesetzliche Vermutung, dass die Klausel dem KMU einseitig auferlegt wurde, erst, wenn das KMU seinerseits einen Verhandlungsversuch nachweist?

201 Art. 13 Abs. 5 Data Act. Näher zu den Regelungen siehe oben Kapitel A.4.

202 So wohl auch Efroni et al. (Weizenbaum Institute), a.a.O., S. 14.

203 Röhl, K.-H./Bolwin, L./Hüttl, P., Datenwirtschaft in Deutschland – Wo stehen die Unternehmen in der Datennutzung und was sind ihre größten Hemmnisse?, Studie des Instituts der deutschen Wirtschaft (iw) im Auftrag des BDI, 24.02.2021, S. 4, 40f., abrufbar unter https://www.iwkoeln.de/studien/klaus-heiner-roehl-lennart-bolwin-wo-stehen-die-unternehmen-in-der-datennutzung-und-was-sind-ihre-groessten-hemmnisse.html.

204 Siehe Art. 1 Abs. 3 und Erwägungsgrund 7 Data Act sowie oben Kapitel A. 2.6].

205 Laut Erwägungsgrund 26 findet die DSGVO auf anonymisierte Daten keine Anwendung.

206 Ebenso Specht-Riemenschneider, L., a.a.O. (BT-Drs. 19/26450) et S. 5, 16 f.

207 Ebenso, wenn auch bezogen auf den Data Governance Act, Veil, W., Data Governance Act II: Datenmittler, CR-online.de Blog vom 11.10.2021, abrufbar unter https://www.cr-online.de/blog/2021/10/11/in-der-datenschutzrechtlichen-todeszone-der-data-governance-act-teil-ii/. Für partielle Modifikationen der DSGVO insoweit auch Specht-Riemenschneider, L., a.a.O. (BT-Drs. 19/26450) et S.16f.

Abgrenzungsprobleme. Der Data Act sollte daher drittens sicherstellen, dass die Abgrenzung praxistauglich machbar ist und nicht zu weiterer Rechtsunsicherheit führt.[208]

12. Förderung des freiwilligen Datenaustauschs

Die EU-Gesetzgeber sollten auch den freiwilligen Datenaustausch im B2B-Bereich stärker fördern. Der freiwillige Datenaustausch wird vom Data Act bislang nur rudimentär erfasst, und zwar insoweit, als die Kommission Mustervertragsklauseln ankündigt und das Kapitel IV zur Missbrauchskontrolle von Klauseln auch für freiwillige Datenaustauschverträge gilt. Die Erarbeitung von Mustervertragsklauseln durch die Kommission kann auch den freiwilligen Datenaustausch wesentlich erleichtern und ist daher auch unter diesem Aspekt sachgerecht. Musterklauseln können Unternehmen zudem helfen, die Kosten für den Abschluss der nötigen Verträge zu senken. Angesichts der großen Unterschiede zwischen den einzelnen Sektoren der Datenwirtschaft sind aber anstelle eines Einheits-Klauselsatzes verschiedene sektorspezifische Musterklauselsätze vorzuziehen. Die Kommission sollte daher zügig für möglichst viele Wirtschaftszweige spezifische praxistaugliche Klauselsätze erarbeiten und vorschlagen. Ausgewogene Musterklauselsätze und ergänzende freiwillige Regeln in wichtigen Bereichen können Datenteilungspflichten zwar nicht durchweg ersetzen. Sie können es aber u.U. ermöglichen, diese Pflichten enger zu fassen und die Vertragsfreiheit so in weiterem Umfang zu erhalten. Um mehr Vertrauen in den Datenaustausch zu schaffen, muss zudem die Entwicklung sicherer Plattformen und praktikabler Kontrollinstrumente in Bezug auf die erlaubte Nutzung der Daten weiter gestärkt werden.

D. Fazit

Die EU-Kommission hat mit dem Data Act einen ambitionierten und tiefgreifenden horizontalen und damit sektorübergreifenden Rechtsakt vorgelegt, um den Zugang zu und die Nutzung von IoT-Daten für Nutzer von vernetzten Produkten und verbundenen Diensten und die Weitergabe dieser Daten an Dritte zu erleichtern. Zentrales Ziel ist es hierbei, die Nutzung von Daten als Ressource für die Sicherung des ökologischen und des digitalen Wandels zu unterstützen. Es ist notwendig und sachgerecht, den Zugang zu und die Nutzung von (IoT-)Daten in der EU zu fördern. Der Vorschlag der Kommission ist aber in mehrfacher Hinsicht nicht zielführend.

Erstens: Die Herangehensweise der Kommission, über alle vernetzten Produkte und Nutzergruppen (B2C und B2B) hinweg einheitliche „horizontale" Vorschriften zur Datennutzung und -weitergabe festzulegen, ist nicht zielführend. Denn ein großflächiges Marktversagen besteht nicht. Allenfalls in B2C-Szenarien ließe sich ein solches feststellen, sodass Datenzugangsansprüche für Verbraucher gerechtfertigt sein können, etwa aufgrund inhärenter Informationsasymmetrien. Eine allgemeine Datenteilungspflicht ist auch rechtlich unverhältnismäßig. Die EU-Gesetzgeber sollte sich für einen differenzierenden, sektorspezifischen Regulierungsansatz stark machen.

Zweitens: Der Geltungsbereich des Data Act ist nicht hinreichend klar geregelt. Rechtsunsicherheit besteht nicht nur bezüglich der Adressaten der Regulierung, sondern auch bezüglich der erfassten vernetzten Produkte und verbundenen Dienste. In seiner jetzigen Fassung wirft der Geltungsbereich jedenfalls mehr Fragen auf, als er Antworten liefert und schafft damit, sowohl für jene Akteure, die Daten bereitstellen müssen als auch für jene, die sie nutzen dürfen, veritable Schwierigkeiten in der Rechtsanwendung.

Drittens: Die vorgesehene Möglichkeit der Weitergabe von IoT-Daten an Dritte kann zwar zur Innovationsfähigkeit von Anbietern von Anschlussdiensten beitragen und Markteintritte auf diesen Märkten fördern. Andererseits bremst sie jedoch auch die Eigenleistung des (potenziellen) Anbieters von Anschlussdiensten aus und kann ihn zu simplem Trittbrettfahrer-Verhalten einladen. Zudem schmälert sie den Wert getätigter Investitionen in die Nutzbarmachung von IoT-Daten für den Dateninhaber. Im Ergebnis kann dies dazu führen, dass dieser weniger gewillt ist, auch künftig in die Vernetztheit seiner IoT-Produkte zu investieren.

Viertens: Die im Data Act vorgesehenen Nutzungsbeschränkungen für Nutzer und Dritte in Bezug auf die Daten sind sachgerecht, reichen aber in der vorgesehenen Form nicht aus. Insbesondere das Verbot, Daten zur Entwicklung von Konkurrenzprodukten zu nutzen, ist zu vage; unklar ist aber u.a. auch, wann Dritte die Daten an andere Dritte weitergeben dürfen, um einen vom Nutzer gewünschten Dienst erbringen zu können. Um den Eingriff in die unternehmerische Freiheit der Dateninhaber verhältnismäßig zu gestalten, müssen zudem hinreichende Kontrollmöglichkeiten geschaffen werden, um das Risiko eines Missbrauchs von Daten und

[208] Näher zu möglichen praktischen Problemen etwa Rammos, T./Wilken, T, DB 2022, S. 1241 (1246).

Geschäftsgeheimnissen zu senken. Präzisiert werden muss auch, welche technischen Schutzmaßnahmen des Dateninhabers angemessen sind, um einen unbefugten Zugang zu den Daten zu verhindern.

Fünftens: Die Regelungen zur Kontrolle missbräuchlicher Vertragsklauseln im B2B-Bereich sind verbesserungswürdig. Die vorgeschlagene Generalklausel ermöglicht Flexibilität und Rechtsfortbildung. Es muss aber konkretisiert werden, welche Aspekte bei der Beurteilung der Missbräuchlichkeit anhand der zahlreichen unbestimmten Rechtsbegriffe zu berücksichtigen sind. Zudem sollte die Klauselkontrolle wie bei der gegenüber Verbraucher geltenden EU-Klauselrichtlinie 93/13/EWG nur greifen, wenn tatsächlich ein Ungleichgewicht in der Verhandlungsmacht der Parteien vorliegt und die Klausel ein erhebliches Missverhältnis der vertraglichen Rechte zum Nachteil des Vertragspartners verursacht.

Sechstens: Die Regeln zur Durchsetzung des Data Act sind noch unzureichend. Ob die behördliche Durchsetzung bei allen Bestimmungen des Data Act erforderlich ist, sollten die EU-Gesetzgeber noch genauer prüfen. Obwohl die Gewährung der Datenzugangsrechte durch zahlreiche vertragsrechtliche Regelungen flankiert wird, bleibt das Verhältnis zur privatrechtlichen Durchsetzung unklar. Es bedarf jedoch einer näheren Abstimmung zwischen behördlicher und privatrechtlicher Durchsetzung. Auch muss genauer geregelt werden, welche nationale Behörde in welchen Fällen für die Durchsetzung zuständig ist.