Datenzugang bei smarten Produkten nach dem Entwurf für ein Datengesetz (Data Act)

Rechtliche Rahmenbedingungen für die Vertragsgestaltung

Prof. Dr. Bernd J. Hartmann / Prof. Dr. Mary-Rose McGuire / Prof. Dr. Hans Schulte-Nölke*

Die Europäische Kommission spricht der Nutzung von Daten ein erhebliches wirtschaftliches Potential zu und nennt als Beispiel, dass in den Sektoren Verkehr, Gebäude und Industrie allein aufgrund der Verfügbarkeit von Echtzeitdaten ein Einsparvolumen zwischen 10 und 20 % besteht. Für andere Bereiche, wie zB den Gesundheits- und Agrarsektor, werden auch die Innovationsförderung und der schonende Ressourceneinsatz und damit die Stärkung der Nachhaltigkeit als Ziel benannt. Um dieses Potential zu realisieren, sollen allen Marktteilnehmern, insbesondere auch den Kleinstunternehmen sowie kleineren und mittleren Unternehmen, hochwertige Daten zur Verfügung stehen. Diesen Zugang zu Daten soll das sogenannte Datengesetz (Data Act) schaffen, das gleichermaßen auf Access-by-Design wie auch auf vertragliche Nutzungsberechtigungen setzt. Wenngleich mit einer Verabschiedung erst Ende 2023 oder 2024 gerechnet wird, sollten sich Unternehmen mit Blick auf die langen Vorlaufzeiten in der Produktentwicklung schon jetzt an den Kategorien des Data Act orientieren, um einerseits die technischen Voraussetzungen zu schaffen, andererseits die Vertragsbeziehungen entsprechend zu ordnen.

I. Der Data Act im Kontext der Europäischen Datenstrategie

1 Mit der Datenstrategie[1] hat die Europäische Kommission angekündigt, einen verlässlichen Rechtsrahmen für eine europäische Datenwirtschaft zu schaffen. Dabei soll die Umsetzung durch unterschiedliche Rechtsakte erfolgen, die mit Blick auf Normadressaten, Regelungsgegenstand und zeitliche Abfolge eine große Bandbreite

aufweisen. Bereits in Kraft getreten sind der *Data Governance Act* (DGA)[2] und die *Free Flow of Data-VO* (FFD-VO).[3]

2 Der DGA und die FFD-VO zielen auf die Schaffung eines Binnenmarktes von Daten ab. Dabei will der DGA die Bereitstellung von Daten durch die sichere Datenweitergabe durch die öffentliche Hand, Datenpools und den Datenaltruismus durch einen sicheren Rechtsrahmen fördern. Die FFD-VO sucht die Segmentierung des Binnenmarktes durch Verbote zu verhindern.

3 Regelungsgegenstand des DGA ist primär die Bereitstellung von Daten durch die öffentliche Hand, die nicht der *Open Data-RL*[4] unterliegen.[5] Für diese schutzbedürftigen Daten werden Rahmenbedingungen geschaffen, um zu verhindern, dass die Weitergabe durch die öffentliche Hand geschäftliche oder statistische Interessen, den Schutz von Geistigem Eigentum oder von personenbezogenen Daten beeinträchtigt (vgl. Art. 3 I DGA). Die sogenannte „sichere Weitergabe" durch öffentliche Stellen wird durch Anonymisierung, Aggregation, sichere Bereitstellungsverfahren, technisch-organisatorische Maßnahmen sowie vertragliche Vereinbarungen gewährleistet (vgl. Art. 5 III, IV, X DGA). Um eine Beeinträchtigung des fairen Wettbewerbs durch selektiven Zugang zu vermeiden, werden ein Verbot der exklusiven

Bereitstellung an einzelne Marktteilnehmer sowie das Gebot der Transparenz und Nichtdiskriminierung für die Weiterverwendung vorgesehen (Art. 5 I 1, II DGA). Daneben enthält der DGA einen Rahmen für Datenvermittlungsdienste sowie datenaltruistische Einrichtungen, der allerdings weder von der Rechtfertigung für die Verarbeitung von personenbezogenen Daten nach der Datenschutzgrundverordnung (DS-GVO) noch von der Berechtigung zur Nutzung von nicht-personenbezogenen Daten nach dem Entwurf des geplanten *Data Act*[6] dispensiert (vgl. ErwG 3 S. 5, 4 S. 1 DGA).

4 Ergänzt wird der DGA durch die FFD-VO. Sie verbietet den Mitgliedstaaten, durch Datenlokalisierungsmaßnahmen die grenzüberschreitende Verarbeitung von nicht-personenbezogenen Daten zu untersagen, da solche Beschränkungen die Entwicklung des *Internet of Things* sowie moderner Cloud-Systeme verhindern könnten.[7] Umgekehrt soll der freie Datenverkehr die Optimierung von Unternehmensabläufen sowie die Wettbewerbsfähigkeit von europäischen Mitbewerbern gegenüber anderen Wirtschaftsregionen stärken. Nur wenn Unternehmen ihre Dienste im gesamten Binnenmarkt anbieten, können Unternehmen die Angebote verschiedener Wettbewerber nutzen. Durch Vorgaben zur Datenportabilität unterstützt, wird ihnen dadurch mehr Flexibilität für ihr Datenmanagement gewährt und die schnellere Anpassung an die Erfordernisse der digitalen Wirtschaft gefördert. Wenngleich primär an die Mitgliedstaaten adressiert, enthält die FFD-VO eine Reihe von Definitionen und Beispiele, die auch für die Auslegung anderer Rechtsakte von Bedeutung sein könnten. Hervorzuheben sind insbesondere die Regelung der „untrennbaren Verbindung" von personenbezogenen und nicht personenbezogenen Daten (*mixed data*) in Art. 2 II 2 FFD-VO und die Beispiele für nicht-personenbezogene Daten (vgl. ErwG 9 FFD-VO).[8]

5 Obwohl auch der geplante *Data Act* (DA-E) mit den Pflichten zur Bereitstellung im Verhältnis *business to government* (B2G) eine Schnittstelle und Ergänzung zum DGA vorsieht, ist er doch in in erster Linie an die Wirtschaft adressiert, d.h. den Datenaustausch *business to business* (B2B) und *business to consumer* (B2C).[9] Dabei zielt der DA-E primär auf Daten, die durch mit dem *Internet of Things* vernetzte Produkte erzeugt werden, sowie auf Industriedaten und regelt, wer darauf zugreifen darf. Entgegen der ursprünglich bestehenden Erwartung, beschränkt sich der Anwendungsbereich des DA-E allerdings nicht auf reine Maschinendaten, sondern umfasst personenbezogene und nicht personenbezogene Daten gleichermaßen.

6 Die zivilrechtlich relevanten Fragen der Zuordnung, der Nutzungsberechtigung an Daten sowie die Rechtsfolgen von Verstößen gegen gesetzliche oder vertragliche Beschränkungen werden daher in Zukunft durch das Zusammenspiel von DS-GVO und *Data Act* normiert. Gemeinsam ist beiden Rechtsakten, dass sie das faktische Monopol der Dateninhaber dadurch aufbrechen, dass die Nutzung eine Rechtfertigung (DS-GVO) bzw. Zustimmung des Nutzers (DA-E) erfordert. Die beiden VO sind nebeneinander anwendbar, stimmen jedoch allenfalls in der konzeptionellen Grundlage überein, wohingegen bei Definitionen, Rechten und Pflichten sowie den Rechtsfolgen von Verstößen deutliche Unterschiede bestehen. Sie sind der unterschiedlichen Regelungstechnik von DS-GVO (insbesondere behördli-

che Regulierung) und *Data Act* (Vertragsrecht) geschuldet. Das beiden Rechtsakten gemeinsame Ziel eines einheitlichen europäischen Datenraums beschränkt sich auf die territoriale Reichweite, während die jeweils anwendbaren Regelungen von der Art der Daten abhängen und bei *mixed data* die Vorgaben beider Rechtsakte beachtet werden müssen.

7 Für das Verständnis des Gesamtkonzepts von Bedeutung ist zudem einerseits der *Digital Markets Act* (DMA),[10] der die vom Zugangsrecht nach dem DA-E ausgeschlossenen *gatekeeper* definiert.[11] Andererseits sind auf vertragsrechtlicher Ebene die Warenkauf-RL[12] und die Digitale-Inhalte-RL[13] von Bedeutung, da die Vertragspartner dieser Verträge in der Regel auch Dateninhaber und -nutzer iSd *Data Act* sind, die Zugangsrechte beanspruchen können.

II. Regulativer Ansatz & weiteres Verfahren

8 Der Entwurf des *Data Act* (sog. „Datengesetz") ist als Verordnung konzipiert, die verbindlich festlegt, wer Daten sammeln und nutzen darf. Durch Datenzugangsrechte soll das Innovationspotential gehoben bzw. einer Fehlmonopolisierung[14] vorgebeugt werden. Die EU-Kommission rechnet mit einem Einsparvolumen in den Sektoren Verkehr, Gebäude und Industrie aufgrund der Verfügbarkeit von Echtzeitdaten von 10–20 %.[15] Schon die Beispiele weisen darauf hin, dass der *Data Act* einen horizontalen, sektorübergreifenden Ansatz verfolgt, wobei die EU-Kommission bereits jetzt auf die mögliche Erforderlichkeit von Sonderregelungen für einzelne Sektoren hinweist.[16]

9 Als unmittelbar anwendbares Recht tritt die Regelung neben das bestehende nationale Recht, wobei sie durch ihre Konzeption Daten (bzw. die Möglichkeit zu deren Nutzung) als ein handelbares Gut definiert und insoweit das Sachenrecht bzw. Immaterialgüterrecht ergänzt, während die Vorgaben für die Berechtigung zur Nutzung fremder Daten auf vertraglicher Grundlage auf dem jeweiligen nationalen Zivilrecht (einschließlich der Umsetzung der Klausel-RL)[17] aufsetzen und dieses – durch Informationspflichten und eine AGB-Kontrolle im Unternehmensverkehr – lediglich punktuell ergänzen.

10 Den Regelungen des DA-E ist zugleich eine weitreichende Steuerungsfunktion immanent, da die Erfüllung der gesetzlichen oder vertraglichen Pflichten entsprechende technische Weichenstellungen voraussetzt, die bereits beim Produktdesign umgesetzt werden müssen. Hinzu treten Informationspflichten, die vor Vertragsschluss zu erfüllen sind, sowie Vorgaben für die Ausgestaltung der Nutzungsbefugnis, die, um effektiv zu sein, in der Lieferkette abgestimmt werden müssen.

11 Da die Konformität von Produkten mit den Regelungen des DA-E bei Markteintritt eine erhebliche Vorlaufzeit voraussetzt, die durch die Übergangsfrist kaum abgedeckt wird, ist aus der Sicht der Praxis der zeitliche Ablauf des weiteren Gesetzgebungsverfahrens von herausgehobener Bedeutung. Erwartet wird, dass die Trilogverhandlungen 2023 abgeschlossen sein werden und der Data Act 2024 verabschiedet wird. Bleibt es bei der Übergangsfrist von zwölf Monaten (Art. 42 DA-E), ist mit Geltung der Regelungen ab Ende 2025/Anfang 2026 zu rechnen.

III. Überblick über den Regelungsinhalt

12 Der aktuelle Entwurf des *Data Act* ist mit 90 Erwägungsgründen etwas kopflastig und sieht mit elf Kapiteln eine relativ kleinteilige und unübersichtliche Gliederung für die „nur" 42 Artikel vor. Für die hier behandelte Fragestellung nach dem Datenzugang bei smarten Produkten sind primär die Allgemeinen Bestimmungen (Kap. 1), die Zugangsrechte der Nutzer (Kap. 2), die korrespondierende Bereitstellungspflicht der Dateninhaber (Kap. 3) und der Fairnesstest für Datennutzungsvereinbarungen (Kap. 4) relevant. Die übrigen Bestimmungen betreffen die Verpflichtung zur Weitergabe an die öffentliche Hand (Kap. 5), die Datenportabilität bei Cloud-Diensten (Kap. 6), den Transfer in Drittstaaten (Kap. 7), Vorgaben für die Interoperabilität

(Kap. 8), die Behördenzuständigkeit für die Durchsetzung (Kap. 9), das Verhältnis zur Datenbank-RL (Kap. 10) sowie Übergangsfragen (Kap. 11).

13 Ausgangspunkt für das Verhältnis zwischen Hersteller bzw. Dienstleister und Nutzer von smarten Produkten oder verbundenen Diensten ist die Verpflichtung der Hersteller und Dienstleister, bei Konzeption und Herstellung der smarten Produkte und Dienstleistungen dafür zu sorgen, dass die bei der Nutzung generierten Daten standardmäßig für den Nutzer einfach, sicher und – soweit relevant und angemessen – direkt zugäng-

lich sind (Art. 3 I DA-E, sog. *Access by Design*). Damit der Nutzer von diesen Daten profitieren kann, muss er vor Abschluss eines Kauf-, Miet- oder Leasingvertrags u. a. über Art und Umfang der Daten, den Dateninhaber, die Speichermodalitäten und die geplante eigene Nutzung sowie darüber informiert werden, wie er Zugang zu diesen Daten erhält (Art. 3 II DA-E).[18]

14 Soweit die Daten für den Nutzer nicht unmittelbar zugänglich sind, stellt ihm der DA-E einen breiten Datenzugangsanspruch zur Seite. Der Anspruch bezieht sich auf alle Daten, zu deren Generierung der Nutzer einen Beitrag geleistet hat. Erfasst ist nicht nur das Recht, vom Dateninhaber die kostenfreie Bereitstellung (ggf. in Echtzeit) zu verlangen (Art. 4 DA-E), sondern auch vom Dateninhaber zu fordern, die bereitgestellten Daten mit Dritten zu teilen (Art. 5 DA-E). Die Rechtsposition des Nutzers wird zudem durch die – überraschend radikale[19] – Vorgabe gestärkt, dass der Dateninhaber die für ihn faktisch verfügbaren Daten nur nutzen darf, wenn der Nutzer dem vertraglich zugestimmt hat (Art. 4 VI DA-E). Dem Interessenausgleich dienen außerdem die Vorbehalte zu Gunsten anderer Regelungsbereiche. Insbesondere wird die Pflicht des Dateninhabers durch das Datenschutzrecht und den Geheimnisschutz eingeschränkt (Art. 4 III, V sowie 5 VI, VIII DA-E). Die Nutzungsbefugnis des Empfängers und Dritter wird durch das Verbot beschränkt, die erlangten Daten zur Entwicklung von Konkurrenzprodukten zu nutzen.

15 Muss der Dateninhaber Daten bereitstellen, wird diese Pflicht durch die aus dem Kartellrecht bekannte Anforderung insoweit konkretisiert, als der Zugang zu FRAND-Bedingungen (*fair, reasonable and non-discriminatory*)[20] zu gewähren ist (Art. 8 I DA-E), der Dateninhaber aber grundsätzlich nicht zur Preisgabe von Geschäftsgeheimnissen verpflichtet ist (Art. 8 VI DA-E). Im Übrigen überlässt der DA-E die Ausgestaltung – vorbehaltlich der Inhaltskontrolle zu Gunsten von Kleinst- und Kleinunternehmen (KKU) sowie von kleinen und mittleren Unternehmen (KMU) – der vertraglichen Vereinbarung zwischen Datengeber und Datenempfänger (Art. 8 II 1 DA-E). Ob der Dateninhaber im Gegenzug für die Bereitstellung eine faire Vergütung oder nur eine Kompensation der Bereitstellungskosten verlangen darf, hängt davon ab, ob sich der Empfänger auf die Privilegierung als KMU oder KKU berufen kann (Art. 9 DA-E).

16 In weiser Voraussicht, dass sowohl die Verpflichtung selbst als auch die Angemessenheit der Vergütung konfliktträchtig ist,[21] sind die Mitgliedstaaten verpflichtet, an der Einführung eines Streitschlichtungsmechanismus mitzuwirken (Art. 10 DA-E). Dem evidenten Risiko eines vertragsüberschreitenden Gebrauchs der erlangten Daten durch den Empfänger trägt der DA-E einerseits durch die Zulässigkeit technischer Schutzmaßnahmen (zB *Smart Contracts*) Rechnung, die die weitergehende Nutzung faktisch verhindern, andererseits durch einen Anspruch auf Löschung der Daten sowie einem dem Geschäftsgeheimnisrecht nachgebildeten Rückruf- und Vernichtungsanspruch (Art. 11 DA-E).

17 Vertraglichen Umgehungsversuchen von diesem Pflichtenprogramm beugt vor, dass von den Regelungen des Kap. III, also insbesondere von dem FRAND-Erfordernis, nicht zum Nachteil des Nutzers und anderer Berechtigter abgewichen werden kann (Art. 12 II DA-E). Auch soweit vertragliche Vereinbarungen über den Datenzugang und die Datennutzung nicht nach dieser Bestimmung einseitig zwingend sind, unterliegen sie in Verträgen mit KMU und KKU einem Fairnesstest, der neben den im *Data Act* geregelten Pflichten auch die Beschränkung von Gewährleistung und Haftung, einseitige Kündigungsrechte und Haftungsbeschränkungen oder nicht interessengerechte Nutzungsbeschränkungen erfasst. Flankiert werden einige ausdrücklich benannte einzelne Klauselverbote durch eine Generalklausel, die gröbliche Abweichungen von der guten Geschäftspraxis beim Datenzugang und der Datennutzung verbietet, wenn sie gegen das Gebot von Treu und Glauben und des redlichen Geschäftsverkehrs verstoßen (Art. 13 DA-E). Im Verhältnis zu Verbrauchern wird der Schutz der Nutzer durch die Klausel-RL gesichert.[22]

IV. Verhältnis zu bestehenden Rechtsakten

18 Das Recht auf Zugang zu nutzergenerierten Daten (Art. 4, 5) und die korrespondierende Pflicht zur Bereitstellung dieser Daten (Art. 8) beschränken zwei externe Regelungen: die DS-GVO und das Geschäftsgeheimnisschutzgesetz (GeschGehG).

1. DS-GVO

19 Entgegen den ursprünglichen Erwartungen ergänzt der DA-E die Regelungen der DS-GVO über personenbezogene Daten nicht etwa durch eine komplementäre Regelung über Maschinendaten. Vielmehr definiert Art. 2 Nr. 1 DA-E „Daten" weit (und vage). Der Begriff umfasst „jede digitale Darstellung von Handlun-

gen, Tatsachen oder Informationen" sowie deren Zusammenstellungen, gleichgültig ob in audio-, visueller oder audiovisueller Form. Der DA-E gilt damit konzeptionell für personen- und nicht-personenbezogene Daten.[23] Dies bestätigt sowohl der Vorbehalt, wonach die DS-GVO unberührt bleibt (Art. 1 III 2 DA-E), als auch die wiederkehrende Begrenzung des Zugangsrechts bzw. der Bereitstellungspflicht durch die DS-GVO (Art. 4 V und Art. 5 VI, VII, IX DA-E). Gelegentlich heißt es ausdrücklich, dass der DA-E die DS-GVO in bestimmter Weise „ergänzt".[24]

20 Die für die DS-GVO konstatierte[25] Unsicherheit über die Reichweite personenbezogener Daten wird daher in den *Data Act* exportiert. Zwar treten die Rechte und Pflichten aus dem DA-E grundsätzlich neben die DS-GVO. Die Abgrenzung ist aber insoweit erheblich, als der Normadressat nicht „vorsorglich" die weiter gehenden Pflichten des DA-E, zB auf Bereitstellung von Daten, erfüllen kann, weil darin zugleich ein Verstoß gegen die DS-GVO liegen kann. Werden Daten demgegenüber fehlerhaft dem Anwendungsbereich der DS-GVO zugerechnet und mit dieser Begründung zB der Zugang gemäß DA-E verweigert, begründet dies umgekehrt einen Verstoß gegen den *Data Act*. Damit erlangt die treffsichere Abgrenzung umso größere Bedeutung.[26]

21 Von Interesse ist daher, ob für die Auslegung des DA-E auch die Definitionen und Beispiele aus anderen Rechtsakten herangezogen werden können. So nennt etwa ErwG 9 S. 2 FFD-VO als drei Beispiele nicht personenbezogener Daten, die von der FFD-VO erfasst sein sollen:

> Daten zum Wartungsbedarf von Maschinen

- •Aggregierte und anonymisierte Daten im Kontext von Big Data

  Daten im Zusammenhang mit der Präzisionslandwirtschaft zwecks Überwachung und Optimierung des Einsatzes von Pestiziden und Wasser

- 22Berücksichtigt man die rechtsaktübergreifend übereinstimmende Terminologie, die zahlreichen Querverweise und den Umstand, dass die Rechtsakte in ihrer Gesamtheit der Umsetzung der europäischen Datenstrategie dienen, spricht dies dafür, diese Einordnung nicht auf die FFD-VO zu beschränken. Soweit dagegen personenbezogene Daten vorliegen, überlagern sich die Pflichtenprogramme von DS-GVO und DA-E. So werden etwa die Informationspflichten, aber auch die Beschränkungen kumuliert. Das hat handfeste Folgen: Für die Verarbeitung bzw. Nutzung nutzergenerierter personenbezogener Daten durch den Dateninhaber ist dann sowohl eine Rechtfertigung nach DS-GVO als auch die Zustimmung nach dem DA-E erforderlich. Auch wenn dem Empfänger in Erfüllung des Zugangsrechts Daten, die personenbezogene Daten eines Dritten sind, bereitgestellt werden, verlangt Art. 4 V DA-E für die Bereitstellung eine Rechtfertigung gem. Art. 6 I UAbs. 1 DS-GVO.[27]

23Praktische Unterschiede bestehen zudem hinsichtlich der Ausgestaltung von Zugangs- und Löschungsanspruch: Der Zugangsanspruch ist jeweils „unverzüglich" zu erfüllen (Art. 12 III 1, Art. 16, 17 DS-GVO und Art. 4 I 1 DA-E). Während die Bereitstellung nach der DS-GVO grundsätzlich[28] „in jedem Fall aber innerhalb eines Monats" (Art. 12 III 1 DS-GVO) zu erfolgen hat, normiert der DA-E keine Obergrenze, sondern umgekehrt die denkbar schnellste Zurverfügungstellung (*„gegebenenfalls kontinuierlich und in Echtzeit*", Art. 4 I 1 DA-E). Der unbestimmte Rechtsbegriff „unverzüglich" (*'without undue delay'*; « *dans les meilleurs délais* ») ist also je nach Kontext und Zweck der Vorschrift ganz unterschiedlich auszulegen. Vor dem Hintergrund, dass der DA-E Echtzeitdaten bzw. zeitnahem Datenzugang ein hohes Innovations- und Wertschöpfungspotential zuspricht, liegt nahe, dass „unverzüglich" binnen weniger Sekunden oder in Sekundenbruchteilen bedeuten kann, wohingegen unter der DS-GVO, welche etwa die Information der betroffenen Person oder die Berichtigung oder Löschung von deren Daten verlangt, der Verantwortliche sicher nicht nur Sekunden, sondern jedenfalls Tage oder eher Wochen Zeit hat.

24Der Löschungsanspruch erfasst nach DS-GVO (Art. 17 I) und DA-E (gem. Art. 11 II lit. a) jeweils die Daten. Nur der DA-E flankiert den Anspruch auf Löschung der Daten mit einem Rückrufanspruch. Bei vertragswidriger Nutzung der Daten muss der Datenempfänger insbesondere Dienstleistungen und Waren, die auf den mit den Daten erlangten Kenntnissen beruhen, beenden bzw. vernichten. Nach DA-E sind also auch „abgeleitete Daten" (Art. 11 II lit. b) zu löschen, zum Primärlöschungs- tritt ein Sekundärlöschungsanspruch auf Beseitigung des datenrechtlichen Folgeschadens. Der Löschungsanspruch des Art. 17 I DS-GVO erfasst dagegen nicht die KI, die mit den zu löschenden Daten angelernt wurde. Die Norm gewährt keinen „Bereicherungsausgleich nach unrechtmäßiger Datenverarbeitung durch den Verantwortlichen"[29].

2. Verhältnis zum GeschGehG

25Das Verhältnis zwischen *Data Act* und Geschäftsgeheimnisschutz wird im DA-E zwar angesprochen,

aber im Wesentlichen durch eine Verweisung in die Richtlinie zum Schutz von Geschäftsgeheimnissen (EU) 2016/943 geregelt, die im GeschGehG umgesetzt wird.

Anwendungsbereich und Systematik des Geschäftsgeheimnisrechts erklären auch, warum die Regelungen im DA-E für Nutzer/Dritte und die öffentliche Hand gesondert geregelt sind.

26 Denn Art. 1 II GeschGeh-RL (bzw. § 1 II GeschGehG) enthält einen „globalen" Vorrang für das öffentliche Recht, in dem klargestellt wird, dass ein Geschäftsgeheimnis einer öffentlich-rechtlichen Informationspflicht nicht entgegengehalten werden kann. Ob und in welchem Umfang die jeweilige Rechtsgrundlage das Interesse des Geheimnisinhabers berücksichtigt, bleibt so der Regelung durch das öffentliche Recht vorbehalten. Mit Blick nur auf § 1 II GeschGehG hat also auch das in Art. 14 DA-E vorgesehene Datenzugangsrecht der Behörden stets Vorrang vor dem Geheimnisschutz.

27 Andererseits stellt der DA-E den Vorrang des öffentlichen Rechts selbst unter einen Abwägungsvorbehalt. Zum Schutz von Geschäftsgeheimnissen, die einen hohen Stellenwert haben, verlangt Art. 17 II lit. c DA-E für das „Ob" ausdrücklich die „Berücksichtigung des Schutzes von Geschäftsgeheimnissen" und für das „Wie" Geheimhaltungsmaßnahmen. So ist nach Art. 19 II DA-E vorgesehen, dass die öffentliche Hand technische und organisatorische Maßnahmen ergreift, um die Vertraulichkeit zu wahren. Zusammen mit dem Zweckbindungsgrundsatz und der Pflicht zur Datenlöschung werden die Anforderungen nach § 2 GeschGehG gewahrt. Dies gilt umso mehr, als nach Art. 19 II DA-E die Vorkehrungen – ähnlich wie im Zivilprozess nach § 16 GeschGehG – schon dann getroffen werden müssen, wenn es sich nur „mutmaßlich" um ein Geschäftsgeheimnis handelt.

28 Für das Verhältnis unter Privaten gilt hingegen, dass der DA-E das GeschGehG „unberührt" lässt; das GeschGehG beansprucht daher vollumfänglich Geltung.[30] Die in Art. 4 III, Art. 5 VIII und Art. 8 VI DA-E enthaltene Regelung, dass die Vertraulichkeit durch Maßnahmen gewährleistet werden muss und eine Zweckbindung vorgesehen werden darf, ist daher als Verweis auf § 2 Nr. 1 GeschGehG zu lesen. Im Fall des vertragsüberschreitenden Gebrauchs durch den Empfänger der Daten tritt neben den Löschungs- und Vernichtungsanspruch nach Art. 11 Abs. 2 DA-E das Rechtsfolgenprogramm der §§ 6 ff. GeschGehG.

29 Soweit trotz der parallelen Anwendbarkeit des GeschGehG die Lückenhaftigkeit der Regelung oder ihre mangelnde Durchsetzbarkeit beklagt wird,[31] ist darauf hinzuweisen, dass das Geschäftsgeheimnis bei den hier relevanten Daten in der Regel in der Summe der aggregierten oder aufbereiteten Daten besteht, die allerdings gerade nicht vom Zugangsanspruch erfasst sind (ErwG 14 DA-E). Die Bereitstellung des einzelnen nutzerspezifischen Datensatzes gefährdet das Geheimnis in der Regel nicht, weil bereits die gesetzlich vorgesehene Zweckbindung dafür sorgt, dass nicht ein Dritter die Daten einer erheblichen Anzahl von Nutzern seinerseits aggregiert.

3. Datenbank-RL

30 Neben dem Geschäftsgeheimnisrecht kommt als wichtiges Tool zum Schutz von *Big Data* das Datenbankherstellerrecht in Betracht (§ 87 a UrhG). Es setzt eine Investition in die Erstellung einer Datenbank voraus und schützt diese gegen die Entnahme wesentlicher Teile. Schon bislang hat eine bloße Sammlung von Rohdaten die Anforderungen an eine Datenbank nicht erfüllt.[32] Der *Data Act* stellt dies klar (vgl. ErwG 84) und grenzt dadurch den Anwendungsbereich des DA-E von der Datenbank-RL[33] ab (Art. 35 DA-E). Daraus folgt umgekehrt, dass das Zugangsrecht gem. DA-E aggregierte und abgeleitete Daten sowie auf dieser Basis erstellte Trainingsdatensätze oder Analyseergebnisse nicht erfasst.

V. Datenzugangsrechte in Vertragsbeziehungen

1. Adressaten: Dateninhaber, Datennutzer und Dritte

31 Das Rechte- und Pflichtenprogramm des DA-E sieht – soweit für die Vertragsbeziehungen von Bedeutung – als maßgebliche Akteure Dateninhaber, Nutzer und Dritte vor. Da die DS-GVO aber unberührt bleibt, die rechtmäßige Nutzung personenbezogener Daten also eine Rechtfertigung nach DS-GVO voraussetzt, tritt als weiterer Akteur die „betroffene Person" (Art. 4 Nr. 1 DS-GVO) hinzu.

a) Dateninhaber

32 Nach der zirkulären[34] Definition des Dateninhabers (Art. 2 Nr. 6 DA-E) handelt es sich bei diesem um eine juristische oder natürliche Person, die berechtigt oder verpflichtet ist, personenbezogene Daten bereitzustellen bzw. im Falle nicht- personenbezogener Daten durch die Kontrolle über die technische Konzeption des Produktes und damit verbundener Dienste

hierzu in der Lage ist. Die unglücklich übersetzte Definition macht nicht recht deutlich, dass es (für personenbezogene und nicht-personenbezogene Daten übereinstimmend) auf die faktische Kontrolle ankommt, bei personenbezogenen Daten aber außerdem das Recht zur Verarbeitung gem. DS-GVO hinzukommen muss.

33 Der Begriff des Dateninhabers setzt neben der faktischen Kontrolle voraus, dass es sich um den Hersteller eines smarten Produkts oder den Anbieter eines mit einem smarten Produkt verbundenen Dienstes handelt. Die Unterscheidung zwischen Hersteller/Anbieter und Dateninhaber ist nicht trennscharf,[35] sie werden idR – aber nicht notwendig – übereinstimmen. Eine erste wichtige Begrenzung des Begriffs des Dateninhabers ergibt sich daher aus der Voraussetzung, dass er – wegen der erforderlichen „Kontrolle über die technische Konzeption des Produktes und damit verbundener Dienste" – der Hersteller von Produkten oder Anbieter der damit verbundenen Dienstleistungen sein muss. Die bloße faktische Kontrolle über die Daten ist also nicht ausreichend. Daher wird nicht jeder, der die Daten faktisch erlangt, Dateninhaber.[36] Sonst wäre jeder Nutzer, der sein Zugangsrecht ausübt, oder jeder Dritte, dem Daten bereitgestellt werden, zugleich ein Dateninhaber. Die Beschränkung auf den originären Inhaber, also auf die Person, die die Daten aufgrund der Kontrolle über die technische Konzeption des Produktes und damit verbundener Dienste erstmals erhoben hat, ist zum einen erforderlich, weil nur dieser die Informationspflichten zum vorgegebenen Zeitpunkt, nämlich vor Vertragsschluss, erfüllen kann (Art. 3 II DA-E). Zum anderen ist der originäre Inhaber gerade der Geheimnisinhaber, der über die Erforderlichkeit von Geheimhaltungsmaßnahmen und den Nutzungszweck entscheidet und den Zugang unter Berufung auf das GeschGehG verweigern kann. Daher ist zwischen dem originären Inhaber als Verpflichtetem und anderen Personen, die die Daten von diesem erhalten, zu unterscheiden.

34 Zweitens muss das Produkt vom DA-E umfasst sein. Bei der Definition der Produkte (Art. 2 Nr. 2 DA-E) spiegelt sich das ursprüngliche Konzept wider, eine Regelung für industrielle Maschinendaten zu schaffen. Denn zu den Produkten zählen „nur" elektronische Geräte, die Umwelt- und Nutzungsdaten erfassen, mit elektronischen Kommunikationsdiensten verbunden sind und deren Hauptfunktion nicht in der Speicherung von Daten besteht. Als Beispiele werden Haushaltsgeräte und Konsumgüter, Medizin- und Gesundheitsprodukte oder landwirtschaftliche und industrielle Maschinen genannt (ErwG 14 DA-E).

35 Die Ausnahme „Speicherung als Hauptfunktion" wird weit gezogen und umfasst alle Produkte, bei denen die Erstellung einen menschlichen Beitrag erfordert, zB PC, Server, Tablets

und Smartphones, Kameras, Webcams, Tonaufnahmesysteme und Textscanner (ErwG 15 DA-E). Mit Blick auf die Frage, ob Geräte/*Smart Devices* erfasst werden, die keine reine Speicherfunktion haben,[37] aber menschlichen Input forderten, sprechen Wortlaut, Anwendungsbeispiele und Regelungszweck klar für deren Einbeziehung.

36 Soweit als weitere mögliche Beschränkung des Anwendungsbereichs die Entgeltlichkeit des Vertrags über das Produkt/die Dienstleitung diskutiert wird,[38] enthält der Wortlaut keinen Anhaltspunkt für eine solche Beschränkung. Zudem liegt auch bei „Bezahlen mit Daten" ein entgeltlicher Vertrag vor.[39] Die Einschränkung ist daher abzulehnen.

b) Nutzer

37 Vergleichsweise einfach ist der „Nutzer" (Art. 2 Nr. 5 DA-E) zu bestimmen. Es handelt sich um die natürliche oder juristische Person, die ein Produkt besitzt, mietet oder least oder eine Dienstleistung in Anspruch nimmt, idR also um den Vertragspartner des Dateninhabers.

38 Diskutiert wird, ob es mehrere Nutzer geben kann.[40] Ohne Zweifel ist das der Fall, wenn diese mehreren Personen gemeinsam Vertragspartner des Dateninhabers sind oder das Produkt in deren gemeinsamen Eigentum steht. Dass es auf die vertraglich berechtigte, und nicht die bloß faktische Nutzung ankommt, ergibt sich bereits aus der Informationspflicht (Art. 3 II DA-E), die ein vorvertragliches Verhältnis „vor Abschluss eines Kauf-, Miet- oder Leasingvertrags für ein Produkt oder verbundenen Dienst" voraussetzt und nur gegenüber potentiellen Vertragspartnern überhaupt umsetzbar ist. Nutzt nicht ein Vertragspartner (zB Arbeitgeber), sondern ein Dritter (zB Arbeitnehmer) das Produkt, führt dies folglich nicht dazu, dass dieser Nicht-Vertragspartner als weiterer Nutzer anzusehen ist.[41] Davon zu unterscheiden ist der Fall, dass mehrere Personen durch die separate Nutzung dieselbe Information generieren (zB zum Grundwasserspiegel oder einem Verkehrsstau). In diesem Fall handelt es sich bei der mehrfach separat aufgezeichneten Information um jeweils gesonderte Daten.

c) Datenempfänger

39 Vom Nutzer zu unterscheiden ist der Datenempfänger (Art. 2 Nr. 7 DA-E). Dabei handelt es sich um „eine juristische oder natürliche Person", die zu kommerziellen Zwecken, aber „ohne Nutzer eines Produktes oder verbundenen Dienstes zu sein", vom Dateninhaber Daten erhält. Ob die Daten auf Verlangen des Nutzers oder in Umsetzung der FRAND-Verpflichtung bereitgestellt werden, ist ohne Belang.

40 Nicht aus der Definition, sondern erst aus der Ausgestaltung des Bereitstellungsanspruchs ergibt sich, dass es zwei Klassen von Datenempfängern gibt. Jeder, der Zugang erlangt, unterliegt dem Pflichtenprogramm des DA-E. Auch sog. *Gatekeeper* iSd DMA sind daher als Dateninhaber zur Bereitstellung verpflichtet. *Gatekeeper* haben aber kein Recht auf Zugang zu solchen nutzergenerierten Daten, die bei anderen Herstellern entstehen. *Gatekeeper* dürfen sich dieses Recht nicht vertraglich zusichern lassen, weder bei dem Nutzer noch über Dritte (Art. 5 II DA-E). Diese Schlechterstellung der *Gatekeeper* soll das rechtspolitische Ziel fördern, die europäische Wirtschaft gegenüber den dominanten Playern aus anderen Märkten zu stärken.

41 Für Hersteller smarter Produkte ergibt sich daraus die Herausforderung, ihre Produkte so zu konzipieren, dass ein Abfluss an *Gatekeeper* vermieden wird. Gerade bei Produkten, die sich für die Nutzung von Diensten eignen, die auch *Gatekeeper* anbieten, ist dies für die Wartung

und Pflege erheblich.[42] Besonders gegenüber *Gatekeepern* dürften die nach Art. 31 III lit. d) DA-E von den Mitgliedstaaten zu schaffenden Behördenkompetenzen zur Verhängung abschreckender finanzieller Sanktionen im Verwaltungsverfahren oder zur Einleitung von Gerichtsverfahren zur Verhängung von Geldbußen praktische Bedeutung erlangen. Ob solche Sanktionen auch gegen Dateninhaber verhängt werden können, die Daten freiwillig an *Gatekeeper* weiterleiten, ist jedoch zweifelhaft, da der DA-E dem Dateninhaber die Weiterleitung nicht ausdrücklich untersagt. Im Gegensatz dazu ist es Dritten, denen Daten auf Verlangen des Nutzers bereitgestellt worden sind, ausdrücklich verboten, diese Daten an *Gatekeeper* weiterzuleiten (Art. 6 II lit. d) DA-E). Eine freiwillige Weiterleitung durch den Dateninhaber kann jedoch der nach Art. 4 VI DA-E mit dem Nutzer zu schließenden Vereinbarung über die Datennutzung widersprechen.

d) Betroffene Person

42Weil die rechtmäßige Nutzung personenbezogener Daten weiterhin eine Rechtfertigung nach DS-GVO voraussetzt, tritt die betroffene Person nach der DS-GVO als weiterer Akteur zu den im DA-E geregelten hinzu. Während der Nutzer nach Art. 2 Nr. 5 DA-E der Vertragspartner des Dateninhabers ist, ist die betroffene Person nach dem Informationsgehalt der Daten zu bestimmen: Sie ist die identifizierte oder identifizierbare natürliche Person, auf die sich die in den Daten enthaltenen Informationen beziehen (Art. 4 Nr. 1 DS-GVO). Der Nutzer im Sinn des DA-E und die betroffene Person nach der DS-GVO fallen häufig zusammen, etwa, wenn sich eine Person eine Smartwatch anschafft und diese mit ihrem Smartphone verbindet oder sich bei einem Dienst anmeldet, um das Gadget zu nutzen.

43Doch das muss nicht immer so sein, denn die Begriffsbestimmungen des Nutzers gem. DA-E und der betroffenen Person gem. DS-GVO unterscheiden sich: Betroffene Person gem. Art. 4 Nr. 1 DS-GVO kann nur eine natürliche Person sein. Dagegen erfasst der DA-E als Nutzer neben natürlichen auch juristische Personen. Kauft bspw. ein als GmbH organisiertes Lohnunternehmen eine smarte Landmaschine von einem Hersteller, der die beim Betrieb der Landmaschine anfallenden Daten sammelt, ist das Lohnunternehmen zwar Nutzer, betroffene Person im Sinn der DS-GVO aber häufig der Eigentümer des Grundstücks und/oder die natürliche Person, welche die Landmaschine steuert. Dagegen kann der Angestellte, der die Daten bei der Nutzung der Landmaschine generiert, oder der Eigentümer des Grundstücks betroffene Person im Sinn der DS-GVO sein, ist aber kein Vertragspartner des Herstellers und daher auch kein (weiterer) Nutzer (neben dem Lohnunternehmen).

2. Rechte- und Pflichtenprogramm

44Der Hersteller oder Diensteanbieter hat zunächst die Pflicht dafür zu sorgen, dass der Nutzer automatisch Zugang zu den nutzergenerierten Daten erlangt (Access-by-Design, Art. 3 I DA-E, s. o.). Ist der Zugang nicht automatisch möglich, hat der Nutzer gegen den Dateninhaber einen Anspruch auf Zugang (Art. 4 I DA-E) und auf die Bereitstellung der Daten an Dritte (Art. 5 I DA-E).

45Unabhängig davon, ob der Nutzer den Zugang automatisch oder erst in Erfüllung des Zugangsanspruchs erhält, muss der Hersteller seinen Vertragspartner, d. h. den Nutzer, über Art, Umfang und Nutzungszweck der beim Dateninhaber erhobenen nutzergenerierten Daten informieren (Art. 3 II DA-E). Will der Hersteller die Daten selbst nutzen, darf er dies nur auf Grundlage einer vertraglichen Vereinbarung mit dem Nutzer, die er praktischerweise

zusammen mit dem Kauf-, Miet- oder Leasingvertrag über das Produkt oder den verbundenen Dienst abschließt (Art. 4 VI DA-E). Die Wirksamkeit der Vereinbarung über die Nutzung

muss dabei, wenn sie, wie regelmäßig, durch AGB erfolgt, im Verhältnis B2C der Klausel-RL und im Verhältnis B2B dem Fairnesstest (Art. 13 DA-E) standhalten.[43] Hinzu tritt die nationale AGB-Kontrolle, soweit – wie im deutschen Recht – auch AGB unter Unternehmen der Inhaltskontrolle unterliegen. Falls der Nutzer vom Inhaber begehrt, dass ein Dritter Zugang erhält, muss nach Art. 6 DA-E zwischen dem Nutzer und dem Dritten eine Nutzungsvereinbarung getroffen werden, die ebenfalls inhaltlichen Beschränkungen unterliegt und dem Fairnesstest standhalten muss.

46 Was gilt, wenn die Vereinbarung zwischen Nutzer und Dateninhaber unwirksam ist oder überschritten wird? Diese Frage beantwortet der DA-E nicht ausdrücklich.[44] Da dem Nutzer bewusst keine Rechtsposition im Sinne eines Dateneigentums zugewiesen wird, ergibt sich ein Nutzungsverbot und ein Verstoß gegen den DA-E, jedoch kein Schadensersatzanspruch gegen den Dateninhaber.[45] Nur falls es sich bei den Daten, für die aufgrund der Unwirksamkeit oder der Überschreitung die Nutzungsbefugnis fehlt, um personenbezogene Daten oder um Geschäftsgeheimnisse handelt, kommen gem. Art. 82 I DS-GVO bzw. §§ 6 ff. GeschGehG Schadensersatzansprüche in Betracht.

47 Der Nutzer ist berechtigt, Zugang zu jenen Daten zu verlangen, zu deren Generierung er einen Beitrag geleistet hat. Es geht um Daten, die „bei" der „Nutzung" der Produkte und Dienste „erzeugt" wurden (Art. 3 I DA-E). Um den Umfang des Zugangsanspruchs zu bestimmen, sind zwei Unterscheidungen von Bedeutung: Daten, die beim Dateninhaber anfallen, ohne durch Art und Umfang der Nutzung beeinflusst zu werden, sind nicht in diesem Sinn „bei" der „Nutzung" des Produkts oder des Dienstes erzeugt. Sie unterliegen der faktischen – und als Geschäftsgeheimnis auch der rechtlichen – Kontrolle des Herstellers bzw. Diensteanbieters. Hierzu gehören zB der Herstellungsprozess, technische Daten, Kundenlisten und Preiskalkulationen. Sie sind nicht Gegenstand des Zugangsanspruchs.

48 Nutzergenerierte Daten werden demgegenüber durch die (Nicht)Nutzung des Produkts oder der Dienstleistung mit Hilfe von Sensoren oder Kameras beim Nutzer aufgezeichnet und in der Regel über ein Kommunikationsnetz an den Dateninhaber, häufig den Hersteller des Produkts, übermittelt. Die Nutzung dieser Daten, die sich in der faktischen Kontrolle des Herstellers/Anbieters befinden, ist nur auf der Grundlage einer vertraglichen Vereinbarung mit dem Nutzer rechtmäßig (Art. 4 VI DA-E). Die Regelung verkehrt die derzeit bestehende Rechtslage, dass derjenige, der faktischen Zugang hat, auch die Nutzung bestimmt, in ihr Gegenteil.[46] Dem offenkundigen Risiko, dass diese Regelung im Unternehmensverkehr durch standardisierte Vertragsgestaltung unterlaufen wird, sucht der DA-E durch eine AGB-Kontrolle zu Gunsten von KMU und KKU zu begegnen.

49 Soweit sich nutzergenerierte von nicht-nutzergenerierten Daten technisch nicht trennen lassen, der Hersteller/Anbieter durch die Bereitstellung der nutzergenerierten Daten also auch eigene generierte Daten preisgäbe, hat der Hersteller ein legitimes Geheimhaltungsinteresse. Dieses kann durch eine „Vertraulichkeitsvereinbarung" gesichert werden, die um effektiv zu sein, allerdings auch eine Beschränkung des Nutzungszwecks vorsehen muss.[47] Im Verhältnis zu Dritten kann der Dateninhaber aus demselben Grund berechtigt sein, den Zugang zu verweigern.

50 Im Wesentlichen dasselbe gilt für die Unterscheidung von personenbezogenen/nicht-personenbezogenen Daten. Erlangt der Hersteller/Anbieter durch die Nutzung des Produkts bzw. der Dienstleistung die faktische Kontrolle über personenbezogene Daten, so ist er zur Nutzung derselben nur berechtigt, wenn hierfür eine Rechtsgrundlage gem. Art. 6 I UAbs. 1 DS-GVO vorliegt. Da auch die Bereitstellung der Daten zur Erfüllung eines Zugangsanspruchs eine Verarbeitung gem. Art. 4 Nr. 2 DS-GVO darstellt, kann der Hersteller diese Erfüllung unter Hinweis auf seine Pflicht aus der DS-GVO unter Umständen verweigern.

51 Falls die Rechtfertigung nicht gem. Art. 6 I UAbs. 1 lit. f DS-GVO (überwiegendes berechtigtes Interesse) gelingt, ist danach zu unterscheiden, ob der Nutzer im Sinne des DA-E zugleich die betroffene Person gemäß DS-GVO ist.[48] Falls ja, ist die Geltendmachung des Datenzugangsanspruchs als Einwilligung gem. Art. 6 I UAbs. 1 lit. a DS-GVO zu werten. Falls nein, kann sich der Dateninhaber auf Art. 6 I UAbs. 1 lit. c DS-GVO berufen: Die Rechtsgrundlage erlaubt die Verarbeitung aufgrund einer Verpflichtung kraft Rechts der Union oder eines Mitgliedstaates, die sich unmittelbar auf die Datenverarbeitung bezieht. Eine solche Rechtsgrundlage stellt Art. 4 I DA-E dar. Ist der Nutzer nicht die betroffene Person und verlangt die Weitergabe an Dritte, hilft Art. 6 I UAbs. 1 lit. c DS-GVO dagegen, aufgrund des Vorbehalts aus Art. 5 V DA-E, nicht.[49]

52 Mit Blick auf den Anspruch des Nutzers auf Bereitstellung der Daten an Dritte ist bemerkenswert, dass

die Art. 20 DS-GVO nachgebildete Regelung des Art. 5 I DA-E vor allem den Wartungs- und Reparaturmarkt mit den nötigen Daten versorgen soll.[50] Eine Beschränkung auf diesen Verwendungszweck sieht Art. 5 I DA-E freilich nicht vor. Vom Wortlaut umfasst ist vielmehr auch die Situation, dass ein Unternehmen Nutzer systematisch auffordert, ihnen Daten zwecks Aggregation von Datensätzen bereitstellen zu lassen, zB um ein kompatibles Produkt zu entwickeln. Dafür spricht auch, dass der Dateninhaber für die Bereitstellung von Daten vom Dritten eine angemessene (FRAND) Vergütung fordern und der Dritte die Daten nicht zur Entwicklung eines konkurrierenden Produkts nutzen darf.[51] Hier ist allerdings die weitreichende Ausnahme zu Gunsten von KMU zu berücksichtigen, die nur den Aufwand für die Bereitstellung ersetzen müssen, aber keine Vergütung schulden (Art. 9 II DA-E).

3. Ausnahmen für KMU & KKU

53 Um sicherzustellen, dass der durch den *Data Act* angestoßene Datenfluss Innovationen fördert und nicht durch hohe Entwicklungs- oder Transaktionskosten beeinträchtigt, sind Ausnahmen für KKU sowie KMU vorgesehen.

54 Für KKU geht die Kommission davon aus, dass schon die Verpflichtung zur technischen Konzeption der Produkte (Art. 3 I DA-E) eine übermäßige Belastung darstellt. Diese Unternehmen sind von der Pflicht zu *Access-by-Design* ausgenommen (Art. 7 I DA-E). Das hat Folgen: Nicht nur KKU selbst sind von der Pflicht, die durch Nutzung eines solchen Produkts generierten Daten bereitzustellen, befreit, sondern jeder Dateninhaber. Denn Art. 7 I DA-E stellt auf das Produkt und den Dienst ab, die KKU herstellen bzw. erbringen. Nicht beschränkt ist aber die Informationspflicht der Hersteller (Art. 3 II DA-E). Sie sollte auch den Hinweis umfassen, dass das Zugangsrecht wegen der Herstellung durch ein KKU entfällt.

55 Demgegenüber gilt auch für KMU, dass sie als Dateninhaber durch entsprechende technische Konzeption für die automatische Bereitstellung der Daten beim Nutzer sorgen

müssen oder andernfalls einem Zugangsanspruch ausgesetzt sind. Ihre Verhandlungsposition als Nutzer sichert der Fairnesstest. Hinzu tritt, dass KMU als Datenempfänger für die Bereitstellung keine Vergütung, sondern nur eine Aufwandsentschädigung schulden. Diese Privilegierung wirkt in beide Richtungen: KMU, die Daten bereitstellen, erhalten folglich ebenso wenig eine Vergütung. Der Mechanismus fördert den *Free Flow of Data* und damit letztlich innovative Geschäftsmodelle.

56 Für die jeweiligen Definitionen von KKU und KMU verweist der DA-E auf Art. 2 des Anhangs der Empfehlung 2003/361/EG der Kommission betreffend die Definition der Kleinstunternehmen sowie der kleinen und mittleren Unternehmen vom 6.5.2003.[52] Da 99 % der Unternehmen in Deutschland unter die Definition des KMU fallen, ist diese „Ausnahme" möglicherweise der statistische Regelfall.[53] Hieran wird deutlich, dass hier dem Ziel des „Free Flow" Vorrang vor dem Interesse des Inhabers an der Verwertung seiner faktischen Position gewährt wird. Umso wichtiger ist es, bei der Nutzungsvereinbarung mit Dritten im Wege der Vertragsgestaltung die Zweckbestimmung zu begrenzen.

57 Soweit die Ausnahmen kritisiert werden, weil für die Verhandlungsposition nicht die Größe des Unternehmens, sondern die Datenexklusivität entscheidend sei,[54] ist darauf hinzuweisen, dass die gem. Art. 13 II–IV DA-E als unwirksam sanktionierten Klauseln primär das Zugangsrecht absichern, um ein großflächiges Unterlaufen durch AGB zu verhindern. In der Tat könnte die Vertragsgestaltung durch ein großes Unternehmen mit mehreren Millionen Kunden entscheidenden Einfluss auf den Datenzugang haben, während umgekehrt eine „unfaire" Bedingung in einer AGB eines KMU wohl keine Auswirkung auf den Markt hätte. Im Übrigen bleibt es für alle – also auch große – Unternehmen bei der AGB-Kontrolle.

VI. Zusammenfassung und Ausblick

58 Das Vorstehende lässt sich wie folgt zusammenfassen:

Der DA-E betrifft nur Daten, die bei der Nutzung eines (körperlichen) Produkts oder eines mit dem Produkt verbundenen Dienstes erzeugt werden.

- •Dateninhaber ist die Person, in deren Kontrolle die Daten originär entstehen; der Dateninhaber hat zunächst eine faktische Position, die aber der DA-E insbesondere durch Rechte des Nutzers auf diese Daten erheblich beschränkt. Nutzer ist nur derjenige, durch dessen Nutzung des Produkts oder verbundenen Dienstes die konkreten Daten entstehen. Dritter ist eine Person, die weder Dateninhaber noch Nutzer ist, aber aus eigenem Interesse oder im Interesse des Nutzers Zugang begehrt. Erhält er Zugang, wird er dadurch zum Datenempfänger (nicht zum Dateninhaber).

Die Informationspflichten gem. DA-E treten zu denen nach DS-GVO hinzu; die Informationen müssen

- transparent sein und sollten auch einen Hinweis enthalten, falls kein Datenzugangsrecht besteht, weil der Hersteller des Produkts bzw. Erbringer der Dienstleistung ein KKU ist.

Dateninhaber müssen eine Vereinbarung mit dem Nutzer schließen, wenn sie bei der Nutzung des Produkts oder verbundenen Diensten erzeugte Daten selbst nutzen möchten. Diese Vereinbarung mit dem Nutzer sollte dessen Zustimmung zur Datennutzung, die Zwecke der Nutzung und, je nach Art der Daten, auch bereits eine Geheimhaltungsvereinbarung und eine Nutzungsbeschränkung enthalten. Praktisch

begrenzt das den Anspruch Dritter und trifft eine wichtige Vorkehrung im Dreiecksverhältnis Dateninhaber/Nutzer/Empfänger.

- •Da die rechtmäßige Nutzung die wirksame Zustimmung des Nutzers voraussetzt, geht eine Unwirksamkeit der Vereinbarung zu Lasten des Dateninhabers. Umso wichtiger ist es, bei der Formulierung von AGB das Leitbild des DA-E zu beachten. Der gem. DA-E vorgesehene Fairnesstest darf nicht den Blick dafür verstellen, dass das Leitbild des DA-E auch für die nationale AGB-Kontrolle relevant ist, aber der Mindeststandard des DA-E durch strengere Anforderungen nach nationalem AGB-Recht überschritten werden kann. Im Verhältnis B2C ist zudem die Klausel-RL zu beachten.

  Die Analyse zeigt, dass der europäische Datenraum „vertragslastig"[55] werden wird. Bis die geplanten Mustervertragsbedingungen zum *Data Act* vorliegen, trifft die Hersteller das Risiko, Daten zwischen DS-GVO, GeschGehG und dem zukünftigen *Data Act* durch die Formulierung wirksamer Vertragsbedingungen zutreffend zuzuordnen.

- **59**Die aktuelle Diskussion um Zugangsrechte vernachlässigt, dass der Datenfluss bereits in der technischen Konzeptionsphase berücksichtigt werden muss, um den Zugang zu Daten zu standardisieren und dadurch zu vereinfachen. Auch unter Berücksichtigung der Dauer des Gesetzgebungsverfahrens und der Umsetzungsfrist werden Produkte betroffen sein, die schon heute in der Entwicklung sind. Die Datenströme nach Art und Nutzer fein zu steuern, ist in diesen Fällen schon heute erforderlich, um die voraussichtlich in naher Zukunft geltende Rechtslage hinsichtlich erzeugter Daten zu erfüllen.

---

* Die Autoren sind Professoren an der Universität Osnabrück. Der Autor Hartmann, LL. M. (Virginia), ist Inhaber des Lehrstuhls für Öffentliches Recht, Wirtschaftsrecht und Verwaltungswissenschaften, die Autorin McGuire, M. Jur. (Göttingen), ist Inhaberin des Lehrstuhls für Bürgerliches Recht, Recht des Geistigen Eigentums sowie deutsches und europäisches Zivilprozessrecht. Der Autor Schulte-Nölke ist Inhaber des Lehrstuhls für Bürgerliches Recht, Europäisches Privat- und Wirtschaftsrecht, Rechtsvergleichung und Europäische Rechtsgeschichte.

1 Mitteilung der Kommission, Eine europäische Datenstrategie, 19.2.2020, COM/2020/66 final.

2 VO (EU) 2022/868 vom 30.5.2022 über europäische Daten-Governance und zur Änderung der Verordnung (EU) 2018/1724 (Daten-Governance-Rechtsakt), ABl. 2022 L 152, 1.

3 VO (EU) 2018/1807 über einen Rahmen für den freien Verkehr nicht-personenbezogener Daten in der Europäischen Union, ABl. 2018 L 303, 59.

4 RL (EU) 2019/1024 vom 20.6.2019 über offene Daten und die Weiterverwendung von Informationen des öffentlichen Sektors, ABl. 2019 L 172, 56.

5 ErwG 3 S. 6 DGA.

6 Vorschlag für eine VO über harmonisierte Vorschriften für einen fairen Datenzugang und eine faire Datennutzung (Datengesetz) 2022/0047 (COD) vom 23.2.2022, COM(2022) 68 final.

7 Vgl. Vorschlag für eine VO über einen Rahmen für den freien Verkehr nicht personenbezogener Daten in der Europäischen Union 2017/0228 (COD) vom 13.9.2017, COM(2017) 495 final, S. 2.

8 Dazu unten, VI. 1.

9 Vgl. Kapitel VII (Bereitstellung von Daten für öffentliche Stellen, Einrichtungen und sonstigen Stellen der Union wegen außergewöhnlicher Notwendigkeit) des Vorschlags für eine VO über harmonisierte Vorschriften für einen fairen Datenzugang und eine faire Datennutzung (Datengesetz) 2022/0047 (COD) vom 23.2.2022, COM(2022) 68 final.

10 VO (EU) 2022/1925 des Europäischen Parlaments und des Rates vom 14.9.2022 über bestreitbare und faire Märkte im digitalen Sektor (Gesetz über digitale Märkte), ABl. 2022 L 265, 1.

11 Die Schnittmenge zwischen dem Digital Services Act, der die Rahmenbedingungen für Online-Plattformen vorgibt, und dem Data Act betrifft demgegenüber primär die Portabilitätsregelungen für Cloud Anbieter, die für die hier im Zentrum stehenden Rechte zur Datennutzung bei smarten Produkten nicht einschlägig sind.

12 RL (EU) 2019/771 über bestimmte vertragsrechtliche Aspekte des Warenkaufs, ABl. 2019 L 136, 28.

13 RL (EU) 2019/770 über bestimmte vertragsrechtliche Aspekte der Bereitstellung digitaler Inhalte und digitaler Dienstleistungen, ABl. 2019 L 136, 1.

14 Vgl. die Gesetzesfolgenabschätzung zum Vorschlag zum Datengesetz, SWD (2022) 34 final vom 23.2.2022, 11 sowie Staudenmayer EuZW 2022, 596 (597).

15 Vgl. Europäische Kommission, Mitteilung über eine Europäische Datenstrategie, COM/2020/66 final, S. 25 f.

16 Dazu näher Podszun/Pfeifer GRUR 2022, 953.

17 RL (EWG) 1993/13 über mißbräuchliche Klauseln in Verbraucherverträgen, Abl. 1993 L 95, 29, zuletzt geändert durch RL (EU), 2011/83, Abl. 2011, L 304, 64; dazu Staudenmayer EuZW 2022, 596 (597).

18 Krit. Ebner ZD 2022, 364 (mit Blick auf die Gefahr, dass „der Information Overload" zu- und das „Interesse am Schutz ‚eigener' Daten" abnehme).

19 Vgl. Staudenmayer EuZW 2022, 596, der in der Ersetzung der faktischen Kontrolle durch eine vertragliche Grundlage neben der AGB-Kontrolle das zentrale Element des Data Act sieht; kritisch dagegen Specht-Riemenschneider MMR 2022, 809 ff. die die Regelung als unzureichend ansieht.

20 Vgl. McGuire GRUR 2018, 128; Podszun/Pfeifer GRUR 2022, 953 (958).

21 Podszun/Pfeifer GRUR 2022, 953 (959).

22 Staudenmayer EuZW 2022, 596 (597 f.); kritisch Specht-Riemenschneider MMR 2022, 809 (816 f.).

23 Vgl. insb. ErwG 7, 24, 30 f. DA-E.

24 Bspw. Art. 1 III 3; ErwG 31, 35 DA-E.

25 Bomhard/Merkle RDi 2022, 168 Rn. 28 f.; Hennemann/Steinrötter NJW 2022, 1481 Rn. 16.

26 Bomhard/Merkle RDi 2022, 168 (172).

27 Vgl. auch ErwG 30 DA-E; Staudenmayer EuZW 2022, 596 (597).

28 Nach S. 2 kann sich die Frist in Folge der Komplexität oder der Anzahl der Anträge verlängern.

29 Marx/Sütthoff ZdiW 2022, 128 (132).

30 AA Specht-Riemenschneider MMR 2022, 809 (816); allerdings mit dem Hinweis, dass des Zugangsrecht dem grundrechtlich geschützten Recht des Dateninhabers nicht gerecht werde.

31 Rammos/Wilken DB 2022, 1241 (1244).

32 EuGH – C-604/10, ECLI:EU:C:2012:115 = GRUR 2012, 386 – Football DataCo Ltd. u. a./ Yahoo; Wiebe GRUR 2017, 338.

33 RL 96/9/EG vom 11.3.1996 über den rechtlichen Schutz von Datenbanken, ABl. 1996 L 077, 20.

34 So zu Recht Bomhard/Merkle RDi 2022, 168 (169).

35 Podszun/Pfeifer GRUR 2022, 953 (956).

36 So wohl Bomhard/Merkle RDi 2022, 168 (169) unter Hinweis auf ErwG 30 DA-E.

37 Bomhard/Merkle RDi 2022, 168; Rammos/Wilken DB 2022, 1241 (1242).

38 Bomhard/Merkle RDi 2022, 168 (169).

39 Vgl. Art. 3 I 2 Digitale-Inhalte-RL; § 312 I a 1 BGB.

40 Bomhard/Merkle RDi 2022, 168 (170).

41 Anders wohl Bomhard/Merkle RDi 2022, 168 (170).

42 Rammos/Wilken, DB 2022, 1241 (1243) nennen als Beispiel die Integration von Onboard-Entertainment.

43 Zum jeweiligen Maßstab sowie den Übereinstimmungen zwischen DA-E und Klausel-RL vgl. Staudenmayer EuZW 2022, 596 (598 ff.).

44 Vgl. aber Art. 13 VI DA-E, wonach der übrige Teil bei Abtrennbarkeit einer missbräuchlichen Klausel bindend bleibt.

45 So auch Specht-Riemenschneider MMR 2022, 809 (816).

46 So auch Rammos/Wilken DB 2022, 1241 (1243). Vgl. dazu Staudenmayer EuZW 2022, 596.

47 Vgl. zu Geheimnisschutzvereinbarungen McGuire WRP 2019, 679.

48 Diese Unterscheidung verdanken wir Frau Wiss. Mit. Alicia Sütthoff.

49 Vgl. Specht-Riemenschneider MMR 2022, 809 (810 f.).

50 Vgl. ErwG 14 DA-E.

51 Dazu Podszun/Pfeifer GRUR 2022, 953 (957).

52 ABl. 2003 L 124, 36.

53 Laut dem Statistischen Bundesamt zählen 99,4 % der 2.5 Mio. Unternehmen in Deutschland zu KMU. Darin enthalten sind 2,1 Mio. Kleinstunternehmen, die 18 % der Beschäftigten zählen, vgl. Statistisches Bundesamt, 55 % in kleinen und mittleren Unternehmen tätig, abrufbar unter: https://beck-link.de/6b5x5 (letzter Abruf: 10.1.2023).

54 Rammos/Wilken DB 2022, 1241 (1246).

55 Rammos/Wilken DB 2022, 1241 (1243); Staudenmayer EuZW 2022, 596 ff.