

Der Zugang zu IoT-Gerätedaten und ihre Nutzung unter dem Data Act

Effektiver Verbraucherschutz auf dem europäischen Binnenmarkt für Daten?

Von Dr. Hannes Henke, LL.M.oec., Halle/Saale*

Spätestens mit der im Februar 2020 von der EU-Kommission vorgelegten Datenstrategie hat sich der europäische Gesetzgeber auf die Fahne geschrieben, bestehende Hindernisse für einen reibungslos funktionierenden Binnenmarkt für Daten zu beheben.¹ Ein wesentlicher Baustein soll hierfür der am 11.1.2024 in Kraft getretene Data Act (DA)² sein, der weitestgehend ab dem 12.9.2025 Geltung beanspruchen wird. Ein Schwerpunkt des DA liegt dabei auf der Eröffnung von Zugängen zu solchen Daten, die bei der Nutzung von Geräten des Internet of Things (IoT) wie vernetzten Autos, Smart Home-Geräten oder Smartwatches erhoben werden. Zwar handelt es sich hierbei nicht um ein genuin verbraucherschützendes Regelungsregime. Vielmehr sollen die Daten zugunsten sämtlicher Nutzer zur Verfügung gestellt werden, um Marktungleichgewichten sowohl im B2C- als auch im B2B-Bereich entgegenzuwirken. Nichtsdestoweniger soll der DA das bestehende Verbraucherschutzrecht ergänzen (Art. 1 Abs. 9 DA) und zur Gewährleistung eines hohen Verbraucherschutzniveaus beitragen (ErwGr 9 DA). Dieses Bekenntnis ist schon deswegen zu begrüßen, weil IoT-Geräte häufig auch von Verbrauchern erworben und genutzt werden. Ob und inwieweit dieses Ziel mit den Regelungen des DA tatsächlich erreicht werden kann, soll im Folgenden eruiert werden. Besondere Aufmerksamkeit soll dabei auch darauf gerichtet werden, wie sich die vorgesehenen Rechte der Nutzer bzw. die Pflichten der beteiligten Wirtschaftsakteure privatrechtlich durchsetzen lassen.

I. Überblick und zentrale Begrifflichkeiten

Oggleich Daten ohne Qualitätsverlust geteilt und nicht-rivalisierend genutzt werden können, wird ihr ökonomisches Potential nach Ansicht des europäischen Gesetzgebers gegenwärtig noch nicht hinreichend ausgeschöpft. Ausgehend von diesem Befund soll der DA Zugänge zu Daten eröffnen und so ihre Nutzbarkeit befördern. Die hier relevanten Artt. 3 – 7 DA beruhen dabei auf der Erwägung, dass eine Vielzahl von ökonomisch werthaltigen Daten durch die Nutzung vernetzter Produkte und verbundener Dienste gewonnen wird. Ersteres meint einen Gegenstand, der (personenbezogene oder nicht-personenbezogene)³ Daten über seine Nutzung oder Umgebung erlangt, generiert oder erhebt und diese Daten – online oder offline – übermitteln kann (Art. 2 Nr. 5 DA). Unter einem verbundenen Dienst ist hingegen ein elektronischer Kommunikationsdienst wie etwa eine MobileApp zur Steuerung eines Smart Home-Gerätes zu verstehen, der zur vollständigen Funktionsfähigkeit des

vernetzten Produktes erforderlich ist oder die Funktionen des vernetzten Produkts ergänzt, aktualisiert oder anpasst (Art. 2 Nr. 6 DA). Zu den erfassten Daten zählen damit neben den Daten, die durch die Nutzung von IoT-Geräten selbst generiert werden (sog. Produktdaten, Art. 2 Nr. 15 DA), auch solche Daten, welche im Zusammenhang mit der Nutzung von IoT-Geräten während der Bereitstellung des Dienstes durch den Anbieter generiert werden (sog. verbundene Dienstdaten, Art. 1 Nr. 16 DA). Vom Regelungsregime der Artt. 3 ff. DA sind dabei auch solche Daten erfasst, die durch die Nutzung von virtuellen Assistenten (wie Alexa oder Siri) generiert werden, soweit diese Assistenten mit einem vernetzten Produkt oder verbundenen Dienst interagieren (Art. 1 Abs. 4 DA). Allerdings unterfallen insgesamt allein die Rohdaten den Art. 3 ff. DA, da hiervon abgeleitete oder aggregierte Daten gerade das Ergebnis zusätzlicher Investitionen seitens des Dateninhabers sind (ErwGr 15 S. 8 ff. DA). Mit Rücksicht auf die beschränkten Kapazitäten für die Erfüllung der Pflichten aus Artt. 3 – 5 DA bleiben nach Art. 7 Abs. 1 DA iVm dem Anhang der Empfehlung 2003/361/EG ferner Produkt- und verbundene Dienstdaten ausgeschlossen, deren Erhebung auf der Nutzung solcher vernetzten Produkte oder verbundenen Dienste beruht, die durch Kleinst- oder Kleinunternehmen hergestellt oder konzipiert werden; für mittlere Unternehmen gilt eine Karenzzeit von einem Jahr.

Insbesondere Artt. 4, 5 DA knüpfen darüber hinaus an „ohne Weiteres verfügbare Daten“ als eine qualifizierte Form der Produktdaten und verbundenen Dienstdaten an. Hierunter versteht Art. 2 Nr. 17 DA solche Daten, die ein Dateninhaber ohne unverhältnismäßigen Aufwand rechtmäßig von dem vernetzten Produkt oder verbundenen Dienst erhält oder erhalten kann. Nach dem Wortlaut des Art. 2 Nr. 12 DA gilt zwar die Einschränkung, dass „über eine einfache Bearbeitung hinausgegangen wird“. Da ein solches Erfordernis die gleichzeitige Voraussetzung der leichten Verfügbarkeit aber letztlich ad absurdum führen würde, muss allein maßgeblich bleiben, dass die Daten auf einfachem Weg zugänglich sind.⁴ Auch ein solches Verständ-

* Der Autor ist wissenschaftlicher Mitarbeiter und Habilitand an der Gundling-Professur für Bürgerliches Recht, Recht des Geistigen Eigentums und Wettbewerbsrecht an der Martin-Luther-Universität Halle-Wittenberg (Prof. Dr. Malte Stieper).

1 KOM(2020) 66 endg.

2 Verordnung (EU) 2023/2854 des Europäischen Parlaments und des Rates vom 13. Dezember 2023 über harmonisierte Vorschriften für einen fairen Datenzugang und eine faire Datennutzung.

3 Siehe Art. 1 Abs. 2 lit. a DA; zum Verhältnis von DA und DS-GVO siehe insbesondere Götz/Blöink MMR 2024, 451 ff.; noch zum DA-E auch Steinrötter GRUR 2023, 216 ff.

4 BeckOK Datenschutzrecht/Schild, 48. Ed., DA Art. 2 Rn. 97 f.

nis ändert aber nichts daran, dass in Bezug auf die Bestimmung der erfassten Daten erhebliches Konfliktpotential besteht.⁵ Ausgeschlossen bleiben aber jedenfalls solche Daten, die zwar bei der Produktnutzung generiert werden, deren Speicherung und Übermittlung außerhalb der sie generierenden Produktkomponente jedoch nicht vorgesehen ist (ErwGr 20 S. 6 DA).

Da die erfassten Daten auf Handlungen des Nutzers eines vernetzten Produkts bzw. verbundenen Dienstes beruhen, rückt der Gesetzgeber gerade den Nutzer ins Zentrum der Regelungen nach Artt. 3 – 5 DA, von denen nicht zum Nachteil des Nutzers abgewichen werden darf (Art. 7 Abs. 2 DA). Unter einem Nutzer versteht der DA eine natürliche oder juristische Person, die ein vernetztes Produkt besitzt oder der vertraglich zeitweilige Rechte für die Nutzung des vernetzten Produkts übertragen wurden oder die verbundenen Dienste in Anspruch nimmt (Art. 2 Nr. 12 DA). Mit Blick auf die Beziehung zwischen dem IoT-Gerät und der Person, die ohne Weiteres Verbraucher sein kann (vgl. ErwGr 18 S. 1 DA), ist damit entscheidend, dass diese rechtmäßigen Besitz am IoT-Gerät innehat.⁶ In der Folge können in Bezug auf ein vernetztes Produkt (wie etwa im Falle des Car-Sharings) durchaus mehrere Personen Nutzer sein, die auf unterschiedliche Weise zur Datengenerierung beitragen.

II. Erfordernis einer Datennutzungsvereinbarung

Die Nutzerzentriertheit des DA zeigt sich insbesondere daran, dass der Dateninhaber nach Art. 4 Abs. 13 DA zur Nutzung von ohne Weiteres verfügbaren Daten, bei denen es sich um nicht-personenbezogene Daten handelt, nur auf Grundlage eines Vertrages mit dem Nutzer nutzen darf. Hiervon bleibt zwar zunächst die Zulässigkeit der Erhebung und Speicherung der Daten unberührt.⁷ Dennoch folgt aus der Obliegenheit des Dateninhabers, eine Verwertungslizenz vom datengenerierenden Nutzer einzuholen, dass der ökonomische Wert von IoT-Gerätedaten zunächst dem Nutzer zugewiesen wird.⁸ Erstaunlich daran ist, dass die Nutzung von nicht-personenbezogenen Daten damit strengeren Voraussetzungen unterworfen wird als die Nutzung von Personendaten, bei denen sich die Zulässigkeit der Nutzung auch im Anwendungsbereich des DA (Art. 1 Abs. 5 DA) weiterhin aus dem Katalog der verschiedenen Erlaubnistatbestände des Art. 6 DS-GVO ergibt.⁹ Allerdings erweist sich das Erfordernis einer vertraglichen Vereinbarung zwischen Dateninhaber und Nutzer, wie sich nachfolgend zeigen wird, ohnehin weitestgehend um eine formale Hürde, da weder der Abschluss noch der Inhalt der Datenlizenz spezifischen Schranken unterliegen.¹⁰

1. Anwendbarkeit der §§ 312 ff. BGB

Zunächst können die §§ 312 ff. BGB im Regelfall keinen Schutz der betroffenen Verbraucher gegenüber dem Dateninhaber bieten, da ein Verbrauchervertrag iSd Vorschriften eine Leistungspflicht des Unternehmers (Dateninhaber) voraussetzt.¹¹ Eine solche wird bei einer Datennutzungsvereinbarung nach Art. 4 Abs. 13 DA im B2C-Verhältnis im Regelfall jedoch fehlen, da entlang der Lieferkette lediglich der Händler vertragliche Pflich-

ten gegenüber dem Verbraucher eingehen wird. Dateninhaber ist hingegen derjenige, der die Daten in der eigenen technisch-faktischen Herrschaftssphäre speichert oder die Datenspeicherung kontrolliert (vgl. Art. 2 Nr. 13 DA),¹² was häufig (aber nicht zwingend) der Hersteller des Produkts ist. Mit Blick auf das Widerrufsrecht nach § 312g BGB hat der BGH auch eine analoge Anwendung auf die Fälle, in denen eine Leistungspflicht seitens des Unternehmers fehlt, ausdrücklich abgelehnt.¹³

Ist der Dateninhaber jedoch im Einzelfall zu einer Leistung an den Verbraucher verpflichtet, so genügt nach § 312 Abs. 1a BGB jedenfalls die Bereitstellung personenbezogener Daten seitens des Verbrauchers, um den Anwendungsbereich der §§ 312 ff. BGB zu eröffnen. Gleiches muss aber auch im Falle der Bereitstellung von nicht-personenbezogenen Daten gelten.¹⁴ Hierfür spricht schon, dass § 312 Abs. 1a BGB nach dem Willen des Gesetzgebers lediglich eine klarstellende Funktion erfüllt und im Vergleich zur vorherigen Rechtslage, bei dem jedwedes vom Verbraucher zu leistende Entgelt genügte, keine Einschränkungen bewirken sollte.¹⁵ Zudem geht der DA gerade davon aus, dass personenbezogene und nicht-personenbezogene Daten gleichermaßen werthaltig sind, sodass sich eine Differenzierung danach, welche Daten als Gegenleistung an den Unternehmer geleistet werden, verbietet. Im Anschluss daran muss es schließlich auch genügen, dass der Verbraucher nicht die nicht-personenbezogenen Daten selbst leistet, sondern lediglich die Erlaubnis zu ihrer Nutzung.

2. Inhaltliche Grenzen

Auch hinsichtlich der inhaltlichen Ausgestaltung der Datennutzungsvereinbarung bestehen nur unzureichende Schranken zugunsten des Verbraucherschutzes. Anders als vom Unionsgesetzgeber angenommen (ErwGr 28 DA) kann insbesondere die Klausel-RL keinen effektiven Schutz versprechen.¹⁶ Aufgrund der unterschiedlichen Vertragsparteien wird die Datenlizenz im Regelfall kein unmittelbarer Bestandteil des Kaufvertrages über das Produkt sein. In der Folge handelt es sich bei der Bereitstellung der Daten um die Hauptleistungspflicht des Nutzers gegenüber dem Dateninhaber – die gemäß Art. 4 Abs. 2 Klausel-RL bzw. § 307 Abs. 3 BGB gerade nicht der Missbrauchskontrolle unterliegt. Mangels eines Kopplungsverbotens entsprechend Art. 6 Abs. 4 DS-GVO kann der Vertrieb von vernetzten Produkten darüber hinaus auch ohne Weiteres davon abhängig ge-

5 Hennemann/Steinrötter NJW 2024, 1 Rn. 11.

6 BeckOK Datenschutzrecht/Schild, 48. Ed., DA Art. 2 Rn. 75; Specht-Riemenschneider MMR 2022, 809 (813 f.); Wiebe GRUR 2023, 1569 (1570); Kaesling GRUR 2024, 821 (822); Antoine CR 2024, 1 Rn. 15.

7 Vgl. Metzger/Schweitzer ZEuP 2023, 42 (54); Hennemann/Steinrötter NJW 2024, 1 Rn. 21.

8 Siehe hierzu Hennemann/Steinrötter NJW 2024, 1 Rn. 35 ff.

9 Bomhard/Merkle RdI 2022, 168 Rn. 45; Metzger/Schweitzer ZEuP 2023, 42 (54 f.).

10 Specht-Riemenschneider MMR 2022, 809 (816).

11 BGH VuR 2021, 23 (24); BeckOK BGB/Martens, 70. Ed., BGB § 312 Rn. 9.

12 Specht-Riemenschneider MMR 2022, 809 (813).

13 BGH VuR 2021, 23 (24 f.).

14 BeckOK BGB/Martens, 70. Ed., BGB § 312 Rn. 9.1, wonach § 312 Abs. 1a BGB teleologisch weit auszulegen sei; für eine analoge Anwendung MüKoBGB/Wendehorst, 9. Aufl. 2022, BGB § 312 Rn. 60.

15 BT-Drs. 19/27653, 34 f.

16 Specht-Riemenschneider MMR 2022, 809 (817).

macht werden, dass die Nutzer dem Dateninhaber vertraglich die unbeschränkte Nutzung der nicht-personenbezogenen Daten erlauben.¹⁷ Insoweit droht folglich sogar ein Total-Buyout. Daher wird es vermutlich auch wenig nützen, dass Dateninhaber gemäß Art. 4 Abs. 14 DA nicht-personenbezogene Produktdaten nur zum Zwecke der Erfüllung ihres Vertrages mit dem Nutzer Dritten bereitstellen dürfen.

Eine Einschränkung der Nutzung der Daten folgt allerdings aus Art. 4 Abs. 13 DA insoweit, als der Dateninhaber die Daten nicht verwenden darf, um daraus Einblicke in die wirtschaftliche Lage und Vermögenswerte des Verbrauchers zu erlangen. Darüber hinaus sieht ErwGr 25 S. 3 DA lediglich vor, dass die Vertragsklauseln insgesamt transparent gestaltet werden müssen, was für die hier relevanten Fälle regelmäßig zugleich aus § 307 Abs. 1 S. 2 BGB folgen wird. Dies vermag indes kaum etwas daran zu ändern, dass die Dateninhaber sich weitreichende Befugnisse in Bezug auf die nicht-personenbezogene Daten einräumen lassen werden. Bei näherer Betrachtung erweist sich die Nutzerzentriertheit des Art. 4 Abs. 13 DA somit weitgehend als leere Hülle.

Allerdings beansprucht die Klausel-RL immerhin für die Nebenabreden der Datenlizenz Geltung. Bei der Beurteilung der Missbräuchlichkeit iSd Art. 3 Abs. 1 Klausel-RL bzw. der unangemessenen Benachteiligung nach § 307 Abs. 1 BGB wird darüber hinaus auch Art. 13 DA zu berücksichtigen sein.¹⁸ Die hier enthaltenen Klauselverbote gelten zwar unmittelbar nur im B2B-Verhältnis.¹⁹ Es wäre jedoch widersprüchlich, wenn der Verbraucherschutz hinter den Anforderungen im B2B-Verhältnis zurückstünde. In entsprechender Anwendung des Art. 13 Abs. 5 lit. d DA darf der Verbraucher durch eine AGB somit auch nicht daran gehindert werden, die Datennutzungsvereinbarung innerhalb einer angemessenen Frist zu kündigen.²⁰

3. IoT-Geräte auf dem Secondhand-Markt

Vor der erstmaligen Inbetriebnahme eines IoT-Gerätes wird es sich für den Dateninhaber im Regelfall als unproblematisch erweisen, eine Datennutzungsvereinbarung mit dem Nutzer abzuschließen. Der Vertragsschluss wird hierbei entweder bei der erstmaligen Inbetriebnahme des Produkts auf elektronischem Wege unmittelbar mit dem Dateninhaber oder vermittelt durch den Händler bei Abschluss des Kaufvertrages über das vernetzte Produkt erfolgen.²¹ Ungleich schwieriger dürfte die Einholung der Datenlizenz zugunsten des Dateninhabers aber werden, wenn IoT-Geräte durch den Erst-Nutzer auf dem Secondhand-Markt veräußert werden. Der Dateninhaber wird die für den Abschluss einer Datennutzungsvereinbarung erforderliche Kenntnis des Nutzerwechsels regelmäßig nur dann haben, wenn er jedwede Nutzung des Produktes von einer jeweiligen vorherigen Anmeldung des Nutzers in seinem Nutzerkonto abhängig macht. Dies dürfte zwar für zahlreiche Produkte wenig nutzerfreundlich sein. Fehlt es hieran, trägt der Dateninhaber aber das Risiko, die nicht-personenbezogenen Daten ohne eine entsprechende Lizenz zu nutzen und insoweit gegenüber dem neuen Nutzer auf Unterlassung zu haften (§ 1004 Abs. 1 BGB analog iVm § 823 Abs. 2 BGB, Art. 4 Abs. 13 DA).

III. Datenzugang zugunsten von Verbrauchern

Über die (vermeintliche) Stärkung der Position des Nutzers durch das Erfordernis einer Datennutzungsvereinbarung hinaus sollen die Vorgaben der Artt. 3 – 5 DA insbesondere auch einen Datenzugang zugunsten des Nutzers gewährleisten. Gerade Verbraucher werden dabei zwar eher selten einen unmittelbaren Nutzen aus dem Datenzugang ziehen können. Allerdings können Verbraucher jedenfalls mittelbar vom Datenzugang profitieren, sofern die Produktdaten und verbundene Dienstdaten für Folgemarkt-Dienste und sonstige Dienste genutzt werden (ErwGr 16, 20 DA). So ist der Zugang zu Daten, die von vernetzten Fahrzeugen erhoben werden, aktuell regelmäßig nur den Fahrzeugherstellern und ihren Vertragspartnern vorbehalten. Freien Kfz-Werkstätten bleibt es daher verwehrt, datengestützte Serviceleistungen zugunsten der Nutzer zu erbringen. Auch Kfz-Versicherern kann der Zugriff auf die erhobenen Daten gegenwärtig nicht ohne Weiteres gewährt werden, obgleich dies für den Nutzer im Rahmen eines „Pay-as-you-drive“-Tarifs durchaus von Interesse sein kann.²² Relevant kann der vorgesehene Datenzugang aber auch für Fälle sein, in denen ein solcher zwar grundsätzlich besteht, seine Art und Weise jedoch als unzureichend empfunden wird. Denkbar ist etwa, dass Nutzer die von ihrem Fitnesstracker erhobenen Daten von Drittanbietern analysieren lassen möchten, denen es bislang an einem effizienten Zugang zu den Daten fehlt.

Zwar begründet der DA keineswegs eine Pflicht seitens der Hersteller und Anbieter, potentiell verfügbare Daten zu erheben. Sofern Daten jedoch durch die Nutzung eines vernetzten Produkts oder eines verbundenen Dienstes generiert werden, sind diese grundsätzlich für eine angemessene Dauer zu speichern (ErwGr 24 S. 6 DA) und schließlich auch zugänglich zu machen. Hierbei statuiert Art. 3 Abs. 1 DA zunächst eine Pflicht zur Accessibility by Design (1.). Fehlt es am direkten Zugang zu den Daten, so hat der Nutzer nach Art. 4 Abs. 1 DA einen Anspruch darauf, dass ihm die Daten bereitgestellt werden (2.). Darüber hinaus kann der Nutzer gemäß Art. 5 Abs. 1 DA auch verlangen, dass die Daten einem Dritten bereitgestellt werden (3.).

1. Accessibility by Design, Art. 3 DA

a) *Inhalt.* Ungeachtet des konkreten Produkts, der Art oder der Nützlichkeit der Daten für den Nutzer sieht Art. 3 Abs. 1 DA vor, dass vernetzte Produkte und die mit ihnen verbundenen Dienste, die nach dem 12.9.2026 in der Union in Verkehr gebracht werden (Art. 1 Abs. 3 lit. a, Art. 50 UAbs. 3 DA), derart zu konzipieren und herzustellen sind, dass die Produktdaten

17 Bomhard/Merkle RDt 2022, 168 Rn. 46; Kerber GRUR Int. 2023, 120 (132); siehe auch Ehlen/Sebulke CR 2024, 84 Rn. 15.

18 Vgl. auch Bomhard MMR 2024, 71 (74); Schwamberger MMR 2024, 96 (98); zum Verhältnis von Art. 13 DA zur Klausel-RL bzw. den §§ 307 ff. BGB insgesamt, siehe Graf von Westphalen BB 2024, 515 ff.

19 Auch hier bleiben die Hauptleistungspflichten von der Klauselkontrolle ausgenommen, Art. 13 Abs. 8 DA.

20 Der Ausschluss des ordentlichen Kündigungsrechts unterliegt freilich bereits jetzt der Inhaltskontrolle nach § 307 Abs. 1 BGB, siehe MüKoBGB/Wurmnest, aaO, BGB § 307 Rn. 148.

21 Vgl. Staudenmayer NJW 2024, 1377 Rn. 16.

22 Auch die EU-Kommission hat diesen konkreten Bedarf als ein zentrales Problem erkannt, vgl. KOM(2022) 68 endg., 140.

– einschließlich der für die Auslegung und Nutzung dieser Daten erforderlichen Metadaten – standardmäßig für den Nutzer direkt zugänglich sind; entsprechendes gilt für die Anbieter verbundener Dienste. Obgleich es an einer ausdrücklichen Aussage hierüber fehlt, kann die Regelung aufgrund der vorausgesetzten Kontrolle über die technische Konzeption (vgl. ErwGr 21 DA) lediglich den Hersteller des vernetzten Produktes und den Anbieter des hiermit verbundenen Dienstes treffen.²³ Diese haben den Zugang einfach, sicher, unentgeltlich in einem umfassenden, strukturierten, gängigen und maschinenlesbaren Format zu gewähren. Erfüllt werden kann diese Pflicht etwa durch die Vorhaltung einer Benutzeroberfläche, über welche der Nutzer die entsprechenden Daten unmittelbar vom Gerät oder einem externen Server (des Herstellers oder eines Dritten, wie eines Cloud-Diensteanbieters) abrufen kann (ErwGr 22 DA). Für den Fall einer Mehrzahl von Nutzern eines IoT-Gerätes und der daraus folgenden (unterschiedlichen) Berechtigungen verweist ErwGr 21 DA auf die Möglichkeit, die jeweiligen Daten über individuelle Nutzerkonten zugänglich zu machen.

Unklar bleibt dabei, ob die Pflicht zur Bereitstellung schon dann erfüllt wird, wenn dem Nutzer lediglich ein In-situ-Zugang gewährt wird.²⁴ So können die Produkte laut ErwGr 22 S. 6 DA zwar derart konzipiert sein, dass die Daten u.a. auch in einer von dem Nutzer oder Dritten ausgewählten IT-Umgebung verarbeitet werden können. Eine Nutzbarkeit der Daten ist hier nach aber gerade nicht zwingend vorgesehen, was im Widerspruch zur allgemeinen Zielsetzung des DA insgesamt steht. So kann ein Leserecht allein kaum als Beitrag zur optimalen Verteilung von Daten zum Nutzen der Gesellschaft (ErwGr 2 S. 1 DA) verstanden werden.²⁵ Ist die Nutzbarkeit jedoch gegeben, so unterliegt der Nutzer keinen Beschränkungen, sodass er die Daten insbesondere auch an Dritte weitergeben darf (ErwGr 30 DA).

Problematisch ist, dass die Pflicht zur Gewährleistung der Zugänglichkeit unter dem Vorbehalt der Relevanz sowie der technischen Durchführbarkeit steht, was den Herstellern und Anbietern auch mangels einer weiteren Konkretisierung durch den DA zunächst einen erheblichen Spielraum bei der Gestaltung ihrer Produkte und Dienste lässt.²⁶ Beachtenswert ist jedoch, dass gemäß ErwGr 14 S. 4, 20 S. 10 DA gegebenenfalls durch das Unionsrecht, das nationale Recht oder durch Entscheidungen der Wettbewerbsbehörden vorgegeben werden kann, welche Daten von einem vernetzten Produkt bereitzustellen sind.

b) Individuelle Durchsetzung. Ungeachtet der damit einhergehenden Rechtsunsicherheit verschafft Art. 3 Abs. 1 DA schon nach seinem Wortlaut kein subjektives Recht der Nutzer gegenüber den Herstellern oder Anbietern. In systematischer Hinsicht wird dies dadurch gestützt, dass Art. 3 DA – anders als Art. 4 Abs. 3, 9 DA – keinen Verweis auf mögliche Rechtsmittel des Nutzers oder eine mögliche Beschwerde bei der zuständigen Behörde nach Art. 34 Abs. 5 lit. b DA enthält. Mangels eines korrespondierenden Rechts kann ein Verstoß gegen die Pflicht aus Art. 3 Abs. 1 DA damit weder unmittelbar eingeklagt noch mittels einer Beschwerde bei der zuständigen Behörde iSd Art. 38 DA durchgesetzt werden.²⁷ Hierfür spricht schließlich auch, dass Nutzern im Falle eines Verstoßes gegen Art. 3 Abs. 1 DA

ohnehin ein Anspruch auf Bereitstellung der Daten nach Art. 4 Abs. 1 DA zusteht.²⁸

Allerdings kann sich die fehlende Zugänglichkeit der Daten als ein Mangel des vernetzten Produktes bzw. des verbundenen Dienstes darstellen, sodass jedenfalls Sekundäransprüche zugunsten des Nutzers bestehen.²⁹ Bei einem vernetzten Produkt handelt es sich regelmäßig um eine Ware mit digitalen Elementen iSd § 327a Abs. 3 BGB, sodass sich das Bestehen eines Mangels nach § 475b BGB richtet. Gemäß 475b Abs. 4 Nr. 1 iVm § 434 Abs. 3 S. 1 Nr. 1 BGB muss sich das Produkt damit insbesondere für die gewöhnliche Verwendung eignen. Bei deren Bestimmung sind im Wege der unionsrechtskonformen Auslegung (Art. 7 Abs. 1 lit. a Warenkauf-RL) auch das bestehende Unionsrecht und nationale Recht, technische Normen oder sektorspezifische Verhaltenskodizes zu berücksichtigen.³⁰ Zwar führt danach nicht jeder Verstoß gegen produktbezogene Regelungen automatisch zu einem Mangel. Einigkeit besteht jedoch insoweit, als ein Mangel jedenfalls dann vorliegt, wenn aufgrund eines Rechtsverstoßes die Gefahr der Untersagung zur bestimmungsgemäßen Nutzung besteht.³¹ Anders als etwa bei Vorschriften des Produktsicherheitsrechts ist dies mit Blick auf einen Verstoß gegen Art. 3 Abs. 1 DA nicht der Fall.³² Vor dem Hintergrund der unionsrechtlich vorgegebenen normativen Prägung des maßgeblichen Erwartungshorizonts kann die Pflicht aus Art. 3 Abs. 1 DA, die sich unmittelbar auf die Funktionalität des Produktes auswirkt, jedoch nicht unberücksichtigt bleiben. Auch mit Blick auf den Grundsatz des *effet utile* muss vielmehr angenommen werden, dass der vernünftige Durchschnittskäufer³³ erwarten darf, dass ein vernetztes Produkt einen direkten Zugang zu den Produktdaten entsprechend Art. 3 Abs. 1 DA gewährt. Mit den gleichen Erwägungen lässt sich ein Sachmangel schließlich auch durch das Fehlen der üblichen Beschaffenheit nach § 475b Abs. 4 Nr. 1 iVm § 434 Abs. 3 S. 1 Nr. 2 begründen.³⁴ Entsprechendes gilt für verbundene Dienste nach § 327e Abs. 3 Nr. 1, 2 BGB (vgl. Art. 8 Abs. 1 lit. a Digitale-Inhalte-RL). Allerdings richten sich die aus dem Vorliegen eines Mangels folgenden Ansprüche der Verbraucher mangels eines entsprechenden Vertragsverhältnisses typischerweise nicht gegen den Her-

23 Steinrötter GRUR 2023, 216 (220); Weinhold/Schröder ZD 2024, 306 (309); so wohl auch Metzger/Schweitzer ZEuP 2023, 42 (52).

24 Siehe Podszun/Pfeifer GRUR 2022, 953 (957); einen In-situ-Zugang als ausreichend erachtend Specht-Riemenschneider MMR 2022, 809 (815); Kaesling GRUR 2024, 821 (824); Ehlen/Sebulke CR 2024, 84 Rn. 11; aA Wiebe GRUR 2023, 1569 (1571).

25 Siehe auch Kaesling GRUR 2024, 821 (825).

26 Kritisch auch Kaesling GRUR 2024, 821 (824).

27 AA wohl Kaesling GRUR 2024, 821 (823).

28 Art. 4 Abs. 1 DA kommt insoweit ein Rechtsbehelfscharakter iSe Nacherfüllung zu, siehe Specht-Riemenschneider MMR 2022, 809 (815); Schmidt-Kessel MMR 2024, 75 (80).

29 So auch Metzger/Schweitzer ZEuP 2023, 42 (52).

30 Vgl. auch BT-Drs. 19/28174, 8, wonach die Rechtsprechung rechtliche Vorschriften „bei der Beurteilung der gewöhnlichen Verwendungseignung einer Sache angemessen berücksichtigen wird“.

31 BGH NJW 2019, 1133 Rn. 4 ff.; BeckOK BGB/Faust, 70. Ed., BGB § 434 Rn. 79.

32 Zu den Sanktionen im Falle eines Verstoßes gegen die Vorgaben des DA, siehe Art. 40 DA.

33 BeckOK BGB/Faust, 70. Ed., BGB § 434 Rn. 75.

34 Drexler et al., Max Planck Institute for Innovation and Competition Research Paper No. 22-05, Rn. 74, DOI: <http://dx.doi.org/10.2139/ssrn.4136484>.

steller, sondern allein gegen den Verkäufer des Produkts. Für den Hersteller selbst folgt eine vertragliche Haftung wegen eines Verstoßes gegen Art. 3 Abs. 1 DA dementsprechend allenfalls gegenüber den Händlern. Anderes mag mit Blick auf die Anbieter verbundener Dienste gelten, die teilweise auch selbst unmittelbar Vertragspartner der Verbraucher sein werden.

c) Kollektive Durchsetzung. Über die mittelbare Durchsetzung der Pflicht aus Art. 3 Abs. 1 DA gegenüber den Händlern von IoT-Geräten hinaus kommt insbesondere auch eine Durchsetzung im Wege des kollektiven Rechtsschutzes in Betracht. Ausgangspunkt hierfür bildet Art. 48 DA, wodurch der DA in den Anhang I der Verbandsklagen-RL aufgenommen wurde. Auch § 2 Abs. 2 UKlaG ist dementsprechend um den DA zu erweitern. Dementsprechend können Verstöße gegen den DA insoweit durch Verbandsklagen verfolgt werden, als die betroffene Bestimmung gerade dem Schutz von Verbrauchern dient (Art. 2 Abs. 1 Verbandsklagen-RL). Mit Blick auf Art. 3 Abs. 1 DA ist es nach ErwGr 14 Verbandsklagen-RL jedenfalls unschädlich, dass die Vorschrift auf „Nutzer“ und damit nicht explizit auf Verbraucher abstellt. Da der DA insgesamt jedenfalls auch die Interessen der Verbraucher schützen sowie ein hohes Verbraucherschutzniveau sicherstellen soll (ErwGr 9, Art. 1 Abs. 9 DA) und der europäische Gesetzgeber ausweislich des Titels des Kapitels II („Datenweitergabe von Unternehmen an Verbraucher und zwischen Unternehmen“) gerade in Bezug auf die Artt. 3-7 DA Verbraucher in den Blick nimmt, kann vielmehr von einem hinreichenden verbraucherschützenden Charakter des Art. 3 Abs. 1 DA ausgegangen werden.³⁵ Im Fall eines Verstoßes gegen die Pflicht zur Accessibility by Design können qualifizierte Einrichtungen damit insbesondere die Unterlassung des Inverkehrbringens der betroffenen vernetzten Produkte und des Anbietens der betroffenen verbundenen Dienstleistungen verlangen. Entsprechendes ergibt sich auch aus dem lauterkeitsrechtlichen Unterlassungsanspruch gemäß § 8 UWG wegen eines Verstoßes gegen eine Marktverhaltensregelung nach § 3a UWG, der zugunsten von Verbraucherverbänden zudem einen Anspruch auf Gewinnabschöpfung nach § 10 UWG eröffnet. Da Art. 3 Abs. 1 DA Anforderungen an vernetzte Produkte und verbundene Dienste stellt, sofern diese in der Union in den Verkehr gebracht werden sollen, hat Art. 3 Abs. 1 DA jedenfalls auch eine sekundäre marktbezogene Schutzfunktion.³⁶

2. Recht auf Datenbereitstellung, Art. 4 DA

a) Inhalt und Modalitäten. Fehlt es an der direkten Zugänglichkeit der Daten, so haben die Nutzer nach Art. 4 Abs. 1 DA einen gesetzlichen³⁷ Anspruch gegen den Dateninhaber, dass ihnen ohne Weiteres verfügbare Daten einschließlich der Metadaten unverzüglich, einfach, sicher, unentgeltlich, in einem umfassenden, gängigen und maschinenlesbaren Format und – falls relevant und technisch durchführbar – in der gleichen Qualität wie für den Dateninhaber kontinuierlich und in Echtzeit bereitgestellt werden. Zur Bestimmung der Modalitäten der Datenbereitstellung können die Maßstäbe herangezogen werden, die für Art. 20 Abs. 1 DS-GVO entwickelt wurden, an den sich Art. 4 Abs. 1 DA auch im Übrigen anlehnt.³⁸ Ausgelöst wird der Da-

tenzugangsanspruch, der ausdrücklich kein „right to hack“ beinhaltet (Art. 4 Abs. 11 DA),³⁹ durch ein einfaches Verlangen des Nutzers. Wünschenswert wäre hierfür eine entsprechende Schnittstelle unmittelbar im Nutzerkonto (vgl. ErwGr 21 S. 4 DA), die jedoch nicht zwingend seitens der Hersteller bzw. Anbieter vorzuhalten ist.⁴⁰ Wird eine solche Benutzeroberfläche jedoch vorgesehen, so muss diese hinreichend transparent sein; auch im Übrigen darf dem Nutzer die Ausübung seiner Rechte nicht durch den Dateninhaber erschwert werden (Art. 4 Abs. 4 DA). Allerdings bleibt auch hier unklar, inwieweit bereits die Gewährung eines In-situ-Zugangs die Pflicht der Bereitstellung erfüllt.⁴¹

Ein Vertrag zwischen Nutzer und Dateninhaber über die Datennutzung ist insoweit nicht erforderlich.⁴² Der Nutzer kann die bereitgestellten Daten vielmehr kraft Gesetzes frei verwenden und insbesondere auch an Dritte weitergeben (ErwGr 30 S. 1, 2 DA). Einschränkungen können nach Art. 4 Abs. 2 DA jedoch insoweit vorgesehen werden, als dies der Einhaltung von Sicherheitsanforderungen dient. Auch der Schutz von Geschäftsgeheimnissen (Art. 4 Abs. 6 – 8 DA) und datenschutzrechtliche Positionen Dritter (Art. 4 Abs. 12 DA) können den Zugangsanspruch begrenzen. Für den B2C-Bereich von geringer Relevanz ist die Einschränkung der Nutzung nach Art. 4 Abs. 10 DA, wonach der Nutzer einem Wettbewerbsverbot hinsichtlich der Entwicklung konkurrierender Produkte sowie einem Verbot des Ausspähens der wirtschaftlichen Lage, der Vermögenswerte oder der Produktionsmethoden des Herstellers unterliegt.

b) Durchsetzung. Zwar kann der Anspruch aus Art. 4 Abs. 1 DA zunächst durch den Nutzer selbst gerichtlich geltend gemacht werden.⁴³ Allerdings dürfte es gerade für Verbraucher jedenfalls bislang an entsprechenden Anreizen fehlen.⁴⁴ In Bezug auf die vertraglichen Beschränkungen und Verbote nach Art. 4 Abs. 2 DA sowie hinsichtlich der Ablehnung der Datenweitergabe aufgrund des Bestehens von Geschäftsgeheimnissen können Nutzer zudem Beschwerde bei der zuständigen Behörde einlegen oder mit dem Dateninhaber vereinbaren, gemäß Art. 10 Abs. 2 DA eine Streitbeilegungsstelle mit der Angelegenheit zu befassen (Art. 4 Abs. 3, Abs. 9 DA). Auch hier muss bezweifelt, jedenfalls aber abgewartet werden, inwieweit sich das Recht auf Beschwerde im Falle eines erfolglosen Datenzugangsverlangens als erfolgversprechend erweist.

Jedenfalls theoretisch kann ein drohendes Defizit bei der individuellen Durchsetzung wiederum durch den Mechanismus des kollektiven Rechtsschutzes zugunsten von Verbrauchern inklusive kleiner Unternehmen (§ 1 Abs. 2 VDuG) überwunden wer-

35 BeckOK Datenschutzrecht/Richter, 48. Ed., DA Art. 48 Rn. 18.

36 Metzger/Schweitzer ZEuP 2023, 42 (52 Fn. 36).

37 Metzger/Schweitzer ZEuP 2023, 42 (47, 62).

38 Steinrötter GRUR 2023, 216 (221).

39 Specht-Riemenschneider MMR 2022, 809 (821).

40 Vgl. auch Art. 3 Abs. 3 lit. e DA.

41 Zum DA-E siehe auch Podszun/Pfeifer GRUR 2022, 953 (957); Kerber GRUR Int. 2023, 120 (124); für ein Recht auf Datenkopie Steinrötter GRUR 2023, 216 (221).

42 Metzger/Schweitzer ZEuP 2023, 42 (47); Hennemann/Steinrötter NJW 2024, 1 Rn. 13.

43 Wiebe GRUR 2023, 1569 (1571); Weinhold/Schröder ZD 2024, 306 (309).

44 So auch Metzger/Schweitzer ZEuP 2023, 42 (58); Kaesling GRUR 2024, 821 (827).

den. Denkbar scheint dies vor allem für solche Fälle, in denen hinsichtlich konkreter Dateninhaber strukturelle Mängel bei der Erfüllung der Pflicht aus Art. 4 Abs. 1 DA erkennbar werden. Als taugliches Instrument kommt hierfür insbesondere auch eine Abhilfeklage gemäß § 14 VDuG in Betracht. Über Art. 9 Verbandsklagen-RL hinaus kann im nationalen Recht über die „Abhilfe“ in Form von Schadenersatz, Reparatur, Ersatzleistung, Preisminderung, Vertragsauflösung oder Preiserstattung hinaus jedwede Leistung und damit auch die gesetzlich⁴⁵ vorgesehene Bereitstellung von Daten begehrt werden. Hierfür spricht auch § 1 Abs. 1 VDuG, wonach eine Abhilfeklage für alle bürgerlichen Rechtsstreitigkeiten zwischen Verbrauchern und Unternehmen in Betracht kommt.⁴⁶ Unschädlich ist dabei, dass die jeweiligen Ansprüche der einzelnen Verbraucher auf individuell erzeugte Datensätze und damit gerade nicht auf einen identischen Leistungsgegenstand gerichtet sind. Nach § 15 Abs. 1 VDuG genügt es, dass die Ansprüche im Wesentlichen gleichartig sind. Das wird hinsichtlich des Anspruchs auf die Bereitstellung der Produkt- und verbundenen Dienstdaten nach Art. 4 Abs. 1 DA regelmäßig dann der Fall sein, wenn den Ansprüchen ein identisches Produkt bzw. ein identischer Dienst zugrunde liegt.

3. Recht auf Datenbereitstellung an Dritte, Art. 5 DA

a) *Inhalt und Modalitäten.* Überwiegend wird das ökonomische Interesse an der Nutzung der Daten vor allem auf Seiten dritter Wirtschaftsakteure zu verorten sein. Vor diesem Hintergrund sieht Art. 5 Abs. 1 DA einen (zusätzlichen)⁴⁷ Anspruch des Nutzers zur Bereitstellung der Daten an Dritte vor. Dieser entspricht sowohl in seinen Voraussetzungen als auch seinem Inhalt nach weitgehend dem Zugangsanspruch aus Art. 4 Abs. 1 DA. So hat der Dateninhaber auf Verlangen eines Nutzers oder einer im Namen eines Nutzers handelnden Partei einem Dritten nach Art. 5 Abs. 1 DA ohne Weiteres verfügbare Daten sowie entsprechende Metadaten unverzüglich in derselben Qualität, die dem Dateninhaber zur Verfügung steht, einfach, sicher, in einem umfassenden, strukturierten, gängigen und maschinenlesbaren Format und, soweit relevant und technisch durchführbar, kontinuierlich und in Echtzeit bereitzustellen. Damit bestehende Ungleichgewichte nicht verfestigt werden, ist dieser Anspruch insoweit eingeschränkt, als Gatekeeper iSd Art. 3 DMA nicht durch die Datenbereitstellung begünstigt werden dürfen (Art. 5 Abs. 3 lit. b DA).⁴⁸ Abgesehen von der weiteren Einschränkungen nach Art. 5 Abs. 2 DA für Testdaten von noch nicht in Verkehr gebrachten Produkten, die für Verbraucher nicht von Relevanz sind, ist die Ausgestaltung der Bereitstellungspflicht nach Art. 5 Abs. 4 – 13 DA weitestgehend mit Art. 4 DA vergleichbar.

Beachtenswert ist, dass das Dreiecksverhältnis zwischen Nutzer, Dateninhaber und Datenempfänger durch ein entsprechendes Vertragsnetz gekennzeichnet ist. Bei dem Dateninhaber wird es sich regelmäßig um einen Unternehmer handeln; entsprechend gilt schon mit Blick auf die Begriffsbestimmung nach Art. 2 Nr. 14 DA auch für den Datenempfänger. Die beidseitige Unternehmereigenschaft ist deswegen von Belang, weil die Bereitstellung der Daten im B2B-Bereich nach Art. 8 DA eine entspre-

chende Vereinbarung zwischen dem Dateninhaber und dem Datenempfänger verlangt. Ein Verlangen des Nutzers zur Weitergabe der Daten an Dritte löst seitens des Dateninhabers folglich einen Kontrahierungszwang aus.⁴⁹ Hierbei muss der Dateninhaber die Daten insbesondere zu fairen, angemessenen und nicht-diskriminierenden Bedingungen und in transparenter Weise zur Verfügung zu stellen, wobei er vom Datenempfänger auch ein angemessenes Entgelt verlangen darf (Art. 9 DA).⁵⁰ Die Vereinbarung unterliegt zudem einer AGB-Kontrolle nach Art. 13 DA.⁵¹

Für das B2C-Verhältnis von Relevanz ist hingegen, dass sich die Befugnis zur Nutzung der an den Datenempfänger bereitgestellten Daten vor allem nach der Vereinbarung des Dritten mit dem Nutzer richtet (Art. 6 Abs. 1 DA).⁵² Diese Vereinbarung hat zunächst die Vorgaben des Art. 6 Abs. 2 DA zu berücksichtigen; entgegenstehende Klauseln sind nach Art. 7 Abs. 2 DA unwirksam. Neben dem allgemeinen Wettbewerbsverbot (lit. e) und der generellen Pflicht zur Wahrung von Geschäftsgeheimnissen (lit. g) gilt gerade gegenüber Verbrauchern, dass diese nicht daran gehindert werden dürfen, die Daten anderen Parteien bereitzustellen (lit. h). Außerdem darf der Dritte den Nutzer bei der Ausübung seines Rechts aus Art. 5 DA nicht manipulieren oder ihm Wahlmöglichkeiten auf nicht neutrale Weise anbieten (lit. a). Abgesehen von den weiteren Einschränkungen in Bezug auf das Profiling (lit. b), die Bereitstellung der Daten gegenüber anderen Dritten (lit. c) sowie insbesondere gegenüber Gatekeepern nach Art. 3 DMA (lit. d) und die Verwendung mit negativen Sicherheitsfolgen für das Produkt bzw. den Dienst (lit. f) können die Nutzungszwecke grundsätzlich frei bestimmt werden. Anders als die Datennutzungsvereinbarung zwischen dem Verbraucher und dem Produkthersteller iSd Art. 4 Abs. 13 DA wird diese Vereinbarung in vielen Fällen einer Inhaltskontrolle nach §§ 307 ff. BGB unterliegen. Grund hierfür ist, dass die Erlaubnis zur Datennutzung regelmäßig neben eine weitere (monetäre) Leistungspflicht des Verbrauchers treten wird. So wird ein Kfz-Versicherer nicht schon allein die Erlaubnis zur Nutzung der vom Kfz-Hersteller erhobenen Fahrdaten als Versicherungsprämie anerkennen. Sofern die Erlaubnis zur Datennutzung aber neben eine weitere monetäre Gegenleistung des Verbrauchers an den Datenempfänger tritt, wird es sich hierbei im Regelfall um eine kontrollfähige Preisnebenabrede handeln.⁵³ Insofern kann sich der Datenempfänger durch AGB nicht die Befugnis einräumen lassen, die Daten schrankenlos und dauerhaft zu

45 Nach Art. 3 Nr. 1 Verbandsklagen-RL gilt ein weiter Verbraucherbegriff, der die Einbeziehung gesetzlicher Ansprüche erlaubt; vgl. auch Röhmer-VuR 2023, 332 (333).

46 Siehe ausdrücklich auch BT-Drs. 20/6520, 69.

47 Specht-Riemenschneider MMR 2022, 809 (816).

48 Entsprechendes gilt für die nach Art. 4 Abs. 1 DA erlangten Daten, Art. 5 Abs. 3 lit. a. c DA.

49 Vgl. auch Art. 12 Abs. 1 DA.

50 Zur „FRAND-isierung“ des digitalen Unternehmensprivatrechts, siehe Deng ZfPW 4/2024 (fE).

51 Umfassend hierzu Schwamberger MMR 2024, 96 ff.; Jung ZIP 2024, 1565 ff.

52 Hennemann/Steinrötter NJW 2022, 1481 Rn. 20; Schmidt-Kessel MMR 2024, 75 (80).

53 Speziell zu Preisnebenabreden in Bezug auf die Bereitstellung von Daten siehe Hacker ZfPW 2019, 148 (187); MüKoBGB/Wurmnest, aaO, BGB § 307 Rn. 22.

nutzen. So ist im Rahmen des § 307 Abs. 1, Abs. 2 BGB auch der in ErwGr 38 S. 1 DA betonte Grundsatz der Datenminimierung zu berücksichtigen, wonach Dritte nur auf solche Daten Zugriff erhalten sollen, die für die Erbringung des vom Nutzer verlangten Dienstes erforderlich sind. Im Zweifelsfall richtet sich der Umfang der eingeräumten Nutzungserlaubnis folglich danach, was zur Erbringung des Dienstes notwendig ist.⁵⁴

Allerdings kann hieraus nicht geschlossen werden, dass Nutzern die Möglichkeit verwehrt bleibt, die Daten unabhängig von einem in Anspruch genommenen Dienst zu monetarisieren. Auch mit Blick auf die betonte Nutzerhoheit muss es vielmehr auch zulässig sein, dass Verbraucher „ihre“ Produktdaten auch isoliert an Dritte veräußern. In diesem Fall bleibt eine AGB-Kontrolle des Inhalts der gegenseitigen Leistungspflichten und damit insbesondere eine Kontrolle des Umfangs der Zweckvereinbarung jedoch ausgeschlossen.

b) Durchsetzung. Auch der Anspruch aus Art. 5 Abs. 1 DA kann zunächst individuell durch die betroffenen Nutzer durchgesetzt werden.⁵⁵ Wiederum ist fraglich, ob der kollektive Rechtsschutz in Form der Abhilfeklage das Instrumentarium zur Durchsetzung des Anspruchs aus Art. 5 Abs. 1 DA ergänzen kann. Dies muss hier aber schon deswegen ausscheiden, da der Anspruch auf Leistung an einen Dritten gerichtet ist, der regelmäßig Unternehmer sein wird. Auch wenn Verbraucher von den hierdurch ermöglichten Diensten auf den nachgelagerten Märkten mittelbar profitieren, kann die Bereitstellung von Daten nicht als Leistung an die betroffenen Verbraucher iSd § 14 VDuG verstanden werden. Obgleich der Nutzer eines IoT-Gerätes zwar im Ausgangspunkt die Hoheit über die Daten hat, zeigen insbesondere die Regelungen der „Gegenleistung“ seitens des Datenempfängers nach Art. 9 DA, dass die Bereitstellung der Daten als Leistung gerade an diesen zu verstehen ist.

Ohnehin fehlt es hinsichtlich der Pflicht zur Datenbereitstellung an Dritte an einem Bedürfnis nach einer kollektiven Durchsetzung zugunsten von Verbrauchern, da der Zugangsanspruch vielmehr unmittelbar von den begünstigten Datenempfängern durchgesetzt werden kann. Auf die Frage der Abtretbarkeit des Anspruchs aus Art. 5 Abs. 1 DA kommt es dabei nicht an,⁵⁶ da der Dritte durch das Verlangen des Nutzers oder einer im Namen eines Nutzers handelnden Partei bereits ein eigenes Forderungsrecht gegenüber dem Dateninhaber erwirbt.⁵⁷ Deutlich wird dies vor allem in Art. 5 Abs. 12 DA. So verweist Art. 5 Abs. 12 lit. a DA für den Fall der Verweigerung der Datenweitergabe seitens des Dateninhabers unter Berufung auf den Schutz von Geschäftsgeheimnissen auf das Recht zur Beschwerde bei der zuständigen Behörde. Dies impliziert, dass durch die Verweigerung zur Datenweitergabe seitens des Dateninhabers ein subjektives Recht des Dritten iSd Art. 38 Abs. 1 DA verletzt wird.

IV. Vorvertragliche Informationspflichten

Die Pflichten zur Accessibility by Design nach Art. 3 Abs. 1 DA sowie zur Bereitstellung der Daten nach Artt. 4, 5 DA werden schließlich durch Informationspflichten nach Art. 3 Abs. 2, 3 DA flankiert, die regelmäßig neben die datenschutzrechtlichen

Informationspflichten nach Artt. 13 f. DS-GVO treten werden (Art. 1 Abs. 5 DA).

1. Inhalt

So sind dem Nutzer nach Art. 3 Abs. 2 lit. a – c DA vor Abschluss eines Kauf-, Miet- oder Leasingvertrags über ein vernetztes Produkt verschiedene produktbezogene Informationen bereitzustellen. Hierzu gehören die Art, das Format und der geschätzte Umfang der potentiellen Produktdaten sowie die Angaben, ob das Produkt in der Lage ist, die Daten kontinuierlich und in Echtzeit zu generieren und auf einem Gerät oder einem externen Server zu speichern. Neben der Speicherdauer der generierten Daten muss auch darüber informiert werden, wie der Nutzer auf die Daten zugreifen, sie abrufen oder gegebenenfalls löschen kann; dies schließt die technischen Mittel sowie die entsprechenden Nutzungsbedingungen und die Dienstqualität ein (lit. d). Diese Informationspflichten treffen dabei nicht zwingend den Hersteller, sondern vielmehr den Verkäufer, Vermieter oder Leasinggeber des vernetzten Produktes und damit gerade den Vertragspartner des Verbrauchers.

Neben die Informationspflichten aus Art. 3 Abs. 2 DA treten die Informationspflichten der Anbieter verbundener Dienste nach Art. 3 Abs. 3 DA. Diese müssen vor Abschluss des Vertrages über die Erbringung des verbundenen Dienstes zunächst über die Art, den geschätzten Umfang und die Häufigkeit der Erhebung von Produkt- bzw. verbundene Dienstdaten, die Modalitäten deren Speicherung sowie die Modalitäten des Zugriffs hierauf durch den Nutzer informieren (lit. a, b). Zugleich hat der Anbieter über die Identität des Dateninhabers einschließlich Mittel zu seiner Kontaktierung (lit. d, e), die Nutzung der erhobenen Daten und ihre mögliche Weitergabe an Dritte durch den Dateninhaber (lit. c) sowie über potentiell betroffene Geschäftsgeheimnisse (lit. h) zu informieren. Die Informationspflicht erstreckt sich zudem auf die Rechte des Nutzers aus Art. 5 DA sowie das Recht zur Beschwerde (lit. f, g). Schließlich hat der Anbieter auch über die nach Art. 4 Abs. 13 DA erforderliche Datennutzungsvereinbarung zwischen Nutzer und Dateninhaber, konkret über dessen Dauer sowie die Möglichkeiten ihrer vorzeitigen Beendigung, zu informieren (lit. i).

2. Modalitäten

Sowohl die Verkäufer, Vermieter und Leasinggeber als auch die Anbieter von verbundenen Diensten haben die genannten Informationen in klarer und verständlicher Weise bereitzustellen. Eine bestimmte Form der Informationen ist hierbei zwar nicht ausdrücklich vorgesehen. Denkbar ist daher auch, eine URL-Adresse im Internet zu unterhalten, auf die per Web-link oder QR-Code – vor Vertragsschluss – verwiesen wird

54 Vgl. Heinzke BB 2023, 201 (204) mit Verweis auf die urheberrechtliche Zweckübertragungslehre (§ 31 Abs. 5 UrhG).

55 Wiebe GRUR 2023, 1569 (1571); Weinhold/Schröder ZD 2024, 306 (309).

56 Gegen eine Abtretbarkeit Wiebe GRUR 2023, 1569 (1572); aA Kaesling GRUR 2024, 821 (828).

57 So wohl auch Etzkorn RDi 2024, 116 Rn. 34; aA Specht-Riemenschneider MMR 2022, 809 (816).

(ErwGr 24 S. 4 DA). Über die bloße Möglichkeit zur Kenntnisnahme hinaus ist dabei auch zu gewährleisten, dass die Informationen abgespeichert werden können (ErwGr 24 S. 5 DA). Das Erfordernis der Klarheit und Verständlichkeit verlangt ferner, dass die Art und Weise der Information einschließlich ihrer Sprache am adressierten Nutzerkreis auszurichten ist.⁵⁸ Um die Information vor Vertragsschluss nicht zu einer bloßen Formalie herabzustufen, sind die Informationen zudem vor Abgabe der Willenserklärung des Nutzers zu erteilen, wobei dem Nutzer eine überlegte Entscheidung über den Vertragsschluss ermöglicht werden muss.

3. Rechtsfolgen von Verstößen

Der DA selbst trifft keine Aussage über die privatrechtlichen Folgen eines Verstoßes gegen die Informationspflichten aus Art. 3 Abs. 2, 3 DA. Die Mitgliedsstaaten haben gemäß Art. 40 Abs. 1 DA lediglich Vorschriften über Sanktionen bei Verstößen gegen den DA vorzusehen. Erfasst werden hiervon jedoch allein straf- und verwaltungsrechtliche Sanktionen.⁵⁹ Art. 40 Abs. 4 DA sieht darüber hinaus vor, dass die Datenschutzbehörden bei Verstößen gegen die Vorgaben des hier relevanten Kapitels II befugt sind, Geldbußen entsprechend Art. 83 DS-GVO zu verhängen. Die privatrechtliche Haftung richtet sich im Übrigen nach den allgemeinen Regelungen des nationalen Rechts (vgl. ErwGr 9 DA).

Sofern es an den Informationen nach Art. 3 Abs. 2, 3 DA fehlt, ist zunächst an mögliche Gewährleistungsrechte des Käufers zu denken, die sich im Falle eines Kaufvertrages über vernetzte Produkte aus § 475b Abs. 1 iVm §§ 434 ff. BGB und im Falle der Erbringung von verbundenen Diensten aus § 327d ff. BGB ergeben. Allerdings kommen derartige Ansprüche schon im Ausgangspunkt nur mit Blick auf die produkt- bzw. dienstbezogenen Informationspflichten in Betracht. Denkbar scheint etwa die Annahme eines Sachmangels, wenn ein vernetztes Produkt ohne einen entsprechenden Hinweis des Verkäufers nicht-personenbezogene Daten⁶⁰ erhebt und diese auf einem externen Server speichert. Ein Abweichen der Ist- von der – auch normativ zu bestimmenden – Soll-Beschaffenheit des Produktes lässt sich dabei nur dann annehmen, wenn Produkte grundsätzlich so zu konzipieren sind, dass diese keine nicht-personenbezogenen Daten erheben und übermitteln. Eine solche Pflicht begründet der DA aber gerade nicht. Zwar verlangt Art. 4 Abs. 13 DA eine Erlaubnis seitens des Nutzers zur Nutzung der Daten. Die Erhebung und Speicherung bleiben aber nach wie vor zulässig. Vor diesem Hintergrund kann es nicht überzeugen, aus den fehlenden Informationen zur Datenerhebung und -speicherung auf eine entsprechende Soll-Beschaffenheit des Produktes zu schließen.

Da aus den fehlenden Informationen nach Art. 3 Abs. 2, 3 DA damit keine unmittelbare Aussage zur Mangelhaftigkeit des Produktes getroffen werden kann, kommt zugunsten des Käufers neben einer Anfechtbarkeit wegen arglistiger Täuschung nach § 123 BGB grundsätzlich auch eine Anfechtbarkeit wegen Eigenschaftsirrtums nach § 119 Abs. 2 BGB in Betracht. Daneben ist auch eine Haftung des Verkäufers nach §§ 280 Abs. 1, 311 Abs. 2, 241 Abs. 2 BGB (culpa in contrahendo) denkbar.

Allerdings werden Verbraucher wohl regelmäßig eine „rationale Ignoranz“⁶¹ gegenüber den betroffenen Informationen aufweisen, sodass die Voraussetzungen der genannten Rechte nur im Ausnahmefall erfüllt sein werden. Aus diesem Grund wird eine wirksame privatrechtliche Durchsetzung der Informationspflichten wiederum in Form des kollektiven Rechtsschutzes erfolgen müssen. Entsprechend den Erwägungen zur kollektiven Durchsetzung der Pflicht aus Art. 3 Abs. 1 DA⁶² kommen dafür auch hier Ansprüche aus §§ 8 ff. UWG sowie aus § 2 UKlaG in Betracht.

4. IoT-Geräte auf dem Secondhand-Markt

Die vorgesehenen Regelungen zugunsten der Nutzer provozieren wiederum besondere Herausforderungen, wenn IoT-Geräte auf dem Secondhand-Markt angeboten werden. So treffen die Informationspflichten nach Art. 3 Abs. 2 DA auch Verbraucher, wenn sie ihrerseits insbesondere als Verkäufer eines vernetzten Produkts auftreten. Eine teleologische Reduktion des Anwendungsbereiches von Art. 3 Abs. 2 DA auf Unternehmer verbietet sich schon vor dem Hintergrund seiner Zielsetzung, die gerade auf die Transparenz zugunsten des Erwerbers und den hierdurch vereinfachten Zugang zu den Produktdaten gerichtet ist. Dieses Ziel beansprucht auch auf dem Secondhand-Markt uneingeschränkt Geltung.

Mit Blick auf die Rechtsfolgen eines Verstoßes dürfte eine Informationspflicht zulasten von Verbrauchern allerdings ohnehin wenig einschneidend sein. So wird eine behördliche Sanktion nach Art. 40 DA im Regelfall schon deswegen ausscheiden, weil die Verbrauchereigenschaft im Rahmen der Ermessensentscheidung zu berücksichtigen ist. Darüber hinaus kommt zwar im Verhältnis zum Zweiterwerber des IoT-Gerätes im Ausgangspunkt eine Haftung aus §§ 280 Abs. 1, 311 Abs. 2, 241 Abs. 2 BGB sowie eine Anfechtbarkeit des Geschäftes nach §§ 119 Abs. 2, 123 BGB in Betracht. Selbst wenn deren Anwendungsbe- reich durch die Pflicht aus Art. 3 Abs. 2 DA erweitert wird, handelt es sich hierbei doch um allgemeine Regelungen, die auch im Übrigen zulasten von Verbrauchern gelten. Auch insoweit besteht damit kein zwingender Korrekturbedarf.

V. Fazit

Der Data Act begründet kein genuin verbraucherschützendes Regime in Bezug auf IoT-Gerätedaten. Dennoch werden sich die Regelungen auch für Verbraucher von (unterschiedlicher) Relevanz erweisen. Verbraucherverbände sehen sich dementsprechend mit der Frage konfrontiert, wie sie sich auf dem Binnenmarkt für Daten insbesondere auch in Bezug auf nicht-perso-

58 In Bezug auf die entsprechenden Anforderungen nach Art. 246 EGBGB siehe BeckOK BGB/Martens, 70. Ed., EGBGB Art. 246 Rn. 7 f.

59 BeckOK Datenschutzrecht/Roth-Isigkeit, 48. Ed., DA Art. 40 Rn. 2; vgl. auch zur insoweit vergleichbaren Regelung in Art. 84 DS-GVO EuGH EuZW 2022, 522 Rn. 49.

60 Zur Begründung eines Sachmangels durch Verstöße gegen die DS-GVO siehe Specht-Riemenschneider MMR 2020 73 f.; Schneider ZD 2021, 458; Lang ZD 2024, 6 f.

61 Vgl. Specht-Riemenschneider FS Tinnefeld, 2022, 77 (87).

62 Siehe hierzu unter III.1.c).

nenbezogene IoT-Gerätedaten positionieren. Zwar stehen Verbrauchern hinsichtlich der Pflicht zur Accessibility by Design und den Informationspflichten aus Art. 3 DA immerhin punktuell individuelle Rechtsbehelfe zur Seite. Nichtsdestotrotz kann sich der kollektive Rechtsschutz gerade hier als ein hilfreicher Baustein zur Verwirklichung von Fairness und Transparenz in der Datenwirtschaft erweisen.

Auffällig ist schließlich, dass die erforderliche Datennutzungsvereinbarung zwischen dem Nutzer und dem Dateninhaber trotz der Betonung eines hohen Verbraucherschutzniveaus nur wenigen Beschränkungen unterliegt. Dies mag damit gerechtfertigt werden, dass jedenfalls nicht-personenbezogene Daten unmittelbar für Verbraucher im Regelfall nur von untergeordneter Bedeutung sind. Gerade dies wird aber verfestigt, wenn Verbraucher nur rein formal selbstbestimmt über die Nutzung von

nicht-personenbezogenen IoT-Gerätedaten entscheiden können. Verbraucher können daher auch zukünftig kaum selbst am Markt für nicht-personenbezogene Daten partizipieren. Nimmt man sowohl das im Data Act formulierte Ziel des Verbraucherschutzes als auch dessen allgemeine Nutzerzentriertheit ernst, verlangt dies de lege ferenda die Materialisierung der Selbstbestimmung durch zwingende Vorgaben zugunsten von Verbrauchern.⁶³ Derartige Forderungen werden sich jedoch nur von einer gesicherten Auffassung über die Legitimation der Nutzerzentriertheit erheben lassen, deren Diskussion noch nicht abgeschlossen scheint.⁶⁴

63 In Bezug auf personenbezogene Daten schon Specht-Riemenschneider FS Tinnefeld, 2022, 77 (80 ff.).

64 Kritisch zur Nutzerzentriertheit etwa Funk CR 2023, 421 Rn. 14 ff.

Die Bedeutung der Gesetzeskonformität bei der Beurteilung der Vertragsmäßigkeit digitaler Produkte

Von Timon-Johannes Engel, Heidelberg*

I. Einleitung

Digitale Produkte (Suchmaschinen, KI-Assistenten, Soziale Medien, Streaming Services etc.)¹ haben in unserer digitalisierten Welt längst denselben Stellenwert wie physische Produkte. Entsprechend wurde mit der RL (EU) 2019/770 (Digitale-Inhalte-Richtlinie) das europäische Verbraucherprivatrecht für Rechtsfragen der Bereitstellung digitaler Produkte angepasst. Die in den §§ 327 ff. BGB umgesetzte Richtlinie regelt unter anderem die Voraussetzungen für die Vertragsmäßigkeit von digitalen Produkten.

Gleichzeitig sind digitale Produkte Gegenstand immer neuer (europäischer) Regulierungen,² wie etwa der gerade in Kraft getretenen KI-Verordnung und dem kommenden Cyber Resilience Act (CRA). Indem Art. 8 Abs. 1 lit. a RL (EU) 2019/770 Unions- und nationales Recht als Bezugspunkte zur Beurteilung der Vertragsmäßigkeit digitaler Produkte nennt, stellt er erstmals eine explizite Verbindung zwischen dem Verbraucherprivatrecht und (primär) öffentlich-rechtlicher Regulierung her. Dadurch wird ein neuer Anknüpfungspunkt für die private Rechtsdurchsetzung (primär) öffentlich-rechtlicher Regulierung geschaffen. Dies ist insbesondere für solche Regulierung bedeutend, bei der die behördliche Rechtsdurchsetzung ihre Aufgabe nicht vollständig erfüllen kann.³ Außerdem eröffnet der Weg über das Mangelgewährleistungsrecht die in § 327i BGB genannten Rechte und Ansprüche (Nacherfüllung, Vertragsbeendigung, Preisminderung, Schadensersatz).

Dieser Beitrag untersucht, ob und in welchen Fällen der Verstoß gegen öffentlich-rechtliche Regulierung zur Mangelhaftigkeit eines digitalen Produktes gem. § 327e BGB führt.

Zunächst wird erörtert, ob die Gesetzeskonformität ein Beschaffenheitsmerkmal des digitalen Produktes darstellt (II.). Danach wird untersucht, unter welchen Umständen eine vertragliche Pflicht zur Gesetzeskonformität aus § 327e III S. 1 Nr. 1 BGB (III.) oder § 327e Abs. 3 S. 1 Nr. 2 BGB (IV.) folgt. Zudem wird geprüft, wann Zertifizierungen und Kennzeichnungen innerhalb des § 327e BGB eine Pflicht zur Gesetzeskonformität begründen können (V.). Der Beitrag schließt mit einem Fazit (VI.) und einer Zusammenfassung in Form von Thesen (VII.).

II. Gesetzeskonformität als Beschaffenheitsmerkmal

Die Vertragsmäßigkeit eines digitalen Produktes beurteilt sich maßgeblich nach dessen „Beschaffenheit“. Innerhalb der subjektiven Anforderungen kann eine bestimmte „Beschaffenheit“ vereinbart werden, § 327e Abs. 2 S. 1 Nr. 1 lit. a BGB, während innerhalb der objektiven Anforderungen die übliche und erwartbare Beschaffenheit geschuldet ist, § 327e Abs. 3 S. 1 Nr. 2

* Der Autor ist studentische Hilfskraft am Lehrstuhl für Bürgerliches Recht, Handels- und Wirtschaftsrecht, Europarecht und Rechtsvergleichung von Univ.-Prof. Dr. Christian Heinze, LL.M. (Cambridge), Universität Heidelberg.

1 Zum Begriff des digitalen Produktes s. BeckOK BGB/Wendland/Soritz, Stand: 1.5.2023, BGB § 327 Rn. 42.

2 Eine Übersicht über abgeschlossene und laufende Gesetzesvorhaben der EU im digitalen Sektor findet sich bei Zenner/Marcus/Sekut, A dataset on EU legislation for the digital world, 2024, https://www.bruegel.org/system/files/2024-06/Bruegel_factsheet_2024_0.pdf (zuletzt abgerufen am 2.10.2024).

3 Dies wird etwa für die KI-Verordnung bereits prognostiziert, Bomhard/Sigmüller RD 2024, 45 (53); Ebert/Spiecker gen. Döhmman NVwZ 2021, 1188 (1193); für grenzüberschreitende datenschutzrechtliche Sachverhalte sieht die Europäische Kommission Handlungsbedarf und hat schon ein entsprechendes Gesetzgebungsverfahren auf den Weg gebracht, COM(2023) 348 final.