

# Kommunikation & Recht

K&R

**3** | März 2024  
27. Jahrgang  
Seiten 157 - 228

**Chefredakteur**

RA Torsten Kutschke

**Stellvertretende**

**Chefredakteurin**

RAin Dr. Anja Keller

**Redakteur**

Maximilian Leicht

**Redaktionsassistentin**

Stefanie Lichtenberg

[www.kommunikationundrecht.de](http://www.kommunikationundrecht.de)

**dfv** Mediengruppe  
Frankfurt am Main

Der AI Act kommt

**Lucia Franke**

- 157** Bereitstellung von Daten nach dem Data Act – offene Fragen und verbleibende Probleme  
**Nils Torben Wiedemann, Thorsten Conrad und Simone Salemi**
- 163** Neue Entwicklungen zum Anzeigenprivileg der Presse im digitalen Bereich?  
**Dr. Lars Querndt**
- 169** Update IT-Sicherheitsrecht 2022/2023 – Teil 1  
**Dr. Florian Deusch und Prof. Dr. Tobias Eggendorfer**
- 176** Privacy Enhancing Technologies – ein Ansatz zur Minimierung datenschutzrechtlicher Risiken beim Einsatz Künstlicher Intelligenz  
**Nadia Schaff und Dragana Dujak**
- 181** Systemische Privatheit für große, reale Datenverarbeitungssysteme  
**Amina Gutjahr, Prof. Dr. Indra Spiecker gen. Döhmann und Prof. Dr. Thomas Wilmer**
- 187** Rechtliche und technische Herausforderungen von Privatheit in Big-Data-Verarbeitungssystemen  
**Prof. Dr. Gerrit Hornung, Till Schaller, Dr. Annika Selzer und Sarah Stummer**
- 192** **EuGH:** Schadensersatzanspruch wegen irrtümlicher Datenweitergabe
- 204** **BVerfG:** Polemik im Gerichtssaal als zulässige Meinungsäußerung
- 209** **BGH:** „Bequemer Kauf auf Rechnung“ als Verkaufsförderung
- 213** **OLG Frankfurt a. M.:** „Amazon’s Choice“ stellt kein Zueigenmachen dar mit Kommentar von **Sebastian Wasner**
- 220** **OLG Stuttgart:** Haftung für Beleidigung über unzureichend gesichertes Social-Media-Konto mit Kommentar von **Benjamin Ferri**

**Beihefter 1/2024**

Der berufs- und rundfunkrechtliche Anspruch auf Erhaltung der UKW-Nutzungslizenz

**Prof. Dr. Dr. Udo Di Fabio**

Nils Torben Wiedemann, LL.M., Thorsten Conrad und Simone Salemi, LL.M.\*

# Bereitstellung von Daten nach dem Data Act – offene Fragen und verbleibende Probleme

## Kurz und Knapp

**Das Gesetzgebungsverfahren des im Dezember 2023 verabschiedeten Data Act ist von der rechtswissenschaftlichen Literatur intensiv begleitet worden. Während die Zielsetzung noch überwiegend begrüßt wurde, offenbarten die konkreten Regelungen zahlreiche Schwächen. Der Beitrag analysiert die bisherige Literatur und zeigt auf, inwieweit die Schwächen in der finalen Fassung adressiert wurden und welche Probleme auch weiterhin Bestand haben dürften.**

## I. Einleitung

Die am 13. 12. 2023 verabschiedete finale Fassung der Datenverordnung<sup>1</sup> (nachfolgend wird die geläufigere englische Bezeichnung Data Act, kurz: DA verwendet) soll die Bereitstellung von Daten innerhalb der Europäischen Union neu regulieren, um bestehende Hindernisse im Binnenmarkt zu beseitigen<sup>2</sup> und so zu mehr Fairness, freiem Wettbewerb und Innovationsförderung führen.<sup>3</sup> Während die Ziele des Vorschlags der Europäischen Kommission zum Data Act (DA-E)<sup>4</sup> von Literatur und Wirtschaft überwiegend begrüßt wurden, stießen die konkreten Regelungen des DA-E auf Kritik, was sich in der großen Anzahl an wissenschaftlichen Veröffentlichungen widerspiegelt. Bis zur Einigung im Trilog wurde der DA jedoch mehrfach angepasst, sodass sich die finale Fassung teils erheblich vom Kommissionsvorschlag unterscheidet. Dieser Beitrag analysiert ausgewählte Kritikpunkte der bisherigen Literatur und zeigt auf, ob und inwieweit die finale Fassung diese berücksichtigt oder gar aufzulösen vermag. Obwohl der DA eine Vielzahl an Regelungsgegenständen adressiert, behandelt die überwiegende Mehrheit der wissenschaftlichen Beiträge lediglich die Bereitstellung und Weitergabe von Daten, die durch Produkte des „Internet of Things“ (IoT) erzeugt wurden, weshalb sich der Beitrag auf die Analyse der Literatur hierzu beschränkt.

## II. Überblick über die Bereitstellung und Weitergabe

Für ein besseres Verständnis soll vorab ein kurzer Überblick über die Konzeption der Bereitstellung und Weitergabe von Daten gegeben werden. Die Vorschriften des DA unterscheiden hier zwischen drei Akteuren: Nutzern (Art. 2 Nr. 12 DA), Dateninhabern (Art. 2 Nr. 13 DA) und Datenempfängern (Art. 2 Nr. 14 DA). Nach Art. 4 DA sollen Nutzer, die nicht schon direkt über das vernetzte Produkt oder den verbundenen Dienst auf die Produkt- und verbundenen Dienstdaten zugreifen können, die Bereitstellung dieser Daten vom Daten-

inhaber verlangen können. So kann beispielsweise der Eigentümer einer Smartwatch oder eines mit dem Internet verbundenen Autos einen Zugang vom Dateninhaber zu den durch die Nutzung des Produktes erzeugten Daten verlangen, wenn ein Zugriff nicht schon direkt über das Produkt selbst möglich ist.

Zudem können Nutzer gemäß Art. 5 DA vom Dateninhaber eine Weitergabe dieser Daten an Dritte – die Datenempfänger – verlangen. Bis zu einer bestimmten Größe werden Unternehmen von diesen Pflichten gemäß Art. 7 DA ausgenommen. Der Dateninhaber kann außerdem für die Weitergabe nach Art. 9 DA eine angemessene Gegenleistung vom Datenempfänger verlangen. Die Beziehungen der einzelnen Akteure untereinander werden – neben den Vorschriften des DA – durch Verträge geregelt, an die der DA teils besondere Anforderungen stellt (beispielsweise in Art. 8, 9, 13 DA).

## III. Verhältnis des DA zu anderen Rechtsakten

Die sektorübergreifende Konzeption des DA führt dazu, dass die Regelungen zu zahlreichen Überschneidungen mit anderen Rechtsakten, insbesondere sektorspezifischem Recht, führen.<sup>5</sup> Bereits zum Kommissionsvorschlag wurden die sich aus den Überschneidungen mit anderen Rechtsakten ergebenden Abgrenzungsprobleme von der Literatur umfassend behandelt.

### 1. Verhältnis zum Datenschutzrecht

Das Verhältnis zum Datenschutzrecht, insbesondere zur DSGVO, dürfte dabei wohl am umfassendsten diskutiert worden sein. Als Teil des sogenannten Datenrechts findet der DA – wie auch der Daten-Governance-Rechtsakt (DGA)<sup>6</sup> – sowohl auf nicht-personenbezogene als auch auf personenbezogene Daten Anwendung (Art. 1 f. DA). Hierdurch kommt es zwangsläufig zu Überschneidungen mit der DSGVO.<sup>7</sup> So wurde bereits während des Gesetzgebungsverfahrens darauf hingewiesen, dass das erklärte Ziel des Datenrechts, die Bereitstellung von Daten zu erleichtern, mit den Schutzziele der DSGVO unvereinbar sein könnte.<sup>8</sup> Das Verhältnis zur DSGVO regelte der

\* Mehr über die Autoren erfahren Sie am Ende des Beitrags. Danksagung: Dieser Beitrag entstand im Rahmen des Projekts „PAIRS“ (www.pairs-projekt.de, Förderkennzeichen 01MK21008H), das durch das Bundesministerium für Wirtschaft und Klimaschutz finanziert wird.

1 VO (EU) 2023/2854.

2 Erwägungsgrund 3 DA.

3 Podszun/Pfeifer, GRUR 2022, 953, 953.

4 Europäische Kommission, COM(2022) 68 final.

5 Podszun/Pfeifer, GRUR 2022, 953, 955.

6 VO (EU) 2022/868.

7 VO (EU) 2016/679.

8 Steinrötter, GRUR 2023, 216, 216.

DA-E in Art. 1 Abs. 3 und sah vor, dass der DA die Anwendbarkeit der Rechtsvorschriften der Union über den Schutz personenbezogener Daten – was neben der DSGVO auch die E-Privacy-Richtlinie<sup>9</sup> umfasst – „nicht berühre“. Allerdings werde unter gewissen Umständen das Recht auf Datenübertragbarkeit nach Art. 20 DSGVO durch die Vorschriften des DA ergänzt.

Aufgrund der Formulierung, dass der DA-E die DSGVO nicht berühre, wurde überwiegend angenommen, dass die Vorschriften der DSGVO und des DA-E nebeneinander anwendbar seien.<sup>10</sup> Die Ergänzung der DSGVO bedeute nicht, dass der DA-E die DSGVO abändere und *lex specialis* zur DSGVO sei.<sup>11</sup> Das Konkurrenzverhältnis zwischen DSGVO und DA-E konnte allerdings aufgrund des uneindeutigen Wortlauts des Art. 1 Abs. 3 DA-E und des Fehlens einer entsprechenden Regelung nicht abschließend geklärt werden,<sup>12</sup> weshalb teils die Einführung einer Kollisionsregel gefordert wurde.<sup>13</sup> Zudem wurde darauf hingewiesen, dass die spezifischen Regelungen des DA-E für nicht-personenbezogene Daten eine klare Abgrenzung zwischen personenbezogenen und nicht-personenbezogenen Daten erfordern.<sup>14</sup> Die vorsorgliche Erfüllung der Pflichten der einen Verordnung sei nicht möglich, da sie zugleich einen Verstoß gegen die andere Verordnung darstellen könnte.<sup>15</sup> Die gängige Praxis, im Zweifel einen Personenbezug anzunehmen – um der praktisch schwierigen Unterscheidung von personenbezogenen und nicht-personenbezogenen Daten zu entgehen –, könne deshalb nicht mehr aufrechterhalten werden.<sup>16</sup> Darüber hinaus könne die „Kontraktualisierung“<sup>17</sup> – also die umfassende vertragliche Ausgestaltung der Beziehungen zwischen den Beteiligten – zu einer faktischen Zuordnung nicht-personenbezogener Daten zu einer natürlichen Person als Teilnehmer führen, sodass aus andernfalls anonymen Produkt- oder Dienstdaten ein Personenbezug hergestellt werden könne und das Datenschutzrecht „ohne Not aktiviert“ werde.<sup>18</sup>

Ebenfalls nicht abschließend geklärt werden konnte, ob und inwieweit das Erfordernis einer Rechtsgrundlage nach Art. 6 DSGVO die Bereitstellung und Weitergabe der Daten beschränken wird. Im Wesentlichen dürfte dies nur relevant sein, wenn die Nutzer nicht zugleich auch betroffene Personen sind. Hinsichtlich des Zugangs solcher Nutzer wurde analysiert, ob die Pflicht des Dateninhabers nach Art. 4 Abs. 1 DA-E als Rechtsgrundlage nach Art. 6 Abs. 1 lit. c DSGVO oder gar als Ausnahme nach Art. 9 Abs. 2 lit. g DSGVO ausgelegt werden könnte, da ErwG 24 DA-E einer solchen Auslegung nicht explizit entgegenstehe.<sup>19</sup> Zudem könne die Weitergabe aufgrund der gesetzgeberischen Normierung zu einer erleichterten Interessenabwägung im Rahmen des Art. 6 Abs. 1 lit. f DSGVO führen.<sup>20</sup> Teils wurde vorgeschlagen, dass die Bereitstellung der Daten an Nutzer und Datenempfänger ausdrücklich als eine Pflicht des Dateninhabers nach Art. 6 Abs. 1 lit. c DSGVO ausgestaltet werden könnte, während für sensible Daten nach Art. 9 Abs. 1 DSGVO weiterhin eine ausdrückliche Einwilligung nach Art. 9 Abs. 2 lit. a DSGVO erforderlich wäre.<sup>21</sup> Gleichwohl werde eine solche Ausgestaltung wohl keine ausreichende Unterstützung finden, weshalb die Anonymisierung von personenbezogenen Daten eine mögliche Lösung sein könnte, deren Voraussetzungen hierfür aber klargestellt werden müssten.<sup>22</sup>

Die finale Fassung des DA wandelt den Wortlaut in Art. 1 Abs. 5 DA leicht ab und erklärt, dass der DA „unbeschadet“ der DSGVO, der E-Privacy-Richtlinie und der VO 2018/1725 gilt. Zudem ergänzt der DA nun nicht nur Art. 20 DSGVO,

sondern auch Art. 15 DSGVO. Die Vorschrift enthält nun auch die geforderte explizite Regelung im Falle eines Konflikts der beiden Verordnungen. Danach sollen im Falle eines Widerspruchs das „Unionsrecht oder das nationale Recht zum Schutz personenbezogener Daten bzw. der Privatsphäre Vorrang“ vor dem DA haben. Aufgrund der „Unbeschadet“-Regelung des DA wurde in den ersten mittlerweile veröffentlichten Beiträgen diese Vorschrift als deklaratorisch und somit „bestenfalls überflüssig“ bezeichnet.<sup>23</sup> Angesichts der zuvor geforderten Klärung des Konfliktfalls ist diese Vorschrift dennoch begründenswert und dürfte im Gegensatz zu anderen Vorschriften des DA – wie beispielsweise die doch recht selbsterklärende Definition von nicht-personenbezogenen Daten in Art. 2 Nr. 4 DA – tatsächlich brauchbar sein.

Der Vorschlag, die Bereitstellung der Daten an Nutzer und Datenempfänger als eine ausdrückliche Pflicht des Dateninhabers nach Art. 6 Abs. 1 lit. c DSGVO auszugestalten, ist in der finalen Fassung des DA nicht umgesetzt worden. Die Ausführungen des ErwG 24 DA-E wurden in der finalen Fassung im Kern in den ErwG 7 DA verschoben. Dieser stellt klar, dass der DA „keine Rechtsgrundlage für die Erhebung oder Generierung personenbezogener Daten durch den Dateninhaber“ darstelle, sie den Dateninhaber aber verpflichte, „Nutzern [oder] Dritten seiner Wahl [...] auf Anfrage eines Nutzers personenbezogene Daten bereitzustellen.“<sup>24</sup> Sofern es sich bei dem Nutzer nicht um die betroffene Person handelt, bietet der DA allerdings „keine Rechtsgrundlage für die Gewährung des Zugangs zu personenbezogenen Daten oder für deren Bereitstellung an Dritte.“ Wie bereits in Art. 4 Abs. 5 DA-E wird dies auch in Art. 4 Abs. 12 DA nochmal klargestellt, weshalb die Vorschriften des DA wohl nicht als eine Pflicht des Dateninhabers nach Art. 6 Abs. 1 lit. c DSGVO ausgelegt werden können.<sup>25</sup> Das Erfordernis einer Rechtsgrundlage und – unter Umständen – einer Ausnahme nach Art. 9 Abs. 2 DSGVO dürfte somit in vielen Fällen das Bereitstellen personenbezogener Daten nach den Vorschriften des DA erschweren. Allerdings sieht beispielsweise der Kommissionsvorschlag für eine Verordnung über den europäischen Gesundheitsdatenraum (EHDS)<sup>26</sup> eine Pflicht der Dateninhaber zur Bereitstellung von elektronischen Gesundheitsdaten an Zugangsstellen für Gesundheitsdaten vor, die gleichzeitig auch Art. 9 Abs. 2 DSGVO erfüllen soll (Art. 33 EHDS, ErwG 37 EHDS). Weitere sektorspezifische Erleichterungen sind nicht auszuschließen und könnten die Bereitstellung von Daten insoweit erheblich erleichtern. Zudem weist ErwG 7 DA darauf hin, dass der Dateninhaber Datenzugangsverlan-

9 RL 2002/58/EG.

10 So: *Specht-Riemenschneider*, MMR 2022, 809, 810; *Hartmann/McGuire/Schulte-Nölke*, RDi 2023, 49, 53; *Steinrötter*, GRUR 2023, 216, 217; *Denga*, GRUR 2022, 1113, 1118.

11 *Specht-Riemenschneider*, MMR 2022, 809, 810.

12 *Steinrötter*, GRUR 2023, 216, 217; *Specht-Riemenschneider*, MMR 2022, 809, 810.

13 *Specht-Riemenschneider*, MMR 2022, 809, 810.

14 *Hartmann/McGuire/Schulte-Nölke*, RDi 2023, 49, 53.

15 *Hartmann/McGuire/Schulte-Nölke*, RDi 2023, 49, 53.

16 *Bomhard/Merkle*, RDi 2022, 168, 172; *Steinrötter*, GRUR 2023, 216, 219.

17 *Hennemann/Steinrötter*, NJW 2022, 1481.

18 *Steinrötter*, GRUR 2023, 216, 219.

19 *Specht-Riemenschneider*, MMR 2022, 809, 811.

20 *Specht-Riemenschneider*, MMR 2022, 809, 811.

21 *Metzger/Schweitzer*, ZEuP 2023, 42, 77 f. mit Verweis auf *Leistner/Antoine*, Study requested by the JURI committee 2022, S. 91; *Schneiderei*, CR 2023, 9, 12.

22 *Metzger/Schweitzer*, ZEuP 2023, 42, 78.

23 So: *Schmidt-Kessel*, MMR 2024, 122, 126.

24 Korrektur durch die Autoren. Die deutsche Fassung scheint hier einen Übersetzungsfehler aufzuweisen.

25 So auch: *Bomhard*, MMR 2024, 71, 74.

26 Europäische Kommission, COM(2022) 197 final.

gen mittels anonymisierter Daten oder einer Beschränkung auf die personenbezogenen Daten des anfragenden Nutzers nachkommen könne.

Letztlich ist noch offen, welche Auswirkungen das Verhältnis und die Abgrenzung von DSGVO und DA für die Praxis haben wird. Teils wird die praktische Relevanz aufgrund der divergierenden Regelungsgegenstände der beiden Verordnungen als sehr eingeschränkt beurteilt.<sup>27</sup> Andere gehen wiederum von „zahllosen Situationen“ aus, in denen die Anwendung des DA durch die DSGVO ausgeschlossen sein wird und über eine weite Auslegung des Personenbezugs gar eine „Flucht ins Datenschutzrecht“ zum Ausschluss der Anwendbarkeit der Pflichten des DA möglich sein könnte.<sup>28</sup> Aufgrund des Konflikts zwischen Gebot und Verbot des Teilens von Daten käme es maßgeblich auf die Bestimmung des Personenbezugs an.<sup>29</sup> Insoweit dürfte erschwerend hinzukommen, dass die Auslegung des Begriffs der personenbezogenen Daten – trotz Einführung der Datenschutzrichtlinie<sup>30</sup> vor nun fast 30 Jahren – noch immer Gegenstand von Verfahren vor dem EuGH ist.<sup>31</sup>

## 2. Verhältnis zu sonstigen Rechtsakten

Auch hinsichtlich des Verhältnisses zu anderen Rechtsakten ließ die eher lückenhafte Regelung im DA-E viele Fragen offen. Die finale Fassung wurde zwar um mehrere Abgrenzungsregelungen – insbesondere durch Erweiterung des Art. 1 DA und Einführung des Art. 44 DA – erweitert, dennoch werden bei weitem nicht alle kollidierenden Rechtsakte adressiert.<sup>32</sup> Insbesondere das Verhältnis zum Verbrauchervertragsrecht wird nur unzureichend geregelt.<sup>33</sup> Auch wird die Abgrenzung zu Art. 101 AEUV weiterhin nur in ErwG 116 DA angesprochen, obwohl darauf hingewiesen wurde, dass insoweit ein erhebliches Konfliktpotenzial bestehe.<sup>34</sup> Ferner wurde die vielfach diskutierte Einschränkung des *sui generis*-Datenbankrechts nach Art. 35 DA-E<sup>35</sup> – nunmehr Art. 43 DA – nur minimal angepasst. Offen ist, ob der angepasste Wortlaut mit Daten als Bezugspunkt nun hinsichtlich der Einschränkung des Schutzes von gemischten Datenbanken differenziert, die im DA-E noch explizit vom Schutzrecht ausgenommen wurden.<sup>36</sup> Auch der Wortlaut des ErwG 112 DA ist insoweit nicht eindeutig.

Darüber hinaus wurde von *Schmidt-Kessel* zu Recht darauf hingewiesen, dass insbesondere in Bezug auf Richtlinienumsetzungen noch teilweise ungeahnte Kollisionen verbleiben dürften.<sup>37</sup>

## IV. Der Zugang des Nutzers

Die konkrete Ausgestaltung des Zugangs des Nutzers nach Art. 4 DA-E war Gegenstand zahlreicher Veröffentlichungen und wurde im Verlauf des Gesetzgebungsverfahrens umfassend angepasst. Die wesentlichen Akteure sind dabei der Dateninhaber und der Nutzer (hierzu IV. 1). Sowohl im DA-E als auch nun in der finalen Fassung ist der Zugang des Nutzers davon abhängig, dass der Nutzer nicht schon direkt auf die Daten zugreifen kann, was bereits über die Konzeption ermöglicht werden soll (hierzu IV. 2). Soweit ein solcher Direktzugang nicht gegeben ist, kann der Nutzer einen Zugang verlangen (hierzu IV. 3). Unter Umständen kann dieser Zugang aber beschränkt oder ausgeschlossen werden (hierzu IV. 4).

### 1. Dateninhaber und Nutzer

Art. 2 Nr. 6 DA-E bestimmte Dateninhaber als „juristische oder natürliche Person, die nach dem DA-E, nach anwend-

barem Unionsrecht oder nach den anwendbaren nationalen Rechtsvorschriften zur Umsetzung des Unionsrechts berechtigt oder verpflichtet bzw. im Falle nicht-personenbezogener Daten und durch die Kontrolle über die technische Konzeption des Produktes und damit verbundener Dienste in der Lage ist, bestimmte Daten bereitzustellen.“ Diese Definition wurde in der Literatur eher kritisch bewertet und teils als „grober Unfug“<sup>38</sup> bezeichnet. Die Bestimmung des Dateninhabers anhand der Pflicht zur Bereitstellung der Daten – also eigentlich die Rechtsfolge der Dateninhaberschaft – habe eine „zirkuläre Tendenz“.<sup>39</sup> Daher wurde vertreten, dass wegen der zirkulären Definition letztlich nur derjenige Dateninhaber sein könne, den unabhängig vom DA eine Pflicht zur Bereitstellung der Daten treffe – beispielsweise über die DSGVO.<sup>40</sup> So geht bei einer Verarbeitung von personenbezogenen Daten der DA-E von einer datenschutzrechtlichen Verantwortlichkeit des Dateninhabers nach Art. 4 Nr. 7 DSGVO aus (ErwG 24 DA-E). Dabei bleibe aber unklar, ob hierdurch Auftragsverarbeiter von einer Dateninhaberschaft ausgeschlossen sind.<sup>41</sup> Auch die Bestimmung des Dateninhabers bei nicht-personenbezogenen Daten anhand der Kontrolle über die technische Konzeption wurde vielfach kritisiert, da die Erhebung eines faktischen Kriteriums zu einem normativen Zuordnungskriterium einerseits gegen den „kantischen Sein-Sollen-Dualismus“ verstoße und andererseits zu unklaren Verhältnissen führe, wenn mehrere Personen die faktische Kontrolle ausüben können.<sup>42</sup> Die Tragweite der Definition des Dateninhabers wurde in der bisherigen Literatur zudem uneinheitlich beantwortet. Teils wurde sie als zu weit kritisiert, da alle Personen mit „faktischen Zugriffsmöglichkeiten“, beispielsweise auch Arbeitnehmer, umfasst sein könnten.<sup>43</sup> In anderen Beiträgen wurde sie wiederum als in ihrer „Reichweite äußerst begrenzt“ bewertet, da die maßgebliche „faktische Kontrolle über die technische Konzeption eines Produktes“ sowie die „technisch-faktische Kontrolle über die Daten“ regelmäßig nur auf Produkthersteller zutreffen würde.<sup>44</sup> Teilweise wurde angenommen, dass der Begriff des Dateninhabers die Eigenschaft als Hersteller eines Produktes oder Anbieter eines mit diesem Produkt verbundenen Dienstes voraussetzt, wodurch verhindert wäre, dass jede Person mit faktischem Zugriff zum Dateninhaber werde.<sup>45</sup>

Die finale Fassung definiert den Dateninhaber nun in Art. 2 Nr. 13 DA als natürliche oder juristische Person, die nach dem DA, nach „geltendem Unionsrecht oder nach nationalen Rechtsvorschriften zur Umsetzung des Unionsrechts berech-

27 *Schmidt-Kessel*, MMR 2024, 122, 126 ff.

28 *Bomhard*, MMR 2024, 71, 74.

29 *Bomhard*, MMR 2024, 71, 74.

30 RL 95/46/EG.

31 Siehe bspw. die noch anhängigen Verfahren: EuGH, C-479/22 P – OC v Europäische Kommission; EuGH, C-413/23 P – EDPS v SRB.

32 *Schmidt-Kessel*, MMR 2024, 122, 122.

33 So: *Schmidt-Kessel*, MMR 2024, 122, 122, 127 ff.

34 *Bomhard/Merkle*, RdI 2022, 168, 172; *Podszun/Pfeifer*, GRUR 2022, 953, 954.

35 Siehe hierzu: *Wiebe*, GRUR 2023, 227.

36 *Wiebe*, GRUR 2023, 227, 230.

37 *Schmidt-Kessel*, MMR 2024, 122, 122.

38 *Hoeren*, MMR 2023, 32, 33.

39 Deutscher Anwaltsverein, Stellungnahme 40/2022, S. 13; *Hoeren*, MMR 2023, 32, 33.

40 Vgl. Deutscher Anwaltsverein, Stellungnahme 40/2022, S. 13.

41 Deutscher Anwaltsverein, Stellungnahme 40/2022, S. 13.

42 So: *Hoeren*, MMR 2023, 32, 33.

43 So: *Bomhard/Merkle*, RdI 2022, 168, 169.

44 *Specht-Riemenschneider*, ZRP 2022, 137, 138; *Specht-Riemenschneider*, MMR 2022, 809, 813.

45 *Hartmann/McGuire/Schulte-Nölke*, RdI 2023, 49, 55; *Bomhard/Merkle*, RdI 2022, 168, 169.

tigt oder verpflichtet ist, Daten – soweit vertraglich vereinbart, auch Produktdaten oder verbundene Dienstdaten – zu nutzen und bereitzustellen, die sie während der Erbringung eines verbundenen Dienstes abgerufen oder generiert hat.“ Die englische Fassung definiert den Dateninhaber als „a natural or legal person that has the right or obligation (...) to use and make available data, including, where contractually agreed, product data or related service data which it has retrieved or generated during the provision of a related service.“ Die deutsche Fassung ist durch die Aufteilung des Satzteils nach „including“ leider missverständlich. Durch diese Aufteilung legt sie eine Einschränkung auf Daten, die während der Erbringung eines verbundenen Dienstes abgerufen oder generiert werden, nahe, womit Produktdaten von vernetzten Produkten nicht umfasst wären. Zudem erscheint es nach der deutschen Übersetzung, als ob Produkt- und verbundene Dienstdaten für die Definition des Dateninhabers nur bei einer vertraglichen Vereinbarung überhaupt von Bedeutung sind. Eine zutreffendere Übersetzung wäre also, dass der Dateninhaber „eine natürliche oder juristische Person ist, die (...) das Recht oder die Pflicht hat, Daten zu nutzen und bereitzustellen, einschließlich – soweit vertraglich vereinbart – Produktdaten oder verbundene Dienstdaten, die sie während der Erbringung eines verbundenen Dienstes abgerufen oder generiert hat.“

Auffällig ist, dass die Bestimmung des Dateninhabers über das faktische Kriterium der Kontrolle über die Daten ersatzlos gestrichen wurde und der Begriff nunmehr allein auf das Recht oder die Pflicht zur Nutzung oder Bereitstellung der Daten abstellt. Leider behält die Definition so ihre zirkuläre Tendenz bei, weshalb eine Dateninhaberschaft allein über die Pflicht zur Bereitstellung der Daten nach den Vorschriften des DA nur schwer zu begründen sein dürfte. Auch wird eine Begründung der Dateninhaberschaft über das Recht zur Nutzung der Daten – beispielsweise über einen Vertrag nach Art. 4 Abs. 13 DA – wohl ebenfalls nicht möglich sein, da auch diese Vorschrift letztendlich voraussetzt, dass bereits ein Dateninhaber nach dem DA vorliegt. Damit verbleiben erhebliche Rechtsunsicherheiten, sofern eine Dateninhaberschaft nicht unabhängig von den Vorschriften des DA – beispielsweise über sektorspezifische Regelungen – begründet werden kann. Zumindest im Anwendungsbereich der DSGVO dürfte aber die Bestimmung des Dateninhabers über die Verantwortlichkeit nach Art. 4 Nr. 7 DSGVO und dessen Pflicht zur Bereitstellung der Daten nach Art. 15, Art. 20 DSGVO erleichtert sein, deren Geltendmachung ihrerseits durch die Ergänzungen des DA wohl deutlich erleichtert wird (siehe ErwG 35 DA). Letztendlich hat die EU mit der finalen Ausgestaltung der Definition des Dateninhabers eine Chance vergeben, den Begriff rechtssicher zu gestalten – beispielsweise durch eine Annäherung an den Begriff des Verantwortlichen mit einem Bezug zur Verarbeitung der Daten.

Eine weitere Diskussion in der bisherigen Literatur drehte sich um die Frage, ob der Nutzer oder der Dateninhaber die zentrale Figur des DA ist. Ausgangspunkt ist, dass nach Art. 4 Abs. 6 DA-E Dateninhaber „nicht personenbezogene Daten, die bei der Nutzung eines Produktes oder verbundenen Dienstes erzeugt werden, nur auf der Grundlage einer vertraglichen Vereinbarung mit dem Nutzer nutzen.“ Diese Vorschrift wurde in den ersten Aufsätzen nach Erscheinen des Kommissionsvorschlages teils als „Revolution“ bezeichnet, da sie dem Nutzer die formale Entscheidungsmacht über die Nutzung der Daten zuweise.<sup>46</sup> Durch das Erfordernis eines Vertrags sei die Nut-

zung der nicht-personenbezogenen Daten beschränkter als die Verarbeitung personenbezogener Daten, da die DSGVO für diese mehrere Rechtfertigungsbestände vorsehe.<sup>47</sup> Jedoch ließ der DA-E offen, unter welches Regelungsregime der Vertrag fällt und wie eine mögliche Rückabwicklung durchzuführen wäre.<sup>48</sup> Zudem sah der DA-E im Gegensatz zur DSGVO kein Kopplungsverbot vor.<sup>49</sup> Angesichts dessen wurde angemerkt, dass dem Nutzer nur scheinbar eine zentrale Stellung im DA eingeräumt werde, da der Dateninhaber nicht daran gehindert sei, sich die Nutzung der Daten über „Buy-Out-Verträge“ zu sichern.<sup>50</sup> Zwar seien Unternehmen über Art. 13 DA-E zu einem gewissen Teil geschützt, für Verbraucher gelte dies aber nicht, da die AGB-Kontrolle mangels Anwendung auf Hauptleistungspflichten kein adäquates Schutzinstrument darstelle.<sup>51</sup> Daher seien zwingende Regelungen für einen adäquaten Schutz des Nutzers vor einseitigen Buy-Out-Verträgen erforderlich.<sup>52</sup> Die finale Fassung sieht derartige zwingende Regelungen allerdings nicht vor und verhindert somit nicht ein solches Vorgehen der Dateninhaber.<sup>53</sup> Dennoch wird zu Recht darauf hingewiesen, dass die Zugangs- und Weitergaberechte der Nutzer nach Art. 7 Abs. 2, Art. 12 Abs. 2 DA nicht eingeschränkt werden können.<sup>54</sup> Daher sollte selbst bei einseitigen Buy-Out-Verträgen nicht vorschnell von einem Verstoß gegen Art. 13 DA oder einer unzulässigen Benachteiligung im Rahmen einer AGB-Kontrolle ausgegangen werden.<sup>55</sup> Zumal Art. 13 DA keine Anwendung finden könnte, wenn dem Vertragsschluss „strategischen Verhandlungsversuche“ vorausgehen.<sup>56</sup>

Im Gegensatz zum Begriff des Dateninhabers ist der Begriff des Nutzers letztendlich nur geringfügig angepasst worden. Im Vorschlag der Kommission wurde der Nutzer noch als „natürliche oder juristische Person, die ein Produkt besitzt, mietet oder least oder eine Dienstleistung in Anspruch nimmt“ definiert (Art. 2 Nr. 5 DA-E). Die finale Fassung abstrahiert diesen Begriff und definiert den Nutzer in Art. 2 Nr. 12 DA als „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.“ Auch in der finalen Fassung knüpft der Begriff des Nutzers somit nicht an die Nutzung der Daten selbst an, wodurch auch Nutzer sein kann, wer die Daten weder nutzt noch die Nutzung überhaupt anstrebt.<sup>57</sup> Zudem wurde aufgrund fehlender Ausführungen im DA-E teils angenommen, aus der Voraussetzung eines vorvertraglichen Verhältnisses nach Art. 3 Abs. 2 DA-E ergebe sich, dass es auf die „vertraglich berechnete und nicht die bloß faktische Nutzung“ ankomme, weshalb ein nutzender Nicht-Vertragspartner kein Nutzer sei.<sup>58</sup> ErwG 18 DA führt hierzu aus, dass auch der Eigentümer eines vernetzten Produkts als Nutzer zu verstehen sein sollte, weshalb es danach wohl nicht zwingend auf das

46 *Bomhard/Merkle*, RDi 2022, 168, 174; *Hennemann/Steinrötter*, NJW 2022, 1481, 1483.

47 *Bomhard/Merkle*, RDi 2022, 168, 174; *Hennemann/Steinrötter*, NJW 2022, 1481, 1483.

48 *Hennemann/Steinrötter*, NJW 2022, 1481, 1483.

49 *Specht-Riemenschneider*, MMR 2022, 809, 819 f.

50 So: *Podszun/Pfeifer*, GRUR 2022, 953, 956; *Specht-Riemenschneider*, GRUR 2022, 937, 938; *Specht-Riemenschneider*, MMR 2022, 809, 818.

51 *Specht-Riemenschneider*, MMR 2022, 809, 816 f.

52 *Specht-Riemenschneider*, ZRP 2022, 137, 139.

53 *Antoine*, CR 2024, 1, 6.

54 *Antoine*, CR 2024, 1, 6.

55 *Antoine*, CR 2024, 1, 6.

56 So: *Schwamberger*, MMR 2024, 96, 97 f.

57 *Hoeren*, MMR 2023, 32, 33; *Heinzke*, BB 2023, 201, 205.

58 *Hartmann/McGuire/Schulte-Nölke*, RDi 2023, 49, 55; vgl. auch *Schneiderei*, CR 2023, 9, 10.

Vorliegen eines vertraglichen Verhältnis anzukommen scheint. Das dürfte beispielsweise bei einem Weiterverkauf des Produktes oder bei einem Auseinanderfallen von Dateninhaber und Verkäufer des Produkts relevant sein. Im Fall mehrerer Nutzer soll nach ErWG 21 DA jedem Nutzer der Zugang zu den generierten Daten ermöglicht werden. Dabei scheint jedoch offen zu bleiben, ob dieser Zugang auf die durch den jeweiligen Nutzer generierten Daten beschränkt ist. Für den Dateninhaber dürfte es häufig schwierig bis unmöglich sein, zu bestimmen, welche Daten von welchem Nutzer generiert wurden. Das dürfte insbesondere zu Schwierigkeiten bei der Bestimmung der datenschutzrechtlichen Rechtsgrundlage führen, wenn auch natürliche Personen Nutzer sind.<sup>59</sup> Zudem stößt bei einer Mehrzahl an Nutzern der Ansatz des DA zur Kontraktualisierung der Beziehungen zwischen den Beteiligten an seine Grenzen, da der Dateninhaber mit jedem Nutzer einen Vertrag abschließen müsste, um die Daten überhaupt nutzen zu dürfen.<sup>60</sup> Insofern wurden als erste Lösungsansätze eine Mitteilungspflicht der Nutzer an den Dateninhaber bei einem Nutzerwechsel oder eine einschränkende Auslegung des Art. 4 Abs. 13 DA vorgeschlagen.<sup>61</sup>

## 2. Data Access by Design und Informationspflichten

Der Direktzugang des Nutzers soll über die Pflicht nach Art. 3 Abs. 1 DA sichergestellt werden, die wahlweise als *data access by default*<sup>62</sup> oder *data access by design*<sup>63</sup> bezeichnet wurde. Die finale Fassung erweitert Art. 3 Abs. 1 DA um einen Zugang zu den relevanten Metadaten, verändert sie sonst aber inhaltlich kaum. So besteht weiterhin die Schwierigkeit, dass nicht ersichtlich ist, wer dafür einzustehen hat, wenn das Produkt den Anforderungen nicht entspricht.<sup>64</sup> Auch ist das Verhältnis zu anderen Vorschriften, beispielsweise den kaufrechtlichen Gewährleistungsrechten,<sup>65</sup> weiterhin unklar. Allerdings berücksichtigt die finale Fassung, dass bei bestimmten Produkten die Umsetzungsfrist aufgrund der langen Produktentwicklungszeit nicht ausreichen könnte.<sup>66</sup> Art. 50 DA sieht nun vor, dass Art. 3 Abs. 1 DA erst für vernetzte Produkte und verbundene Dienste gilt, die 12 Monate nach Geltung des DA – also nach dem 12. 9. 2026 – in den Verkehr gebracht wurden.

Darüber hinaus enthält Art. 3 Abs. 2 DA-E Informationspflichten, die den einfachen Zugang des Nutzers durch Transparenz verbessern sollen und neben die Informationspflichten der DSGVO treten.<sup>67</sup> Ein *Information Overload* sei dabei aber „ebenso augenfällig wie ein aus dem Datenschutz bekanntes ‚Click and Forget‘ wahrscheinlich“ sei.<sup>68</sup> Trotz dieser Kritik reduziert die finale Fassung die Informationspflichten grundsätzlich nicht, differenziert jedoch nun hinsichtlich der Pflichten zwischen vernetzten Produkten und verbundenen Diensten.

## 3. Umfang des Zugangs des Nutzers nach Art. 4 DA

Der Zugang nach Art. 4 Abs. 1 DA-E sah vor, dass der Dateninhaber dem Nutzer – soweit ein Direktzugang zu den Daten nicht möglich ist – auf einfaches Verlangen hin „die bei der Nutzung eines Produktes oder verbundenen Dienstes erzeugten Daten, unverzüglich, kostenlos und gegebenenfalls kontinuierlich und in Echtzeit zur Verfügung“ stellt. Das Zugangsrecht erstreckt sich auf alle Nutzungs- und Umgebungsdaten, die von einem Produkt bei der Nutzung erzeugt wurden, wobei abgeleitete oder zusammengeführte Daten nicht erfasst werden.<sup>69</sup> Dabei blieb jedoch offen, welche Schwelle die Bearbeitung durch den Dateninhaber überschreiten müsste,

damit die Daten nicht mehr vom Zugangsanspruch erfasst werden,<sup>70</sup> und wie aufbereitete Datensätze zu bewerten sind, in denen teilweise noch Ausgangsdaten enthalten sind.<sup>71</sup> Zudem wurde angemerkt, dass die Effektivität des Zugangs erheblich gefährdet sei, soweit abgeleitete und zusammengeführte Daten nicht umfasst seien, da die Daten häufig eine Aufbereitung und weiteren Kontext bräuchten, um überhaupt verwertbar zu sein.<sup>72</sup> Abhelfen könnten hier Ausnahmen, die einen sektoralen Zugang zu den Analysedaten ermöglichen, wie beispielsweise im Bereich Wartung und Reparatur.<sup>73</sup> Ferner könne der Umfang des Zugangs auch um abgeleitete Daten erweitert werden und zum Ausgleich deren Nutzung Restriktionen unterworfen werden.<sup>74</sup> Die finale Fassung des DA erweitert den Zugang des Nutzers um die „zur Auslegung und Nutzung der Daten erforderlichen Metadaten“. Zudem führt die finale Fassung den Begriff der „ohne Weiteres verfügbaren Daten“ ein, die Art. 2 Nr. 17 DA bestimmt als „Produktdaten und verbundene Dienstdaten, die ein Dateninhaber ohne unverhältnismäßigen Aufwand rechtmäßig von dem vernetzten Produkt oder verbundenen Dienst erhält oder erhalten kann, wobei über eine einfache Bearbeitung hinausgegangen wird.“ Dabei enthält ErWG 15 DA weiterhin die Formulierung, dass abgeleitete Daten nicht vom Zugang umfasst sein sollen. Letztlich dürfte insoweit klargestellt sein, dass eine reine Aufbereitung der Daten, um sie überhaupt anschließend verwerten zu können, nicht dazu führt, dass sie vom Umfang des Zugangs ausgeschlossen werden. Offen bleibt jedoch weiterhin, welcher Grad an Bearbeitung erforderlich ist, damit aus „ohne Weiteres verfügbare Daten“ schließlich abgeleitete Daten werden.

Ferner wurde kritisiert, dass der Begriff des „Produktes“ nach Art. 2 Nr. 2 DA-E nur körperliche bewegliche Gegenstände umfasse. Damit klammere der DA-E rein digitale Produkte mangels Körperlichkeit gänzlich aus, was aufgrund deren wachsender wirtschaftlicher Bedeutung kaum zu vertreten sei.<sup>75</sup> Zudem bereitete die Abgrenzung der umfassten Produkte ebenfalls einige Schwierigkeiten. Während ErWG 14 DA-E einige Positivbeispiele benannte, führte ErWG 15 DA-E aus, dass bestimmte Produkte, die in erster Linie dazu bestimmt sind Inhalte anzuzeigen – beispielsweise Server, Tablets der Smartphones, – nicht umfasst sein sollten, da sie „einen menschlichen Beitrag“ erfordern, um Inhalte zu erstellen, obwohl nach ErWG 17 DA-E vom Nutzer absichtlich aufgezeichnete Daten umfasst sind.<sup>76</sup> Auch nach der finalen Fassung dürften nur körperliche Gegenstände vernetzte Produkte nach Art. 2 Nr. 5 DA darstellen können, wenngleich nun auch

59 *Heinzke*, BB 2023, 201, 205.

60 *Antoine*, CR 2024, 1, 6 f.

61 *Antoine*, CR 2024, 1, 7.

62 *Hennemann/Steinrötter*, NJW 2022, 1481, 1483; *Specht-Riemenschneider*, MMR 2022, 809, 815.

63 *Podszun/Pfeifer*, GRUR 2022, 953, 956; *Hartmann/McGuire/Schulte-Nölke*, RD 2023, 49, 52.

64 Max-Planck-Institut für Innovation und Wettbewerb, Stellungnahme zum Data Act, S. 30.

65 Max-Planck-Institut für Innovation und Wettbewerb, Stellungnahme zum Data Act, S. 30.

66 Bitkom, Bitkom Position Paper EU Data Act Proposal, S. 20.

67 *Ebner*, ZD 2022, 364.

68 *Hennemann/Steinrötter*, NJW 2022, 1481, 1483.

69 *Heinzke*, BB 2023, 201, 204.

70 *Hennemann/Steinrötter*, NJW 2022, 1481, 1483.

71 *Schneiderei*, CR 2023, 9, 11.

72 Max-Planck-Institut für Innovation und Wettbewerb, Stellungnahme zum Data Act, S. 10.

73 Max-Planck-Institut für Innovation und Wettbewerb, Stellungnahme zum Data Act, S. 11.

74 *Specht-Riemenschneider*, MMR 2022, 809, 819.

75 *Gerpott*, CR 2022, 271, 274.

76 *Bomhard/Merkle*, RD 2022, 168, 170.

unbewegliche Gegenstände umfasst sein sollten. Die Liste des ErwG 15 DA-E wurde zudem zugunsten abstrakter Ausführungen in ErwG 16 DA gestrichen.

#### 4. Ausschluss des Anspruchs

Der Zugang des Nutzers kann unter Umständen beschränkt oder ausgeschlossen werden. Nach Art. 4 Abs. 3 DA-E stehen Geschäftsgeheimnisse einem Zugangsanspruch nicht mehr grundsätzlich entgegen.<sup>77</sup> Voraussetzung für den Datenzugang zu Geschäftsgeheimnissen gemäß Art. 4 Abs. 3 DA-E ist, dass alle besonderen Maßnahmen getroffen werden, um die Vertraulichkeit zu wahren – also insbesondere Geheimhaltungsvereinbarungen.<sup>78</sup> Mangels konkreter gesetzlicher Vorgaben werde die Ausgestaltung der Geheimhaltungsvereinbarungen für private Nutzer von IoT-Geräten eine weitere Herausforderung darstellen, die neben die bereits komplexen Regelungen des DA trete.<sup>79</sup> Indem die Norm den Datenzugang an Konkurrenten nicht gänzlich ausschließe, erscheine es fraglich, ob ein solches gesetzliches Verbot einen ausreichenden Schutz der Geschäftsgeheimnisse biete.<sup>80</sup> Unklar sei, wann ein solcher Verstoß vorliegt und welche konkreten Folgen ein Verstoß hätte.<sup>81</sup> Die finale Fassung präzisiert den Schutz von Geschäftsgeheimnissen in Art. 4 Abs. 6 DA und sieht nun in Art. 4 Abs. 7 DA vor, dass der Zugang verweigert werden kann, wenn keine Einigung über die zu ergreifenden Maßnahmen mit dem Nutzer gelingt oder dieser die Maßnahmen nicht umsetzt. Soweit der Dateninhaber nachweisen kann, dass er durch den Zugang zu den Daten – trotz getroffener Maßnahmen – einen hohen wirtschaftlichen Schaden durch Offenlegung des Geschäftsgeheimnisses erleiden wird, kann er das Verlangen des Nutzers hinsichtlich der betroffenen Daten nach Art. 4 Abs. 8 DA nun sogar ablehnen. Der Dateninhaber hat in beiden Fällen die zuständige Behörde zu benachrichtigen und der Nutzer kann gegen die Entscheidung des Dateninhabers nach Art. 4 Abs. 9 DA vorgehen.

Das in Art. 4 Abs. 4 DA-E enthaltene Konkurrenzverbot wurde im Wesentlichen unverändert in die finale Fassung in Art. 4 Abs. 10 DA übernommen. Dies betrifft weiterhin nur die Entwicklung konkurrierender vernetzter Produkte und nicht die Entwicklung konkurrierender Dienste.<sup>82</sup> Das Konkurrenzverbot wurde zudem um ein Verbot der Weitergabe und Nutzung der Daten zu bestimmten Zwecken erweitert, das zuvor nur den Dateninhaber im Verhältnis zu Nutzern und Dritte getroffen hatte.<sup>83</sup>

Bereits zum Kommissionsvorschlag wurde darauf hingewiesen, dass der Zugangsanspruch des Nutzers nicht dazu führe, dass die Daten zum Zwecke des Zugangs vorgehalten werden müssen und konsequenterweise entfallen, sobald der Dateninhaber die Daten löscht.<sup>84</sup> Somit könne der Dateninhaber durch eine Löschung seiner Pflicht entgehen, insbesondere wenn die Daten bereits analysiert und daher nicht mehr gebraucht würden.<sup>85</sup> Dabei sei bedenklich, dass dem Nutzer keine Gelegenheit gegeben werden müsse, vor der Löschung Zugang zu den Daten zu erlangen.<sup>86</sup> Auch die finale Fassung des DA enthält keine explizite Vorschrift, die den Dateninhaber zu einer Aufbewahrung der Daten verpflichtet, weshalb er den Zugang des Nutzers durch eine Löschung umgehen könnte. Allerdings dürfen Dateninhaber nach Art. 4 Abs. 4 DA die Ausübung der Rechte des Nutzers nicht unangemessen erschweren, was neben den genannten Beispielen erst recht die Löschung der Daten des Nutzers umfassen dürfte. Zudem gelten im Verhältnis zwischen Unternehmen nach Art. 13 Abs. 5 DA verschiedene Vertragsklauseln als missbräuchlich, die auf eine Verhinderung des Zugangs zu den

Daten gerichtet sind. Letztendlich wird bereits anhand dieser Regelungen deutlich, dass – selbst ohne eine explizite Aufbewahrungspflicht oder ein Verbot des Löschens – der Zugang des Nutzers wohl eher selten auf diese Weise ausgeschlossen werden kann, ohne gleichzeitig gegen eine Vorschrift des DA zu verstoßen. Darüber hinaus könnte aufgrund der oben angesprochenen Zuordnung der Daten bei natürlichen Personen als Nutzer die DSGVO Anwendung finden und den Dateninhaber insoweit zusätzlich einschränken.

#### V. Weitergabe von Daten an Datenempfänger

Der in der finalen Fassung inhaltlich im Wesentlichen unveränderte Art. 5 Abs. 1 DA gibt dem Nutzer das Recht, einen grundsätzlich gleichwertigen Datenzugang zugunsten eines Datenempfängers zu verlangen.<sup>87</sup> Aufgrund des gleichwertigen Zugangs lassen sich die hinsichtlich des Zugangs des Nutzers bestehenden Fragestellungen weitestgehend auf das Verhältnis Dateninhaber – Datenempfänger übertragen. Der Dateninhaber hat dem Datenempfänger den Zugang unverzüglich, formfrei und ohne weitere Kosten für den Nutzer zur Verfügung zu stellen.<sup>88</sup> Im Gegensatz zum Nutzer unterliegt der Datenempfänger aber noch weiteren Einschränkungen. So sieht Art. 6 Abs. 1 DA für die Verarbeitung der Daten eine Zweckbindung vor, womit den Datenempfänger die Pflicht trifft, die Daten zu löschen, wenn sie zur Zweckerreichung nicht mehr benötigt werden.<sup>89</sup> Im Gegensatz zum Verhältnis Nutzer – Dateninhaber werden die vertraglichen Beziehungen im Verhältnis Dateninhaber – Datenempfänger deutlich umfangreicher geregelt.<sup>90</sup> Auch in der finalen Fassung besteht nach Art. 8 Abs. 1 DA ein Kontrahierungszwang.<sup>91</sup> Dieser ist in der finalen Fassung jedoch auf die Bereitstellung im Rahmen von Geschäftsbeziehungen zwischen Unternehmen beschränkt und findet daher keine Anwendung, wenn der Datenempfänger Verbraucher ist.<sup>92</sup> Ferner hat der Dateninhaber die Daten zu „fairen, angemessenen und nichtdiskriminierenden Bedingungen und in transparenter Weise“ bereitzustellen (sog. FRAND-Bedingungen<sup>93</sup>), die durch Art. 13 DA flankiert werden, soweit ein Vertrag abgeschlossen wird.<sup>94</sup> Hierzu sieht der DA in Art. 10 zudem ein Streitbeilegungsverfahren vor.<sup>95</sup> Weiterhin sieht auch die finale Fassung in Art. 11 DA die Möglichkeit vor, dass der Dateninhaber technische Schutzmaßnahmen zum Schutz vor einer unbefugten Nutzung oder Offenlegung der Daten ergreifen kann. Im Gegensatz zu Art. 11 DA-E sieht die finale Fassung dabei nun auch einen Lösungsanspruch gegen den Nutzer vor, wenn dieser versucht, die technischen Schutzmaßnahmen zu ändern oder zu umgehen (Art. 11 Abs. 4

77 Bomhard/Merkle, RDi 2022, 168, 171.

78 Bomhard/Merkle, RDi 2022, 168, 171.

79 Hennemann/Steinrötter, NJW 2022, 1481, 1484; Bomhard/Merkle, RDi 2022, 168, 172.

80 Schneider, CR 2023, 9, 12.

81 Bomhard/Merkle, RDi 2022, 168, 172.

82 Bomhard/Merkle, RDi 2022, 168, 172.

83 Siehe Art. 4 Abs. 6, Art. 5 Abs. 5 DA-E.

84 Bomhard/Merkle, RDi 2022, 166, 173 ff.; Specht-Riemenschneider, MMR 2022, 809, 815.

85 Bomhard/Merkle, RDi 2022, 166, 173 f.

86 Specht-Riemenschneider, MMR 2022, 809, 815.

87 Podszun/Pfeifer, GRUR 2022, 953, 957.

88 Heinzke, BB 2023, 201, 207.

89 Podszun/Pfeifer, GRUR 2022, 953, 957; Bomhard/Merkle, RDi 2022, 168, 171.

90 Staudenmeyer, EUZW 2022, 596, 596.

91 Zum DA-E siehe: Bomhard/Merkle, RDi 2022, 168, 171; Heinzke, BB 2023, 201, 207.

92 Louven, MMR 2024, 82, 83.

93 Bomhard/Merkle, RDi 2022, 168, 171.

94 Schwamberger, MMR 2024, 96, 97.

95 Siehe hierzu: Weiß, MMR 2024, 101.

DA). Dazu wurde angemerkt, dass die Möglichkeit der Anwendung von technischen Schutzmaßnahmen zu einer „de-facto-Herrschaft“ des Dateninhabers über die Daten führe.<sup>96</sup> Zudem dürfte mit Art. 11 Abs. 1 S. 3 DA nun klargestellt worden sein, dass eine eigenmächtige Umgehung unzulässiger technischer Schutzmaßnahmen aufgrund des Erfordernisses der Zustimmung des Dateninhabers nicht rechtmäßig ist.<sup>97</sup>

## VI. Fazit

Die finale Fassung des DA adressiert zahlreiche Kritikpunkte des DA-E, präzisiert einige der Vorschriften und beantwortet damit bisher offene Fragestellungen. Allerdings werden viele Kritikpunkte nur unzureichend aufgelöst, sodass auch in der finalen Fassung ein großes Maß an Rechtsunsicherheit verbleibt. Aufgrund der gestiegenen Regelungsdichte dürften bis zur Anwendbarkeit des DA im September 2025 zudem noch zahlreiche Probleme entdeckt werden. Die Aufarbeitung des DA in der rechtswissenschaftlichen Literatur hat somit gerade erst begonnen.

<sup>96</sup> So: Steege, MMR 2024, 91, 93.

<sup>97</sup> Siehe dazu: Steege, MMR 2024, 91, 93 f.



### Nils Torben Wiedemann

Studium der Rechtswissenschaften an der Universität Konstanz und am University College Cork, Irland; Referendariat am LG Karlsruhe; LL.M. in Intellectual Property and Information Technology Law am Trinity College Dublin, Irland. Seit 2022 wiss. Mitarbeiter am ZRD Saar und seit 2023 Doktorand am Lehrstuhl für Rechtsinformatik der Universität des Saarlandes.



### Thorsten Conrad

Studium der Rechtswissenschaften an der Universität des Saarlandes und an der University of Oslo, Norwegen. Seit 2020 als Mitarbeiter am Lehrstuhl für Rechtsinformatik der Universität des Saarlandes und seit 2023 Referendar am OLG Zweibrücken.



### Simone Salemi

Studium der Rechtswissenschaften an der Universität des Saarlandes; LL.M. in Informationstechnologie und Recht am Institut für Rechtsinformatik der Universität des Saarlandes. Seit 2021 wiss. Mitarbeiterin am ZRD Saar und seit 2022 Doktorandin am Lehrstuhl für Rechtsinformatik der Universität des Saarlandes.

RA Dr. Lars Querndt, LL.M. (Madrid)\*

# Neue Entwicklungen zum Anzeigenprivileg der Presse im digitalen Bereich?

## Kurz und Knapp

**Die Presse haftet bei der Prüfung von Anzeigen im Printbereich nur im Hinblick auf evidente Rechtsverletzungen. Gleiches gilt nach einer neueren Entscheidung des BGH für die Haftung eines Rundfunkveranstalters für ausgespielte Werbespots. Nachdem dieser Beitrag die Herleitung des Anzeigenprivilegs der Presse für die beiden Medien Print und Rundfunk beleuchtet, wird außerdem untersucht, ob es Besonderheiten bei der Prüfung digitaler Werbeanzeigen auf den Webseiten von Presseunternehmen gibt.**

## I. Herleitung des Anzeigenprivilegs der Presse

Das Anzeigenprivileg der Presse ist rechtlich gesehen ein „alter Hut“. Es gibt zahlreiche Instanz- und auch höchstgerichtliche Rechtsprechung, die der Presse bei der Prüfung von Werbemitteln eine Haftungsprivilegierung zubilligen. Bereits im Jahr 1972 arbeitete der BGH das Problem heraus, dem sich die Presse bei der Prüfung von Anzeigen im Printbereich gegenüber sah.<sup>1</sup> Wäre die Anzeigenabteilung bei der Entgegennahme von Aufträgen zu einer umfassenden rechtlichen Prüfung dieser Anzeigen verpflichtet, so ginge dies unweigerlich zulasten des Kerngeschäfts der Presse, der Veröffentlichung journalistisch-redaktioneller Inhalte. Denn diese rechtliche Prüfung würde eine umfassende Expertise im Tätigkeitsbereich der Anzeigenkunden erfordern, zu der der Verlag und seine Anzeigenmitarbeiter nicht, oder nur mit unverhältnismäßigem Aufwand, in der Lage wären. Der BGH stellte zwar

schon damals fest, dass Verlag und Redaktion gehalten sind, Anzeigen mit rechtswidrigem Inhalt abzulehnen. Eine verfassungskonforme Auslegung im Hinblick auf Art. 5 Abs. 1 Grundgesetz gebiete es jedoch, die Prüfungspflicht nicht auf sämtliche Gesetzesverstöße zu erstrecken, sondern auf grobe, vom Verlag oder Redaktion unschwer zu erkennende Verstöße zu beschränken.<sup>2</sup>

### 1. Die klassischen Fälle der Evidenzhaftung der Presse

An diese Entscheidung des BGH aus dem Jahr 1972 schloss sich vor allem Anfang der 1990er und 2000er Jahren weitere Rechtsprechung an, die sich ausschließlich auf den Printbereich bezog.<sup>3</sup> Dieser Bezug zum Printbereich spiegelte sich dabei in den Argumenten für die Haftungsprivilegierung der Presse bei der Anzeigenprüfung wider. So findet sich etwa in der Entscheidung „Pressehaftung“ der Hinweis des BGH, dass die Presse bei der Anzeigenprüfung unter Zeitdruck stehe und

\* Mehr über den Autor erfahren Sie am Ende des Beitrags.

- 1 BGH, 30. 6. 1972 – I ZR 1/71, GRUR 1973, 203 – Badische Rundschau.
- 2 BGH, 30. 6. 1972 – I ZR 1/71, GRUR 1973, 203, 204 – Badische Rundschau.
- 3 BGH, 26. 4. 1990 – I ZR 127/88, GRUR 1990, 1012, 1014 – Pressehaftung; 7. 5. 1992 – I ZR 119/90, NJW 1992, 2765 – Pressehaftung II; 10. 2. 1994 – I ZR 316/91, GRUR 1994, 454 – Schlankheitsmittel; 9. 11. 2000 – I ZR 167/98, GRUR 2001, 529 – Werbung für Knoblauch-Präparate; 14. 6. 2006 – I ZR 249/03, GRUR 2006, 957 – Stadt Geldern; 26. 1. 2006 – I ZR 121/03, GRUR 2006, 429 – Schlank-Kapseln; ebenfalls OLG München, 22. 2. 2001 – 29 U 3333/00, NJW-RR 2001, 1716; ähnlich z. B. zur Prüfpflicht bei Urheberrechtsverletzungen in Anzeigen KG, 14. 1. 2005 – 5 W 1/05, NJOZ 2005, 1094.