

Kommunikation & Recht



Betriebs-Berater für

● Medien ● Telekommunikation ● Multimedia

4

K&R

- Im Telegrammstil nach Dubai
Dr. Jonas Kahl
- 225 Personenbezogene Daten als „Preis“ für digitale Produkte
Prof. Dr. Jochen Schneider und **Isabell Conrad**
- 232 Das neue Schuldrecht 2022 – Teil 3
Prof. Dr. Felix Buchmann und **Chiara Panfili**
- 240 Neue Rahmenbedingungen für den Einsatz von Algorithmen im Mediensektor
Dr. Judit Bayer und **Prof. Dr. Bernd Holznagel**
- 247 Aktuelle Rechtsentwicklungen bei Suchmaschinen im Jahre 2021
Dr. Sebastian Meyer und **Dr. Christoph Rempe**
- 254 Der fliegende Gerichtsstand im UWG als Gretchenfrage an den Gesetzgeber: „Nun sag, wie hast du’s mit dem Internet?“
Dr. Steffen Wettig
- 258 Länderreport Österreich
Prof. Dr. Clemens Thiele
- 260 **EuGH:** Auskunftersuchen der Steuerverwaltung zu Online-Inseraten muss datenschutzkonform erfolgen
- 266 **BVerfG:** Erfolgreiche Verfassungsbeschwerde gegen Normen zu verdeckten Zugriffen auf informationstechnische Systeme
- 269 **BGH:** Unwirksame AGB zu Klarnamenpflicht in sozialem Netzwerk
- 281 **OLG Düsseldorf:** Fliegender Gerichtsstand beim Streit um irreführende Werbung mit Internetbezug
- 290 **OLG Köln:** Unwirksame AGB zur eingeschränkten Nutzung von SIM-Karten in Routern
- 298 **FG Köln:** Gewinne aus privaten Kryptowert-Veräußerungen sind steuerpflichtig
mit Kommentar von **Prof. Dr. Jens M. Schmittmann**

25. Jahrgang

April 2022

Seiten 225 – 304

RA Prof. Dr. Jochen Schneider und RAin, Fachanwältin IT-Recht Isabell Conrad*

Personenbezogene Daten als „Preis“ für digitale Produkte

Ein Marktmodell mit vielen Herausforderungen für die praktische Umsetzung

Kurz und Knapp

Die neuen §§ 327ff. BGB für Verbraucherverträge über digitale Produkte gelten auch, wenn der Verbraucher dem Unternehmer personenbezogene Daten bereitstellt oder sich dazu verpflichtet. Praktisch wird insoweit Datenhergabe mit Entgelt gleichgesetzt. Andererseits entkoppelt § 327q BGB die Datenschutzthemen vom Vertrag. Der Beitrag geht den Problemen nach, die mit dieser Trennung verbunden sind und einem sicheren Geschäftsmodell entgegenstehen.

I. Entstehung der Diskussion über „Bezahlen mit Daten“

Das plakativ „Bezahlen¹ mit Daten“ genannte Konzept der DID-RL² und die Umsetzung in §§ 312, 327, 327q BGB abstrahieren trotz Anwendbarkeit der §§ 327 ff. BGB bei Datenbereitstellung durch den Verbraucher die datenschutzrechtliche Zulässigkeit der Verarbeitung von der Wirksamkeit des Verbrauchervertrags und dem Anspruch des Verbrauchers auf die Leistung. Die bisherige Herangehensweise im Datenschutz, Kartellrecht³ und UWG⁴ ist, vom datenschutzwidrig handelnden Unternehmer Unterlassung, Schadensersatz und Bußgeld zu fordern. Die Pläne der EU-Kommission,⁵ den Einzelnen schuldrechtlich an der Ökonomisierung seiner Daten partizipieren zu lassen und Lock-in-Effekte hinsichtlich der großen Plattformen zu durchbrechen, sind ähnlich alt wie die DSGVO. Auch die Etablierung „neutraler Vermittler“, die „persönliche Datenräume“ für Verbraucher anbieten oder fördern, dass der Einzelne sicher allgemein verwendbare digitale Identitäten nutzen kann, ist ein Baustein, damit der Verbraucher mit personenbezogenen Daten „Entgelt“-ähnlich „zahlen“ kann.⁶

Bei dem Vorschlag für die DID-RL (Art. 3 Abs. 1) war die Gegenleistung in Form personenbezogener (oder anderer) Daten der Zahlung eines Preises gleichgestellt worden.⁷ Dieser Art. 3 Abs. 1 des RL-Vorschlags sollte gem. Abs. 4 nicht gelten, wenn die Daten für die „Erfüllung des Vertrags“ (und rechtlicher Anforderungen) unbedingt erforderlich sind,⁸ was hinsichtlich Daten als für die Vertragserfüllung erforderliche Gegenleistung zirkulär war, wenn auch ähnlich der Formulierung in Art. 6 Abs. 1 lit. b DSGVO. Der Europäische Datenschutzbeauftragte hatte sich ausdrücklich gegen diese Regelung ausgesprochen.⁹ Anders

als ursprünglich vorgesehen, regelt Art. 3 Abs. 2 DID-RL v. 20. 5. 2019 nur noch ein stark abgeschwächtes „Modell“, bei dem von Zahlung o. ä. nicht (mehr) die Rede ist.¹⁰ Es geht nur darum, den Anwendungsbereich zu erweitern auf die Fälle, bei denen vom Verbraucher (auch) Daten bereitgestellt werden oder Bereitstellung zugesagt wird.¹¹

Art. 3 Abs. 1 DID-RL spricht nicht mehr – etwa im Kontext eines Preises – von der Bereitstellung personenbezogener Daten als Gegenleistung. Stattdessen dehnt § 327 Abs. 3 S. 2 BGB die Anwendung auch auf Fälle aus, in denen der Verbraucher personenbezogene Daten bereitstellt oder deren Bereitstellung zusagt – mit der in §§ 327 Abs. 3, 312 Abs. 1a S. 2 BGB geregelten Ausnahme für Datenverarbeitung ausschließlich zur Erfüllung der Leistungspflicht des Unternehmers oder seiner gesetzlichen Pflichten.

* Mehr über die Autoren erfahren Sie am Ende des Beitrags.

- 1 Nicht im Sinne einer virtuellen Währung (EZB, Opinion 2014/08 v. 4. 7. 2014) oder eines Zahlungsmittels im Sinne ZAG.
- 2 RL (EU) 2019/770 v. 20. 5. 2019. Die deutsche Umsetzung im BGB ist am 1. 1. 2022 in Kraft getreten.
- 3 Bezüglich der Facebook-AGB hat der BGH dem EuGH (C-252/21 – Vorlage des BGH v. 22. 4. 2021) die Frage vorgelegt, ob eine nationale Kartellbehörde im Rahmen der kartellrechtlichen Missbrauchsaufsicht einen Verstoß der Vertragsbedingungen gegen DSGVO feststellen und eine Abstellungsverfügung erlassen darf.
- 4 Der EuGH (C-319/20 – Vorlage des BGH v. 15. 7. 2020) wird darüber entscheiden, ob das Sanktionsregime der DSGVO abschließend ist oder ob daneben eine Abmahnfähigkeit nach UWG, UKlaG etwa durch Verbraucherverbände auch ohne Auftrag von betroffenen Personen möglich ist.
- 5 Mitteilung der Kommission „Aufbau einer europäischen Datenwirtschaft“, 10. 1. 2017, COM(2017) 9 final, S. 17 f.: Datenübertragbarkeit und Interoperabilität als wesentliche Bausteine; Recht auf Datenübertragbarkeit in Art. 20 DSGVO. Siehe auch Mitteilung „Eine europäische Datenstrategie“, 19. 2. 2020, COM(2020) 66 final, S. 23 f. Die EU-Kommission will die Datenübertragbarkeit u. a. durch „strengere Anforderungen an Schnittstellen für den Echtzeit-Datenzugriff“ etwa bei Internet of Things (IoT)-Geräten oder Wearables stärken.
- 6 COM(2020) 66 final, S. 24. Mit Spannung wird die Rechtsverordnung der deutschen Bundesregierung für „anerkannte Dienste zur Einwilligungsverwaltung, Endnutzereinstellungen“ (§ 26 Abs. 2 TTDSG) erwartet.
- 7 Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über bestimmte vertragsrechtliche Aspekte der Bereitstellung digitaler Inhalte, v. 9. 12. 2015, COM(2015) 0634.
- 8 Art. 3 Abs. 1 der endgültigen DID-RL ist folgerichtig wesentlich enger: „ausschließlich zur Bereitstellung digitaler Inhalte oder digitaler Dienstleistungen im Einklang mit dieser Richtlinie“.
- 9 EDSB Stellungnahme 4/2017 v. 14. 3. 2017, S. 9 ff., auf die auch Schulze, BGB, 11. Aufl. 2021, § 327 Rn. 12 verweist.
- 10 Klink-Straub, NJW 2021, 3217; Spindler, MMR 2021, 451, 452 weist darauf hin, dass die Umsetzung über die DID-RL hinausgeht und generell für diesen Fall der Preisgabe der Daten der Verbraucher als Verbraucherverträge den §§ 312 ff. BGB zuzuordnen sind – und stellt in der Begr. (S. 32) „entsprechend Erwägungsgrund 31 der sog. Modernisierungs-RL²⁶ klar, dass dieser Fall schon zuvor von § 312 Abs. 1 BGB bzw. der Verbraucherrechts-RL 2011/83/EU erfasst worden war“.
- 11 § 327 Abs. 3 setzt dies und die vorgesehene Ausnahme (§ 312 Abs. 1a S. 2 BGB) um.

II. Vermeintliche Neutralität der DID-RL und der §§ 327 ff. BGB gegenüber dem Datenschutz

Ausgangspunkt und Richtschnur bei der Auslegung der §§ 312, 327 und 327q BGB¹² ist die Datenschutz-Neutralität der DID-RL:¹³ Deren EG 37 S.2 besagt: „Diese Richtlinie lässt insbesondere die VO (EU) 2016/679 [...] und die RL 2002/58/EG [...] unberührt.“¹⁴ Im Verhältnis zur DID-Richtlinie regelt die deutsche Umsetzung aber mit § 327q BGB das Thema nicht losgelöst vom Datenschutz.¹⁵

Durch die Einbeziehung der Wirkung von Einwilligung und Widerspruch im Verhältnis zur Reaktion des Unternehmers (Beendigung gem. § 327q Abs. 2) kommt Datenschutzinstrumentarium in das Vertragsgefüge hinein. Zwar wird allgemein entsprechend auch bei § 327q Abs. 1 bezüglich etwaiger Rechte und Erklärungen des Betroffenen angenommen, dass der Bestand des Vertrags von der datenschutzrechtlichen Zulässigkeit unabhängig ist. Aber zum Beispiel stellt sich die Frage, ob eine nicht Datenschutz-gerechte und -geeignete Ausprägung¹⁶ des digitalen Produkts nicht zugleich einen Mangel darstellt. Dies betrifft nicht nur die Sicherheit, sondern auch die Datenschutz-Compliance.

Es deutet sich an, dass die Regelung schon im Ansatz nicht einfach den Datenschutz *unberührt* lässt, sondern die Realisierung der §§ 327 ff. kaum ohne massive Berücksichtigung der DSGVO und weiterer Vorschriften, ggf. § 25 TTDSG, möglich sein wird. Umso gravierender ist, dass das Geschäftsmodell „Daten gegen Leistung“ auf sehr unsicherem Boden steht, was näher gezeigt werden soll. *Bach* hatte schon zur DID-RL Skepsis bezüglich des zu erwartenden Erfolgs des Modells geäußert u. a. wegen des Art. 7 Abs. 4 DSGVO („Kopplungsverbot“) und der damit verbundenen Unsicherheit über die Wirksamkeit der Einwilligung.¹⁷

III. Geschäftsmodell der Rechtsunsicherheit

Welchen Gefallen würde sich ein Unternehmer tun, der sein Geschäft auf Angebote gegen Zahlung eines Preises oder Bereitstellung (oder deren Zusage) personenbezogener Daten aufbaut? Er geht ein erhebliches Risiko ein, v. a. datenschutzrechtlich und auch wirtschaftlich, weil er am Ende nichts Konkretes erhält.

1. Unklar ist schon, ob es sich nur um personenbezogene Daten des Verbrauchers, also des unmittelbaren Vertragspartners, handeln soll und kann, oder auch um Daten Dritter. Daten Dritter können z. B. bei Smart Home-Anwendungen (Daten der Mitbewohner oder Besucher) oder Daten über Fahrzeuginsassen relevant sein. Vom Wortlaut in § 327 Abs. 3 her wäre die Erstreckung auch auf Daten Dritter möglich, ist evtl. sogar notwendig. Allerdings passt dies nicht zu § 327q Abs. 2: dort ist nur vom Widerruf des Verbrauchers, also des direkten Vertragspartners die Rede. Da § 327q nicht bewirken kann, dass der Dritte keine Datenschutz-Rechte hätte, bleibt praktisch nur die Auslegung, dass es sich nur um die Daten des Verbrauchers, der der konkrete Vertragspartner ist, handeln kann, oder der Verbraucher wird zugleich zum Verantwortlichen (die Grenze familiärer oder rein privater Sphäre i. S. Art. 2 Abs. 2 lit. c DSGVO ist schnell überschritten).

2. Zumindest bei der deutschen Konstruktion, § 327 i. V. m. § 312 Abs. 1a ist die Bereitstellung der Daten bzw. die Verpflichtung dazu nicht als „Gegenleistung“ zu qualifizieren. Es wird lediglich gem. § 327 Abs. 3 die Anwendung der §§ 327 ff. auf diesen Fall ausgedehnt. Der Verbraucher kommt dadurch auch bei kostenloser Nutzung digitaler Produkte in den Schutz zahlreicher Vorschriften.¹⁸ D. h. ein Synallagma besteht wohl nicht.¹⁹ Die Nicht-Bereitstellung der Daten durch den Verbraucher ist keine Vertragsverletzung, wie sich aus § 327q Abs. 3 ergibt. Die Beibringung der Daten bzw. der Bereitstellung ist nicht einklagbar. Angesichts des jederzeit durch den Verbraucher ausübbareren Rechts auf Widerruf und Widerspruch würde eine Klage auf Bereitstellung keinen Sinn machen.

3. In der Praxis dürfte eine synallagmatische Bereitstellung von Daten eher ermittelbar sein als eine nicht-synallagmatische. Die deutsche Regelung, die kein Synallagma verlangt, führt u. a. zu folgender Rechtsunsicherheit im Anwendungsbereich: Fällt bereits jede Webseite, die Google Analytics oder andere Werbe-Tracker/-Tools einsetzt, in den Anwendungsbereich von § 327 – und zwar unabhängig davon, ob der Nutzer dafür die Einwilligung erteilt, oder ob (entgegen § 25 TTDSG) keine Einwilligung eingeholt, aber trotzdem Werbe-Tracker eingesetzt werden?

4. Werden Daten von Minderjährigen verarbeitet, was für den Unternehmer bei Online-Angeboten nicht ohne weiteres erkennbar ist, stellt sich neben den Problemen von Art. 8 DSGVO und ggf. der Einwilligungsbedürftigkeit hinsichtlich der Erziehungsberechtigten auch schuldrechtlich das Problem der schwebenden Unwirksamkeit des schuldrechtlichen Vertrags.

5. Ob und wann sich der Unternehmer auf Art. 6 Abs. 1 S. 1 lit. b DSGVO stützen kann, ist unklar. Nach überwiegender Ansicht v. a. der Datenschutzbehörden²⁰ wird die Erforderlichkeit von Online-Werbung zur Vertragserfüllung verneint. Dem EuGH liegt die Frage vor, ob Datenverarbeitung zur Produktverbesserung, Personalisierung der Inhalte und der Werbung Gegenstand einer Einwilligung sein muss (wegen des höheren Schutzes v. a. aufgrund

12 Im Folgenden ohne Zusatz („BGB“) angegebene §§ beziehen sich auf Vorschriften des BGB in der seit 1. 1. 2022 geltenden Fassung.

13 RL 2019/770/EU vom 20. 5. 2019.

14 EG 38 DID-RL stellt die Folgerungen dar und verweist hinsichtlich der Rechtmäßigkeit der Verarbeitung auf die DSGVO. „Die vorliegende Richtlinie sollte nicht die Gültigkeit der gegebenen Einwilligung regeln. [...]“

15 Der RegE vom 17. 3. 2021 verweist bei § 327q auf das Gutachten der Datenethikkommission der BReg vom Oktober 2019, S. 105.

16 Neben Verstößen gegen Art. 5 Abs. 1 lit. c, Art. 25, Art. 32 DSGVO kommt z. B. in Betracht, dass bei Nutzung eines digitalen Produkts Standortdaten oder andere Daten des Verbrauchers unbemerkt und ohne Rechtsgrundlage an Dritte (evtl. auch in Drittländern) offengelegt werden. Automatisierte Entscheidungsfindung und Profiling (Art. 20 DSGVO) sind bei digitalen Produkten ebenfalls häufig relevant.

17 *Bach*, NJW 2019, 1705, 1706 mit Verweis: „So etwa *Frenzel*, in: Paal/Pauly, DSGVO, 2. Aufl. 2018, Art. 7 Rn. 21; *Klement*, in: Simitis/Hornung/Spiecker gen. Döhmman, Datenschutzrecht, 2019, Art. 7 DSGVO Rn. 60 f.“

18 Lt. *Rosenkranz*, ZUM 2021, 195 brachte die vertragsrechtliche Erfassung der Daten als Wirtschaftsfaktor zunehmender Bedeutung für den Richtliniengeber viel Lob; s. a. zum Problem und zur Disk. „Dienste gegen Daten“: *Leistner/Antoine/Sagstetter*, Big Data, 2021, S. 253 ff. m. w. N.

19 A. M. z. B. *Bach*, NJW 2019, 1705, eingangs zitiert. Zum Streit mit tendenziell ebenfalls a. M. s. *Schulze*, BGB, 11. Aufl. 2021, § 327 Rn. 12 mit Verweis auf tatsächliche wirtschaftliche Bedeutung und übliche zivilrechtliche Begriffsverwendung und auf EU Digital Law, *Staudenmayer*, DCD, Art. 3 Rn. 46 ff., 137 ff.; *Lohsse/Schulze/Staudenmayer*, in: *Lohsse/Schulze/Staudenmayer* (Hrsg.), Data as Counter-Performance – Contract Law 2.0?, 2020, S. 15 ff.

20 EDSA, Leitlinien 2/2019, Rn. 52.

freier Widerruflichkeit und Art. 7 Abs. 4 DSGVO) oder ob diese Datenverarbeitungszwecke vertraglich vereinbart werden können und ob die Willenserklärung des Verbrauchers „unter das Rechtskonzept nach Art. 6 Abs. 1 lit. b DSGVO verschoben werden kann“.²¹

6. Ebenfalls unklar ist, ob der Unternehmer die Verarbeitung nach Widerruf der Einwilligung auf Art. 6 Abs. 1 lit. b DSGVO stützen kann, ob dann schon mangels Transparenz die ursprüngliche Einwilligung unwirksam wäre oder ob die Einwilligung (bzw. deren Verweigerung oder Widerruf) eine Sperrwirkung hinsichtlich anderer Rechtsgrundlagen des Art. 6 Abs. 1 DSGVO entfaltet.²² Nach str. M. besteht bei Einforderungen von „unnötigen“ – durch Art. 6 Abs. 1 lit. b oder lit. f gedeckte – Einwilligungen bei deren Wegfall keine Möglichkeit, auf die bestehenden Grundlagen einer Rechtfertigung „umzusteigen“,²³ – der Widerruf führt zum Ende der Zulässigkeit der Nutzung. Die Gesetzesbegründung²⁴ zu § 327q schließt andere Rechtsgrundlagen als die Einwilligung nicht aus. Bei Widerruf dürfte eine Rechtsgrundlage für eine über reine Leistungspflichterfüllung des Unternehmers oder Erfüllung gesetzlicher Pflichten hinausgehende Verarbeitung – etwa auf Basis von Art. 6 Abs. 1 lit. f DSGVO – wegen entgegenstehendem Willen der betroffenen Person fraglich sein. Soweit der deutsche Gesetzgeber bei Widerruf die Verarbeitung auf anderer (wenn auch reduzierter) Grundlage für zulässig erachtet,²⁵ hätte er wegen Anwendungsvorrang der DSGVO dafür keine Regelungskompetenz.

7. Ob eine Einwilligung erforderlich ist, ist unklar und wohl auch nicht generell entscheidbar. Theoretisch könnten §§ 327 ff. die Rechtsgrundlage für die Verarbeitung der Daten im Sinne von Art. 6 Abs. 1 lit. b DSGVO darstellen. Die Ausnahme von der Anwendung der §§ 327 ff. greift nach § 312 Abs. 1a nur, wenn die Datenverarbeitung zur Erfüllung der Leistungspflicht des Unternehmers erforderlich ist und keine anderweitige Verwendung erfolgt. Ist die Verarbeitung erforderlich, um die Gegenleistung des Verbrauchers zu erfüllen, gilt Art. 6 Abs. 1 lit. b DSGVO hinsichtlich der Daten des Verbrauchers (Vertragspartners) und §§ 327 ff. sind anwendbar. Falls auch Daten Dritter betroffen sind, ist das praktisch ohne Einwilligung²⁶ der Dritten keine Option. Soweit die Einwilligung Dritter beizubringen ist, könnte dies Teil der Gegenleistung sein. Dies hat aber angesichts der jederzeitigen Widerruflichkeit keinen wirklichen Wert.

8. Der Widerruf der Einwilligung richtet sich nach Art. 7 Abs. 3 DSGVO (auch hins. der Einfachheit der Widerrufsmöglichkeit), der Widerspruch nach Art. 21 DSGVO. Die ansonsten im Zusammenhang mit der DSGVO und dem Widerrufsrecht zugunsten des Unternehmers diskutierten Positionen wie etwa Treuwidrigkeit o. Ä.²⁷ sind angesichts des Wortlauts des § 327q, insbes. auch Abs. 3 und der DID-RL kaum auf die §§ 327 ff. anwendbar.

9. Ob die Einwilligung wirksam angesichts Art. 7 Abs. 4 DSGVO (Kopplung) gegeben werden kann bzw. wird, wenn es darum geht, Geldbeträge zu sparen, ist ebenfalls unklar.²⁸ Von den Gerichten v. a. in Österreich wird Art. 7 Abs. 4 mit Blick auf ErwG 43 S. 2 DSGVO teilweise nicht wie eine Abwägungsnorm, sondern wie ein Verbot ausgelegt.²⁹ Es bestehen also stetig drohende Bedenken hinsichtlich der Freiwilligkeit. Das berührt

aber die Zulässigkeit der Datenverarbeitung, nicht den Bestand des Vertrags.

10. Bei vielen digitalen Produkten sind Drittlandübermittlungen in der Praxis selten auszuschließen und die Anforderungen des EDSA an technische Maßnahmen gegen mögliche Zugriffsbefugnisse von z. B. US-Behörden nur selten erfüllbar.³⁰ Wegen des von den Datenschutzbehörden propagierten (aber über den Wortlaut von Art. 49 Abs. 1 UA 1 DSGVO eigentlich hinausgehenden)³¹ Ausnahmecharakters sind Art. 49 Abs. 1 lit. a und b DSGVO als Rechtsgrundlagen bei „personenbezogene[n] Daten, die im Zusammenhang mit der regelmäßigen Nachverfolgung von Nutzerverhalten auf Webseiten oder in Apps verarbeitet werden,“³² fraglich und riskant. Ebenso unsicher ist Art. 49 Abs. 1 UA 2 DSGVO.

11. Im Hinblick auf den Ausnahmetatbestand in § 312 Abs. 1a S. 2 wäre eine technisch/logische Abschichtbarkeit der Daten notwendig, ist aber kaum möglich: Konkret welche Daten sind etwa bei der Personalisierung von Online-Angeboten für die Erfüllung der Leistungspflicht des Unternehmers erforderlich und welche nicht? Für den Fall des Widerrufs/Widerspruchs muss klar differenziert entscheidbar und trennbar sein, was an Daten darf weiter, was nicht mehr genutzt werden? Das ist auch Voraussetzung, um Löschungen bzw. Sperrungen vornehmen zu können.

12. Zwar ist unklar, ob am Ende die Leistung des Verbrauchers in der Bereitstellung bzw. Verpflichtung dazu oder der Einwilligung besteht, – jedenfalls hat der Unternehmer auch nach Widerruf weiter zu leisten bzw. besteht der Vertrag weiter, einschl. Aktualisierungspflicht. D. h., dass den Unternehmer, der einmalig bereitgestellt hat, nach Widerruf die unklar lange Aktualisierungspflicht³³ weiterhin trifft.

13. Bei der Vielzahl von Inhalten und Dienstleistungen, die unter §§ 327 ff. fallen, ist die Wahrscheinlichkeit, dass Daten Dritter beteiligt sind, groß. Es ist unklar, ob nicht die Konstruktion der Bereitstellung gem. § 327b – soweit es um personenbezogene Daten Dritter geht – zu Auftragsverarbeitung oder Joint Control (JC) führt. Ausdrücklich verpflichten sich die Parteien zur Einrichtung gegenseitiger Bereitstellungen, was Art. 26 DSGVO näherliegend

21 OGH Österreich, 23. 6. 2021 – 6 Ob 56/21k – Schrems III, Vorlage an den EuGH, C-446/21: Facebook hatte ursprünglich Einwilligungen eingeholt, später aber statt Einwilligungen die AGB geändert. Die Formulierung in den Facebook-AGB lautet „Anstatt dafür zu zahlen ... erklärst du dich durch Nutzung der Facebook-Produkte, für die diese Nutzungsbedingungen gelten, einverstanden, dass wir dir Werbeanzeigen zeigen dürfen ... Wir verwenden deine personenbezogenen Daten ... um dir Werbeanzeigen zu zeigen, die relevanter für dich sind.“

22 Die Sperrwirkung verneinend: *Buchmüller/Roos*, ZD 2022, 8, 11.

23 Z. B. *Taeger*, in: *Taeger/Gabel*, DSGVO – BDSG – TTDSG, 4. Aufl. 2022, Art. 6, Rn. 47–53 und *Frenzel*, in: *Paal/Pauly*, DSGVO BDSG, 3. Aufl. 2021, Art. 6 DSGVO Rn. 8 u. Art. 7 Rn. 12a zum Streit weiterer Erlaubnis bei Einwilligungswiderruf.

24 BT-Drs. 19/27653, S. 76.

25 BT-Drs. 19/27653, S. 76. Zustimmung *Buchmüller/Roos*, ZD 2022, 8, 11.

26 Und selbst diese Option ist ggf. kritisch hinsichtlich der Wirksamkeit zu sehen.

27 S. z. B. bei *Klement*, in: *Simitis/Hornung/Spiecker* gen. *Döhmann* (Fn. 17), Art. 7 DSGVO, Rn. 91, 92; *Bräutigam*, MMR 2012, 635.

28 *Becker*, CR 2021, 230.

29 OGH Österreich, 31. 8. 2018 – 6Ob140/18h.

30 EDSA, Recommendations 1/2020, Version 2, 18. 6. 2021.

31 *Conrad/Siara*, ZD 2021, 455.

32 DSK, Orientierungshilfe Telemedien, 20. 12. 2021, S. 30.

33 § 327f Abs. 1 S. 3 Nr. 2 „... Zeitraum, den der Verbraucher aufgrund der Art und des Zwecks des digitalen Produkts und unter Berücksichtigung der Umstände und der Art des Vertrags erwarten kann“.

erscheinen lässt³⁴ als Art. 28 DSGVO (Auftragsverarbeitung), wobei der Verbraucher gemäß § 327b Abs. 3 die Einrichtung bestimmt, mittels derer ihm die Daten zur Verfügung gestellt werden. Aber der Umstand, dass der Verbraucher die Einrichtung gem. § 327b Abs. 4 bestimmen kann, über die ihm gegenüber die Bereitstellung erfolgen soll, spricht eher für Joint Control. Das gilt auch für Informationen, z. B. erläuternd zu Fotos, auf denen (auch) Dritte abgebildet sind. Dazu werden eventuell von der Plattform zusätzliche Daten abgefragt. Für die Dritten liegt kein Auftrag, kein JC und kein Vertrag vor, aber die Zulässigkeit der Verarbeitung der Daten beurteilt sich insoweit im Verhältnis Unternehmer/Dritte. Inzwischen verarbeiten viele Dienste die Daten zu Beziehungsgeflechten mit Dritten, sodass die Daten sowohl eigene des Verbrauchers als solche von Dritten sind.

14. Zu den zahlreichen Informationspflichten im Bereich des E-Commerce treten die gem. §§ 327 ff., die indirekt über das Thema Einwilligung mit den Informationspflichten gem. Art. 12 ff. DSGVO zusammentreffen, wobei nicht ganz klar ist, welche Rolle genau der Verbraucher spielt, s. vorstehend 1. und 13.

15. Nicht abschließend geklärt ist auch das Verhältnis der AGB-rechtlichen Unwirksamkeit und Abmahnbarkeit von datenschutzwidrigen Klauseln³⁵ zum Grundgedanken des § 327q. Sind Daten der „Preis“ im Sinne der hauptvertraglichen Gegenleistung, unterliegen (verglichen mit einer Geldzahlung als Vergütung) das Ob und die Höhe der Gegenleistung nicht der Inhaltskontrolle, anders aber Nebenabreden, Intransparenz des Preismodells u. ä.³⁶ Hinsichtlich Daten als Gegenleistung müsste eine Bestimmung erfolgen über Art und Umfang der Daten, Zweckbestimmung und Dauer der Verarbeitung sowie ggf. weitere Empfänger der Daten. Eine Ausnahme von der Inhaltskontrolle³⁷ wird dabei nicht bestehen und eine transparente Regelung häufig schwierig sein.

16. Der Unternehmer hat nach § 327q Abs. 3 keinen Entschädigungsanspruch. Das heißt aber nicht, dass dem Unternehmer bei Widerruf/Widerspruch oder Lösch-/Einschränkungsbegehren keine Schäden drohen. Welchen monetären Wert die Daten haben, dürfte eine Frage des Einzelfalls sein.³⁸ Hat der Unternehmer z. B. Daten aus unterschiedlichen Quellen (online und offline) und über verschiedene Endgeräte, Plattformen und E-Commerce-Anwendungen hinweg in einen Identity Graph eingebaut,³⁹ kann der ID Graph bei erzwungenem Ausbau von Daten beschädigt werden. Inwieweit solche und andere Umstände zumindest bei der Abwägung zu berücksichtigen sind, ob der Unternehmer – ggf. fristlos – kündigen darf, ist noch nicht geklärt.

IV. Richtigkeit, Mitwirkung als weitere rechtspolitische Überlegung und Fazit

Müssen die Daten, die der Kunde bereitstellt, richtig sein?⁴⁰ Geregelt ist, dass die Ausübung der Datenschutzrechte die Wirksamkeit des Vertrags nicht berührt (§ 327q Abs. 1). Angesichts des fehlenden Gegenseitigkeitsverhältnisses und des geringen Rangs der Datenbereitstellung durch den Verbraucher wären ohnehin kaum Sanktionen denkbar. Ob allerdings der Ausschluss etwaiger Ersatzansprüche gem. § 327q Abs. 3 auch bei Falschlieferung gilt, darf bezweifelt werden. Diese sind keine datenschutzrechtlich privilegierten Rechte. Unklar

ist aber, ob sich etwaige Ansprüche des Unternehmers auf die Bereitstellung richtiger Daten oder z. B. auf die Einwilligung in eine entsprechende Datenverarbeitung richten würden. Zumindest bei Nichtlieferung trotz schuldrechtlicher Pflicht des Verbrauchers zur Bereitstellung dürfte der Unternehmer praktisch keine Möglichkeit der Ersatzansprüche haben, soweit der Verbraucher hinsichtlich der Datenverarbeitung jederzeit widerrufen oder widersprechen kann.

Ungeregelt ist also eine eventuelle Sanktion bei Schlecht-/Falschlieferung von Daten seitens des Verbrauchers. Soweit die Parteien überhaupt eine Haftung beidseitig annehmen, könnte man an eine Qualifizierung als Verletzung der Mitwirkungspflicht denken und insoweit § 642 analog heranziehen. So gesehen käme es für die genaue Einordnung der Bereitstellung der Daten durch den Verbraucher auf den Vertrag und dessen Gestaltung an.

V. Fragestellung: Trennbarkeit, Abschichtung der Daten auf der Verbraucherseite

Am Ende der Vertragslaufzeit, aber v. a. bei Widerruf wird genau zu trennen sein, welche Daten der Unternehmer evtl. (noch) verarbeiten darf, u. a. zu Beweis Zwecken im Kontext des Vertrags, und welche Daten gelöscht werden müssen. Sind die Daten überhaupt so trennbar? § 327q wirkt auch bezüglich dieser Frage des Datenspektrums missglückt.⁴¹ Das liegt wohl daran, dass § 327q ein schmaler Weg zwischen zwei Dämmen ist, wovon zumindest ein Damm zugunsten einer konsequenten Lösung durchbrochen werden müsste: Ein Dammbruch wäre die Aufwertung der Daten mit Lizenz, Geldwert⁴² und Rechtsschutz, Letzteres nicht zwingend, aber die Folge der beiden ersten, oder (zweiter Dammbruch) das Recht auf Widerruf und Widerspruch wird zugunsten des Unternehmers beschränkt/relativiert. Zudem wäre das sog. *Kopplungsverbot* zu lockern bzw. neu zu regeln.⁴³

34 S. EuGH, 5. 6. 2018 – C-210/16, K&R 2018, 475 ff. – Facebook-Fanpage; EuGH, 10. 7. 2018 – C-25/17 – Zeugen Jehova, EuGH, 29. 7. 2019 – C-40/17, K&R 2019, 562 ff. – Fashion ID.

35 § 2 Abs. 2 Nr. 11 UKlaG, siehe etwa LG Berlin, 16. 1. 2018 – 16 O 341/15.

36 BGH, 13. 7. 2005 – IV ZR 83/04; BGH, 25. 11. 2015 – VIII ZR 360/14.

37 Zu Art. 4 Abs. 2 der RL 93/13/EWG über missbräuchliche Klauseln in Verbraucherverträgen: *Hacker*, in: Lohsse/Schulze/Staudenmayer (Fn. 19), S. 66 f.

38 In Adresshändler-Verträgen bemisst sich die Vergütung regelmäßig nicht an einzelnen Daten und betroffenen Personen, sondern ist z. B. eine Lizenzgebühr für regelmäßige (etwa vierteljährliche) Komplettkopien von Adress-Datenbanken. Die Mehrheit der Verbraucher scheinen ihre Daten schon gegen eine geringe Preisersparnis herzugeben, siehe ENISA, Study on monetising privacy – An economic model for pricing personal information, 27. 2. 2012. Siehe aber unten VIII. 3. zu Informationsasymmetrien.

39 Sowohl im Bereich des Online-Marketings als auch bei z. B. Auskunftfeiern findet das statt. Eine transparente Einwilligung wäre erforderlich, dürfte aber auf Webseiten, v. a. auch wegen der Übermittlungen zwischen verschiedenen Parteien, nur schwer zu erlangen sein.

40 Die Zulässigkeit der Klarnamenpflicht bei Facebook verneint auf Basis § 13 Abs. 6 TMG a. F.: BGH, 27. 1. 2022 – III ZR 3/21, K&R 2022, 269 und III ZR 4/21, K&R 2022, 268; a. A. Vorinstanz u. a. wegen Anwendungsvorrang der DSGVO: OLG München, 8. 12. 2020 – 18 U 2822/19 Pre und 18 U 5493/19 Pre.

41 Wenn die Lösung in Datenschutzregeln liegt, hätte man darauf nur verweisen müssen.

42 S. speziell dazu: *Kühling/Sackmann*, ZD 2020, 24, (s. 29 f. zur „Ökonomisierung von personenbezogenen Daten durch die Einwilligung“); s. a. *Denga*, NJW 2018, 1371; *Eichberger*, VersR 2019, 709; *Hacker*, ZfPW 2019, 148; *Schur*, GRUR 2020, 1142; *Hennemann*, RD 2021, 61; *Klink-Straub*, NJW 2021, 3217.

43 *Kroh/Müller-Peltzer*, ZD 2017, 551; s. a. zum Verbot im Kontext „Bezahlen“ mit Daten *Becker*, CR 2021, 230.

§ 327q legt vom Wortlaut her nahe, dass es zwei Schichten gibt: Die untere Schicht bilden die Daten, die der Unternehmer benötigt, um seinen Dienst, seine Leistung zu erbringen. Für diese Daten bedarf es keiner Einwilligung. Werden allein diese Daten bereitgestellt und werden sie vom Unternehmer gemäß § 312 Abs. 1a S. 2 ausschließlich verarbeitet, um dessen Leistungspflicht oder an ihn gestellte rechtliche Anforderungen zu erfüllen, und werden sie zu keinem anderen Zweck verarbeitet, erfolgt gem. § 327 Abs. 3 keine Anwendung der §§ 327 ff. Werden weitere Daten vom Verbraucher dem Unternehmer bereitgestellt, müsste der Verbraucher zugleich seine Einwilligung (gem. Art. 6 Abs. 1 S. 1 DSGVO) geben, wenn nicht eine der anderen Rechtfertigungen gem. Art. 6 greift.

Insofern kommt eine dritte Schicht in Betracht, die aber nicht völlig andersartige Daten enthält. Dazu könnten auch die Daten gem. Art. 6 Abs. 1 lit. b DSGVO gehören: die Verarbeitung ist für die Erfüllung eines Vertrags, dessen Vertragspartei die betroffene Person ist, oder zur Durchführung vorvertraglicher Maßnahmen erforderlich, die auf Anfrage der betroffenen Person erfolgen. Es liegt keine vollständige Deckung mit dem Spektrum gem. § 312 Abs. 1a vor.

Eigentlich müsste die Wirkung bzw. Geltung der §§ 327 ff. entfallen, wenn die Einwilligung widerrufen wird, der Vertrag aber weiterbesteht. Stattdessen sieht § 327q eine sehr spezielle Lösung vor: der Vertrag bleibt gem. Abs. 1 weiter wirksam, der Unternehmer kann gemäß Abs. 2 unter Umständen, die ihm nicht zumutbar sind, mit sofortiger Wirkung kündigen, vorausgesetzt, der Vertrag sieht eine Reihe einzelner Bereitstellungen oder eine dauerhafte Bereitstellung vor.⁴⁴

D. h. aber, dass der Unternehmer bei einmaliger Bereitstellung keine „Waffe hat“, der Vertrag zwar erfüllt ist, was einmalige i. S. erstmaliger Bereitstellung, nicht aber was Aktualisierung betrifft.

Es wäre denkbar, dass neben den mehr technisch bedingten Daten auch solche zusätzlich noch eine Schicht bilden, die keiner Einwilligung bedürfen, die der Unternehmer möglicherweise unmittelbar gemäß Art. 6 Abs. 1 lit. b DSGVO verarbeiten darf, und darüberhinausgehend solche, die unter Abwägung nach Art. 6 Abs. 1 S. 1 lit. f erlaubterweise (wenn die Abwägung positiv ausfällt) verarbeitbar sind. Dann gäbe es also drei und mehr Schichten.⁴⁵

VI. „Grauzone“: Online-Tracking und personalisierte Online-Werbung

Wenig beachtet ist, dass es sehr wahrscheinlich noch mehr Schichten, weil mehr Anwendungsfälle für § 327q durch die breite Wirkung der §§ 327 ff. gibt, als oft angenommen. Bei reinem Webseiten-Besuch ohne weitergehende Leistungsanspruchnahme und ohne Login/Nutzerkonto liegt wohl (noch) kein Vertragsschluss vor.⁴⁶

Analog der Argumentation, ein haftungsrechtliches Sonderkonzept abzulehnen, wenn „die unentgeltliche Leistung nach den äußeren Rahmenbedingungen ihrer Erbringung auch im Wesentlichen einem regulären (d. h.: entgeltlichen) professionellen Verhalten entspricht“,⁴⁷ wird ein Vertragsschluss etwa zu bejahen sein, wenn der Internetnutzer im Consent Banner seine Auswahl treffen muss und

seine Einwilligung in die Datenverarbeitung zu Online-Werbung u. a. abgibt.⁴⁸

Bei werbefinanzierten Webseiten ist die Nutzung gerade nicht frei möglich, sondern dem Internetnutzer wird der Consent Banner präsentiert und er kann erst dann weiter surfen, wenn er seine Auswahl getroffen hat. Die Behinderung der freien Nutzung der Webseite durch einen Consent Banner dürfte dann am geringsten sein, wenn der Internetnutzer im Consent Banner auf der ersten Ebene (ohne Behinderung durch Nudging)⁴⁹ die Abgabe einer Einwilligung ablehnen kann. Ob § 327q künftig dazu führt, dass die Gerichte eine widerlegliche Vermutung für einen Rechtsbindungswillen des Verbrauchers bei Webseiten-Besuchen annehmen, wenn der Verbraucher im Consent Banner seine Einwilligung abgibt, bleibt abzuwarten. Der deutsche Gesetzgeber scheint dies jedenfalls dann zu befürworten, wenn der Unternehmer werbefinanzierte Einnahmen hat, die von Zugriffszahlen abhängen, oder wenn er durch personalisierte Werbung Vorteile anstrebt.⁵⁰

Die Unklarheiten für den Unternehmer, inwieweit er bei minderjährigen Internetnutzern (§§ 106 - 108, Art. 8 DSGVO) Pflichten nach §§ 327 ff. zu erfüllen hat, sind damit nicht geklärt – zumal eine verlässliche Altersverifikation im Internet zwar möglich (etwa mittels Video-Ident), aber häufig nicht verhältnismäßig und auch nicht datensparsam ist.

Auch beim Online-Tracking sind verschiedene Schichten von Daten und Gruppen von betroffenen Personen zu unterscheiden. Insoweit ist zu klären, für welche Daten jenseits der technisch notwendigen wirksam eine Einwilligung eingeholt werden kann und, selbst wenn alles wirksam geregelt ist, wie bei Widerruf die Trennung erfolgen kann. Der Unternehmer darf Informationen (Cookies und andere Tracker) in der Endeinrichtung speichern und darauf zugreifen, wenn der Internetnutzer auf der Grundlage von klaren und umfassenden Informationen eingewilligt hat (§ 25 TTDSG).⁵¹

§ 25 Abs. 2 TTDSG erlaubt als Ausnahmen von der Einwilligungspflicht die Speicherung von und den Zugriff auf Tracker, die „unbedingt erforderlich“ sind, um „einen vom Nutzer ausdrücklich gewünschten Teledienst zur Verfügung [zu] stellen“. Das Kriterium der Erforderlichkeit ist ausschließlich technisch im Hinblick auf die Funktionalität der Webseite zu beurteilen. Eine wirtschaftliche Erforderlichkeit des Trackings für das Geschäftsmodell des Webseiten-Betreibers (etwa bei werbefinanzierten Online-Angeboten), führt nicht zur Ausnahme von der Einwilligungsbedürftigkeit.⁵²

Lehnt der Verbraucher ab, dem Unternehmer die Erlaubnis zu geben, Cookies zu setzen, will aber den Dienst nutzen,

44 S. Buchmüller/Roos, ZD 2022, 8.

45 Die Ausnahme regelt § 312 Abs. 1a S. 2, auf den § 327 verweist; s. a. sogleich zur Zweckbindung.

46 Kreuz, ZUM 2018, 162. S. zu Differenzierung bei unentgeltlicher Leistung in professionellem Rahmen Grigoleit, VersR 2018, 769; s. a. Bräutigam, MMR 2012, 635.

47 Grigoleit, VersR 2018, 769, 789.

48 S. a. Begr. RegE S. 36, wonach die die Ausnahmebestimmung in § 312 Abs. 1a S. 2 BGB nur eingreift, wenn der Unternehmer die erhobenen Daten nach deren Erhebung auch zu keinem anderen Zweck verwendet.

49 Loy/Baumgartner, ZD 2021, 404.

50 BT-Drs. 19/27653, S. 40.

51 Zur neuen Regelung s. Schumacher/Sydow/von Schönfeld, MMR 2021, 603. Zur Rechtslage vor § 25 TTDSG: BGH, 28. 5. 2020 – I ZR 7/16, K&R 2020, 611 ff. – Cookie-Einwilligung II; EuGH, 1. 10. 2019 – C-673/17, K&R 2019, 705 ff.

52 DSK, Orientierungshilfe (OH Telemedien), 20. 12. 2021, S. 22.

darf der Unternehmer nur die technisch notwendigen Cookies setzen. Dies entspricht speziell für das Speichern der technisch „unbedingt erforderlichen“ Tracker und den Zugriff darauf der Maßgabe gemäß § 312 Abs. 1a S. 2, sodass insoweit §§ 327 ff. keine Anwendung finden, auch wenn es sich bei den Trackern um personenbezogene Daten handelt (was § 25 TTDSG nicht notwendigerweise voraussetzt).⁵³ Die nachfolgende Analyse und Nutzung der mittels der Tracker gesammelten bzw. verknüpften Daten richtet sich nicht nach § 25 TTDSG,⁵⁴ sondern nach Art. 6, ggf. auch Art. 9 DSGVO.⁵⁵

Besondere Arten personenbezogener Daten sind eine weitere Schicht von Daten, die speziell berücksichtigt werden müssen. Solche Daten können z. B. dann anfallen, wenn der Internetnutzer soziale Netzwerke nutzt und dort Daten über seine Gesundheit, seine sexuelle Orientierung oder politische Gesinnung angibt, die vom Betreiber des Netzwerks z. B. für personalisierte Werbung ausgewertet werden.⁵⁶ Ob dafür eine Rechtsgrundlage in Betracht kommt, kann u. a. davon abhängen, ob die Daten offensichtlich öffentlich gemacht wurden (Art. 9 Abs. 2 lit. e DSGVO) und ob der EuGH zusätzlich zu Art. 9 DSGVO eine Rechtsgrundlage nach Art. 6 DSGVO fordert.⁵⁷

Bei sog. Pay Walls, die v. a. bei Medienverlagen verbreitet sind, kann der Internetnutzer nur auf digitale Inhalte zugreifen, wenn er die Auswahl trifft zwischen einem online-werbefreien Angebot ohne Tracking, für das er aber eine z. B. monatliche Abonnement-Gebühr (meist unter 10 EUR) bezahlen muss. Alternativ muss der Internetnutzer seine Einwilligung in Tracking zu Analyse- und Werbezwecke, Datenübermittlung an diverse Partnerunternehmen und Drittlandübermittlung abgeben.

Hinderlich für die Wirksamkeit der Einwilligung ist, dass bei diesen Angeboten häufig hinsichtlich der Tracker bzw. Verarbeitungen keine granulare und leicht zugängliche Auswahlmöglichkeit ersichtlich ist und dass nicht transparent ist, welche Verarbeitungen konkret auf eine Einwilligung gestützt werden und welche auf Art. 6 Abs. 1 lit. b oder lit. f DSGVO.

Eine Drittlandübermittlung gestützt auf Art. 49 Abs. 1 UA 1 lit. a DSGVO dürfte wegen der restriktiven Haltung der Datenschutzbehörden riskant sein.⁵⁸ Allerdings ist es wegen § 25 TTDSG auch nicht möglich, die gesamte Datenverarbeitung ausschließlich auf Art. 6 Abs. 1 lit. b DSGVO zu stützen. Hinsichtlich Art. 49 Abs. 1 UA 1 lit. b DSGVO wenden die Datenschutzbehörden denselben strengen Ausnahmecharakter an wie bei der Einwilligung in – bei Einsatz von z. B. Google-Werbeprodukten wohl unvermeidbaren – Drittlandübermittlung.⁵⁹ Der Pay Wall-Lösung kann man zugutehalten, dass sie einer „an § 312j II, IV BGB orientierte Button Lösung auch für das ‚Zahlen mit Daten‘“⁶⁰ sehr nahe kommt.

VII. Benachteiligung des Unternehmers, v. a. einzelne Bereitstellung

Im Ergebnis besteht eine Schieflage vor allem, wenn man nach Bereitstellungszeitraum unterscheidet. Nur für die Fälle der Reihe einzelner oder der dauerhaften Bereitstellung(en) bietet § 327q Abs. 2 die Lösung an, dass der Unternehmer bei Unzumutbarkeit weiteren Festhaltens nach dem Widerruf oder Widerspruch mit sofortiger Wirkung kündigt. Bei einzelner Bereitstellung hat der Unternehmer diese „Waffe“ nicht, vielmehr besteht der Vertrag

weiter; wenn die Bereitstellung bereits erfolgte, ist zwar erfüllt. Aber die Mängelhaftung und die Aktualisierungspflicht bleiben bestehen. Der Unternehmer ist insofern rechtlos. Indirekt kommt über die Vertragstypik und als maßgeblich dafür die Art/Dauer der Rechtseinräumung ins Spiel, s. a. VIII. 1.

Das Gebot der Datenminimierung (Art. 5, 24, 25 DSGVO) gilt unmittelbar für den Unternehmer (und evtl. auch für den Verbraucher, falls Daten Dritter bereitgestellt werden). Demgegenüber holt sich der Unternehmer mit der Einwilligung ein „Plus“ an Daten, das er auf rechtmäßige Weise ansonsten nicht erhalten würde, auch wenn im Übrigen die Einwilligung eventuell nicht erforderlich ist, jedenfalls was den Graubereich der Vertragsdaten und der Zulässigkeit nach Art. 6 Abs. 1 lit. f DSGVO betrifft.

Wichtig ist noch die besondere Betonung bzw. Ausprägung der Zweckbindung in § 312 Abs. 1a.

VIII. Perspektiven

1. Opportunitätsmodell Green-IT?

Im Ergebnis könnte die Berücksichtigung des vorstehenden Szenarios dazu führen, dass die Unternehmer eine Konstruktion bevorzugen, die das Problem der Aktualisierungspflicht weit über die Gewährleistungsfrist hinaus bei einzelner Bereitstellung günstig für sie löst: Als urheberrechtlich Berechtigter räumt der Unternehmer dem Erwerber einer Programmkopie das Recht zur Nutzung für die gesamte Zeit der Funktionsfähigkeit des Computerprogramms ein. Laut BGH liegt damit eine Veräußerung i. S. v. § 69c Nr. 3 S. 2 UrhG vor, die zur Erschöpfung des Verbreitungsrechts an der Programmkopie führen kann.⁶¹ Tatsächlich greift aber nach fester Laufzeit eine Sperre, die die Nutzbarkeit beendet: „Die Kl. räumt dem Erwerber somit das Recht zur Nutzung der Software für die gesamte Zeit der Funktionsfähigkeit des Computerprogramms ein [...]“⁶²

Es handelt es sich um die Taktung im Abonnement, die vom Unternehmer als Kauf eines wiederkehrenden Abonnements, das nach der erstmaligen Laufzeit automatisch verlängert wird, angeboten wird. Trotz der Qualifizierung als kaufähnlich – durch die Rechtseinräumung für die Zeit der Funktionsfähigkeit – erfolgt also eine einem Abonnement entsprechende Gestaltung, die den Unternehmer in die Position „Reihe einzelner Bereitstellungen“ und damit des § 327 Abs. 2 bringt, bei Unzumutbarkeit des Festhaltens kündigen zu können. Unklar ist,⁶³ ob dies auch für die Aktualisierung gilt, die aber jedenfalls zum Ende der Abo-Laufzeit als Bereitstellungszeitraum gekündigt werden kann, wenn sie nicht ohnehin endet. *Spindler*⁶⁴ hat zu

53 S. Hanloser, ZD 2021, 399, 400 f.

54 DSK, OH Telemedien, 20. 12. 2021, S. 5.

55 Oben III. Nr. 5 bis 10.

56 OGH Österreich, 23. 6. 2021 – 6 Ob 56/21k – Schrems III, Vorlage an den EuGH, C-446/21.

57 BAG, 26. 8. 2021 – 8 AZR 253/20 – Vorlage an den EuGH, C-667/21; DSK, Kurzpapier Nr. 17, 27. 3. 2018.

58 DSK, Orientierungshilfe Telemedien, 20. 12. 2021, S. 32.

59 EDSA Recommendations 1/2020, 18. 6. 2021, Rn. 25; Leitlinien 2/2018.

60 Schmidt-Kessel, Stellungnahme zu den Gesetzgebungsentwürfen, S. 15 f. <https://www.bundestag.de/resource/blob/854468/0047e158059c8d64016946a653d0458e/stellungnahme-schmidt-kessel-data.pdf>, zuletzt abgerufen am 17. 3. 2022.

61 BGH, 19. 3. 2015 – I ZR 4/14, K&R 2015, 727, LS 2 – Green-IT.

62 BGH, 19. 3. 2015 – I ZR 4/14, K&R 2015, 727 ff., Rn. 37.

63 Zur unklaren dogmatischen Einordnung der Aktualisierung s. Felsch/Kremer/Wagener, MMR 2022, 18.

64 Spindler, MMR 2021, 528, 530 f.

Recht darauf hingewiesen, dass in § 327q ungerichtet ist, „welche Gewährleistungsrechte ab Einwilligungswiderruf und bis zu einer etwaigen Kündigung des Unternehmers bestehen.“

2. Nachlauffrist als rechtspolitische Überlegung

Wenn schon die Gegenleistung des Verbrauchers nicht in Geld bestehen muss, kann sich die Entgeltlichkeit auch darin ausdrücken, dass die Einwilligung als diese Gegenleistung⁶⁵ gesehen wird. Sie steht aber bei der DID-RL nicht im Synallagma, erst recht nicht bei der Umsetzung gem. BGB. Weder sollen die Datenverarbeitung und ihre Zulässigkeit noch die Frage, ob der Verbraucher seine Daten überhaupt bereitstellt, Voraussetzung für den Bestand des Vertrags sein. Der Unternehmer hat allenfalls die Handhabe des § 327 Abs. 2 bei Widerruf bzw. Widerspruch.

Fair wäre es, wenn der Unternehmer mit den Daten noch innerhalb einer angemessenen Nachfrist nach Widerruf/Widerspruch arbeiten dürfte, verbunden mit der Erlaubnis, eine Verarbeitung zu einer Datenbasis als einer Art Verdichtung der Daten vorzunehmen, die längerfristig Bestand haben soll (zum Beispiel für KI-Entwicklungen mit Tests, Lernfähigkeiten und Ähnlichem). Dann würde bei einzelner Bereitstellung mit dem Ende des Erwartungszeitraums bzw. Ende des Bereitstellungszeitraums bei dauerhafter Bereitstellung das Recht zur Nutzung der Daten primär enden, aber für die verdichteten Daten weiterhin Zulässigkeit bestehen. Theoretisch wäre auch denkbar, diese „Verwertung“ an eine monetäre Vergütung zu knüpfen, die der Unternehmer dem Verbraucher zahlt. Diese Monetarisierung⁶⁶ ist perspektivisch⁶⁷ vorbereitet.

3. Fazit für das Marktmodell „Bezahlen mit Daten“

Das Konzept „Bezahlen mit Daten“ erfordert einen funktionierenden Markt, in dem der Verbraucher wissentlich und willentlich und v. a. ausreichend aufgeklärt personenbezogene Daten zur Verfügung stellt bzw. sammeln lässt. Informationsasymmetrien sind ein wesentliches Hemmnis.⁶⁸ „Bezahlen mit Daten“ setzt digitale Kompetenz der Verbraucher und transparente⁶⁹ Informationen in der Klickstrecke von Webseiten (statt überbordender oder zu pauschaler Datenschutzerklärungen) voraus. Es muss zudem eine ausreichende Wahlmöglichkeit zwischen Varianten eines digitalen Produktes mit (1) minimaler Datenverarbeitung (Art. 5 Abs. 1 lit. c, Art. 25 DSGVO) oder (2) auf z. B. einzelne Marketingzwecke ausgeweiteter oder (3) umfassend profilbildender Datenverarbeitung bestehen. Nicht nur Verbraucher,⁷⁰ auch Unternehmer und sogar öffentliche Stellen fühlen sich von den großen etablierten, meist unweigerlich mit Drittlandübermittlung einhergehenden Cloud- und Werbeplattformen⁷¹ abhängig. Die Alternativlosigkeit gegenüber den zentralen Plattformen (auch im Bereich der Cloud-Infrastrukturen und SaaS) scheint so groß, dass selbst Gerichtsurteile,⁷² konsequentere Durchsetzung der EU-Datenschutzbehörden⁷³ und das Drohpotential sehr erfolgreicher Datenschutzaktivisten⁷⁴ nur langsam einen Umschwung einleiten können. Die bewusste Ökonomisierungsmöglichkeit für den Verbraucher ist als Idee zu begrüßen, erfordert aber im Gegenzug Rechtssicherheit für den Unternehmer.

Aktuell krankt das Geschäftsmodell aus Unternehmenssicht an unklaren datenschutzrechtlichen Rechtsgrundla-

gen. Obwohl die Datenverkehrsfreiheit ein Ziel der DSGVO ist (Art. 1 Abs. 1), ist sie weitgehend abwehrrechtlich konzipiert und berücksichtigt nicht ausreichend das informationelle Drittverhältnis zwischen Privaten.⁷⁵ Schon vor der DID-RL war und ist das Problem z. B. bei Werbe- und Sponsoring-Verträgen B2B und B2C virulent und zeigt sich an dem nach wie vor unklaren Verhältnis von DSGVO und KUG hinsichtlich Werbe-Fotos: Besteht die Einwilligungsbedürftigkeit nach KUG und/oder DSGVO mit oder ohne jederzeitiger Widerruflichkeit? Auch das Medienprivileg nach Art. 85 DSGVO hilft im werblichen, nicht-redaktionellen Bereich nicht weiter. Wenn sich der Unternehmer zu einer Leistung (sei es ein digitales Produkt oder Geldzahlung) verpflichtet, damit der Verbraucher – auf informierter und freiwilliger Basis – personenbezogene Daten bereitstellt, scheint Vertragserfüllung als Rechtsgrundlage (Art. 6 Abs. 1 lit. b DSGVO) besser zu passen als die freie Widerruflichkeit der Einwilligung. Leider fehlt es an Rechtssicherheit (s. III. – VII.). Die Beseitigung der Rechtsunsicherheit wäre eine weitere wichtige Voraussetzung für das Funktionieren des Marktmodells. Das aktuelle Fazit lautet, dass dem Unternehmer das Geschäft mit unentgeltlichen digitalen Produkten gegen Datenhergabe nur sicher Pflichten, aber keine Rechte, insbes. keine vermögenswerten Rechte bringt.

65 S. Spindler, MMR 2021, 451, 452 (m. w. N. in Fn. 33); ders., MMR 2021, 528.

66 S. z. B. allg. zum Geschäftsmodell Koehler, in: Leupold/Wiebe/Glossner, Münchener Anwaltshandbuch IT-Recht, 4. Aufl. 2021, 6.2; speziell im digitalem Privatrecht Kroschwald/Polenz, in: Brönneke/Föhlich/Tonner, Das neue Schuldrecht, 2022, § 6, Rn. 11 ff.

67 S. z. B. Kilian, Strukturwandel der Privatheit, in: Garstka/Coy (Hrsg.), Wovon – für wen – wozu? Systemdenken wider die Diktatur der Daten, Wilhelm Steinmüller zum Gedächtnis, 2014, S. 195–224, sowie Nachweise in Fn. 59.

68 Metzger, in: Lohsse/Schulze/Staudenmayer (Fn. 19), S. 42 ff.

69 Trotz der hohen Anforderungen der DSGVO an die Transparenz (etwa Art. 5 Abs. 2, 7, 13, 14 DSGVO).

70 BGH, 23. 6. 2020 – KVR 69/19, K&R 2020, 683 ff.

71 Suchmaschinen-Marketing, Behavioral Targeting, Remarketing.

72 OVG Schleswig-Holstein, 25. 11. 2021 – 4 LB 20/13, K&R 2022, 294 ff.; LG München, 20. 1. 2022 – 3 O 17493/20.

73 Zu Google Analytics: Entscheidung der Österreichischen Datenschutzbehörde v. 22. 12. 2021 – GZ: D155027 2021-0.586.257; Pressemitteilung der CNIL v. 10. 2. 2022; Meldung der niederländischen Datenschutzbehörde vom 13. 1. 2022. Nicht zu Schrems II, sondern zur gemeinsamen Verantwortlichkeit beim Consent Banner (TCF 2.0 von IAB): Entscheidung der belgischen Datenschutzbehörde v. 2. 2. 2022 – DOS-2019-01377.

74 Z. B. 101 Beschwerden eingereicht von NOYB.

75 Sattler, NJW 2020, 3623, 3627. Gallwas, in: Conrad/Grützmacher, Recht der Daten und Datenbanken im Unternehmen, 2014, S. 347.



Jochen Schneider

ist selbständiger Rechtsanwalt seit 1984 in München. Er ist Seniorpartner bei CSW, München, und Honorarprofessor an der Universität München. Beratungsschwerpunkte sind IT-Vertrags-Recht und Datenschutz. Er ist Hrsg. des „Handbuch des EDV-Rechts“ und Mitautor, Herausgeber des „ITRB“, Mitherausgeber der „ZD“ und Mitglied der Schriftleitung der „CR“.



Isabell Conrad

ist seit 2005 Rechtsanwältin in München und Gründungspartnerin von CSW. Sie ist seit 2013 für den DAV Mitglied der EU Expert Group on Cloud Computing Contracts, Wissenschaftsbeirätin der „ZD“ und Mitherausgeberin von Auer-Reinsdorff/Conrad (Hrsg.), Handbuch des IT- und Datenschutzrechts.