ANDREAS SATTLER

Informationelle Privatautonomie

Jus Privatum
264

Mohr Siebeck

JUS PRIVATUM

Beiträge zum Privatrecht

Band 264

Andreas Sattler

Informationelle Privatautonomie

Synchronisierung von Datenschutz- und Vertragsrecht

Mohr Siebeck

Andreas Sattler, geboren 1982; Studium der Rechts- und Wirtschaftswissenschaften in Bayreuth und Nottingham (LL.M.); Promotionsstipendium der DFG und Mitgliedschaft im DFG-Graduiertenkolleg „Geistiges Eigentum und Gemeinfreiheit", Universität Bayreuth; Dissertation (Emanzipation und Expansion des Markenrechts, Mohr Siebeck, 2015); Rechtsanwalt im Bereich IT-Recht bei CMS Hasche Sigle, Stuttgart; Akademischer Rat a.Z. am Lehrstuhl für Bürgerliches Recht, Recht des Geistigen Eigentums und Wettbewerbsrecht an der Ludwig-Maximilians-Universität München; Habilitation; Lehrbefähigung für die Fächer Bürgerliches Recht, Immaterialgüterrecht, deutsches und europäisches Wirtschaftsrecht und Datenrecht; Gründung und Co-Leitung des Center for Intellectual Property Law, Information and Technology (CIPLITEC); seit April 2022: Vertretung des Lehrstuhls für Zivil- und Wirtschaftsrecht, Medien- und Informationsrecht an der Albert-Ludwigs-Universität Freiburg.

Gedruckt und als Open Access Dokument zugänglich gemacht mit der freundlichen Unterstützung des *LMU Open Access Fonds*, des *LMU Post Doc Fonds*, der *Johanna und Fritz Buch Gedächtnisstiftung e.V.* und der Studienstiftung *ius vivum e.V.*

ISBN 978-3-16-161905-2 / eISBN 978-3-16-161906-9
DOI 10.1628/978-3-16-161906-9

ISSN 0940-9610 / eISSN 2568-8472 (Jus Privatum)

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliographie; detaillierte bibliographische Daten sind über *http://dnb.dnb.de* abrufbar.

Das Buch wurde von Gulde Druck aus der Garamond gesetzt, in Tübingen auf alterungsbeständiges Werkdruckpapier gedruckt und von der Buchbinderei Spinner in Ottersweier gebunden.

Printed in Germany.

Vorwort

Daten werden seit einigen Jahren als „neues Gold“ oder „Öl des 21. Jahrhunderts“ bezeichnet. Diese Vergleiche hinken. Im Gegensatz zu Gold und Öl sind Daten immaterielle Güter. Infolgedessen ist ihre Nutzung weder ausschließlich noch rival. Ohne rechtliche Zuweisung beruht die Möglichkeit zur Datennutzung lediglich auf einem faktischen Zugang, allgemein zugängliche Daten kann jedermann nutzen (keine Ausschließbarkeit). Die Nutzung durch eine Person hindert nicht die zeitgleiche Nutzung dieser Daten durch weitere Personen (keine Rivalität). Kurzum: Aufgrund ihrer immateriellen Eigenschaften können Daten eine sehr vielseitig nutzbare Ressource sein.

Dies erklärt, warum Daten zunehmend in den Fokus der Gesetzgeber im europäischen Mehrebenensystem geraten und warum die Gesetzgeber nach Wegen suchen, um die Nutzung von Daten zu fördern; stets in der Erwartung, dass dadurch die wirtschaftliche Effizienz, die technische Innovation und damit letztlich der volkwirtschaftliche Wohlstand gesteigert werden. Die Vorschläge für Ansprüche auf Datenzugang und Datenüberlassung (Data Act), aber auch das Konzept einer Datentreuhand (Data Governance Act) sind aktuelle Beispiele dafür, dass der unionale Gesetzgeber nach Mechanismen sucht, um den „Datenschatz“ zu heben. Dabei bezieht der Gesetzgeber zunehmend auch personenbezogene Daten ein. Er folgt damit der wirtschaftlichen Realität. Zahlreiche Dienstleistungen der Betreiber von mehrseitigen Plattformen, insbesondere von Suchmaschinen oder Kommunikationsnetzwerken, werden derzeit maßgeblich durch personalisierte Werbung finanziert. Diese basiert auf dem Einsatz von Tracking-Technologien und der Erstellung von Interessenprofilen anhand des Online-Verhaltens der Nutzer/innen. Weil diese omnipräsenten Geschäftsmodelle bei der Verabschiedung der DS-GVO jedoch weitgehend ausgeblendet wurden und zudem auch nicht berücksichtigt wurde, dass zahlreiche prominente Persönlichkeiten die vermögenswerten Bestandteile ihrer Persönlichkeitsrechte kommerziell verwerten, befindet sich die DS-GVO auf einem Kollisionskurs mit dem Schuldrecht und der ökonomischen Realität. Der Konflikt zwischen der staatlichen Pflicht zum Schutz der informationellen Selbstbestimmung einerseits und der gleichzeitigen Achtung der Privatautonomie der Datensubjekte und der datenverarbeitenden Unternehmen andererseits ist mittlerweile offenkundig. Dennoch besteht derzeit kein überzeugender rechtlicher Rahmen, der die grundrechtliche Pflicht zum Schutz der Datensubjekte und die

wirtschaftliche Realität zum Ausgleich bringt. Diese schwierige Aufgabe wird stattdessen an die Rechtsanwender und damit insbesondere an den EuGH überantwortet.

Die vorliegende Arbeit macht einen Vorschlag, wie dieses Spannungsverhältnis aus dem Schutz von Datensubjekten und der Anerkennung von personenbezogenen Daten als Objekt vertraglicher Austauschbeziehungen aufgelöst werden kann. Dabei bewahrt der Vorschlag den tradierten Rahmen des Rechts auf informationelle Selbstbestimmung, erweitert aber den Handlungsspielraum für Datensubjekte und solche datenverarbeitende Unternehmen, die keine dominanten Gatekeeper sind. Infolgedessen ermöglicht das nachfolgend vorgeschlagene Modell einer abgestützten informationellen Privatautonomie die Synchronisierung von Datenschutz- und Vertragsrecht.

Die Arbeit lag der Juristischen Fakultät der Ludwig-Maximilians-Universität München im Wintersemester 2021/22 als Habilitationsschrift vor. Sie hat entscheidend von einer Reihe von Personen profitiert. Mein Dank gilt in erster Hinsicht meinem akademischen Lehrer, Herrn Professor Ansgar Ohly, der sich früh für dieses Thema begeistern konnte und mir für diese Untersuchung ideale Bedingungen und größtmögliche Freiheiten am Lehrstuhl gewährt hat. Herrn Professor Hans Christoph Grigoleit danke ich herzlich für die sehr zügige Erstellung des Zweitgutachtens und wertvolle inhaltliche Hinweise und Anregungen. Herrn Professor Herbert Zech und Herrn Professor Matthias Leistner danke ich für zahlreiche anregende Gespräche und Diskussionen zum Thema. Herrn Professor Franz Hofmann und Herrn Professor Martin Stierle danke ich für die gute und freundschaftliche Zusammenarbeit an der LMU. Der Druck und die Zugänglichmachung als Open-Access-Publikation wurden großzügig durch den LMU Open Access Fonds, den LMU PostDoc Fonds, die Johanna und Fritz Buch Gedächtnis-Stiftung und die Studienstiftung ius vivum gefördert.

Besonders herzlich danke ich meiner Familie. Meine Frau und mein Sohn mussten mit mir durch die düsteren Täler schreiten, die eine Habilitationsschrift regelmäßig mit sich bringt. Ihnen ist diese Arbeit gewidmet.

Stuttgart, im Mai 2022 Andreas Sattler

Inhaltsübersicht

Inhaltsverzeichnis

Einführung

I. Gegenstand und Zielsetzung

Der rechtliche Schutz vor einer Verarbeitung von personenbezogenen Daten (verkürzt: Datenschutzrecht) ist ein sehr konfliktreiches Rechtsgebiet. Untersucht man das Datenschutzrecht aus privatrechtlicher Perspektive, so sind zwei große Konflikte besonders augenfällig.

Erstens befinden sich das Datenschutzrecht und die besonders erfolgreichen Geschäftsmodelle mehrseitiger Plattformen auf einem Kollisionskurs. Die amerikanischen Unternehmen *Google* (*Alphabet*), *Amazon*, *Facebook* (*Meta Platforms*), *Apple* und *Microsoft* (zusammengefasst: GAFAM) und ihre chinesischen Wettbewerber *Baidu*, *Alibaba* und *Tencent* (zusammengefasst: BAT) stehen stellvertretend für Geschäftsmodelle, die in einem großen Ausmaß auf der Verarbeitung von personenbezogenen Daten ihrer Endnutzer (und Dritter) für ein Profiling beruhen. Dieses Profiling, das durch den Einsatz von Techniken der sog. Künstlichen Intelligenz stetig verbessert wird, liefert die Grundlage dafür, Werbekunden gegen Geld eine personalisierte oder zumindest stratifizierte Werbung gegenüber den Endnutzern anbieten zu können.

Die Kollision zwischen dem Datenschutzrecht und den Geschäftsmodellen mehrseitiger Plattformen ist nicht neu. Solange Plattformbetreiber bei Verstößen gegen das Datenschutzrecht jedoch kaum ökonomische Konsequenzen zu befürchten hatten, genügte es aus ihrer Sicht, den Schutz personenbezogener Daten am Horizont zu beobachten. Das Datenschutzrecht zwang die großen Plattformbetreiber zu keinen oder allenfalls sehr geringen Anpassungen ihrer Geschäftsmodelle.

Am 25.05.2018 hat sich dieses Bild verändert. Obwohl das Potenzial für *tatbestandliche* Konflikte seit der Anwendbarkeit der DS-GVO[1] kaum zugenommen hat – die DS-GVO behält wesentliche Regelungsinhalte der Datenschutz-RL von 1995[2] bei – ist für die datenschutzrechtlich Verantwortlichen das Risiko, also die Kombination aus der Entdeckungswahrscheinlichkeit von Rechtsver-

[1] Verordnung (EU) 2016/679 v. 27.04.2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG, ABl. L 119, v. 04.05.2016, S. 1 ff.

[2] Richtlinie 95/46/EG v. 24.10.1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, ABl. L 281, v. 23.11.1995, S. 31 ff.

stößen und der Höhe des potenziellen Bußgelds, mit der DS-GVO grundlegend gestiegen. Indem das potenzielle Bußgeld proportional mit dem ökonomischen Erfolg des Verantwortlichen steigt, bewahrt das Datenschutzrecht seine Relevanz auch mit zunehmender Größe des datenschutzrechtlich Verantwortlichen.

Unabhängig davon, ob die Auslegung und Anwendung der DS-GVO in der Praxis ein ausreichendes Mindestmaß an Rechtssicherheit bietet,[3] ob die Kriterien und Details für die Bestimmung eines angemessenen und abschreckenden Bußgelds im Einzelfall überzeugen und ob es sinnvoll und ökonomisch tragfähig ist, den gleichen Regelungsansatz auf andere Rechtsverstöße auszudehnen.[4] Es bestehen keine Zweifel: Die potenzielle Höhe eines Bußgelds gemäß Art. 83 DS-GVO hat die alte Erkenntnis bestätigt, dass die Steuerungsfunktion des Rechts maßgeblich von effektiven Mechanismen zu dessen Durchsetzung abhängt.[5] Um Kollisionen mit der DS-GVO und potentiell hohe Bußgeldbescheide zu vermeiden,[6] sind die Plattformbetreiber zunehmend gezwungen, ihre Geschäftsmodelle, jedenfalls aber die rechtliche Beziehung zu ihren Endnutzern anzupassen.

---

[3] Erst im Jahr 2021 erreichten den EuGH erste Auslegungsfragen von fundamentaler Bedeutung: *OLG Düsseldorf*, Vorlagebeschl. v. 24.03.2021, Kart 2/19 (V) = NZKart 2021, 306 ff.; *ÖOGH*, Vorlagebeschl. v. 22.07.2021, 6 Ob 56/21k – *Schrems* [*III*].

[4] Vgl. Art. 26 (Geldbußen) des Vorschlags der EU-Kommission für eine Verordnung über bestreitbare und faire Märkte im digitalen Sektor (Gesetz über digitale Märkte) vom 15.12.2020, COM(2020) 842 final (englisch: Digital Markets Act oder kurz: DMA-Vorschlag); sowie Art. 42 (Sanktionen) des Vorschlags der EU-Kommission für eine Verordnung über einen Binnenmarkt für digitale Dienste (Gesetz über digitale Dienste) und zur Änderung der Richtlinie 2000/31/EG vom 15.12.2020, COM(2020) 825 final (englisch: Digital Service Act oder kurz: DSA-Vorschlag).

[5] Die Frage, wer neben den Datensubjekten und im Auftrag der betroffenen Datensubjekte (Art. 80 Abs. 1 DS-GVO) zusätzlich gemäß Art. 80 Abs. 2 und Art. 84 Abs. 1 DS-GVO zur Durchsetzung von Ansprüchen aus UWG und UKlaG aktivlegitimiert sein sollte, hat der BGH dem EuGH vorgelegt: *BGH*, Beschl. v. 28.05.2020, I ZR 186/17 = GRUR 2020, 896 (Rn. 35 ff.) – *App-Zentrum*; Für eine Begrenzung auf qualifizierte Verbände: *Köhler*, WRP 2018, 1269 (1272); *ders.*, WRP 2019, 1279 (1283); *Ohly*, GRUR 2019, 686 (688 f.); für eine durch die DS-GVO unbeeinflusste Aktivlegitimation von Mitbewerber nach dem UWG: *Uebele*, GRUR 2019, 694 (697 f.).

[6] Die luxemburgische Datenschutzbehörde (CNPD) verhängte gegen die europäische Tochter von *Amazon* mit Sitz in Luxemburg ein (nicht rechtskräftiges) Bußgeld in Höhe von 746 Mio. Euro (https://www.heise.de/news/Datenschutz-Rekordstrafe-von-746-Millionen-Euro-fuer-Amazon-in-Luxemburg-6152051.html, zuletzt abgerufen am 19.05.2022). Die französische Datenschutzbehörde (CNIL) verhängte 2019 – jeweils nur für Frankreich – eine Strafe von 50 Mio. Euro gegen *Google* (https://www.heise.de/news/DSGVO-Verstoesse-Conseil-d-Etat-bestaetigt-50-Millionen-Strafe-gegen-Google-4790235.html, zuletzt abgerufen am 19.05.2022) sowie im Dezember 2020 in Höhe von 100 Mio. Euro gegen *Google* und 35 Mio. Euro gegen *Amazon* (https://www.heise.de/news/Frankreich-Datenschuetzer-verhaengen-Millionen-Bussgelder-gegen-Google-und-Amazon-4985956.html, zuletzt abgerufen am 19.05.2022). Der Hamburgische Datenschutzbeauftragte hat wegen Verstößen gegen die DS-GVO im Beschäftigungsverhältnis für Deutschland ein Bußgeld von knapp 35,3 Mio. Euro gegen *Hennes & Mauritz* (H&M) verhängt (https://www.heise.de/news/DSGVO-Deutsche-Rekordbusse-von-35-3-Millionen-Euro-gegen-H-M-4917437.html, zuletzt abgerufen am 19.05.2022).

Besonders deutlich wird dies an dem Sachverhalt, der einem Vorlagebeschluss des *ÖOGH* zum *EuGH* zugrunde liegt.[7] Darin geht es maßgeblich darum, ob *Facebook* (jetzt: *Meta Platforms*) die personenbezogenen Daten der Endnutzer – soweit es sich dabei nicht um besonders sensible personenbezogene Daten handelt – vertragsakzessorisch und somit auf Grundlage des Nutzungsvertrags i. V. m. Art. 6 Abs. 1 lit. b DS-GVO rechtmäßig verarbeiten kann, oder ob insoweit spezifische Einwilligungen der Endnutzer erforderlich sind. Dem Vorlagebeschluss des *ÖOGH* ging ein Urteil des *OLG Wien* voraus, in dem dieses das Profiling für personalisierte Werbung durch *Facebook* auf Grundlage eines in der österreichischen Rechtsordnung nicht ausdrücklich geregelten, also atypischen Schuldverhältnisses für rechtmäßig erachtet hatte. Nach Ansicht des *OLG Wien* ist diese Datenverarbeitung (auch) zur Finanzierung des Angebots von *Facebook* und damit zur Erfüllung dieses atypischen Nutzungsvertrags i. S. d. Art. 6 Abs. 1 lit. b DS-GVO erforderlich.[8]

Die Antwort des *EuGH* auf die nun erfolgte Vorlage des *ÖOGH* wird grundlegende Auswirkungen auf die Geschäftsmodelle der Betreiber von solchen mehrseitigen Plattformen haben, die Datensubjekten digitale Produkte bereitstellen und dieses Angebot finanzieren, indem sie mit Hilfe von personenbezogenen Daten Profile über ihre Endnutzer erstellen und diese im Verhältnis zu ihren Werbekunden für personalisierte Werbeansprache monetisieren. Abhängig davon, welche datenschutzrechtliche Grundlage der *EuGH* für solche Austauschverhältnisse zwischen Datensubjekten und Verantwortlichen heranzieht, kommt es für die Rechtmäßigkeit dieser Geschäftsmodelle auf die unionsrechtlich vereinheitlichten Anforderung an die datenschutzrechtliche Einwilligung oder auf das lediglich teilweise harmonisierte nationale Vertragsrecht der Mitgliedstaaten an.[9]

Zweitens wird anhand des Vorlagebeschlusses des *ÖOGH* auch deutlich, dass sich das europäische Datenschutzrecht und das nationale Schuldrecht der Mitgliedstaaten auf einem Kollisionskurs befinden. Die europäische DS-GVO ist weder mit dem nationalen Schuldrecht noch den privatrechtlichen Grundprinzipien synchronisiert.

Sprachlich lässt sich diese Dominanz der DS-GVO daran festmachen, dass die schuldrechtlich zutreffende Bezeichnung von personenbezogenen Daten als „Gegenleistung" einem postmodernen Sakrileg gleichgestellt wird.[10] In voraus-

---

[7] *ÖOGH*, Vorlagebeschl. v. 22.07.2021, 6 Ob 56/21k – *Schrems* [*III*].

[8] *OLG Wien*, Urt. v. 07.12.2020 (nicht rechtskräftig), GZ 11 R 153/20f, 11 R 154/20b-99 S. 27. Diese Ansicht ist nicht überzeugend, hierzu unten: Kapitel 3 C.II.4./5 und III.3.

[9] Obwohl es wenig überrascht, dass *Meta Platforms* (ehemals: *Facebook*) häufig beklagte Partei ist, birgt dieses Vorlageverfahren die Gefahr, dass der EuGH sich die Folgen seiner Entscheidung für andere, kleinere Verantwortliche zu wenig bewusst macht.

[10] *EDSB*, Stellungnahme 4/2017 zu dem Vorschlag für eine Richtlinie über bestimmte vertragsrechtliche Aspekte der Bereitstellung digitaler Inhalte, 14.03.2017, S. 10/Nr. 17; sowie: Rede von *Giovanni Buttarelli* (ehemaliger EU-Datenschutz-Beauftragter), verfügbar unter

eilender *political correctness* meidet der europäische Gesetzgeber deshalb mittlerweile[11] diesen Begriff, ohne dadurch den tatsächlich bestehenden Konflikt zwischen Datenschutz- und Schuldrecht zu lösen.[12] Zwar soll mit dem europäischen Data Act auch die Nutzung von personenbezogenen Daten verbessert werden; wie dieses Ziel sich jedoch mit den Anforderungen der DS-GVO synchronisieren lässt, bleibt einstweilen offen.[13]

Rechtlich bringen Art. 3 Abs. 8 der Richtlinie (EU) 2019/770 über bestimmte vertragsrechtliche Aspekte der Bereitstellung digitaler Inhalte und digitaler Dienstleistungen (DID-RL)[14] und § 327q BGB[15] diese Dominanz der DS-GVO zum Ausdruck. Zwar versucht der deutsche Gesetzgeber das nationale Schuldrecht gegenüber der DS-GVO zu immunisieren. Gemäß § 327q Abs. 1 BGB soll die Abgabe einer datenschutzrechtlichen Erklärung des Verbrauchers nach Vertragsschluss die Wirksamkeit des Vertrags unberührt lassen. Weil jedoch per-

---

https://edps.europa.eu/sites/edp/files/publication/17-01-12_digital_content_directive_sd_en.pdf, zuletzt abgerufen am 19.05.2022 („So, even if some people treat personal data as commodity, under EU law it cannot be a commodity. There might well be market for personal data, just like there is, tragically, a market for live human organs.")

[11] Anders noch *EU-Kommission* Vorschlag für eine Richtlinie über bestimmte vertragsrechtliche Aspekte der Bereitstellung digitaler Inhalte, COM/2015/0634 final. (Art. 3 Abs. 1 des Vorschlags erstreckte den Anwendungsbereich auf „alle Verträge, auf deren Grundlage ein Anbieter einem Verbraucher digitale Inhalte bereitstellt oder sich hierzu verpflichtet und der Verbraucher *als Gegenleistung* einen Preis zahlt oder aktiv eine andere Gegenleistung als Geld in Form *personenbezogener* oder anderer *Daten erbringt*".

[12] Ohne Bezugnahme auf die zu diesem Zeitpunkt bereits verabschiedete, aber noch nicht umsetzungspflichtige Richtlinie (EU) 2019/770 über bestimmte vertragsrechtliche Aspekte der Bereitstellung digitaler Inhalte und digitaler Dienstleistungen (DID-RL) kam das *OLG Wien* zu einer anderen Beurteilung. Danach sei es insbesondere „legitim, dass ein marktwirtschaftlich operierendes Unternehmen, das für bestimmte Dienstleistungen kein Geld verrechnet, im Rahmen der Gesetze auf anders geartete Finanzierungsquellen zurückgreift. […]. Denn nur diese Datenverwertung ermöglicht maßgeschneiderte Werbung, die das von der Beklagten geschuldete „personalisierte Erlebnis" in wesentlichem Maße prägt und der Beklagten zugleich die für den Aufrechterhaltung der Plattform und die Erzielung eines Gewinns notwendigen Einkünfte verschafft." *OLG Wien*, Urt. v. 07.12.2020 (nicht rechtskräftig), GZ 11 R 153/20f, 11 R 154/20b-99 S. 28. Zur fehlenden Synchronisierung zwischen DS-GVO und DID-RL, unten Kapitel 3 C.III.2.

[13] *Europäische Kommission*, Inception of Assessment, Ref. Ares(2021)3527151 v. 28.05. 2021, S. 7 (Likely impacts on fundamental rights): „Since personal data […] fall into the scope of some elements of this initiative (e. g. improving usability of data linked to natural persons), the measure will be designed in a way that fully complies with the existing rules on personal data protection and ePrivacy".

[14] ABl. v. 22.05.2019, L 136/1. Art. 3 Abs. 8 DID-RL lautet: „Das Unionsrecht betreffend den Schutz personenbezogener Daten gilt für alle personenbezogenen Daten, die im Zusammenhang mit Verträgen gemäß Absatz 1 verarbeitet werden. Insbesondere lässt diese Richtlinie die Verordnung (EU) 2016/679 und die Richtlinie 2002/58/EG unberührt. Im Fall von Widersprüchen zwischen Bestimmungen dieser Richtlinie und dem Unionsrecht zum Schutz personenbezogener Daten ist letzteres maßgeblich."

[15] Eingeführt durch das Gesetz zur Umsetzung der Richtlinie über bestimmte vertragsrechtliche Aspekte der Bereitstellung digitaler Inhalte und digitaler Dienstleistungen v. 25.06. 2021, BGBl. 2021 Teil I Nr. 37, 30.06.2021, 2123 ff.

sonenbezogene Daten tatsächlich und rechtlich zunehmend als Leistungsgegenstand behandelt und vereinbart werden und einige der derzeit ökonomisch besonders erfolgreichen Geschäftsmodelle von *GAFAM* und *BAT* – in unterschiedlichem Ausmaß – auf dem Zugang zu personenbezogenen Daten beruhen, entspricht dieser schlichte Abgrenzungsversuch in § 327q Abs. 1 BGB eher einem Wunschdenken, als dem Anspruch, die tatsächliche Realität rechtlich abzubilden.[16]

Indem § 327q Abs. 3 BGB alle Ersatzansprüche des *Unternehmers* gegen den *Verbraucher* wegen Abgabe einer datenschutzrechtlichen Erklärung ausschließt, die eine Einschränkung der rechtmäßigen Datenverarbeitung bewirkt, hat der deutsche Gesetzgeber zwar zu einem kräftigen Befreiungsschlag ausgeholt, um den gordischen Knoten aus europäischem Datenschutz- und nationalem Schuldrecht zumindest im B2C-Verhältnis zu lösen. Auf den zweiten Blick erinnert dieser Befreiungsversuch des Gesetzgebers jedoch an den verzweifelten Versuch des *Laokoon*, sich aus dem Griff der Schlangen zu befreien. § 327q BGB ist nicht in der Lage, den tatsächlich bestehenden Konflikt zwischen einer jederzeit und grundlos widerruflichen Einwilligung und dem schuldrechtlichen Prinzip des *do ut des* befriedigend aufzulösen.[17] Eine solche Lösung ist aber jedenfalls in Fällen erforderlich, in denen Datensubjekte ihre personenbezogenen Daten bewusst dafür einsetzen, um ihr monetäres Konsumbudget zu schonen (Verbraucher) oder um selbst Gewinne zu erwirtschaften (Unternehmer).

Die Ursache dafür, dass das Datenschutzrecht und das Schuldrecht sich auf Kollisionskurs befinden, ist leicht zu identifizieren. Beginnend mit dem ersten BDSG von 1977[18] beruht das deutsche und im Anschluss hieran das europäische Datenschutzrecht auf einem Verarbeitungsverbot mit Erlaubnisvorbehalt (§ 3 Abs. 1 BDSG von 1977 – jetzt: Art. 6 Abs. 1 und Art. 9 Abs. 1 DS-GVO). Das Schuldrecht hingegen beruht auf einer Erlaubnis mit Verbotsvorbehalt (§§ 311, 241 BGB).[19]

---

[16] Insbesondere dürfte damit auch noch nicht „jedweder Diskussion um eine mögliche Einschränkung des Widerrufsrechts […] ein Riegel vorgeschoben" worden sein. So aber: *Spindler*, MMR 2021, 528 (530). Hierzu unten Kapitel 5 C.III.

[17] Zum hier unterbreiteten Vorschlag eines befristeten Ausschlusses der Widerruflichkeit durch teleologische Reduktion von Art. 7 Abs. 3 S. 1 DS-GVO unten Kapitel 5 C.III, sowie zuvor: *Sattler*, JZ 2017, 1036 (1041 f.). Sollte der EuGH der Rechtsauffassung von *Facebook*, des LG Wien und des OLG Wien folgen, würde das Geschäftsmodell von *Facebook* und anderen durch personalisierte Werbung finanzierten Kommunikationsplattformen nicht nur gemäß Art. 6 Abs. 1 lit. b DS-GVO weitgehend den Vorgaben der DS-GVO entgehen, sondern es entstünden auch schwerwiegende Abgrenzungsschwierigkeiten zum Anwendungsbereich der DID-RL bzw. von §§ 327 ff. BGB. Hierzu Kapitel 3 C.III.3.

[18] Gesetz zum Schutz vor Mißbrauch personenbezogener Daten bei der Datenverarbeitung v. 27.01.1977, BGBl. I Nr. 7 S. 201 ff.

[19] Pointiert: *Engert*, in: Grundmann/Möslein (Hrsg.), Innovation und Vertragsrecht, 2020, S. 153 (159: „Datenverarbeitung durch Private wird umstandslos einem staatlichen Grundrechtseingriff gleichgestellt und einem umfassenden Rechtfertigungsgebot unterworfen […]. Strukturell ist das nichts anderes als eine ins Horizontalverhältnis gekippte, unmittelbare Grundrechtsbindung Privater").

Kurzum: Bislang ist es weder dem europäischen noch dem – insoweit durch Unionsrecht gebundenen deutschen – Gesetzgeber gelungen, das Datenschutzrecht und das Schuldrecht zu synchronisieren. Auch das dem unternehmerisch handelnden Verantwortlichen gemäß § 327q Abs. 2 BGB eingeräumte, komplexe Kündigungsrecht für den Fall, dass ein als Verbraucher handelndes Datensubjekt die Datenverarbeitung für die Zukunft beendet, ist lediglich ein erster – deutscher – Versuch, diese Kollision abzumildern. Ein *Datenschuldrecht*,[20] das auch personenbezogene Daten als Leistungsgegenstand anerkennt und die ökonomische Realität rechtlich abbildet oder sogar gestaltet, lässt sich auf dieser Grundlage jedoch nicht entwickeln.

Es ist eine banale Erkenntnis, dass die Verarbeitung von personenbezogenen Daten ubiquitär ist. Sie ist zentral für Entwicklungen, die derzeit mit den schillernden Chiffren „Big Data“[21] und „künstliche Intelligenz“ (KI)[22] umschrieben werden. Beiden Entwicklungen ist gemeinsam, dass sie die Verarbeitung von personenbezogenen Daten nicht voraussetzen, ihre Vorteile aber insbesondere durch eine Verarbeitung von Daten mit Personenbezug entfalten können.

Zwar sind anonymisierte Daten im Kontext von Big Data und KI nicht wertlos, solange ein abstrakter und damit wissenschaftlicher Erkenntnisgewinn angestrebt wird. Allerdings knüpfen auch der wissenschaftliche, jedenfalls aber der ökonomische Wert von Datenanalysen häufig an den Personenbezug als eine wesentliche semantische Ebene von maschinenlesbar codierter Information (kurz: personenbezogenes Datum) an.[23] Deshalb liegt der Fokus der Arbeit nicht auf der – primär technisch spannenden – Frage, wie eine Verarbeitung von personenbezogenen Daten durch Methoden der Anonymisierung effektiv vermieden oder das Risiko der Verarbeitung durch Pseudonymisierung (Art. 4 Nr. 5 DS-GVO) und Datenminimierung (Art. 5 Abs. 1 lit. c DS-GVO) verringert werden kann. Vielmehr steht die Frage im Zentrum, inwieweit die Auslegung und Anwendung der DS-GVO eine rechtmäßige und rechtssichere Verarbeitung von personenbezogenen Daten im Privatrechtsverhältnis[24] ermöglicht, ohne dabei gegen das gemäß Art. 8 GRCh (Schutz personenbezogener Daten)

---

[20] Begriffsprägend *Schmidt-Kessel*, Daten als Gegenleistung in Verträgen über die Bereitstellung digitaler Inhalte, BMJV, 03.05.2016, https://www.bmjv.de/SharedDocs/Downloads/DE/Praesentationen/05032016_digitalesVertragsrecht_Schmidt_Kessler.pdf?__blob=publicationFile&v=1, zuletzt abgerufen am 19.05.2022.

[21] Aus rechtlicher Perspektive: *Leistner/Antoine/Sagstetter*, Big Data, 2021.

[22] Mit technischer Einführung: *Zech*, Entscheidungen digitaler autonomer Systeme: Empfehlen sich Regelungen zu Verantwortung und Haftung?, Gutachten für den 73. Deutschen Juristentag, 2020.

[23] Zum Informationsbegriff: *Wiebe*, in: Fiedler/Ullrich (Hrsg.), Information als Wirtschaftsgut, 1997, S. 93 (99 ff.); *Zech*, Information als Schutzgegenstand, 2012, S. 14 ff./114. f./441.

[24] Die Datenverarbeitung im Rahmen von Beschäftigungsverhältnissen (Art. 88 DS-GVO i. V. m. § 26 BDSG) weist Besonderheiten auf und bleibt unberücksichtigt: Hierzu: m. w. N.: *Neighbour*, in: Sassenberg/Faber (Hrsg.), Industrie 4.0 und IoT, 2020, S. 277 ff.; *Forgó/Helfrich/Schneider* (Hrsg.), Betrieblicher Datenschutz, 2019.

und gemäß Art. 7 GRCh (Privatsphäre) zu gewährleistende Untermaßverbot zu verstoßen.

Notwendig ist eine privatrechtssensible Auslegung deshalb, weil zunehmend deutlich wird, dass der europäische Gesetzgeber bei Verabschiedung der DS-GVO die rechtliche und ökonomische Realität in den Mitgliedstaaten nur unzureichend erfasst hat. Die DS-GVO nimmt zu wenig Rücksicht auf die tatsächliche Verwertung der vermögenswerten Bestandteile von Persönlichkeitsrechten, die wiederum eine Verarbeitung von personenbezogenen Daten voraussetzt.[25]

Die Notwendigkeit, bei dieser privatrechtssensiblen Auslegung und Anwendung der DS-GVO auf die Unionsgrundrechte zurückzugreifen, ist der Vielzahl der unbestimmten Rechtsbegriffe in der DS-GVO geschuldet. Diese erschweren die gerichtliche und behördliche Rechtsanwendung derzeit fundamental. Infolgedessen ist es auch für die Wissenschaft eine zentrale Herausforderung *de lege lata* und – soweit dies nicht mehr möglich ist – auch *de lege ferenda* Vorschläge für die Ausgestaltung eines Datenschuldrechts zu unterbreiten, das die informationelle Privatautonomie der Datensubjekte stärkt, dabei aber die multipolaren Grundrechtskonstellationen hinreichend berücksichtigt.[26]

Das nachfolgend vorgeschlagene Stufenmodell der Erlaubnistatbestände zur Gewährleistung einer abgestützten informationellen Privatautonomie stellt bereits begrifflich die Privatautonomie und insbesondere die Vertragsfreiheit als ihre wichtigste Ausprägung in den Mittelpunkt. Dabei weicht der Begriff der informationellen Privatautonomie von dem bekannten Begriff der informationellen Selbstbestimmung ab. Letztere ist bereits seit dem *Volkszählungsurteil* des *BVerfG*[27] bekannt.

Diese begriffliche Unterscheidung ist jedoch kein bloßes Glasperlenspiel. Im Gegenteil: Die Gewährleistung einer abgestützten informationellen Privatautonomie ist Ausdruck eines Perspektivenwechsels und dient dazu, Grundannahmen des geltenden Datenschutzrechts kritisch zu hinterfragen, soweit personenbezogene Daten als Gegenstand eines vertraglichen Synallagmas vereinbart werden.

Im Zentrum des hier vorgeschlagenen Stufenmodells der Erlaubnistatbestände für das Privatrechtsverhältnis steht die datenschutzrechtliche Einwilligung, die ihrerseits in zwei Stufen ausdifferenziert wird. Infolgedessen ist dieses Stufenmodell in der Lage, eine Synthese aus dem datenschutzrechtlichen Verbot und der schuldrechtlichen Erlaubnis herzustellen und dadurch einem künftiges

---

[25] Zuletzt mit dieser Kritik, jedoch aus Perspektive einer Stärkung von Verbraucherrechten: *Wendehorst*, JZ 2021, 974 (984: „die DSGVO [ist] überhaupt nicht auf den Schutz vermögensrechtlicher Verbraucherinteressen […] zugeschnitten").

[26] Mit dieser Forderung an die Privatrechtswissenschaft: *Marsch*, Das europäische Datenschutzgrundrecht, 2018, S. 372.

[27] BVerfGE 65, 1 (43) = NJW 1984, 419 ff. – *Volkszählung*.

Datenschuldrecht den Boden zu bereiten. Dadurch gewährleistet das nachfolgend vorgeschlagene Stufenmodell der Erlaubnistatbestände die unionsgrundrechtlich verankerte abgestützte informationelle Privatautonomie und ermöglicht die Umsetzung von drei wesentlichen Zielen, ohne dabei den Schutz der Datensubjekte wesentlich zu beeinträchtigen:

Erstens wird die bisherige Kommerzialisierung der vermögenswerten Bestandteile von Persönlichkeitsrechten (wieder) ermöglicht, soweit diese auf eine Verarbeitung von personenbezogenen Daten angewiesen ist.

Zweitens werden personenbezogene Daten – wie von der *EU-Kommission* immer wieder und zuletzt im Kontext des Data Act gefordert – für Innovation und Wachstum im Binnenmarkt nutzbar gemacht, ohne dabei über die Präferenzen der Datensubjekte hinwegzugehen.

Drittens hilft dieses Stufenmodell und insbesondere die kartellrechtsakzessorische und damit asymmetrische Auslegung und Anwendung des Einwilligungstatbestands dabei, die durch die DS-GVO entstandenen Marktzutrittsbarrieren für KMU zu senken.

II. Forschungsstand

Spätestens seit Anfang der 1970er Jahre fordert der technische Fortschritt im Bereich der automatischen Datenverarbeitung den Schutz des Individuums vor einer Verarbeitung personenbezogener Daten immer wieder heraus.[28] Nach einer frühen kritischen Auseinandersetzung mit den ersten deutschen Gesetzen zum Schutz von natürlichen Personen vor einer Verarbeitung von personenbezogenen Daten[29] stagnierte das Interesse, das Privatrechtswissenschaftler dem Datenschutzrecht entgegenbrachten.[30] Das Feld wurde weitgehend dem Verwaltungs- und insbesondere dem Verfassungsrecht überlassen.[31]

---

[28] Hierzu frühzeitig: *Kilian*, Personalinformationssysteme in deutschen Großunternehmen, 1967; *ders.*, Juristische Entscheidung und Elektronische Datenverarbeitung, 1974; *Steinmüller/Lutterbeck/Malmann/Harbort/Kolb/Schneider*, Grundfragen des Datenschutzes, Gutachten im Auftrag des Bundesministeriums des Innern, 1971, BT Drs. VI/3826; *Steinmüller*, EDV und Recht: Einführung in die Rechtsinformatik und das Recht der Informationsverarbeitung, Juristische Arbeitsblätter 1970; *ders.* (Hrsg.), Informationsrecht und Informationspolitik, 1976.

[29] Kapitel 1 A.II.

[30] Zu den wenigen Ausnahmen zählen: *Ebnet*, Der Informationsvertrag, 1995; *A. Wagner*, Binäre Information als Gegenstand des Rechtsverkehrs, 1999; *Kilian*, CR 2002, 921 ff.; *Buchner*, Die Informationelle Selbstbestimmung im Privatrecht, 2006; *Unseld*, Die Kommerzialisierung personenbezogener Daten, 2010; *Specht*, Konsequenzen der Ökonomisierung informationeller Selbstbestimmung, 2012; *Sandfuchs*, Privatheit wider Willen?, 2015. Zudem ist *Spiros Simitis*, der erste Hessische Datenschutzbeauftragte und Herausgeber des langjährigen Standardkommentars zum BDSG, von Hause aus Privatrechtwissenschaftler.

[31] Hierzu: *Sattler*, in: Bakhoum u. a. (Hrsg.), 2018, Personal Data in Competition, Consumer Protection and Intellectual Property Law, 2018, S. 27 ff.

Obwohl einige wissenschaftliche Beiträge einen vermittelnden Ansatz wählen,[32] leidet die rechtswissenschaftliche Auseinandersetzung weiterhin unter einem – auch institutionell durch die zahlreichen Datenschutzbehörden begünstigten – Übergewicht der öffentlich-rechtlichen Perspektive. Dennoch hat die privatrechtlich ausgerichtete Forschung gerade in den letzten Jahren wegweisende Untersuchungen hervorgebracht.

Besonders hervorzuheben sind die Arbeiten von *Benedikt Buchner*,[33] *Louisa Specht-Riemenschneider*,[34] *Carmen Langhanke*,[35] *Philipp Hacker*[36] *und Jan Niklas Bunnenberg*.[37] Die nachfolgende Analyse profitiert von dieser Forschung und baut hierauf teilweise auf. Dennoch unterscheidet sich das hier vorgeschlagene Stufenmodell der Erlaubnistatbestände und die dadurch gewährleistete abgestützte informationelle Privatautonomie in mehreren wesentlichen Punkten vom bisherigen Forschungsstand.

Der Untersuchungsgegenstand der Arbeiten von *Benedikt Buchner*, *Louisa Specht-Riemenschneider* und *Carmen Langhanke* war das alte BDSG, so dass mit der Anwendbarkeit der DS-GVO – trotz deren weitreichender Kontinuität zur Datenschutz-RL von 1995 – eine Neubewertung erforderlich ist. Zudem gehen alle vorgenannten Autorinnen und Autoren – mit Ausnahme von *Benedikt Buchner* – von einer jederzeitigen und grundlosen Widerruflichkeit der datenschutzrechtlichen Einwilligung aus. Infolgedessen dominiert das Datenschutzrecht das Schuldrecht in einer Weise, die – zumindest im B2B-Verhältnis – nach hier vertretener Ansicht nicht mit dem Verhältnismäßigkeitsgrundsatz vereinbar ist. *Benedikt Buchner* wiederum spart das Verhältnis zwischen Datenschutzrecht und AGB-Recht weitgehend aus.[38]

Weil alle bisherigen Arbeiten von einer Dominanz des Datenschutzrechts gegenüber dem Schuldrecht ausgehen,[39] bleibt – jedenfalls nach hier vertretener Auffassung – nicht viel vom Grundsatz der Privatautonomie, einschließlich der Möglichkeit zur Selbstbindung, übrig.

---

[32] *Masing*, NJW 2012, 2305 ff.; *Kingreen/Kühling*, JZ 2015, 213 ff.; *von Lewinski*, Die Matrix des Datenschutzrechts, 2014.

[33] Die informationelle Selbstbestimmung im Privatrecht, 2006.

[34] *Specht*, Die Konsequenzen der Ökonomisierung informationeller Selbstbestimmung – Die zivilrechtliche Erfassung des Datenhandels, 2012.

[35] Daten als Leistung, 2018.

[36] Datenprivatrecht, 2020.

[37] Privates Datenschutzrecht, 2020.

[38] Das ist im Ergebnis wenig schädlich, weil infolge der seit 2018 vorrangig anzuwenden Grundsätze aus Art. 5 Abs. 1 DS-GVO der AGB-Kontrolle lediglich geringe Bedeutung zukommt. Hierzu: Kapitel 3 C.I.3.; a. A. *Hacker*, Datenprivatrecht, 2020, 417 ff. (430 ff.), sowie *Wendehorst*, JZ 2021, 974 (983 f.).

[39] Für eine stärkere Berücksichtigung schuldrechtlicher Grundsätze: *Metzger*, JIPITEC 2017, 2 (6 f.); *ders.*, AcP 216 (2016), 817 (833); *ders.*, in: Lohsse/Schulze/Staudenmayer (Hrsg.), Data as Counter-Performance: Contract Law 2.0?, 2020, S. 25 (36 ff.).

Jan Niklas Bunnenberg will der Bindungswirkung einer Erklärung von Datensubjekten nur dann gemäß Art. 6 Abs. 1 lit. b DS-GVO (sog. vertragsakzessorische Datenverarbeitung) einen Vorrang vor dem Widerrufsinteresse des Datensubjekts einräumen, wenn das Interesse des Verantwortlichen infolge einer Abwägung im Einzelfall ausnahmsweise überwiegt.[40] Dieser Ansatz überzeugt systematisch nicht, weil er die beiden Erlaubnistatbestände gemäß Art. 6 Abs. 1 lit. b DS-GVO (vertragsakzessorische Datenverarbeitung) und gemäß Art. 6 Abs. 1 lit. f DS-GVO (Datenverarbeitung infolge einer Interessenabwägung) im Ergebnis vermengt und stets auf eine *ex post*-Interessenabwägung im Einzelfall angewiesen ist.[41]

Philipp Hacker ordnet die frei widerrufliche Einwilligung (Art. 7 Abs. 3 S. 1 DS-GVO) als schuldrechtliche Bedingung für die Leistungserbringung durch den Verantwortlichen ein.[42] Infolgedessen verschmelzen Software und Recht potenziell zu dem von *Lawrence Lessig* konstatierten „Code is Law".[43] Allerdings soll es dem Verantwortlichen im Fall eines allzu „opportunistischen Widerrufs" der Einwilligung durch das Datensubjekt ausnahmsweise möglich sein, die Datenverarbeitung auf Grundlage einer Interessenabwägung gemäß Art. 6 Abs. 1 lit. f DS-GVO fortzusetzen.[44] Sofern personenbezogene Daten vertraglich als Leistungsgegenstand vereinbart werden, soll deren Verarbeitung gemäß Art. 6 Abs. 1 lit. b DS-GVO rechtmäßig sein, soweit dieses Synallagma einer gerichtlichen Angemessenheitskontrolle standhält.[45]

Obwohl sich die von *Hacker* und in dieser Arbeit bearbeitete Thematik teilweise überschneidet, wird nachfolgend eine andere Lösung vorgeschlagen. Die Skepsis gegenüber einer gerichtlichen Angemessenheitsprüfung des vertraglichen Synallagmas mündet in den nachfolgend herausgearbeiteten Vorschlag einer abgestützten informationellen Privatautonomie, der im Unterschied zu

---

[40] *Bunnenberg*, Privates Datenschutzrecht, 2020, S. 264 f.

[41] Das Interesse des Datensubjekts am Widerruf der Einwilligung (Art. 6 Abs. 1 lit. a i. V. m. Art. 7 Abs. 3 S. 1 DS-GVO) wird mit einer Interessenabwägung (Art. 6 Abs. 1 lit. f DS-GVO) kombiniert und soll anschließend die Fortsetzung der Datenverarbeitung auf Grundlage eines bindenden Vertrags gemäß Art. 6 Abs. 1 lit. b ermöglichen. Hierzu unten Kapitel 3 B.II.

[42] *Hacker*, ZfPW 2019, 148 (172 ff.); *ders.*, Datenprivatrecht, 2020, S. 228 f.; so auch *Rafał Mańko*, Contracts for the supply of digital content and digital services, Bericht des Wissenschaftlichen Dienstes des EU-Parlaments (EPRS) vom 27.11.2017, S. 8 („The report deletes the term *counter-performance*, criticized by the EDPS, and replaces it with the term *condition*"), verfügbar unter http://www.europarl.europa.eu/RegData/etudes/BRIE/2018/614707/EPRS_BRI%282018%29614707_EN.pdf, zuletzt abgerufen am 19.05.2022; *EDSA*, Leitlinien 05/2020 zur Einwilligung gemäß Verordnung 2016/679, Version 1.1, v. 04.05.2020, Nr. 37; ähnlich: *Riehm*, in: Pertot (Hrsg.), Rechte an Daten, 2020, S. 194 f. Hierzu: Kapitel 4 A.II.5.

[43] *Lessig*, Code is law, 1999.

[44] *Hacker*, Datenprivatrecht, 2020, S. 278. In diese Richtung auch bereits: *Buchner*, Die informationelle Selbstbestimmung im Privatrecht, 2006, S. 272 ff.

[45] *Hacker*, Datenprivatrecht, 2020, S. 445 ff./473 ff. Zu den Bedenken an einer praktischen Umsetzung dieses Ansatzes: Kapitel 3 C.I.2.e. und C.I.3. Zu den Nachteilen für die unionsweit einheitliche Wirkung der DS-GVO: Kapitel 3 C.II.

Hacker und zu *Bunnenberg* auf einem Vorrang der Einwilligung vor den anderen datenschutzrechtlichen Erlaubnistatbeständen beruht. Statt über Art. 6 Abs. 1 lit. b DS-GVO (*Bunnenberg*) oder Art. 6 Abs. 1 lit. f DS-GVO (*Hacker*) eine Notlösung im Einzelfall zu suchen, wird den Beteiligten die Gestaltung ihrer Rechtsbeziehungen zunächst überlassen, das Datensubjekt dabei jedoch durch mehrere Instrumente abgestützt.

Insofern knüpft das nachfolgend herausgearbeitete Stufenmodell der Erlaubnistatbestände grundsätzlich an die von *Benedikt Buchner* betonte Bedeutung der datenschutzrechtlichen Einwilligung an. Im Unterschied zur Arbeit von *Benedikt Buchner* genügt es nach hier vertretener Auffassung jedoch, wenn neben der schlichten und jederzeit widerruflichen Einwilligung lediglich die schuldrechtliche Gestattung als zweite Stufe der Einwilligung anerkannt wird.[46] Zudem werden im fünften und sechsten Kapitel diejenigen Maßnahmen herausgearbeitet, die notwendig sind, um die informationelle Privatautonomie der Datensubjekte so abzustützen, dass sowohl der Schutz der Datensubjekte (Art. 1 Abs. 2 DS-GVO) gewährleistet als auch der freie Verkehr personenbezogener Daten im europäischen Binnenmarkt (Art. 1 Abs. 3 DS-GVO) ermöglicht wird.

Infolgedessen kann mit dem nachfolgend unterbreiteten Vorschlag das Desiderat einer „Ertüchtigung der Einwilligung“[47] erreicht und die „fehlende vertragsrechtliche Unterfütterung“[48] der DS-GVO nachträglich durch Auslegung kompensiert werden.

III. Gang der Untersuchung

Die Arbeit ist in sechs Kapitel gegliedert. Das *erste Kapitel* analysiert wesentliche Merkmale der Entstehungsgeschichte des Datenschutzrechts. Es dient nicht als disparate „Einleitungshistorie“, sondern offenbart, warum das Datenschutzrecht auf einen Kollisionskurs zum Schuldrecht geraten ist. Zudem wird deutlich, dass die DS-GVO einer unionsgrundrechtskonformen Auslegung bedarf, die nicht einseitig an Art. 8 Abs. 1 GRCh (Schutz personenbezogener Daten) und Art. 7 GRCh (Schutz der Privatsphäre) ausgerichtet werden darf, sondern ebenfalls die unternehmerische Freiheit der Verantwortlichen und der Datensubjekte (Art. 16 GRCh) und die allgemeine Vertragsfreiheit (Art. 6 Abs. 3 EUV) gewährleistet.

Dies ist erforderlich, damit die datenschutzrechtlichen Verarbeitungsverbote in Art. 6 Abs. 1 und Art. 9 Abs. 1 DS-GVO mit Blick auf die unternehmerische Freiheit (Art. 16 GRCh) und den allgemeinen Rechtsgrundsatz der Vertragsfrei-

---

[46] Kapitel 4 C.II.
[47] Mit dieser Forderung: *Leistner/Antoine/Sagstetter*, Big Data, 2021, S. 403.
[48] *Staudenmayer*, ZEuP 2019, 663 (676).

heit (Art. 6 Abs. 3 EUV) nicht gegen das Übermaßverbot und damit gegen den Verhältnismäßigkeitsgrundsatz verstoßen (Art. 52 Abs. 1 S. 2 GRCh), sondern im Wege der praktischen Konkordanz in eine abgestützte informationelle Privatautonomie der Datensubjekte münden.

Anschließend werden die in der DS-GVO für das Privatrechtsverhältnis vorrangig vorgesehenen Erlaubnistatbestände daraufhin analysiert, inwieweit sie geeignet sind, die informationelle Privatautonomie der Datensubjekte zu verwirklichen, ohne das unionsgrundrechtlich gemäß Art. 8 Abs. 1 GRCh und Art. 7 GRCh zu gewährleistende Untermaß zu verletzen.

Im *zweiten Kapitel* wird die Möglichkeit zur rechtmäßigen Datenverarbeitung auf Grundlage einer Interessenabwägung gemäß Art. 6 Abs. 1 lit. f DS-GVO analysiert. Neben den Vorteilen dieser nur im Privatrechtsverhältnis anwendbaren Generalklausel werden deren Nachteile offenkundig. Paradoxerweise ist die Vorschrift einerseits potenziell zu weit geraten, soweit sie eine Direktwerbung, einschließlich Profiling, *de lege lata* privilegiert. Andererseits ist sie zu eng geraten, weil auch eine Verarbeitung besonders sensibler personenbezogener Daten – im Fall von Spontanäußerungen und für das Trainieren von sog. künstlicher Intelligenz – auf Grundlage einer Interessenabwägung *de lege ferenda* ermöglicht werden sollte.

Im *dritten Kapitel* wird die vertragsakzessorische Datenverarbeitung gemäß Art. 6 Abs. 1 lit. b DS-GVO untersucht. Obwohl dieser Erlaubnistatbestand auf den ersten Blick am besten für die Entwicklung eines Datenschuldrechts geeignet scheint, ist er nach hier vertretener Auffassung durch eine restriktive Auslegung auf die Funktion zu beschränken, den Tatbestand der Einwilligung und infolgedessen die Aufmerksamkeits- und Entscheidungskapazitäten der Datensubjekte zu entlasten.

Im *vierten Kapitel* wird herausgearbeitet, warum die Einwilligung am besten dafür geeignet ist, die informationelle Privatautonomie der Datensubjekte zu gewährleisten. Im Privatrechtsverhältnis ist der Einwilligung ein Vorrang vor den anderen Erlaubnistatbeständen einzuräumen.

Im *fünften Kapitel* münden die zuvor gefundenen Ergebnisse in ein Stufenmodell der Erlaubnistatbestände für das Privatrechtsverhältnis. Dieses Stufenmodell ermöglicht eine abgestützte informationelle Privatautonomie, setzt aber voraus, dass die sog. freie Widerruflichkeit der Einwilligung (Art. 7 Abs. 3 S. 1 DS-GVO) – im Grundsatz – dispositiv ist und die Anforderungen an die Freiwilligkeit der Einwilligung (Art. 7 Abs. 4 DS-GVO) flexibel als Berücksichtigungsgebot und nicht – wie derzeit zumeist vertreten – im Sinne eines strengen Kopplungsverbots angewendet wird. Soweit Datensubjekte als Unternehmer handeln, ist diese Flexibilisierung zwingend, um den Grundsatz der Verhältnismäßigkeit zu wahren. Indem diese Flexibilisierung des Einwilligungstatbestands zugleich in kartellrechtsakzessorischer und damit asymmetrischer Weise beschränkt wird, werden zwei Ziele verwirklicht.

Erstens wird die informationelle Privatautonomie der Datensubjekte gegenüber sog. *Gatekeeper*n bzw. Unternehmern mit überragender marktübergreifender Bedeutung für den Wettbewerb abgestützt. *Zweitens* wird vermieden, dass Art. 7 Abs. 3 S. 1 und Art. 7 Abs. 4 DS-GVO als Marktzutrittsbarrieren wirken und dadurch die Wettbewerbsposition von KMU insbesondere gegenüber *GAFAM* und (künftig) gegenüber *BAT* verschlechtern.

Im *sechsten Kapitel* werden zwei wesentliche Maßnahmen als Abstützungen der informationellen Privatautonomie vorgeschlagen. Weil die europäische Gesetzgebung auf das sog. Informationsmodell[49] und das dezentrale Instrument der Einwilligung setzt, ergibt sich hieraus eine Folgenverantwortung. Die informationelle Privatautonomie muss mittelfristig durch eine Kombination aus farblicher Kennzeichnung und *Privacy Score* und die Implementierung eines *Kontroll-Cockpits* zusätzlich „materialisiert" werden. Die Arbeit schließt mit einer Zusammenfassung in sechs Haupt- und insgesamt 30 (Unter-)Thesen.

[49] Hierzu instruktiv: *Grundmann*, in: Riesenhuber (Hrsg.), Europäische Methodenlehre, 4. Aufl. 2021, S. 264 Rn. 41 ff.; umfassend: *Grigoleit*, Vorvertragliche Informationspflichten, 1997; *Fleischer*, Informationsasymmetrien im Vertragsrecht, 2001.

1. Kapitel

Grundrechtliche Gewährleistung von informationeller Privatautonomie

Der Begriff der *informationellen Privatautonomie* dürfte Experten für Verfassungsrecht irritieren. Aus der deutschen verfassungsgerichtlichen Perspektive ist das *Recht auf informationelle Selbstbestimmung* (RaiS) seit 1983 etabliert, so dass der Begriff der informationellen Privatautonomie ein fehlerhaftes Verständnis nahelegt. Bestätigt wird diese Einschätzung durch eine Suche in juristischen Datenbanken. Sie fördert eine Fehlanzeige zu Tage.[1] Dennoch lässt sich die hier vorgeschlagene Flexibilisierung und Privatrechtssensibilisierung der DS-GVO mit dem Begriff der informationellen Privatautonomie auf den Punkt bringen.

Die begriffliche Abgrenzung der informationellen Privatautonomie zur informationellen Selbstbestimmung[2] und den im Anschluss hieran vom *BVerfG* entwickelten IT-Grundrechten[3] ist bewusst gewählt. Diese Abweichung dient dazu, bereits sprachlich eine erkennbare Unterscheidung zum grundrechtlichen Schutz der informationellen Selbstbestimmung vorzunehmen.

Der Begriff hat einen weiteren Vorteil: Weder der europäische Gesetzgeber noch der *EuGH* kennen das Recht auf informationelle Selbstbestimmung.[4] Infolgedessen kann der Begriff und die Gewährleistung der informationellen Privatautonomie originär in der DS-GVO und den europäischen Grundrechten verortet werden.[5]

---

[1] Eine Suchanfrage mit dem Stichwort „informationelle Privatautonomie" in der Datenbank Beck-Online (Datum 28.08.2021) erzielt einen Treffer, der eine beiläufige Verwendung des Begriffs enthält: *Schantz*, NJW 2016, 1841 (1845).

[2] Begriffsprägend: *Steinmüller u. a.* Grundfragen des Datenschutzes, Gutachten im Auftrag des Bundesministeriums des Innern, 1971, BT Drs. VI/3826, 84 (93: „Recht auf Selbstbestimmung über Individualinformation"); Zum Recht auf informationelle Selbstbestimmung: *Vogelgesang*, Grundrecht auf informationelle Selbstbestimmung?, 1987, S. 25; *di Fabio*, in: Maunz/Dürig, GG, 2001, Art. 2 Rn. 173 („interpretatorische Fortschreibung des Selbstdarstellungsschutzes aus Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG").

[3] Zum Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität (eigengenutzter) informationstechnischer Systeme: *Hoffmann-Riem*, JZ 2008, 1009 ff.

[4] Für eine Vermeidung des Begriffs, auch weil diesem eine für Art. 8 GRCh abzulehnende herrschaftsrechtliche Konzeption zugrunde liegt: *Marsch*, Das Europäische Datenschutzgrundrecht, 2018, S. 105 ff.

[5] Allerdings ist zu beachten, dass eine grundrechtliche Gewährleistung von Privatautonomie als Ausdruck der allgemeinen Handlungsfreiheit und Vertragsfreiheit auf Ebene der Unionsgrundrechte unterentwickelt ist: *Herresthal*, ZEuP 2014, 238 (265: „Schwerwiegender Konstruktionsfehler der Grundrechtecharta").

Die vorgeschlagene begriffliche Unterscheidung zwischen dem deutschen Recht auf informationelle Selbstbestimmung und der unionsrechtlichen Gewährleistung der informationellen Privatautonomie ist nur auf den ersten Blick trivial oder ein bloßes Spiel mit Worten. Der Begriff ist nicht das privatrechtlich geprägte Pendant zum deutschen Recht auf informationelle Selbstbestimmung.[6] Vielmehr ist er Ausdruck eines Perspektivenwechsels[7] und Ausgangspunkt einer privatrechtlichen Betrachtung des weitgehend unionsrechtlich determinierten Datenschutzrechts.[8] Zugleich bildet die informationelle Privatautonomie den Nukleus eines Datenschuldrechts, dessen Leistungsgegenstand auch personenbezogene Daten sein können. Damit dient die informationelle Privatautonomie dazu, die fehlende „vertragsrechtliche Unterfütterung der DS-GVO"[9] nachträglich im Wege der Auslegung und Anwendung zu korrigieren.[10]

Obwohl die nachfolgend vorgeschlagene abgestützte informationelle Privatautonomie eine Analyse der DS-GVO aus privatrechtlicher Perspektive ermöglichen soll, ist es dennoch erforderlich, zunächst auf das deutsche Recht auf informationelle Selbstbestimmung und seine relevanten unionsrechtlichen Funktionsäquivalente einzugehen. Dadurch werden grundlegende Strukturen des Datenschutzrechts offengelegt, die bis heute prägend sind und die es erschweren, den monolithischen Block „DS-GVO" mit den Bedingungen der automatisierten und künftig autonomen Datenverarbeitung in einen sinnvollen Ausgleich zu bringen.[11]

---

[6] Hierzu bereits: *Buchner*, Die informationelle Selbstbestimmung im Privatrecht, 2006, S. 76 f.

[7] Diesen Perspektivenwechsel ebenfalls fordernd: *Leistner/Antoine/Sagstetter*, Big Data, 2021, S. 401 („Bei der Konzeption der DSGVO wurde vielfach, auf Jahrzehnte alte Grundsätze und Prinzipien zurückgegriffen, die für die heutige Praxis nur noch teilweise tragen.").

[8] Letztlich verbleiben im Kontext der Öffnungsklauseln der DS-GVO – insbesondere Art. 85 DS-GVO – um „Korridorlösungen, innerhalb derer die Mitgliedstaaten eigenständige Entscheidungen treffen können", wenngleich diese an die Konventionsrechte der EMRK gebunden sind: Hierzu: *Marsch*, Das Europäische Datenschutzgrundrecht, 2018, S. 366.

[9] *Staudenmayer*, ZEuP 2019, 663 (676).

[10] Damit soll auch das Spannungsverhältnis aufgelöst werden, das sich bereits aus Sicht der unionsgrundrechtlichen Bewertung der DS-GVO ergibt. So scheut beispielweise *Nikolaus Marsch* mehrfach davor zurück, Vorschriften der DS-GVO als zu unbestimmt oder als Verstoß gegen die Verhältnismäßigkeit klar zu benennen. So mit Blick auf Art. 6 Abs. 1 lit. f DS-GVO: „einen nicht unerheblichen Eingriff in die Grundrechte des Datenverarbeiters dar. Ob dieser wenig zielgenaue Eingriff durch den bloßen Verweis auf die potenzielle Gefährlichkeit von Datenverarbeitungsmaßnahmen zu rechtfertigen ist, scheint mehr als fraglich" (*ders.*, Das Europäische Datenschutzgrundrecht, 2018, S. 264 f.); sowie zu den Ansprüchen des Datensubjekts auf Auskunft, Löschung und Berichtigung: „Nur als Ergebnis einer Interessenabwägung können sich gegen Private gerichtete Auskunfts- und Einwirkungsrechte somit als in bestimmten Konstellationen grundrechtlich geboten erweisen, nicht jedoch im Sinne einer dieser Abwägung vorausliegenden Rechtsposition" (S. 267). Allerdings räumt *Marsch* dem EU-Gesetzgeber auf Grundlage von Art. 8 Abs. 1 GRCh einen weiten „Korridor" zur Regulierung und Strukturierung privater Datenverarbeitungsmaßnahmen ein (S. 260/268).

[11] So mit Blick auf Art. 4 Nr. 1 DS-GVO: *Leistner/Antoine/Sagstetter*, Big Data, 2021, S. 226 („Eine *beschränkende Auslegung* des Begriffs der personenbezogenen Daten fällt nach

Das Recht auf informationelle Selbstbestimmung wurde aus Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG abgeleitet und hat das deutsche Datenschutzrecht über Jahrzehnte geprägt. Der Blick auf die Entstehungsgeschichte des Datenschutzrechts verdeutlicht, dass für diesen Schutz von Menschen vor einer Verarbeitung personenbezogener Daten zu wenig zwischen der vertikalen und der horizontalen Bedeutung von Grundrechten differenziert wurde. Auch die DS-GVO und das BDSG basieren – wie die vorherigen deutschen Datenschutzgesetze und die europäische Datenschutz-RL (1995)[12] – primär auf einem abwehrrechtlichen Verständnis von Grundrechten (A).

Der europäische Gesetzgeber berücksichtigte kaum den in der deutschen Grundrechtslehre bekannten Unterschied zwischen einer Grundrechtsbindung staatlicher Stellen einerseits und den im Privatrechtsverhältnis lediglich bestehenden staatlichen Gewährleistungspflichten andererseits. In der Folge greift der unionsrechtliche Datenschutz in die unternehmerische Freiheit der Verantwortlichen und die persönliche Freiheits- und Verantwortungssphäre der Datensubjekte ein (B).

Ausdruck dieser potenziellen Gefährdung der informationellen Privatautonomie ist das einfachgesetzliche Verbot einer Verarbeitung von personenbezogenen Daten (C). Die hier vorgeschlagene abgestützte informationelle Privatautonomie ist mit den primärrechtlichen Vorgaben vereinbar und bietet einen Ansatzpunkt, um die DS-GVO (und künftig: ePrivacy-VO und Data Act) so auszulegen und weiterzuentwickeln, dass die individuelle Gestaltungsfreiheit durch einen Vorrang der Einwilligung gestärkt wird, ohne dabei das gemäß Art. 8 Abs. 1 GRCh (Art. 16 Abs. 1 AEUV) und Art. 7 GRCh grundrechtlich gebotene Untermaß zu unterschreiten (D).

A. Dominanz der abwehrrechtlichen Dimension der Grundrechte

Nicht nur den mit der grundrechtlichen Terminologie vertrauten Spezialisten des Verfassungsrechts dürfte der Begriff der informationellen Privatautonomie irritieren. Ähnlich irritiert dürften Spezialisten für das Immaterialgüterrecht und das Medienrecht – noch immer – sein, wenn sie erfahren, dass der europä-

dem derzeit geltenden Verständnis schwer. Diese schon auf der ersten Stufe des Anwendungsbereichs vollkommen ausgeuferte Reichweite datenschutzrechtlicher Regulierung ist *kritikwürdig*" [Hervorhebungen im Original.]. Mit Überlegungen für eine Reduktion der Anforderungen für KMU: Mitteilung der EU-Kommission, Datenschutz als Grundpfeiler der Teilhabe der Bürgerinnen und Bürger und des Ansatzes der EU für den digitalen Wandel – zwei Jahre Anwendung der Datenschutz-Grundverordnung, 24.06.2020 COM(2020) 264 S. 12/19 ff. (Evaluierung DS-GVO).

[12] Richtlinie 95/46/EG v. 24.10.1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, ABl. L 281 v. 23.11.1995, S. 31 ff.

ische Gesetzgeber weite Teile des allgemeinen Persönlichkeitsrechts (APR) und des Rechts am eigenen Bild – abgesehen von äußerungsrechtlichen Konstellationen – in den Anwendungsbereich der DS-GVO und damit unter das Primat des Unionsrechts gebracht hat.[13] Lediglich im Bereich der Öffnungsklauseln, insbesondere gemäß Art. 85 Abs. 2 (sog. Medienprivileg) kann das *BVerfG* versuchen,[14] ein nationales äußerungsrechtliches Persönlichkeitsrecht neben der DS-GVO aufrecht zu erhalten.[15]

Im Immaterialgüterrecht wurde über mehrere Jahrhunderte diskutiert und gestritten, welche unkörperlichen Güter als Immaterialgüterrechte und welche als Persönlichkeitsrechte geschützt sind.[16] Es folgte eine jahrzehntelange Diskussion darüber, ob und inwieweit Persönlichkeitsrechte trotz ihrer unverbrüchlichen Verbindung zu einem Individuum als Vermögensrechte kommerzialisiert werden können.[17] Die Publikationen zu diesem Rechtsgebiet füllen Bibliotheken. Diese Arbeiten sind infolge der DS-GVO nicht obsolet. Allerdings

---

[13] Mit der frühzeitigen Warnung, dass die DS-GVO in wichtigen Bereichen wie der Internetkommunikation zur Unanwendbarkeit des Rechts auf informationelle Selbstbestimmung, der grundgesetzlichen Presse- und Meinungsfreiheit sowie des allgemeinen Persönlichkeitsrechts führen könnte: *Masing*, Ein Abschied von den Grundrechten, SZ v. 09.01.2012, S. 10; *Kühling*, Die Europäisierung des Datenschutzrechts, 2014, S. 12. Ob diese Konsequenz den an den Beratungen zur DS-GVO Beteiligten bewusst war, ist zweifelhaft. Die Anwendbarkeit von §§ 22, 23 KUG und von § 1004 BGB analog bzw. §§ 823 Abs. 1 jeweils i. V. m. Art. 2 Abs. 1, Art. 1 Abs. 1 GG schrumpft erheblich zusammen. Für die nationalen Traditionen im Bereich des Persönlichkeitsrechts lässt die Öffnungsklausel gemäß Art. 85 Abs. 2 DS-GVO zugunsten von journalistischen, wissenschaftlichen, künstlerischen oder literarischen Zwecken einen kleinen Anwendungsbereich übrig. Unter Anwendung der Datenschutz-RL plädierte *Ohly* noch dafür, den Anwendungsbereich des Datenschutzrechts im Verhältnis zu den (sonstigen) Persönlichkeitsrechten einzuschränken: *ders.*, AfP 2011, 428 (438).

[14] *BVerfG*, Beschl. v. 06.11.2019, 1 BvR 16/13 = GRUR 2020, 74 (Rn. 39/74/91 f.) – *Recht auf Vergessen I*.

[15] Das Urteil des *BVerfG* ist insoweit nicht eindeutig. Während für eine Fortsetzung der deutschen Rechtsprechung zum äußerungsrechtlichen allgemeinen Persönlichkeitsrecht immerhin die Öffnungsklausel des Art. 85 Abs. 2 DS-GVO ins Feld geführt werden kann, scheint das *BVerfG* auch am allgemeinen Recht auf informationelle Selbstbestimmung festhalten zu wollen, Beschl. v. 06.11.2019, 1 BvR 16/13 = GRUR 2020, 74 (Rn. 83 ff.) – *Recht auf Vergessen I*. Tatsächlich kann das Recht auf informationelle Selbstbestimmung aus Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG jedoch nur auf solche Sachverhalte angewendet werden, für die in der DS-GVO eine Öffnungsklausel besteht (beispielsweise im Arbeitsrecht oder für journalistische Zwecke). Im Anwendungsbereich der DS-GVO sind dagegen die europäischen Grundrechte der Beurteilungsmaßstab. Zur vorherigen Diskussion, wie sich das *BVerfG* wieder „ins Spiel bringen" könne: *Thym*, JZ 2015, 53 (61); *Bäcker*, EuR 2015, 389 (400 f.); *Marsch*, Das Europäische Datenschutzgrundrecht, 2018, S. 298 ff.

[16] Hierzu: *Dölemeyer/Klippel*, in: Beier u. a. (Hrsg.), FS 100 Jahre GRUR, 1991, 185 ff.

[17] *Hubmann*, Das Persönlichkeitsrecht, 2. Aufl., 1967; *Götting*, Persönlichkeitsrechte als Vermögensrechte, 1995; *Helle*, Besondere Persönlichkeitsrechte im Privatrecht, 1991, S. 37 ff.; sowie *Forkel*, in: ders./Kraft (Hrsg.), Beiträge zum Schutz der Persönlichkeit und ihrer schöpferischen Leistung, FS Hubmann, 1985, 93 (101 f.); Kritisch gegenüber einer zunehmenden Kommerzialisierung von Persönlichkeitsaspekten mittels translativer Übertragungen: *Schack*, JZ 2000, 1060 (1062); *Peifer*, Individualität im Zivilrecht, 2001, S. 291 ff.

haben Wissenschaft und Praxis die Persönlichkeitsrechte bislang weitgehend parallel zum Datenschutzrecht behandelt. Bisher war das Verhältnis zwischen Persönlichkeitsrechten und Datenschutzrecht – jedenfalls in Deutschland – durch freundliches Desinteresse geprägt.[18]

Spätestens seit dem 25.05.2018 kreuzen sich jedoch die Pfade des (nationalen) Persönlichkeitsrechts und des europäischen Datenschutzrechts. Umso verblüffender ist es, dass die Bedeutung der Persönlichkeitsrechte für das Datenschutzrecht während den Verhandlungen zur DS-GVO keine wesentliche Rolle spielten. Grund dafür könnte sein, dass das Datenschutzrecht die privatrechtliche Forschung kaum interessierte,[19] weil der Schutz von personenbezogenen Daten als Domain des Verfassungs- und (Wirtschafts-)Verwaltungsrechts wahrgenommen wurde, die mit persönlichkeitsrechtlichen Fragestellungen nur am Rande in Zusammenhang zu stehen schien.[20] Diese fehlende Synchronisierung von Persönlichkeitsrechten und Datenschutzrecht beruht auf einer jahrzehntealten Tradition und der weiten Auslegung der verfassungsrechtlichen Urteile durch den Gesetzgeber.

Seit dem *Volkszählungsurteil* des *BVerfG* von 1983 wird das deutsche Datenschutzrecht unmittelbar durch die Grundrechte geprägt (I). Zwar bemühten sich einige Privatrechtswissenschaftler im Anschluss an das Urteil darum, die unterschiedlichen Funktionen von Grundrechten als Abwehrrechte gegen staatliche Maßnahmen und als staatliche Gewährleistungspflichten im Privatrecht zu verdeutlichen. Dieser Versuch blieb aber weitgehend erfolglos (II).

I. Das RaiS als Grundlage des deutschen Datenschutzrechts

Diese Untersuchung leistet keine vollständige ideengeschichtliche Analyse von Privatheit als Ursprung des Datenschutzrechts. Inwieweit das Bedürfnis von Privatheit als soziologisches Massenphänomen eine Folge der Industrialisie-

---

[18] *Engert*, in: Grundmann/Möslein (Hrsg.), Innovation und Vertragsrecht, 2020, 153 (159). Als Ausnahme: *Ohly*, AfP 2011, 428 (438); sowie die Problematik andeutend: *Spindler*, GRUR-Beilage 2014, 101: „Auch wenn Datenschutz und (zivilrechtlicher) Schutz des Persönlichkeitsrechts im Grunde denselben verfassungsrechtlichen Wurzeln entspringen und zahlreiche Berührungspunkte aufweisen, beschränkt sich der nachfolgende Beitrag auf einige offene Fragen des Datenschutzes […] nur am Rande kann das Verhältnis zum zivilrechtlichen Persönlichkeitsschutz beleuchtet werden".

[19] Wichtige Ausnahmen: *Buchner*, Die informationelle Selbstbestimmung im Privatrecht, 2006; *Specht*, Konsequenzen der Ökonomisierung informationeller Selbstbestimmung – Die zivilrechtliche Erfassung des Datenhandels, 2012.

[20] *BVerfG*, Beschl. v. 14.02.1973, 1 BvR 112/65, NJW 1973, 1221 – *Soraya*; *BVerfG*, Urt. v. 13.02.2007, 1 BvR 421/05, NJW 2007, 753 – *Heimlicher Vaterschaftstest*; *BVerfG*, Beschl. v. 13.06.2007, 1 BvR 1783/05B, NJW 2008, 39 – *Esra*; *BVerfG*, Beschl. v. 08.12.2011, 1 BvR 927/08, NJW 2012, 756 – *Caroline von Hannover*; zuletzt: *BVerfG*, Beschl. v. 28.01.2019, 1 BvR 1738/16, NJW 2019, 1277 – *Kunstfreiheit*.

rung und der hiermit einhergehenden Urbanisierung ist, bleibt eine spannende Forschungsfrage.[21]

Für den Gegenstand dieser Untersuchung genügt es, vier wesentliche Einflussfaktoren herauszustellen, welche die Entstehung des deutschen Datenschutzrechts geprägt haben.[22] Diese *plausibilisieren*, warum dem Recht auf informationelle Selbstbestimmung (RaiS) sowohl im vertikalen Verhältnis zwischen Datensubjekt und Staat als auch im horizontalen Verhältnis zwischen Privatrechtsubjekten eine nahezu unterschiedslose Geltung zuerkannt wurde. Die wesentlichen Faktoren sind die Veränderung der Lebensverhältnisse infolge der Industrialisierung (1), der für die ersten Datenschutzgesetze prägende Einfluss der (Rechts-)Soziologie (2), die Erfahrungen in der nationalsozialistischen Diktatur (3) und die anschließende extensive Auslegung der Rechtsprechung des *BVerfG* durch den deutschen Gesetzgeber (4).

1. Industrialisierung und technischer Fortschritt

Als ganz wesentlicher Faktor verstärkte die Industrialisierung die Änderung der Lebensverhältnisse und begründete Forderungen nach einem rechtlichen Schutz von Privatheit.[23] Obwohl Privatheit keine Innovation des 18. und 19. Jahrhunderts ist, waren die Entstehung großer Städte und die Entwicklung eines städtischen Bürgertums Voraussetzungen für den modernen Individualismus.[24] Dem städtischen Bürgertum standen zunächst keine Instrumente zur Verfügung, um auf die wachsende Anzahl und die Reichweite der Berichterstattung zu reagieren, die aus der Gewährleistung von Presse- und Meinungsfreiheit und den technischen Entwicklungen von Medien, insbesondere zur Reproduktion von Text und Bild resultierten.[25]

Die Gerichte in den USA setzten dieser Entwicklung die Anerkennung eines *right to privacy* entgegen[26] und differenzierten es im Laufe der Zeit als *intru-*

[21] Hierzu im Verhältnis zwischen Bürger und Staat: *Nissenbaum*, Privacy as Contextual Integrity, 79 Wash. L. Rev. 119 (2004). Zum Verhältnis zwischen Privatrechtsubjekten: *Posner*, 72 The American Economic Review, 405 ff.; grundlegend: *Warren/Brandeis* Harv. L. Rev. 1890, 193.

[22] Ausführlicher zur Entstehung des Datenschutzrechts: m. w. N. *Sattler*, in: Bakhoum u. a. (Hrsg.), 2018, Personal Data in Competition, Consumer Protection and Intellectual Property Law, 2018, 27 ff.

[23] *Shils*, 31 Law and Contemporary Problems (1966), 292, verfügbar unter: http://scholarship.law.duke.edu/cgi/viewcontent.cgi?article=3109&context=lcp, zuletzt abgerufen am 19.05.2022.

[24] *Mallmann*, Zielfunktionen des Datenschutzes, 1977, S. 16 ff., 32; *Posner*, AEI Journal on Government and Society, 1978, 19 (20); *Shils*, 31 Law and Contemporary Problems, 1966, 292 ff. ("golden age of privacy"); *Westin*, 25 Washington and Lee Law Review 166, 1967, 22 ff.

[25] *Götting*, in: ders./Schertz/Seitz (Hrsg.), HdB Persönlichkeitsrecht, 2. Aufl. 2019, Teil 2, Rn. 1 ff. und 16.

[26] *Warren/Brandeis*, Harv. L. Rev. 1890, 193; rechtsvergleichende Übersicht bei: *Götting*, ebda, Teil 10. Allerdings hatte auch US-Amerikanische Gerichte immer wieder Schwierigkei-

sion, *public disclosure*, *false light* und *appropriation* weiter aus.[27] Das Reichsgericht zog zunächst noch das Hausrecht und das „natürliche Rechtsgefühl" heran,[28] um die Verwertung von Fotografien des toten *Otto von Bismarck* zu untersagen. Erst 1907 reagierte der deutsche Gesetzgeber mit der Einführung des Rechts am eigenen Bild in §§ 22 ff. KUG. Es war eine – im Vergleich zu den USA – späte rechtliche Antwort auf den reproduktionstechnischen Fortschritt, beispielweise die immer kompakteren und günstigeren Fotoapparate[29] und die infolgedessen veränderten Rahmenbedingungen für einen Schutz von Privatsphäre.

Auf Grundlage von zivilrechtlichen Generalklauseln, einer weiten Auslegung von § 22 KUG und mithilfe des Urheberrechts gelang es allmählich, den Schutz der Persönlichkeit auszubauen.[30] Ab 1954 setzte der *BGH* mit seiner *Leserbrief*-Entscheidung[31] diese Entwicklung fort und erweiterte den Schutz von Persönlichkeitsrechten kontinuierlich.[32] Erst infolge der flächenmäßigen Einführung von Computern in die Verwaltung entschied sich das Land Hessen im Jahr 1970 für die Verabschiedung eines ersten Datenschutzgesetzes.[33]

2. Prägender Einfluss der (Rechts-)Soziologie

Das Datenschutzrecht wurde als besonderer Bereich des Persönlichkeitsrechts wesentlich durch rollensoziologische Erkenntnisse geprägt.[34] *Niklas Luhmann* wird für das Jahr 1970 eine – aus heutiger Sicht – eklatante Fehleinschätzung anekdotisch zugeschrieben:

„Recht und Datenverarbeitung haben miteinander genauso viel zu tun wie Autos und Rehe: Meist gar nichts, nur manchmal stoßen sie zusammen".[35]

---

ten damit, neue Technologien in das bestehende Rechtssystem einzuordnen. Hierzu: *Richards/Smart*, in: Calo/Froomkin/Kerr (Hrsg.), Robot Law, 2016, 3 (13 ff.).

[27] *Prosser*, 48 Cal. L. Rev. 1960, 383 (389 ff.); *McCarthy*, The rights to Publicity and Privacy, 2008, § 1:19–24.

[28] *RG*, Urt. v. 28.12.1899 – VI 259/99, RGZ 45, 170 (173). Mit Kritik am Urteil: *Kohler* GRUR 1900, 208 ff.

[29] Zur Geschichte des Rechts am eigenen Bild: *Götting*, Persönlichkeitsrechte als Vermögensrechte, 1995, S. 12 ff.

[30] RGZ 69, 401 (403) – *Nietzsche-Briefe*; Grundlegende Analyse bei: *Hubmann*, Das Persönlichkeitsrecht, 2. Aufl. 1967.

[31] BGHZ 13, 334 = NJW 1954, 1404 – *Leserbrief*; *BGH*, I ZR 266/52 = GRUR 1955, 201, *Cosima Wagner Tagebücher*.

[32] *BGH*, GRUR 1956, 427 – *Paul Dahlke*; BGHZ 26, 349 = *BGH*, NJW 1958, 827 – *Herrenreiter*; *BGH*, GRUR 1965, 254 – *Soraya*; Überblick bei: *Götting*, in: ders./Schertz/Seitz (Hrsg.), Handbuch der Persönlichkeitsrechte, (2008), Teil 2, Rn. 15 ff.

[33] Hess. GVBl. II 1970, 300-10. Zur Begründung: *Osswald* (Hessicher Ministerpräsident), Der Spiegel (Heft 20/1971), S. 88.

[34] Hierzu bereits ein Überblick: *Sattler*, in: Ochs/Friedewald/Hess/Lamla (Hrsg.), Die Zukunft der Datenökonomie, 2019, S. 213 (222 ff.).

[35] Zurückgehend auf einen Vortrag von *Herbert Fiedler*, zitiert nach *Konzelmann*, JurPC

Diese Annahme hat sich in mehrfacher Hinsicht umgekehrt. Während die Wahrscheinlichkeit eines Zusammenstoßes von Kfz und Reh infolge der Fortschritte im Bereich des automatisierten Fahrens und damit aufgrund von automatischer Datenverarbeitung zurückgehen, ist die Kollision von Recht und Datenverarbeitung mittlerweile keine Ausnahme, sondern die Regel, insbesondere sofern personenbezogene Daten involviert sind. Mit Blick auf dieses Bonmot ist es paradox, dass gerade *Luhmanns* Forschung einen wesentlichen Anteil an der Zunahme der Kollisionen hatte.

Der Bericht „Grundfragen des Datenschutzes" von 1971, den mehrere Autoren um *Wilhelm Steinmüller* im Auftrag des Bundesministerium des Inneren ausgearbeitet hatten,[36] beruhte maßgeblich auf den soziologischen Forschungsarbeiten von *Niklas Luhmann* und *Jürgen Habermas*.[37] Dieser Bericht wiederum prägte nicht nur die Systematik des ersten BDSG von 1977, sondern beeinflusste unmittelbar die rechtwissenschaftliche Diskussion und – jedenfalls mittelbar – das *Volkszählungsurteil* des *BVerfG* von 1983.

Eine wesentliche Schlussfolgerung des Berichts von *Steinmüller u. a.* war die Einschätzung, dass die traditionelle Trennung zwischen öffentlicher und privater Sphäre nicht länger als regulatorischer Ausgangspunkt geeignet sei:

> „Der Dualismus Staat – Gesellschaft wird den Problemen unserer Zeit nicht mehr gerecht. Vielmehr sind beide Bereiche untrennbar zu einem Gemeinwesen verschmolzen. Sie bilden eine Wirkungseinheit".[38]

Folgt man dieser Annahme einer *faktischen* Verschmelzung, so ist es konsequent, auch einen einheitlichen *regulatorischen* Ansatz zu wählen, unabhängig davon, ob die Datenverarbeitung durch eine Behörde oder durch ein Unternehmen erfolgt.[39] Zwar schlossen sich *Steinmüller u. a.* der Theorie der unmittelbaren Drittwirkung der Grundrechte nicht an. In der Sache griffen sie aber stark auf die Ansätze von *Hans Carl Nipperdey* und *Walter Leisner* zurück[40] und

---

110/2003, Abs. 36. Eine ähnliche Fehleinschätzung wird *Thomas Watson* (IBM) zugeschrieben, der nach anekdotischer Überlieferung im Jahr 1943 den weltweiten Bedarf an Computern mit fünf Exemplaren beziffert haben soll: *Maney*, The Maverick and his machine, 2003, S. 355 f.; Sieg der Mikrosekunde, in: Der Spiegel, Nr. 22, 1965, S. 52 f.

[36] *Steinmüller/Lutterbeck/Malmann/Harbort/Kolb/Schneider*, Grundfragen des Datenschutzes, Gutachten im Auftrag des Bundesministeriums des Innern, 1971, BT Drs. VI/3826, S. 84 ff.

[37] Der Bericht zitiert insbesondere: *Luhmann*, Grundrechte als Institution. Ein Beitrag zur politischen Soziologie, 1965; *ders.*, Recht und Automation in der öffentlichen Verwaltung, 1966; *Habermas*, Strukturwandel der Öffentlichkeit: Untersuchungen zu einer Kategorie der bürgerlichen Gesellschaft, 1962. Zur Kritik hieran, unten II.1.

[38] *Steinmüller u. a.*, Grundfragen des Datenschutzes, Gutachten im Auftrag des Bundesministeriums des Innern, 1971, BT Drs. VI/3826, S. 35.

[39] So aktuell auch: *Roßnagel*, in: Simitis/Hornung/Spiecker gen. Döhmann (Hrsg.), 2019, Art. 6 Rn. 2.

[40] In diesem Zusammenhang werden u. a. *Nipperdey* (Grundrechte und Privatrechte, ders. (Hrsg.), in: FS Molitor, 1962, 17 ff.), *Hesse* (Der Rechtsstaat im Verfassungssystem des Grund-

kamen infolgedessen zu einer sehr weitgehenden Anwendbarkeit von Verfassungsrecht im Privatrecht.[41]

Der Regierungsentwurf eines „Gesetzes zum Schutz vor Mißbrauch personenbezogener Daten bei der Datenverarbeitung" von 1973 übernahm diesen nahezu einheitlichen, vorsorgenden Ansatz.[42] Immerhin unterschied das letztlich verabschiedete BDSG von 1977 noch ansatzweise zwischen der Datenverarbeitung durch öffentliche Stellen und – mit symptomatischer Wortwahl für diesen einseitig ausgerichteten Ansatz – der Datenverarbeitung durch „nicht-öffentliche Stellen",[43] also durch (juristische) Personen des Privatrechts.

3. Prägung durch Erfahrungen der nationalsozialistischen Diktatur

Dass (West-)Deutschland ein Vorreiter im Bereich des Datenschutzrechts war,[44] ist nicht nur auf die Einführung erster Computer in der Verwaltung zurückzuführen.[45] Vielmehr wurde der einheitliche datenschutzrechtliche Regelungsansatz auch durch die Erfahrungen in der NS-Diktatur geprägt. Die seinerzeitige Auseinandersetzung mit der nationalsozialistischen Diktatur hatte grundlegenden Einfluss auf die Ausgestaltung des deutschen Datenschutzrechts. Dies wird am Bericht von *Steinmüller u. a.* deutlich. Darin erläutern die Autoren die Gefahren der Verarbeitung von personenbezogener Information anhand eines besonders wirkmächtigen – die historischen Bezüge gleichwohl noch verharmlosenden – Beispiels („*X ist Jude und auszuweisen*").[46]

Die Beispiele in der Studie – als weiteres Beispiel: „*Y ist Student und* [politisch] *links*" – sind im Kontext der historischen Erfahrung zulässig. Allerdings wähl-

---

gesetzes, in: Hesse u. a. (Hrsg.), FS Smend, 1962, 71 ff.), *Stein* (Lehrbuch des Staatsrechts, 1968) und *Leisner* (Grundrechte und Privatrecht, 1960) zitiert.

[41] So ausdrücklich *Walter Schmidt*: „Insofern ist das zwingende Privatrecht heute nichts anders als konkretisiertes Verfassungsrecht", *ders.*, JZ 1974, 241 (247).

[42] RegE BDSG, BT-Drs. 7/1027, S. 14: „Wir stehen zwar erst am Anfang dieser Entwicklung, dennoch ist der Gesetzgeber bereits jetzt aufgerufen, sie durch geeignete Maßnahmen so zu steuern, daß schwerwiegende und kaum reparable Schäden nicht erst eintreten und die Privatsphäre des einzelnen angesichts des technischen Fortschritts, den wir alle wünschen, unangetastet bleibt."

[43] Das Gesetz zum Schutz vor Missbrauch personenbezogener Daten bei der Datenverarbeitung (BDSG) vom 27.01.1977, BGBl. Teil I vom 01.02.1977, S. 201 ff. regelte im Abschnitt 2 die Datenverarbeitung durch Behörden und sonstige öffentliche Stellen. Die Abschnitte 3 und 4 regelten die Verarbeitung von personenbezogenen Daten durch „nicht-öffentliche Stellen", abhängig davon, ob die Verarbeitung zu eigenen Zwecken oder für fremde Zwecke erfolgte.

[44] *Simitis*, BDSG, 2014, Einleitung, Rn. 82. Zu den zeitgleichen Anfängen des Datenschutzes in den USA durch den Fair Credit Reporting Act (1970), 15 U.S.C. § 1681 und den Federal Privacy Act (1974), 5 U.S.C. § 552: *Buchner*, Die Informationelle Selbstbestimmung im Privatrecht, 2006, S. 6 ff.

[45] Der Hessische Ministerpräsident begründete das Hessische Datenschutzgesetz von 1970 (Hess. GVBl. II 1970, 300-10) mit der flächenmäßigen Einführung von Computern in die Verwaltung: *Osswald*, Der Spiegel (Heft 20/1971), S. 88.

[46] *Steinmüller* u. a. (Hrsg.), 1971, 55 ff., BT Drs. VI/3826.

ten die Autoren damit zugleich einen Ausgangspunkt, den man heute als ein, für ein wissenschaftliches Rechtsgutachten ungünstiges *Framing* beanstanden kann.

4. Extensive Auslegung der verfassungsgerichtlichen Urteile

Zuletzt wird rückblickend deutlich, dass das Urteil des *BVerfG* vom 15.12.1983[47] anschließend durch den Gesetzgeber sehr extensiv interpretiert wurde. Mit diesem Urteil hat das *BVerfG* das Gesetz über eine Volks-, Berufs-, Wohnungs- und Arbeitsstättenzählung vom 25.03.1982[48] (Volkszählungsgesetz) für mit dem Grundgesetz unvereinbar erklärt. Bekanntlich leiteten die Verfassungsrichter in ihrem Urteil[49] ein Recht auf informationelle Selbstbestimmung aus dem allgemeinen Persönlichkeitsrecht ab.[50] Nach Ansicht des *BVerfG* hatte sich das Gefährdungspotenzial für das Individuum aufgrund einer Verarbeitung von personenbezogenen Daten infolge des technischen Fortschritts erheblich verändert. Deshalb müsse die Entscheidung darüber, wer personenbezogene Daten erheben, verarbeiten und nutzen darf,[51] grundsätzlich bei der jeweiligen natürlichen Person liegen.[52] Um das Recht auf informationelle Selbstbestimmung gegen Beeinträchtigungen zu schützen, verpflichtete das *BVerfG* den Gesetzgeber, Verfahren zum Schutz der Datensubjekte („Betroffene") vorzusehen und zusätzlich organisatorische Schutzmaßnahmen einzuführen.[53]

Gegenstand der Verfassungsbeschwerden war die Eingriffsverwaltung gegenüber Bürgern auf Grundlage des Volkszählungsgesetzes.[54] Somit entschied das *BVerfG* nur

> „über die Tragweite dieses Rechts *für Eingriffe*, *durch* welche *der Staat* die Angaben personenbezogener Daten vom Bürger verlangt".[55]

Die Frage einer möglichen Drittwirkung im Privatrechtsverhältnis war nicht entscheidungserheblich und wurde auch nicht ausdrücklich angesprochen. Des-

---

[47] BVerfGE 65, 1 = NJW 1984, 419 – *Volkszählung*; bereits zuvor zu den Grenzen staatlicher Erhebung von personenbezogenen Daten als Schutz des engeren Lebensbereichs vor staatlicher Ausforschung: BVerfGE 27, 1 (7) – *Mikrozensus.*

[48] BGBl. I, S. 369.

[49] Laut *Hoffmann-Riem* die „Magna Charta" des Datenschutzrechts, *ders.*, AöR 123 (1998), 513 (515).

[50] Dabei handelt es sich nach Ansicht von *di Fabio* nicht um ein neues Grundrecht, sondern einen neuen Begriff, der die Selbstdarstellung als Bestandteil des Privatsphärenschutzes lediglich interpretatorische fortschreibt, *ders.*, in: Maunz/Dürig, GG, 2011, Art. 2 Rn. 173.

[51] Nach aktueller Terminologie gemäß Art. 4 Nr. 2 DS-GVO insgesamt: Verarbeitung.

[52] BVerfGE 65, 1 (43) – *Volkszählung.*

[53] Die vom *BVerfG* geforderten Maßnahmen umfassen die Pflicht, den Betroffenen zu informieren, die Art und Weise der Datenverarbeitung zu erläutern und die personenbezogenen Daten anschließend zu löschen: BVerfGE 65, 1 (48 ff.) – *Volkszählung.*

[54] Gesetz über eine Volkszählung, Berufszählung, Wohnungszählung und Arbeitsstättenzählung vom 25.03.1982 (BGBl. I S. 369).

[55] BVerfGE 65, 1 (44 f.) – *Volkszählung* [Hervorhebung durch den Verfasser].

halb lässt sich der Urteilsbegründung keine eindeutige Aussage entnehmen, ob und inwieweit das Recht auf informationelle Selbstbestimmung nach Ansicht des *BVerfG* auch Auswirkungen im Rechtsverhältnis zwischen Privatrechtsubjekten entfalten sollte.[56]

Allerdings enthielt das *Volkszählungsurteil* mehrere generalisierende Aussagen, die sich als umfassenden Regelungsauftrag interpretieren lassen. Bekannt und häufig zitiert ist die Aussage:

„[I]nsoweit gibt es unter den Bedingungen der automatischen Datenverarbeitung kein belangloses Datum mehr".[57]

Dieser Satz ließ sich aus Sicht der Legislative als Einladung dazu interpretieren, die Bedeutung des Rechts auf informationelle Selbstbestimmung auf den Bereich des Privatrechts auszudehnen.[58] Auch die Bezugnahme des Urteils auf die „soziale Umwelt",[59] bot einen Ansatzpunkt für ein derart weites Verständnis.[60]

Im Anschluss an das *Volkszählungsurteil* entwickelte das *BVerfG* das Recht auf informationelle Selbstbestimmung stetig fort, um die Bürger vor staatlichen Maßnahmen zu schützen, die in ihre Privatsphäre eingriffen.[61] Zudem leitete das *BVerfG* mit dem Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme ein weiteres IT-Grundrecht[62] aus Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG ab.[63] Überdies bestätigte das *BVerfG* diesen grundrechtlichen Abwehranspruch wiederholt gegen die Tendenz von Exe-

---

[56] Die Urteilsbegründung des BVerfG war hinsichtlich der Reichweite des Rechts auf informationelle Selbstbestimmung ambivalent BVerfGE 65, 1 = NJW 1984, 419 (422/Rn. 44 f.) – *Volkszählung*: „Die Verfassungsbeschwerden geben keinen Anlass zu erschöpfenden Erörterungen des Rechts auf informationelle Selbstbestimmung. Zu entscheiden ist nur über die Tragweite des Rechts für Eingriffe, durch welche der Staat die Angabe personenbezogener Daten vom Bürger verlangt." Diese salomonische Formulierung ließ unterschiedliche Interpretationen zu, je nachdem, ob man den ersten (nicht erschöpfend) oder den zweiten Satz („durch welche der Staat) betonte.

[57] BVerfGE 65, 1 (43) = NJW 1984, 419 (422) – *Volkszählung*.

[58] Hierfür plädierte: *Simitis*, NJW 1984, 398 (401).

[59] BVerfGE 65, 1 (42) = NJW 1984, 419 (422) – *Volkszählung*: „Wer nicht mit hinreichender Sicherheit überschauen kann, welche ihn betreffende Informationen in bestimmten Bereichen seiner *sozialen Umwelt* bekannt sind, und wer das Wissen möglicher Kommunikationspartner nicht einigermaßen abzuschätzen vermag, kann in seiner Freiheit wesentlich gehemmt werden, aus eigener Selbstbestimmung zu planen oder zu entscheiden. Mit dem Recht auf informationelle Selbstbestimmung wären eine *Gesellschaftsordnung* und eine diese ermöglichende Rechtsordnung nicht vereinbar, in der Bürger nicht mehr wissen können, wer was wann und bei welcher Gelegenheit über sie weiß". [Hervorhebungen durch den Verfasser].

[60] In diese Richtung weiterhin: *Brink*, in: Wolff/Brink (Hrsg.), BeckOK Datenschutzrecht, 30. Ed., Stand: 01.11.2017, Verfassungsrechtliche Grundlagen, Rn. 140; *Spiecker gen. Döhmann*, in: Vesting/Korioth (Hrsg.), Der Eigenwert des Verfassungsrechts, 2011, S. 263 (266).

[61] BVerfG 109, 279 = NJW 2004, 999 – *Lauschangriff*; BVerfGE 130, 151 = NJW 2012, 1419 – *Telekommunikationsdaten*; BVerfGE 133, 277 = NJW 2013, 1499 – *Antiterrordatei*.

[62] *Luch*, MMR 2011, 75 (78 f.)

[63] BVerfGE 120, 274 = NJW 2008, 822 – *Online Durchsuchung*; hierzu: *di Fabio*, NJW 2008, 424 ff.

kutive und Legislative, die Schranken der grundrechtlich gewährten Freiheiten im Interesse der Bekämpfung von Terrorismus und Straftaten auszudehnen.[64]

Retrospektiv fällt auf, dass das *BVerfG* den Begriff des *Rechts* auf informationelle Selbstbestimmung bis heute unverändert verwendet und dadurch sprachlich einen Unterschied zum deutlich jüngeren *Grundrecht* auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme aufrechterhält.[65] Bedeutender als die sprachliche Ambivalenz in den Urteilen des *BVerfG* ist jedoch der in der Folge des *Volkszählungsurteils* vom deutschen Gesetzgeber beibehaltene und – im Anschluss hieran – vom europäischen Gesetzgeber übernommene,[66] weitgehend einheitliche, grundrechtlich geprägte Ansatz zum Schutz personenbezogener Daten. Im Ergebnis beeinflussten die Entscheidungen des *BVerfG* auch den Datenschutz im Privatrecht direkt.

Die aus privatrechtlicher Perspektive frühzeitig geäußerte Warnung davor, aus den Grundrechten *unmittelbare* Folgen auch für das Privatrechtsverhältnis abzuleiten, verhallte ungehört.

II. Folgenlose Kritik am einheitlichen Schutzansatz

Im Ergebnis war das *Volkszählungsurteil* die Quintessenz einer langjährigen Diskussion in der (verfassungsrechtlichen) Wissenschaft. Es wurde deshalb von der Mehrheit der wissenschaftlichen „Vordenker" als Durchbruch gefeiert.[67] Dennoch wurde im Anschluss an das Urteil aus privatrechtlicher Perspektive eine stärkere Differenzierung zwischen staatlicher Eingriffsverwaltung und grundrechtlicher Gewährleistung in Form von Schutzpflichten im privatrechtlichen Bereich gefordert.

Die Kritik war grundlegend und knüpfte bereits an die maßgebliche Prägung des Berichts von *Steinmüller u. a.* durch die Arbeiten der Frankfurter Schule der Sozialwissenschaften an (1). Zudem wurde aus privatrechtlicher Perspektive die Umsetzung des Rechts auf informationelle Selbstbestimmung im Datenschutzrecht als überschießend kritisiert (2).

---

[64] Zur Unvereinbarkeit von Art. 2 Nr. 2 des sog. Gesetzes zur Vorratsdatenspeicherung (Gesetz zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten vom 10. Dezember 2015 (BGBl. I S. 2218 ff.) mit Art. 15 I der ePrivacy-RL (2002/58/EG): *EuGH*, C-203/15 und C-698/15. Im Anschluss hieran *OVG Münster*, Beschl. v. 22.06.2017, Az. 13 B 238/17. Zur einstweiligen Aussetzung der auf Art. 2 Nr. 2 Art. 2 Nr. 2 des sog. Gesetzes zur Vorratsdatenspeicherung beruhenden § 113b TKG geregelten Speicherverpflichtungen: Bundesnetzagentur, Mitteilung vom 28.06.2017.

[65] BVerfGE 120, 274 (Rn. 167 f./196/198 ff./309 f./314 ff.) = NJW 2008, 822 – *Online Durchsuchung*.

[66] Hierzu: *Marsch*, Das Europäische Datenschutzgrundrecht, 2018, S. 248 ff.

[67] *Steinmüller*, DuD 1984, 91 (92): „Manches liest sich wie ein Destillat aus 15 Jahren zunächst unbeachteter Vorarbeiten".

1. Kritik am rechtssoziologisch determinierten Zeitgeist

Insbesondere *Horst Ehmann* beanstandete, dass aus soziologischen Erkenntnissen unmittelbare rechtliche Konsequenzen gezogen wurden.[68] Nach seiner Ansicht hatten die Autoren um *Steinmüller* die Aussagen von *Luhmann* zudem missverstanden.[69] Aus *Luhmanns* Interaktionenlehre und Rollentheorie könnten eher Argumente gegen eine weite Auslegung des Rechts auf informationelle Selbstbestimmung und dessen Expansion ins Privatrecht abgeleitet werden.

Tatsächlich hatte *Luhmann* bereits mit Blick auf das Verwaltungsrecht selbst vor der Gefahr gewarnt, dass eine zu umfangreiche grundrechtliche Anerkennung der Entfaltungsmöglichkeiten von Individuen „die öffentlichen Interessen in die enger und enger geflochtenen Maschen des Verfassungsrechts treibt".[70] Danach münde eine zu umfassende „Verrechtlichung"[71] in die Sisyphusarbeit,

> „die von den Gipfeln der Grundrechte herabrollende Problematik aufzufangen und wieder nach oben zu wälzen, stets in Versuchung, schon auf halber Höhe ein Pathos anzuwenden, das nur Göttern ziemt".[72]

Die Kritik *Ehmanns* am Bericht von *Steinmüller u. a.* (1972) setzte sich in seiner Skepsis gegenüber dem *Volkszählungsurteil* fort, zumal die Vermutung nahelag, dass der Bericht nicht nur dem BDSG von 1977, sondern auch dem *Volkszählungsurteil* des *BVerfG* als Blaupause gedient hatte.[73]

Leider hielten es die Verfassungsrichter seinerzeit nicht für erforderlich, die rechtssoziologischen Ursprünge des Rechts auf informationelle Selbstbestimmung durch ein Zitat des Berichts von *Steinmüller u. a.* oder auch nur ihrer eigenen Vorarbeiten und die der anderen Verfahrensbeteiligten offenzulegen.[74] Insofern vermittelt bereits das *Volkszählungsurteil* teilweise den Eindruck, das Recht auf informationelle Selbstbestimmung sei – göttergleich – zur Erde gefallen.

---

[68] *Ehmann*, AcP 188 (1988), 230 (335).

[69] *Ehmann*, AcP 188 (1988), 230 (323/336 ff.).

[70] *Luhmann*, Grundrechte als Institution, 1965, S. 80.

[71] *Ehmann*, AcP 188 (1988), 230 (335). Ähnlich warnt *Hoffmann-Riem* im Zusammenhang mit dem Recht auf informationelle Selbstbestimmung davor, dass ohne eine „funktional-teleologische Interpretation" die „Verrechtlichung des Alltäglichen" droht, *ders.*, AöR 123 (1998), 513 (527 f.).

[72] *Luhmann*, Grundrechte als Institution, 1965, S. 59.

[73] Der vom BVerfG gewählte Begriff des Rechts auf informationelle Selbstbestimmung erinnert deutlich an das im Bericht vorgeschlagene „Recht auf Selbstbestimmung über Individualinformationen" bzw. „informationelle Selbstbestimmungsrecht" *Steinmüller u. a.* Grundfragen des Datenschutzes, Gutachten im Auftrag des Bundesministeriums des Innern, 1971, BT Drs. VI/3826, 84 (93 und 139). Hierzu ausführlich: *Ehmann*, AcP 188 (1988), 230 (229 ff.).

[74] Hierzu ausführlich: *Ehmann*, AcP 188 (1988), 230 (330/Fn. 446).

2. Kritik an der überschießenden Umsetzung des RaiS

Die „Vordenker" des Rechts auf informationelle Selbstbestimmung waren zugleich die „Nachdenker" des *Volkszählungsurteils*. Sie interpretierten das Urteil extensiv und plädierten anlässlich der anschließenden Reformvorschläge dafür, die Anforderungen, die das *BVerfG* dem Gesetzgeber für staatliche Grundrechtseingriffe auferlegt hatte, auf den Bereich der Datenverarbeitung durch Private zu übertragen.[75]

Hiergegen wendeten sich mehrere Rechtswissenschaftler mit privatrechtlichem Hintergrund (insbesondere *Ehmann*, *Krause* und *Zöllner*). Ihrer Ansicht nach hatte das *BVerfG* das Recht auf informationelle Selbstbestimmung aus dem allgemeinen Persönlichkeitsrecht für das Verhältnis zwischen Bürger und Staat und ausschließlich als Schranken-Schranke entwickelt, um dadurch den Gesetzgeber bei einer Konstitution von gesetzlichen Schranken des APR (Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG) – beispielweise durch das streitgegenständliche Volkszählungsgesetz – zu Normenklarheit zu zwingen.[76]

Eine unmittelbare Drittwirkung für das Privatrecht könne aus dem *Volkzählungsurteil* nicht abgeleitet werden. [77] Die Tendenz, einzelne Sätze aus dem Urteil auch zur Regulierung des privaten Informationsverkehrs unmittelbar anzuwenden, sei eine abzulehnende „Schmalspurjurisprudenz".[78] Anzuerkennen sei allenfalls eine mittelbare Drittwirkung im Rahmen der Auslegung von zivilrechtlichen Vorschriften, insbesondere der Generalklauseln zum Schutz des APR und innerhalb des BDSG. Eine solche mittelbare Drittwirkung sei

> „gar nicht zu vermeiden, sie findet kraft der Bewusstseinsänderungen, die das Volkszählungsurteil und die gesamte Datenschutzkampagne ausgelöst haben, nahezu unvermeidbar in allen juristischen Köpfen statt, die vom Pathos des [Rechts auf informationelle Selbstbestimmung] getroffen worden sind".[79]

Unverkennbar war das *Volkzählungsurteil* ein Kristallisationspunkt für unterschiedliche rechtspolitische und sogar ideologische Auffassungen darüber, welche Reichweite dem gesetzlichen Datenschutz künftig eingeräumt werden sollte. Diese Auseinandersetzung über die Reichweite des Schutzes ist damit zu-

---

[75] Vgl. Anhörungsverfahren zu den Entwürfen eines Gesetzes zur Änderung des BDSG, Kurzprotokoll des Innenausschusses des 10. Deutschen Bundestages, 110. Sitzung, BT-Drs. 10/1180, S. 125 (*Podlech*) und S. 104 (*Gallwas*: „jede Erhebung, jegliche Übermittlung, jegliche Nutzung von Daten [ist] zu einem Eingriff geworden").

[76] *Ehmann*, AcP 188 (1988), 230 (301 f.).

[77] *Ehmann*, AcP 188 (1988), 230 (303 ff.).

[78] *Zöllner*, RDV 1985, 3 (5).

[79] *Ehmann*, AcP 188 (1988), 230 (303). *Ehmann* unterschied zwischen dem Recht auf informationelle Selbstbestimmung (RaiS) und der erweiterten – und nach seiner Ansicht abzulehnenden – Interpretation als Grundrecht auf informationelle Selbstbestimmung (GRaiS).

gleich ein wichtiger Ausschnitt aus der umfangreichen, bis heute andauernden Diskussion über das Verhältnis zwischen Verfassungs- und Privatrecht.[80]

Wie tief die Gräben der Auseinandersetzung über die Ausgestaltung des Datenschutzrechts verliefen, verdeutlicht ein Vorwurf von *Horst Ehmann*. Er ist der Ansicht, dass die Drittwirkung des Rechts auf informationelle Selbstbestimmung den Befürwortern eines umfassenden Datenschutzrechts seinerzeit dazu diente, um

> „die durch die starke Sozialbindung des Eigentums gebrochene Ideologie eines nur durch Klassenkampf zu überwindenden Interessengegensatzes zwischen Besitzenden und Nichtbesitzenden [zu] ersetzen durch den Interessengegensatz zwischen Wissenden und Unwissenden, zwischen Datenverarbeitern und davon Betroffenen, um daraus eine neue Rechtfertigung für die Fortführung des Klassenkampfes zur Herstellung einer klassen- und autoritätslosen Gesellschaft abzuleiten. […] Unter den Voraussetzungen dieser neuen Kampfziele ist eine vernünftige Interessenabwägung zwischen notwendigem Informationsschutz und erforderlicher Informationsfreiheit praktisch unmöglich".[81]

Ehmann wollte die „verfehlte These" begrenzen,[82] wonach jedes personenbezogene Datum an sich bereits schutzwürdig sei.[83] Nach seinem Verständnis hatte das *BVerfG* das Recht auf informationelle Selbstbestimmung auf die massenhafte automatisierte Verarbeitungen von Daten beschränkt.

Deshalb könne es nicht dazu dienen, auch die nicht automatisierte Datennutzung im Privatrechtsverkehr dem gleichen „Informationsverbot" zu unterwerfen.[84] Die verfassungsrechtliche Literatur habe insoweit einen über das Urteil hinausgehenden Prinzipienwechsel vollzogen, indem sie dem Recht auf informationelle Selbstbestimmung einen grundsätzlichen Vorrang vor den Grundrechten aus Art. 2, 5, 12 und 14 GG eingeräumt habe, obwohl letztere die Hand-

---

[80] Hierzu jeweils m. w. N.: *Schmidt-Rimpler*, AcP 147 (1941), 130 ff.; *Nipperdey*, Grundrechte und Privatrecht, 1961; *M. Wolf*, Rechtsgeschäftliche Entscheidungsfreiheit und vertraglicher Interessenausgleich, 1970; *Raiser*, Die Zukunft des Privatrechts, 1971; *E. A. Kramer*, Die Krise des liberalen Vertragsdenkens, 1974; E. *v. Hippel*, Der Schutz des Schwächeren, 1982; *Hönn*, Kompensation gestörter Vertragsparität, 1982; *Canaris*, AcP 184 (1984), 201 ff.; *Rittner*, AcP 188 (1988), 101 ff.; *Hesse*, Verfassungsrecht und Privatrecht, 1988; *Dietlein*, Die Lehre von den grundrechtlichen Schutzpflichten, 1992; *Lerche*, in: Baur u. a. (Hrsg.), FS Steindorff, 1990, 897 ff.; *Fastrich*, Richterliche Inhaltskontrolle im Privatrecht, 1992; *Wiedemann*, JZ 1994, 411; *Hager*, JZ 1994, 373; *Zöllner*, AcP 196 (1996), 1; *Drexl*, Die wirtschaftliche Selbstbestimmung der Verbraucher, 1998; *Ruffert*, Vorrang der Verfassung und Eigenständigkeit des Privatrechts, 2011; sowie Teil 2, in: Möslein (Hrsg.), Private Macht, 2016; *Starke*; EU-Grundrechte und Vertragsrecht, 2016; *Schmolke*, Grenzen der Selbstbindung im Privatrecht, 2014; *Hellgardt*, Regulierung und Privatrecht, 2016; *Lüttringhaus*, Vertragsfreiheit und ihre Materialisierung im Europäischen Binnenmarkt, 2018. Für das 19. Jahrhundert: *Kaiser*, Zum Verhältnis von Vertragsfreiheit und Gesellschaftsordnung während des 19. Jahrhunderts, 1972.

[81] *Ehmann*, AcP 188 (1988), 230 (261/298 f.).

[82] *Ehmann*, AcP 188 (1988), 230 (267).

[83] Dies findet aktuell in der Forderung einer restriktiven Auslegung der Anforderungen der DS-GVO Widerhall: *Leistner/Antoine/Sagstetter*, Big Data, 2021, S. 226/260.

[84] *Zöllner*, RDV 1985, 3 (15); *Krause*, JZ 1984, 656 (657); *Ehmann*, AcP 188 (1988), 230 (267).

lungs- und Informationsfreiheit der Bürger schützen. Dieser Prinzipienwechsel sei jedenfalls jenseits von einer automatischen Datenverarbeitung und für bloße Datenverwendungen nicht gerechtfertigt.[85] Während die Bindung einer Datenverarbeitung an den ursprünglichen Zweck im öffentlichen Bereich die bürgerliche Freiheit durch Einschränkung der Staatsmacht schütze, würden durch die Zweckbindung der Datennutzung im privaten Bereich mehr bürgerliche Freiheiten eingeschränkt als gewährleistet.[86] Insofern sei die Bindung der Datenverarbeitung an einen vorher bestimmten Zweck praktisch unbrauchbar und verfassungsrechtlich nicht zu rechtfertigen.[87]

3. Fazit: Fehlende privatrechtliche Unterfütterung des Datenschutzes

Rückblickend lässt sich denjenigen Privatrechtswissenschaftlern, welche die Konsequenzen des *Volkszählungsurteils* auf das Verfassungs- und Verwaltungsrecht beschränken oder allenfalls eine Schutzpflicht des Staates im Bereich der automatisierten Verarbeitung von Daten anerkennen wollten, vorwerfen, dass sie die Gefahren der Datenverarbeitung durch Private unterschätzt haben.

Zwar ist ihr Plädoyer konsequent, wonach die durch einen allwissenden und allmächtigen Staat drohenden Gefahren nicht mit denjenigen vergleichbar seien, die durch eine *nicht automatisierte* private Datensammlungen entstehen können. Auch die Verteidigung der Neugier[88] und des „Gebots der Lebensklugheit", möglichst viel über andere Menschen und deren Beziehungen zueinander wissen zu wollen,[89] sind im Grundsatz überzeugend.[90]

Allerdings gleicht diese Verteidigung der Privatautonomie für den Bereich der *nicht automatisierten* Datenverarbeitung aus heutiger Sicht einem Kampf gegen Windmühlen. Die Bereiche, in denen Daten nicht automatisiert verarbeitet werden, sind seitdem drastisch zurückgegangen. Insofern war die dem *Volkszählungsurteil* zugrunde gelegte tatsächliche Analyse der technischen Verarbeitungsmöglichkeiten zutreffend. Der seit Verkündung des *Volkszählungsurteils* eingetretene technische Fortschritt im Bereich der automatisierten Datenverarbeitung (sog. *ubiquitous computing*)[91] begünstigte den sich daran

---

[85] *Ehmann*, AcP 188 (1988), 230 (289).

[86] *Ehmann*, AcP 188 (1988), 230 (322).

[87] *Ehmann*, AcP 188 (1988), 230 (329); *Zöllner*, RDV 1985, 3 (13); *Krause*, Kurzprotokoll des Innenausschusses des 10. Deutschen Bundestages, 110. Sitzung, BT-Drs. 10/1180, S. 85. Zuletzt: *Giesen*, JZ 2007, 918 (927): „Der Gesetzgeber des BDSG hat die beiderseitigen Rechtspositionen der Datenverarbeiter und der Betroffenen unzureichend erkannt und ihren Konflikt in einer Schieflage zwischen Verstößen gegen das Übermaß- und das Untermaßverbot verfassungswidrig zu lösen versucht".

[88] *Ehmann*, AcP 188 (1988), 230 (287)

[89] *Ehmann*, AcP 188 (1988), 230 (326).

[90] Dies wieder aufgreifend: *Giesen*, JZ 2007, 817 (921).

[91] Hierzu *Roßnagel/Müller*, CR 2004, 625 ff.; *Kühling*, DV 40 (2007), 153 ff.

anschließenden, nahezu einheitlichen Ansatz des deutschen und im Anschluss hieran, unionsrechtlichen Datenschutzrechts.

Als Konsequenz der extensiven Interpretation des *Volkszählungsurteils* wurden die Anforderungen an eine rechtmäßige Datenverarbeitung zunehmend angeglichen, unabhängig davon, ob die Verarbeitung durch eine öffentliche oder eine „nicht-öffentliche Stelle" erfolgt. Die hieran aus privatrechtswissenschaftlicher Perspektive geäußerten Bedenken blieben folgenlos. Nach einer grundlegenden Kritik in den 1980er Jahren kehrten die Privatrechtswissenschaftler dem Datenschutzrecht den Rücken zu und überließen das Feld der öffentlich-rechtlichen und insbesondere – genährt durch weitere Urteile des *BVerfG* – der verfassungsrechtlichen Perspektive.[92] Diese Entwicklung wurde in zweifacher Hinsicht begünstigt:

Erstens wurden traditionelle Kommunikationsinfrastrukturen zunehmend privatisiert. Daraus erwuchsen dem Staat zusätzliche Gewährleistungspflichten in Form einer Privatisierungsfolgenverantwortung,[93] vgl. Art. 87f Abs. 1 GG. Soweit neue – insbesondere internetbasierte – Kommunikationstechniken aufkamen, wurden diese von Anfang an privatrechtlich bereitgestellt. Mit steigender Bedeutung der durch Privatrechtsubjekte bereitgestellten Kommunikations-Infrastruktur nahm auch das von privater Seite ausgehende Gefährdungspotenzial zu. Die „privatisierten Leviathane"[94] rückten ins Zentrum der rechts- und sozialstaatlichen Aufmerksamkeit. Zu den traditionellen Gefährdungen infolge des staatlichen Gewaltmonopols trat ein neues Gefahrenpotenzial infolge der ökonomischen Marktmacht von Unternehmen.[95] Diese technischen und wirtschaftlichen Entwicklungen begünstigen einen Regulierungsansatz, der jegliche Verarbeitung von personenbezogenen Daten unter den Anwendungsbereich des Datenschutzrechts bringt.[96] Er mündet in eine informationelle Prophylaxe oder – im datenschutzrechtlichen Jargon – in einen präventiven Vorfeldschutz.[97]

---

[92] Obwohl der führende Kommentar zum Datenschutzrecht von *Spiros Simitis* (Hessischer Datenschutzbeauftragter von 1975–1991) und damit von einem Privatrechtswissenschaftler bearbeitet wurde, wurde der Kommentar wegen seiner geringen privatrechtlichen Fundierung kritisiert: Hierzu: *Giesen*, JZ 2007, 918 (924 f./Fn. 43).

[93] *Bauer*, VVDStRL 54 (1995), 243 (278 f.).

[94] *Hoffmann-Riem*, 123 AöR (1998), 512 (525).

[95] *BVerfG*, Beschl. v. 22.05.2019, 1 BvQ 42/19 = NJW 2019, 1935 (Rn. 15) – *Nutzung sozialer Netzwerke*.

[96] Zur Videoüberwachung: *Bull*, JZ 2017, 797 (800): „basiert auf einer abstrakten Gefährlichkeitsvermutung, die das Datenschutzrecht in seiner herrschenden Interpretation charakterisiert – ein wesentlicher Grund für den verbreiteten freiheitsfeindlichen Datenpaternalismus. […] Datenschutz wird zum Selbstzweck."

[97] *Brink/Eckhardt*, ZD 2015, 205 (209): „Wesentliche Leistung der Volkszählungsentscheidung war nämlich, dem ‚Verletzungsdelikt APR' ein ‚Gefährdungsdelikt iSB' [zur Seite zu stellen]. Die Umkehr der Rechtfertigungslast für Datenverwendungen zielt gerade darauf ab, Vorfeldschutz schon gegen Rechtsgefährdungen zu leisten". *Marsch* führt diese Entwicklung

Zweitens begünstigte die geringe Durchsetzung des Datenschutzrechts,[98] dass dieses Rechtsgebiet in der Privatrechtswissenschaft eine Nischenexistenz führte.[99] Die durch einen Verstoß verursachten individuellen Streuschäden lohn(t)en keine individuelle gerichtliche Durchsetzung. Die möglichen, aber seltenen verwaltungsrechtlichen Bußgelder ließen keine großen finanziellen Belastungen befürchten.[100] Das Interesse der Privatrechtswissenschaft beschränkte sich auf die wenigen Sachverhalte mit ökonomischer Relevanz.[101] Infolgedessen blieben die privatrechtlichen Auswirkungen des *Volkszählungsurteils*[102] und des Datenschutzrechts lange Zeit unterbelichtet.

Die Aufmerksamkeit für das Datenschutzrecht nahm erst im Vorfeld der Anwendbarkeit der DS-GVO ab 25.05.2018 schlagartig zu. Dies lässt sich einerseits auf die potenziell hohen Bußgelder bei Verstößen gegen die DS-GVO, aber auch damit erklären, dass die Geschäftsmodelle, die auf eine umfangreiche Verarbeitung von personenbezogenen Daten angewiesen sind, in den letzten Jahren rasant zunehmen.[103]

B. Asymmetrische Grundrechtssensibilität der DS-GVO

Parallel zum nationalen Datenschutzrecht nahm das *Europäische Parlament* mehrfach Anlauf, um die Datenschutzrechte der Mitgliedstaaten zu harmonie-

---

auf das Fehlen eines klar konturierten Schutzguts zurück: *ders.*, Das Europäische Datenschutzgrundrecht, 2018, S. 87 ff./256 ff./260.

[98] *Giesen*, JZ 2007, 918 (926: „grotesk" geringe Durchsetzung).

[99] Ausnahmen: *Buchner*, Die Informationelle Selbstbestimmung im Privatrecht, 2006; *Unseld*, Die Kommerzialisierung von personenbezogenen Daten, 2010; *Specht*, Konsequenzen der Ökonomisierung informeller Selbstbestimmung, 2012. Im Arbeitsrecht war das Datenschutzrecht dagegen kontinuierlich Gegenstand wissenschaftlicher Untersuchungen.

[100] Zur insgesamt niedrigen Anzahl an Bußgeldern vor Anwendbarkeit der DS-GVO: *Ashkar*, DuD 2015, 796 (797); zu den Unterschieden bei der Verhängung von Bußgeldern zwischen des Bundesländern: *Hoeren*, ZD 2011, 145 (146).

[101] Beispielsweise: *BGH*, Urt. v. 19.09.1985 – III ZR 213/83 = NJW 1986, 46 ff. – *Schufa-Klausel*.

[102] Dabei enthielt das Volkszählungsurteil auch Formulierungen, anhand derer eine privatrechtssensiblere Ausgestaltung des Datenschutzrechts möglich gewesen wäre: „Dieses [Recht auf informationelle Selbstbestimmung] ist nicht schrankenlos gewährleistet. Der einzelne hat nicht ein Recht im Sinne einer absoluten, uneinschränkbaren Herrschaft über ‚seine' Daten; er ist vielmehr eine sich innerhalb der sozialen Gemeinschaft entfaltende, auf Kommunikation angewiesene Persönlichkeit. Information, auch soweit sie personenbezogen ist, stellt ein Abbild sozialer Realität dar, das nicht ausschließlich dem Betroffenen allein zugeordnet werden kann. Das Grundgesetz hat, wie in der Rechtsprechung des BVerfG mehrfach hervorgehoben ist, die Spannung Individuum – Gemeinschaft im Sinne der Gemeinschaftsbezogenheit und Gemeinschaftsgebundenheit der Person entschieden". BVerfGE 65, 1 (42) = NJW 1984, 419 (422) – *Volkszählung*.

[103] Hierzu als Überblick: *Leistner/Antoine/Sagstetter*, Big Data, 2021, S. 199 ff.

ren.[104] Diese Versuche mündeten zunächst in die Richtlinie zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-RL von 1995)[105] und in einem weiteren Schritt der harmonisierenden Angleichung[106] durch die DS-GVO.

Bei der Verabschiedung von Sekundärrecht kommt dem Unionsgesetzgeber hinsichtlich der Wahl der Mittel und Mechanismen eine große Einschätzungs- und Ausgestaltungsprärogative zugute.[107] In Erfüllung ihrer Schutzpflichten haben die Union[108] und – soweit durch Öffnungs- und Delegationsklauseln zugelassen – die Mitgliedstaaten[109] einen großen Spielraum.

Die Kontrolle der Grenzen dieses gesetzgeberischen Gestaltungskorridors durch den *EuGH* ist im Vergleich zur Rechtsprechung des *BVerfG* weniger einheitlich. Obwohl in abwehrrechtlichen Konstellationen einzelne *EuGH*-Entscheidungen existieren, deren Grundrechtsprüfung derjenigen des *BVerfG* funktional entspricht,[110] ist die Vorgehensweise des *EuGH* nicht einheitlich. Dies gilt insbesondere für Streitigkeiten zwischen Privaten (I).

Als Schwierigkeit kommt hinzu, dass die Gewährleistungsbereiche von Art. 8 GRCh (Schutz personenbezogener Daten) und Art. 7 GRCh (Schutz der Privatsphäre) vom *EuGH* bislang nicht aufgearbeitet wurde und von der (verfassungsrechtlichen) Wissenschaft erst jüngst systematisch untersucht werden (II).[111]

Auch für den europäischen Grundrechtschutz ist die Notwendigkeit anerkannt, unterschiedliche Grundrechte gegen- und miteinander abzuwägen. Allerdings sind die Grundrechte der unternehmerischen Freiheit (III) und insbesondere die allgemeine Handlungsfreiheit (IV) als diejenigen Grundrechte, die potenziell mit dem Schutz personenbezogener Daten kollidieren, bislang in den Unionsgrundrechten unterentwickelt. Die Kombination aus einer zunehmenden Bedeutung der europäischen Grundrechte und einer gleichzeitig nur geringen dogmatischen Differenzierung dieser Grundrechte, kann zumindest teil-

---

[104] *Simitis/Hornung/Spiecker gen. Döhmann*, in: dies. (Hrsg.), Datenschutzrecht, 2019, Einleitung Rn. 133 ff.

[105] Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24.10.1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, ABl. L 281 v. 23.11.1995, S. 31 ff.

[106] Aufgrund der zahlreichen Öffnungsklauseln steht die DS-GVO im Ergebnis teilweise zwischen einer lediglich harmonisierenden, umsetzungspflichtigen Richtlinie und eine umfassenden Vereinheitlichung durch eine direkt anwendbare Verordnung.

[107] Ausführlich: *Marsch*, Das Europäische Datenschutzgrundrecht, 2018, S. 265 ff.

[108] *Herresthal*, ZEuP 2014, 238 (258/269).

[109] *Herresthal*, ZEuP 2014, 238 (274 f.).

[110] *EuGH* (Große Kammer), Urt. v. 08.04.2014, C-293/12, C-594/12 = NJW 2014, 2146 – *Digital Rights Ireland*. Das Urteil basiert auf der Prüfungsreihenfolge: Schutzbereich, Eingriff und Rechtfertigung, einschließlich einer Verhältnismäßigkeitsprüfung.

[111] Zuletzt *Marsch*, Das Europäische Datenschutzgrundrecht, 2018, S. 265 ff.; Zuvor: *Britz*, EuGRZ 2015, 275 ff.; *Blume*, IDPL 2 (2012), 26 ff; *ders.*, IDPL 4 (2014), 269 ff. *Albers*, in: Hoffmann-Riem/Schmidt-Aßmann/Voßkuhle (Hrsg.), Grundlagen des Verwaltungsrechts. Band II, 2. Aufl., 2012, § 22.

weise erklären, warum das *BVerfG* sich zunehmend dazu berufen fühlt, seine nationalen Erfahrung auf Grundlage des Grundgesetzes aktiver bei der Entwicklung der europäischen Grundrechte einzubringen (V).

I. Wirkung europäischer Grundrechte im Privatrechtsverhältnis

Auch die Unionsgrundrechte wirken primär als Abwehrrecht im Verhältnis zwischen natürlichen Personen und staatlichen Institutionen. Eine unmittelbare Wirkung im Verhältnis zwischen Grundrechtsträgern im Rahmen von privatrechtlichen Rechtsbeziehungen besteht nach einhelliger Ansicht – jedenfalls jenseits von auf Gleichbehandlung abzielenden Grundrechten[112] – (noch) nicht.[113]

Dennoch gewährleisten die Grundrechte der europäischen Grundrechts-Charta nicht nur Schutz im Verhältnis zwischen Bürger und Staat, sondern auch bei Auseinandersetzungen zwischen Privaten.[114] Sofern ein Unionsgrundrecht selbst hinreichend konkret ist, besteht sogar eine ausgeprägte Tendenz des *EuGH*,[115] den europäischen Grundrechten auch unter Privaten eine weitreichende Wirkung zukommen zu lassen. Diese kann der Wirkung für staatliche Grundrechtsverpflichtete in bestimmten Konstellationen entsprechen[116] oder – jedenfalls im Bereich des europäischen Anti-Diskriminierungsrechts[117] – sogar darüber hinausgehen.[118]

---

[112] Die Leitentscheidungen sind vor allem: *EuGH*, Urt. v. 08.04.1976, C-43/75 = NJW 1976, 2068 – *Defrenne II*; *EuGH*, Urt. v. 19.01.2010, C-555/07 = NJW 2010, 427 – *Kücükdeveci*.

[113] *Huber*, NJW 2011, 2385 (2389 f.); *Herresthal*, ZEuP 2014, 238 (254); *Jarass*, in: ders. (Hrsg.), GRCh, 4. Aufl. 2021, Art. 8, Rn. 3; eine Rechtsprechungstendenz zur unmittelbaren Drittwirkung erkennend: *Ruffert*, JuS 2020, 1 (5 f.). Ausführlich zum Schutz personenbezogener Daten: *Marsch*, Das Europäische Datenschutzgrundrecht, 2018, S. 253 ff.

[114] *EuGH*, GRUR 2008, 241 (Rn. 65 ff.) – *Promusicae*; *EuGH*, GRUR 2015, 894 (Rn. 33 ff.) – *Coty Germany*; *EuGH*, GRUR 2019, 940 (Rn. 51 ff.) – *Spiegel Online*; dazu *Streinz/Michl*, EuZW 2011, 384 (385 f.); *Lock,* in: Kellerbauer/Klamert/Tomkin (Hrsg.), The EU Treaties and the Charter of Fundamental Rights, 2019, Art. 8 GRCh, Rn. 5

[115] Beginnend mit: *EuGH*, Slg. 2005, I-9981 = NJW 2005, 3695 Rn. 76 – *Mangold*. Speziell zur Unabhängigkeit der Aufsicht über die Verarbeitung personenbezogener Daten durch Private gemäß Art. 28 Abs. 1 Unterabs. 2 der DatenschutzRL (95/46/EG): *EuGH* (Große Kammer), Urt. v. 09.03.2010, C-518/07 = NJW 2011, 1265 (Rn. 23–30) – *Kommission/Deutschland*.

[116] *Jarass*, ZEuP 2017, 310 (332 f.).

[117] *EuGH*, C-414/16 = NZA 2018, 569 (Rn. 77–82) – *Egenberger*. zuvor: *EuGH*, C-114/04 = NJW 2005, 3695 (Rn. 74 ff.) – *Mangold*; *EuGH*, C-555/07 = NJW 2010, 427 (Rn. 50) – *Kücükdeveci*; *EuGH*, C-476/11 = EuZW 2013, 951 – *Experian*; *EuGH*, C-441/14 =EuZW 2016, 466 – *Dansk Industri*.

[118] *Herresthal*, ZEuP 2014, 238 (265: „teilweise höher, teilweise aber auch deutlich niedriger"). Mittlerweile wird zumindest für einige europäische Grundrechte – soweit diese konkrete rechtliche Positionen bestimmen – eine Wirkung im Verhältnis zwischen Privaten in Betracht gezogen. Dies gilt jedoch nicht, soweit die Gewährleistung des jeweiligen Grund-

Die Grenzziehung zwischen der abwehrrechtlichen und der gewährleistungsrechtlichen Dimension der europäischen Grundrechte fällt im Unionsrecht deshalb besonders schwer, weil weder dem europäischen Gesetzgeber noch dem *EuGH* die Unterscheidung zwischen einer unmittelbaren und einer mittelbaren Wirkung von Grundrechten geläufig ist. Stattdessen prüft der *EuGH* die Grundrechte regelmäßig in abstrakter Weise innerhalb der Verhältnismäßigkeit und ohne die jeweils betroffenen Interessen spezifisch herauszuarbeiten, zu konkretisieren und sie jeweils einem oder mehreren Unionsgrundrechten zuzuordnen.[119] Diese Herangehensweise lässt sich auf eine im Ausgangspunkt vom deutschen Grundrechtsverständnis abweichende Konzeption zurückführen, für die das nach französischem Verständnis herrschende objektiv-rechtliche Grundrechtsverständnis ausschlaggebend sein soll.[120]

Im Gegensatz dazu knüpft die dem deutschen Recht – jedenfalls jenseits des Datenschutzrechts – vertraute Unterscheidung zwischen mittelbarer und unmittelbarer Drittwirkung an die im deutschen Verfassungsrecht herausgearbeitete Differenzierung zwischen Privatrecht und öffentlichem Recht an;[121] eine Differenzierung, die zudem der verfahrensrechtlichen Eigenart der Verfassungsbeschwerde geschuldet ist.[122]

Unabhängig davon, ob die Unterscheidbarkeit zwischen öffentlichem Recht und Privatrecht für das Unionsrecht sinnvoll sein könnte, ist das europäische Sekundärrecht von jeher

> „weder an der privatrechtlichen Struktur eines Regelungsziels orientiert noch wird dieser Unterscheidung eine Bedeutung bei der Formulierung und Strukturierung des Unionsrechts eingeräumt".[123]

---

rechts zunächst einer Konkretisierung durch den Gesetzgeber bedarf: *Hellgardt*, Regulierung und Privatrecht, 2016, S. 288 ff.; *Jarass*, ZEuP 2017, 310 (322 f.).

[119] Hierzu spezifisch für den Schutz aus Art. 7 und Art. 8 GRCh; *Nettesheim*, Privatleben und Privatsphäre, in: EnzEuR II, 2014, § 9 Rn. 58 f.

[120] Hierzu: *Huber*, Staat und Wissenschaft, 2008, S. 29; mit Hinweis auf das französische Datenschutzgesetz aus dem Jahr 1978 und dessen Formulierung als Programm in Art. 1 Loi 78–17 vom 06.01.1978 (J.O. 1978, S. 227): „L'informatique doit être au service de chaque citoyen" (dt. „Die Datenverarbeitung muss im Dienste jedes Bürgers stehen": *Marsch*, Das Europäische Datenschutzgrundrecht, 2018, S. 86/121 ff.

[121] Zur historischen Bedingtheit dieser Unterscheidung: *Lepsius*, in: Grünberger/Jansen (Hrsg.), Privatrechtstheorie heute, 2017, S. 82 ff.

[122] Womöglich aufgrund des Mangels an einem unionsrechtlichen Äquivalent zu Art. 93 Abs. 1 Nr. 4a GG, fühlt sich der Erste Senat des *BVerfG* nunmehr dazu berufen,– soweit dies wegen des Vorrangs des Unionsrechts überhaupt in Betracht kommt – Abhilfe zu schaffen. Das *BVerfG* möchte künftig die Einhaltung und Gewährleistung der Unionsgrundrechte kontrollieren und hat dem *EuGH* deshalb eine Kooperation angedient. Diese ist deshalb gefährlich, weil sie – abhängig vom jeweils nationalen Verfassungsrecht – von allen nationalen Verfassungsgerichte für sich in Anspruch genommen werden könnte: *BVerfG*, GRUR 2020, 88 (60/67 f.) – *Recht auf Vergessen II*.

[123] *Herresthal*, ZEuP 2014, 238 (258).

Dennoch lässt sich die Pflicht zur Gewährleistung eines Mindeststandards im Bereich von Privatrechtsverhältnissen – aus deutscher Perspektive – mit der mittelbaren Drittwirkung von Grundrechten vergleichen, wenngleich die begriffliche Unterscheidung zwischen einer mittelbaren und einer unmittelbaren (Dritt-)Wirkung für das autonome Unionsrecht nicht maßgeblich ist.[124]

Immerhin hat der *EuGH* das Grundrecht auf Schutz von personenbezogenen Daten und das Grundrecht auf Schutz der Privatsphäre bereits mehrfach zur Auslegung im Rahmen von privatrechtlichen Streitigkeiten herangezogen und dabei die Notwendigkeit betont, diese mit den anderen Grundrechtspositionen der Beteiligten im Rahmen einer Abwägung in Ausgleich zu bringen.[125] Infolgedessen kommt den Unionsgrundrechten – jedenfalls in der Rezeption des *EuGH* durch das *BVerfG*[126] – im Privatrechtsverhältnis eine den Grundrechten des Grundgesetzes *ähnliche Wirkung* zu. Während die Grundrechte des Grundgesetzes bekanntlich über unbestimmte Rechtsbegriffe und Generalklauseln in das Privatrecht ausstrahlen, können die europäischen Grundrechte in das Privatrecht „hineinwirken".[127]

II. Schutz- und Gewährleistung durch Art. 7 und Art. 8 GRCh

Das deutsche Recht auf informationelle Selbstbestimmung findet sich weder begrifflich noch inhaltlich im europäischen Primär- und Sekundärrecht.[128] Allerdings hat das Recht einer jeden Person auf Schutz der sie betreffenden persönlichen Daten eine lange Tradition in der europäischen Rechtsprechung, die sich bis zur *Stauder*-Entscheidung[129] – und damit bis zur ersten Entscheidung des *EuGH* zum europäischen Grundrechtsschutz überhaupt – zurückverfolgen lässt.[130] Der

---

[124] So auch *BVerfG*, GRUR 2020, 74 (Rn. 76 f.) – *Recht auf Vergessen I*. Mit Hinweis auf Art. 51 Abs. 1 GRCh als Verankerung von Schutzpflichten: *Herresthal*, ZEuP 2014, 238 (269).

[125] *EuGH*, GRUR 2008, 241 (Rn. 68) – *Promusicae*; *EuGH*, EuZW 2009, 108 (Rn. 53) – *Satakunnan Markkinapörssi und Satamedia*; *EuGH*, EuZW 2012, 37 (Rn. 43) – *ASNEF*; *EuGH*, Rs. C-131/12 = NJW 2014, 2257 (Rn. 80) – *Google Spain*; *EuGH*, GRUR 2019, 940 (Rn. 38/42) – *Spiegel Online*.

[126] *BVerfG*, GRUR 2020, 88 (Rn. 97) – *Recht auf Vergessen II*.

[127] *BVerfG*, GRUR 2020, 88 (Rn. 97) – *Recht auf Vergessen II*. Aufgrund dieser – aus deutscher Perspektive – diffusen Rechtsprechung des *EuGH* befürchtet *Huber* eine Einebnung der Unterscheidung zwischen öffentlichem Recht und Privatrecht: *ders.*, Zur Drittwirkung von Grundrechten und Grundfreiheiten, in: Ruffert (Hrsg.), FS Schröder, 2012, S. 336 (336/339).

[128] *Pedro Cruz Villalón*, der Generalanwalt beim EuGH, hat im Rahmen seines Schlussantrags v. 12.12.2013 zu C-293/12, C-594/12 – *Digital Rights Ireland* den Begriff des „Rechts auf informationelle Selbstbestimmung" vom BVerfG übernommen: *ders*, BeckRS 2013, 82347 (Rn. 57). Dies hat der EuGH (Berichterstatter mit deutscher Herkunft: *v. Danwitz*) jedoch nicht aufgegriffen.

[129] *EuGH*, C-29/69, ECLI:EU:C:1969:57, Rn. 6 f. – *Stauder*.

[130] Zur Herleitung: *Michl*, DuD 2017, 349 ff.

Datenschutz oder mit Blick auf die unionsrechtliche Entstehungsgeschichte genauer: Der Schutz der Privatsphäre der Datensubjekte steht also am Beginn der europäischen Grundrechtsgewährleistung durch die Judikative.[131]

Seit dem Vertrag von Maastricht ist die EMRK gemäß Art. 6 Abs. 2 EUV a. F. (entspricht weitgehend Art. 6 Abs. 3 AEUV) als europäische Rechtserkenntnisquelle anerkannt und der *EuGH* konnte infolgedessen an das in Art. 8 EMRK verankerte Recht auf Achtung des Privatlebens anknüpfen, um daraus beispielsweise den Schutz der Geheimhaltung des individuellen Gesundheitszustands abzuleiten.[132] Mit der Verabschiedung der Datenschutz-RL (1995) musste nicht mehr direkt auf Art. 8 EMRK und damit auf das Primärrecht zurückgegriffen werden, weil dem *EuGH* nun eine spezifischere sekundärrechtliche Grundlage zur Verfügung stand.

Diese sekundärrechtliche Ebene wirkte sich ihrerseits wiederum auf das Primärrecht aus. Beispielsweise begnügte sich der *Europäische Grundrechtekonvent* bei der Ausarbeitung der GRCh nicht mit dem durch Art. 7 GRCh gewährleisteten Schutz der Privatsphäre, sondern er etablierte mit Art. 8 GRCh zusätzlich ein Grundrecht der natürlichen Person auf Schutz der sie betreffenden personenbezogenen Daten. Dieses Grundrecht wird durch Art. 7 GRCh flankiert, soweit zusätzlich das Privat- und Familienleben, die Wohnung sowie die Kommunikation des Individuums tangiert sind. Mit Inkrafttreten von Art. 6 Abs. 1 EUV am 01.12.2009 wurden Art. 7 und Art. 8 GRCh in den Rang des Primärrechts erhoben.

Seitdem zieht der *EuGH* beide Normen regelmäßig als einheitliche Rechtsquelle heran, ohne zwischen deren jeweiligem Schutz- und Gewährleistungsbereich zu differenzieren (1). In der Literatur wurden kürzlich erste Ansätze für eine sinnvolle Systematisierung der beiden Schutzbereiche unterbreitet, die jedoch für das Privatrecht sehr vage bleiben (2). Dies hat zur Konsequenz, dass die gemäß Art. 8 Abs. 2 S. 1 GRCh verbürgte Einwilligungsmöglichkeit und die für das Privatrecht fundamentale Selbstbestimmung des Datensubjekts bislang (zu) wenig Beachtung gefunden haben (3).

1. Keine Abgrenzung der Schutzbereiche durch den EuGH

Die fehlende Abgrenzung zwischen den Schutzbereichen von Art. 7 und Art. 8 GRCh geht bereits auf die Entscheidung *Promusicae* des *EuGH* zurück.[133] Mit den Schlussanträgen der Generalanwältin *Kokott* hatte sich der Eindruck verfestigt, dass Art. 8 GRCh lediglich den Schutz der Privatsphäre ergänzt, indem

[131] Grundlegend zur Entwicklung des europäischen Datenschutzgrundrechts aus dem Recht auf Schutz des Privatlebens durch EGMR und EuGH: *Marsch*, Das Europäische Datenschutzgrundrecht, 2018, S. 7 ff.

[132] *EuGH*, C-202/92 P, ECLI:EU:C:1994:361, Leitsatz 1 – *X/Kommission*.

[133] *EuGH*, EuZW 2008, 113 ff. – *Promusicae*.

er den Schutz personenbezogener Daten „hervorhebe". [134] Dem folgte der *EuGH* mit der Formulierung, dass Art. 7 GRCh den Schutz der Privatsphäre „garantiere", während Art. 8 den Schutz personenbezogener Daten „proklamiere".[135]

In der Sache prüfte der *EuGH* in *Promusicae* lediglich das Recht auf Achtung der Privatsphäre,[136] was den Gerichtshof in späteren Entscheidungen mit einem datenschutzrechtlichen Kontext jedoch nicht daran hinderte, Art. 7 und Art. 8 GRCh stets gemeinsam zu zitieren.[137] Missglückt ist dieser Ansatz, wenn der *EuGH* beide Grundrechte gemeinsam zitiert, obwohl kein Eingriff in die Privatsphäre vorliegt, weil die zu überprüfenden Maßnahmen ausschließlich die berufliche oder unternehmerische Tätigkeit eines Datensubjekts betreffen.[138]

Bislang ist völlig offen, ob es sich bei dieser Kombination aus Art. 7 und Art. 8 GRCh nach Ansicht des *EuGH* um ein einheitliches Grundrecht handelt, das sich aus zwei Quellen speist, oder ob beide Grundrechte einen jeweils eigenen Gewährleitungsbereich haben und in welchem Verhältnis diese Gewährleistungsbereiche zueinanderstehen.[139]

Auf einen Versuch des Generalanwalts *Pedro Cruz Villalón*, die Gewährleistungsbereiche klarer abzugrenzen, ließ der *EuGH* sich nicht ein.[140] Der Generalanwalt wollte in Übereinstimmung mit den Vorlagefragen des *irischen High Court* zu *Digital Rights Ireland*,[141] die Schutzbereiche der beiden Grundrechte voneinander abgrenzen, um damit der gesetzgeberischen Entscheidung für zwei Grundrechte Rechnung zu tragen.[142] Obwohl gerade das Urteil *Digital Rights Ireland* maßgeblich vom deutschen Berichterstatter *Thomas von Danwitz* geprägt wurde und deshalb auf einer – aus deutscher Perspektive – geradezu mus-

---

[134] GA *Kokott*, Schlussanträge zu C-275/06, ECLI:EU:C:2007:454, Rn. 51 – *Promusicae*; mit einer Analyse, wonach in den Schlussanträgen der GA Kokott erste Indizien für eine unmittelbare Drittwirkung des Datenschutzgrundrechts angelegt sind: *Marsch*, Das Europäische Datenschutzgrundrecht, 2018, S. 252 f.

[135] *EuGH*, EuZW 2008, 113 (Rn. 64) – *Promusicae*.

[136] Hierzu *Michl*, DuD 2017, 349 (351).

[137] *EuGH*, verb. C-92/09 und C-93/09 = EuZW 2010, 939 (Rn. 47, vor Rn. 56 ff. und vor Rn. 65 ff.) – *Schecke und Eifert*; *EuGH*, C-131/12, ECLI:EU:C:2014:317 – *Google Spain*; *EuGH*, verb. C-293/12 und C-594/15, ECLI:EU:C:2014:238 – *Digital Rights Ireland*.

[138] Einen Eingriff in die Privatsphäre annehmend, soweit eine Übermittlung von Daten über das berufliche oder unternehmerische Einkommen an weitere Behörden erfolgt: *EuGH*, C-138/01, C-139/01, C-465/00 = EuR 2004, 276 (Rn. 73 f.) – *Österreichischer Rundfunk*; im Anschluss hieran: *EuGH*, verb. C-92/09 und C-93/09 = EuZW 2010, 939 (Rn. 58 ff.) – *Schecke und Eifert*.

[139] Mit einer Analyse der Verflechtungen der Rechtsquellen und Schutzebenen: *Marsch*, Das Europäische Datenschutzgrundrecht, 2018, S. 73 ff.

[140] Auch auf den erneuten Versuch des englischen Court of Appeal für England und Wales ging der EuGH nicht ein: *EuGH*, verb. C-203/15 und C-698/15, ECLI:EU:C:2016:970, Rn. 129 – *Tele2Sverige*.

[141] Vorlagefragen 2. ii) und 2. iii) des Vorabentscheidungsersuchens des *High Court of Ireland* C-293/12 = BeckEuRS 2012, 688064.

[142] Schlussantrag v. 12.12.2013 zu C-293/12, C-594/12 = BeckRS 2013, 82347 (Rn. 55 ff./ 60 ff.) – *Digital Rights Ireland*.

tergültigen Grundrechtsprüfung beruht, differenziert der *EuGH* dennoch nicht zwischen Art. 7 und Art. 8 GRCh.[143]

Lediglich im Urteil *Schrems I* geht der *EuGH* immerhin isoliert auf Art. 8 GRCh ein.[144] Diese Besonderheit beruhte jedoch darauf, dass das Verfahren mit der Gewährleistung der Unabhängigkeit der Datenschutzbehörde einen Verfahrensgegenstand hatte, für den es spezifisch auf Art. 8 Abs. 3 GRCh und gerade nicht (zusätzlich) auf die Privatsphäre von Datensubjekten (Art. 7 GRCh) ankam. Dennoch nutzte der *EuGH* auch diese Möglichkeit nicht, um dem Schutzbereich des Art. 8 GRCh eine eigenständige Bedeutung zu verschaffen.[145]

2. Keine (klare) Schutzbereichsabgrenzung in der Literatur

Auch die wissenschaftlichen Einordnungsversuche sind – jedenfalls aus privatrechtlicher Perspektive – bislang wenig erhellend. Im Ausgangspunkt ist es offensichtlich, dass beide Gewährleistungsbereiche sich jedenfalls überlagern können.[146] So wird vertreten, dass beide Schutzbereiche konzentrische Kreise bilden, wobei Art. 7 GRCh den größeren Bereich abdecken soll, so dass sich der Schutz- und Gewährleistungsbereich von Art. 8 GRCh vollständig innerhalb des Bereichs des Art. 7 GRCh bewege.[147]

Für dieses Bild der konzentrischen Kreise findet sich ein Anknüpfungspunkt in der Rechtsprechung, weil der *EuGH* einen Eingriff in die Privatsphäre angenommen hat, soweit eine Übermittlung von Daten über das berufliche oder unternehmerische Einkommen an weitere Behörden erfolgte.[148] Diese Rechtsprechung könnte jedoch primär einen strategischen Hintergrund haben. Sie erleichterte es dem *EuGH*, über Art. 7 GRCh unmittelbar an die Rechtsprechung des *EGMR* zum Schutz der Privatsphäre gemäß Art. 8 EMRK anzuknüpfen, Art. 52 Abs. 3 S. 1 GRCh. Diese Anknüpfung an die Rechtsprechung des *EGMR* wäre bei isolierter Anwendung von Art. 8 GRCh nicht möglich, weil für den Schutz von personenbezogenen Daten keine Vorgänger-Vorschrift in der EMRK existiert.

Dennoch hatte die Heranziehung der Privatsphäre in einem Bereich, der durch Berufsausübung und unternehmerische Tätigkeit geprägt ist, eindeutige Nachteile. Der *EuGH* konstruiert dadurch eine Kontinuität seiner eigenen Rechtsprechung mit derjenigen des *EGMR*, die der zwischenzeitlichen Einführung des Art. 8 GRCh nicht gerecht wird. Der Schutz- und Gewährleistungs-

---

143 *EuGH*, C-293/12, C-594/12 = NJW 2014, 2169 (33/36 f.) – *Digital Rights Ireland*.

144 *EuGH*, C-362/14; ECLI:EU:C:2015:650, Rn. 58, 72 – *Schrems I*.

145 *EuGH*, C-362/14; ECLI:EU:C:2015:650, Rn. 66 – *Schrems I*.

146 *Bock/Engeler*, DVBl. 2016, 593 (595); *Eichenhofer*, Der Staat 55 (2016), 41 (62).

147 *Michl*, DuD 2017, 349 (353).

148 *EuGH*, verb. C-138/01, C-139/01, C-465/00 = EuR 2004, 276 (Rn. 73 f.) – *Österreichischer Rundfunk*; im Anschluss hieran: *EuGH*, verb. C-92/09, C-93/09 = EuZW 2010, 939 (Rn. 58 ff.) – *Schecke und Eifert*.

bereich des Art. 8 GRCh kann gerade auch dann eröffnet sein, wenn kein Bezug zur Privatsphäre i. S. d. Art. 7 GRCh vorhanden ist.

Nach hier vertretener Auffassung muss Art. 8 GRCh – ebenso wie die DS-GVO – unabhängig davon Anwendung finden, ob die personenbezogenen Daten den privaten Rückzugsbereich tangieren. Auch im Bereich der beruflichen oder unternehmerischen Tätigkeit eines Datensubjekts ist der Schutz personenbezogener Daten grundsätzlich zu gewährleisten,[149] obwohl diese gerade nicht in den Bereich der Privatsphäre gemäß Art. 7 GRCh fallen. Deshalb ist es überzeugend, Art. 8 GRCh im Fall einer Verarbeitung von personenbezogenen Daten vorrangig anzuwenden,[150] wobei der Gewährleistungsbereich des Art. 8 GRCh im Bereich des Privatlebens nochmals durch Art. 7 GRCh verstärkt wird.[151] Infolgedessen kann an die Rechtsprechung des *EGMR* zu Art. 8 EMRK gemäß Art. 52 Abs. 3 S. 1 GRCh nur angeknüpft werden, soweit durch eine Verarbeitung personenbezogener Daten auch der Bereich des Privatlebens zusätzlich beeinträchtigt ist.[152]

Für eine Datenverarbeitung durch Private lässt sich Art. 8 Abs. 1 GRCh zwar als Ausgestaltungsauftrag und Schutzpflicht an die Legislative und Judikative verstehen,[153] dabei müssen jedoch – stärker als bisher – die entgegenstehenden Grundrechte der Verantwortlichen und Datensubjekte herausgearbeitet und berücksichtigt werden. Problematisch wird dies insbesondere dann, wenn auf der Grundlage der Unionsgrundrechte das europäische Sekundärrecht – insbesondere durch das datenschutzrechtliche Verbot mit Erlaubnisvorbehalt (Art. 6 Abs. 1 und Art. 9 Abs. 1 DS-GVO) und den Grundsatz der Zweckbindung

---

[149] Deshalb hatte das vorlegende FG Düsseldorf den EuGH um Auslegung lediglich im Lichte des Art. 8 GRCh gebeten. Der EuGH griff für seine Urteilsbegründung jedoch nicht auf die GRCh zurück. Dem Gerichtshof genügte eine Auslegung anhand der Datenschutzrichtlinie (1995) und der DS-GVO: *EuGH*, C-496/17 = EuZW 2019, 746 (Rn. 57 ff.) – *Deutsche Post/Hauptzollamt Köln*).

[150] Mit knapper Begründung a. A.: *Marsch*, Das Europäische Datenschutzgrundrecht, 2018, S. 269 f. Danach soll das „Kombinationsgrundrecht" aus Art. 7 i. V. m. Art. 8 GRCh in einem Subsidiaritätsverhältnis zu Art. 7 GRCh stehen. Über das – vage bleibende – Kriterium der „Gefährdung der inneren Entfaltungsmöglichkeit" soll der Schutzbereich des Kombinationsgrundrechts gegenüber dem Ausgestaltungsauftrag gemäß Art. 8 GRCh abgrenzbar sein.

[151] Statt vieler *Augsberg*, in: von der Groeben/Schwarze/Hatje (Hrsg.), Europäisches Unionsrecht, Band 1, 7. Aufl. 2015, Art. 8 GRCh, Rn. 1; *Bernsdorff*, in: Meyer, GRCh, 4. Aufl. 2014, Art. 8, Rn. 13; *Guckelberger*, EuZW 2011, 126 (127); *Kingreen*, in: Calliess/Ruffert, EUV/AEUV, 5. Aufl. 2016, Art. 8 GRCh, Rn. 1a; *Schiedermair*, Der Schutz des Privaten als internationales Grundrecht, 2012, S. 349.

[152] Für einen im vertikalen Verhältnis gestuften Schutz, der eine enge Abwehrdimension enthält (S. 129 ff.) und eine dem Gesetzgeber „weite Spielräume belassene Ausgestaltungsdimension für innovative Regelungsansätze" (S. 277): *Marsch*, Das Europäische Datenschutzgrundrecht, 2018, S. 129 ff. bzw. 137 ff.

[153] Gegen eine eigenständige Schutzpflicht des Kombinationsgrundrechts aus Art. 7 i. V. m. Art. 8 GRC, weil dieses „instrumentell auf den Schutz vor Gefährdungen anderer Grundrechte abzielt und ihm daher ein Schutzgut im klassischen Sinne fehlt": *Marsch*, Das Europäische Datenschutzgrundrecht, 2018, S. 260 ff.

(Art. 5 Abs. 1 lit. b DS-GVO) – ebenfalls im Privatrechtsverhältnis „konstitutionalisiert" wird,[154] und damit Gefahr läuft, einen überschießenden und mit Blick auf die Freiheiten der Verantwortlichen und Datensubjekte unverhältnismäßigen Schutz personenbezogener Daten zu etablieren.

3. Geringe Berücksichtigung der aktiven Entfaltungsfreiheit

Bislang beschränkt sich das Verständnis der Unionsgrundrechte aus Art. 7 und Art. 8 GRCh vorrangig auf deren abwehrrechtliche Funktion. Dies lässt sich für den Schutz des Privat- und Familienlebens gemäß Art. 7 GRCh aus dessen Wurzel in Art. 8 EMRK und dessen grundsätzlich am *status negativus* ausgerichteten Schutz begründen (a). Im Gegensatz dazu, sieht Art. 8 Abs. 2 S. 1 GRCh mit der Möglichkeit zur Einwilligung ausdrücklich die eigenverantwortliche Selbstbestimmung der Datensubjekte vor und beschränkt dadurch zugleich die Möglichkeit, dieses Recht zur Einwilligung durch gesetzliche Erlaubnistatbestände zurückzudrängen (b).

a) Achtung des Privat- und Familienlebens, Art. 7 GRCh

Art. 7 GRCh schützt das Recht auf Achtung des Privat- und Familienlebens und sichert damit einen Bereich, in dem das Individuum seine Persönlichkeit frei entfalten kann. Insoweit könnte Art. 7 GRCh als eine Auffangfreiheit verstanden werden, die als europäisches Funktionsäquivalent zur allgemeinen Handlungsfreiheit fungiert.[155]

Dieser Ansatz wird jedoch überwiegend abgelehnt.[156] Zwar hat der *EuGH* die allgemeine Handlungsfreiheit in Gestalt eines allgemeinen Gesetzesvorbehalts bei Eingriffen in die Sphäre der privaten Betätigung als allgemeinen Grundsatz des Gemeinschaftsrechts angesehen.[157] Der *Europäische Grundrechtekonvent* hat einen solchen Auffangtatbestand, der über denjenigen des Art. 8 EMRK hinausgeht, nach den Erläuterungen zu Art. 7 und Art. 52 Abs. 3 GRCh jedoch ausdrücklich nicht gewollt.[158] Wie sein Vorbild in Art. 8 Abs. 2 EMRK dient Art. 7 GRCh deshalb vorrangig als Abwehrrecht gegen hoheitliche Eingriffe.[159]

---

[154] Hierzu unten C.II.

[155] *Uerpmann-Wittzack*, in: Ehlers (Hrsg.), Grundrechte, 4. Aufl., § 3 Rn. 3, unter Hinweis auf: *EGMR*, EuGRZ 2002, 234 – *Pretty/Großbritannien*.

[156] *Jarass*, in: ders. (Hrsg.), GRCh, 4. Aufl. 2021, Art. 7, Rn. 3; *ders.*, EU-Grundrechte, § 12, Rn. 5; *Kingreen*, in: Calliess/Ruffert, EUV/AEUV, 5. Aufl., Art. 7 GRCh, Rn. 3, Stern/Sachs/*Weber*, GRC, Art. 7, Rn. 4/9 und *Schmitz*, JZ 2001, 837; *Magiera*, DÖV 2000, 1025; ferner *Bogdandy*, JZ 2001, 168.

[157] *EuGH*, EuGRZ 1989, 395 (Rn. 19) – *Hoechst*.

[158] *Bernsdorff*, in: Meyer/Hölscheidt (Hrsg.), GRCh, 5. Aufl. 2019, Art. 7, Rn. 11.

[159] Hierzu: *Marsch*, Das Europäische Datenschutzgrundrecht, 2018, S. 206 f.

Allerdings wird Art. 7 GRCh gerade im Zusammenhang mit dem Schutz personenbezogener Daten gemäß Art. 8 GRCh auch in Streitigkeiten zwischen Privatrechtsubjekten berücksichtigt[160] und zur Begründung von verfahrensrechtlichen Sicherungen der Privatsphäre durch Private herangezogen.[161] Der Begriff des Privatlebens ist nach dem Verständnis des *EGMR* zwar mehr als das von *Warren* und *Brandeis* proklamierte „Recht in Ruhe gelassen zu werden" (*right to be let alone*).[162] Dennoch sind dem Recht auf Achtung des Privatlebens nach der Rechtsprechung des *EGMR* diejenigen Lebensbereiche zugeordnet, die durch eine Nicht-Öffentlichkeit geprägt sind.[163] Infolgedessen fallen Tätigkeiten mit erkennbarem Öffentlichkeitsbezug nicht in den Gewährleistungsbereich des Art. 7 GRCh.[164]

Indem Art. 7 GRCh die Gewährleistung der freien Persönlichkeitsentfaltung sichern soll, diese aber terminologisch aus der Achtung des Privatlebens abgeleitet wird, ist die individuelle Persönlichkeitsentfaltung in den europäischen Grundrechten nur unvollständig geschützt. Die Achtung und der Schutz des Privatlebens als Rückzugsort[165] ist zwar notwendige, aber noch nicht hinreichende Bedingung für die Bildung und die aktive Entfaltung der Persönlichkeit. Dennoch fehlt dem Art. 7 GRCh und den Unionsgrundrechten insgesamt eine Gewährleistung der allgemeinen, nach außen und damit in die Gesellschaft gerichteten Persönlichkeitsentfaltung, die über den spezifischen Schutz der Berufsfreiheit (Art. 15 GRCh) und der unternehmerischen Freiheit (Art. 16 GRCh) hinausgeht.

Dieser Mangel eines europäischen Funktionsäquivalents zur allgemeinen Handlungsfreiheit ist Ausdruck einer Asymmetrie der europäischen Grundrechte zugunsten eines Schutzes vor Eingriffen in die Freiheitssphäre. Obwohl Art. 7 GRCh der Persönlichkeitsentfaltung des Individuums dient, ist die Freiheit des individuellen Handels und die mit der Freiheitsbetätigung stets einhergehende Verantwortlichkeit für eigenes Handeln auf Ebene der Unionsgrundrechte unterentwickelt. Der gewichtige gesellschaftliche Raum, der unterhalb der Schwelle von beruflicher oder unternehmerischer Tätigkeit, aber oberhalb

---

[160] *EuGH*, Rs. C-131/12 = NJW 2014, 2257 (Rn. 71 f./80 f./99) – *Google Spain*; *Wolff*, in: Pechstein/Nowak/Häde (Hrsg.), Frankfurter Kommentar, 1. Aufl. 2017, GRCh, Art. 7, Rn. 9; ferner *Streinz*, in: ders. (Hrsg.), EUV/AEUV, GRCh, Art. 7, Rn. 11 und *Jarass*, in: ders. (Hrsg.), GRCh, 4. Aufl. 2021, Art. 7, Rn. 8.

[161] *Wolff*, in: Pechstein/Nowak/Häde (Hrsg.), Frankfurter Kommentar, 1. Aufl. 2017, GRCh, Art. 7, Rn. 45 m. w. N.; *Jarass*, in: ders. (Hrsg.), GRCh, 4. Aufl. 2021, Art. 7, Rn. 43/45 f.

[162] *Warren/Brandeis*, (1890), 4 Harv. L. Rev., 193 ff.

[163] *Bernsdorff*, in: Meyer/Hölscheidt (Hrsg.), GRCh, 5. Aufl. 2019, Rn. 15.

[164] Zur Rechtsprechung des *EGMR*: NJW 2004, 2647 – *Caroline von Hannover*; NJW 2000, 2089 – *Smith and Grady*; NJW 1999, 3185 – *Guerra ua.*; EuGRZ 1995, 530 – *Lopez Ostra*. Zur Rechtsprechung des *EuGH*: C-62/90 – Slg 1992, I-2575 – *Kommission/Bundesrepublik Deutschland*.

[165] Zu den Konkretisierungen des Art. 7 GRCh als Recht auf Achtung der Kommunikation: *Bernsdorff*, in: Meyer/Hölscheidt (Hrsg.), GRCh, 5. Aufl. 2019, Rn. 20.

des Privatlebens angesiedelt ist, ist der blinde Fleck der durch das Unionsrecht primärrechtlich gewährleisteten Freiheit zur Persönlichkeitsentfaltung.[166]

b) Schutz personenbezogener Daten, Art. 8 GRCh (Art. 16 AEUV)

Art. 8 GRCh dient dem Schutz von Menschen (natürlichen Personen).[167] Der sachliche Anwendungsbereich des Art. 8 GRCh ist durch das Schutzobjekt der personenbezogenen Daten und durch die Handlung der Datenverarbeitung determiniert (aa). Indem Art. 8 Abs. 2 S. 1 GRCh die Einwilligung des Datensubjekts ausdrücklich als Grundlage für eine rechtmäßige Datenverarbeitung nennt, liefert das Primärrecht ein unionsgrundrechtliches Argument für einen Vorrang der Einwilligung gegenüber den gesetzlichen Erlaubnistatbeständen (bb).

aa) Schutzbereich des Art. 8 GRCh

Art. 8 GRCh ist durch Sekundärrecht geprägtes Primärrecht.[168] Das sekundärrechtliche Datenschutzrecht – in Form der Datenschutz-RL (1995) – war älter und von Anfang an detaillierter ausdifferenziert, als der primärrechtliche Schutz aus Art. 8 GRCh. Infolgedessen verwundert es nicht, dass der *EuGH* – entgegen der formellen Normhierarchie – das Sekundärrecht zur Auslegung und Anwendung von Art. 8 GRCh herangezogen hat.[169] Seit Mai 2018 übernimmt die DS-GVO diese prägende Rolle.

Infolge dieses umgekehrten Verhältnisses zwischen Primär- und Sekundärrecht und weil Art. 8 GRCh neben Art. 7 GRCh in der Rechtsprechung des *EuGH* bislang keine eigenständige Bedeutung zukommt, besteht stets die Gefahr, einem materiell-rechtlichen Zirkelschluss zu erliegen, sofern der abstrakte Art. 8 GRCh für die Auslegung des europäischen Datenschutzrechts herangezogen wird. Dennoch hängt eine Definition des Schutz- und Gewährleistungsbereichs von Art. 8 GRCh – mangels eigenständiger primärrechtlicher Konkretisierungen – weiterhin von der Anwendung und Auslegung des Sekundärrechts ab.

---

[166] Somit könnte die Erweiterung des Schutzbereichs von Art. 7 GRCh auf berufliche und unternehmerische Kontexte (*EuGH*, verb. C-138/01, C-139/01, C-465/00 = EuR 2004, 276 (Rn. 73 f.) – *Österreichischer Rundfunk*; *EuGH*, verb.C-92/09, C-93/09 = EuZW 2010, 939 (Rn. 58 ff.) – *Schecke und Eifert*) auch als Kompensationsversuch für eine auf primärrechtlicher Ebene empfundene Lücke verstanden werden.

[167] Zur Menschenrechtsqualität: *Bernsdorff*, in: Meyer/Hölscheidt (Hrsg.), GRCh, 5. Aufl. 2019, Rn. 14.

[168] Zu den daraus folgenden Schwierigkeiten bei der Bestimmung des Verhältnisses zwischen Primär- und Sekundärrecht und für den Schutzbereich des Art. 8 GRCh: *Bernsdorff*, in: Meyer/Hölscheidt (Hrsg.), GRCh, 5. Aufl. 2019, Rn. 15 ff./20 f.

[169] In Anlehnung an *Jan Henrik Klement* (Wettbewerbsfreiheit, 2015, S. 23 ff.) ordnet *Nikolaus Marsch* diese Rückkopplung aus dem Sekundärrecht zutreffend als Beispiel für eine aus dem einfachen Recht „lernende Grundrechtstheorie": *Marsch*, Das Europäische Datenschutzgrundrecht, 2018, S. 59 ff.

Schutzgegenstand des Art. 8 GRCh sind personenbezogene Daten. Im Anschluss an die *Breyer*-Entscheidung des *EuGH*[170] umfassen personenbezogenen Daten gemäß Art. 2 lit. a der Datenschutz-RL von 1995 (jetzt: Art. 4 Nr. 1 DS-GVO) alle, auf eine bestimmte oder bestimmbare Person bezogenen Informationen, nicht nur sensible Daten. Infolge dieses weiten Verständnisses genügt es beispielsweise, wenn eine dynamische IP-Adresse von dem (behördlichen) Anbieter einer allgemein zugänglichen Webseite beim Zugriff einer Person auf diese Webseite gespeichert wird. Für den Webseiten-Betreiber stellt diese IP-Adresse ein personenbezogenes Datum dar, wenn er über solche (technischen oder rechtlichen) Mittel verfügt, die es ihm ermöglichen, die betreffende Person anhand der Zusatzinformationen, über die beispielsweise der Internetzugangsanbieter verfügt, bestimmen zu lassen.[171] Infolge dieser weiten sekundärrechtlichen Definition[172] ist auch der Anwendungsbereich von Art. 8 GRCh sehr weit.

Dies gilt ebenfalls für den Begriff der Datenverarbeitung. Im Anschluss an Art. 2 lit. b der Datenschutz-RL von 1995 (jetzt: Art. 4 Nr. 2 DS-GVO) erfasst auch der Begriff der Verarbeitung i. S. d. Art. 8 GRCh jede Verwendung personenbezogener Daten und damit jeden Vorgang mit oder ohne Hilfe automatisierter Verfahren. Hierzu gehören das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, der Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung. Diese denkbar weite Definition ist zudem entwicklungsoffen für neue Formen der Verwendung personenbezogener Daten.[173]

Neben dem – aus deutscher Perspektive – klassischen Abwehrrecht gegenüber Beeinträchtigungen durch öffentliche Stellen entfaltet Art. 8 GRCh auch eine Gewährleistungsdimension,[174] die den Schutz gegenüber Privaten, vergleichbar der mittelbaren Drittwirkung einbezieht.[175] Für *Carsten Herresthal* ist der weite Schutz der Persönlichkeit gegen das Eindringen in die Privatsphäre

---

[170] *EuGH*, C-582/14 = NJW 2016, 3549 – *Breyer*.

[171] *EuGH*, C-582/14 = NJW 2016, 3549 (Rn. 49) – *Breyer*.

[172] *Leistner/Antoine/Sagstetter*, Big Data, 2021, S. 226 („Diese schon auf der ersten Stufe des Anwendungsbereichs vollkommen ausgeuferte Reichweite datenschutzrechtlicher Regulierung ist *kritikwürdig*" [Hervorhebungen im Original.]).

[173] *Bernsdorff*, in: Meyer/Hölscheidt (Hrsg.), GRCh, 5. Aufl. 2019, Rn. 22; Stern/Sachs/*Johlen*, GRCh, Art. 8, Rn. 34.

[174] *Wolff*, in: Pechstein/Nowak/Häde (Hrsg.), Frankfurter Kommentar, 1. Aufl. 2017, Art. 8 GRCh, Rn. 16 f.; Stern/Sachs/*Johlen*, GRCh, Art. 8, Rn. 21 f.; *Jarass*, in: ders. (Hrsg.), GRCh, 3. Aufl. 2016, Art. 8, Rn. 2/10.

[175] *EuGH*, C-131/12 = NJW 2014, 2257 (Rn. 38) – *Google Spain*; *Kingreen*, in: Calliess/Ruffert, EUV/AEUV, Art. 8 GRCh, Rn. 12; *Reinhardt*, AöR 142 (2017), 544 ff.; *Streinz/Michl*, EuZW 2011, 384 und *Roßnagel*, NJW 2019, 3; Als einen Fall der unmittelbare Drittwirkung ordnet *Marsch* das Google-Spain-Urteil ein: *ders.*, Das Europäische Datenschutzgrundrecht, 2018, S. 253 ff.

(Art. 7 GRCh) und der Schutz personenbezogener Daten gemäß Art. 8 GRCh geradezu „paradigmatisch" für die Schutzpflichten als Ausprägung der mittelbaren Drittwirkung der europäischen Grundrechte.[176] Darüber hinaus sprechen *Rudolf Streinz und Walter Michl* dem europäischen Gesetzgeber im Zusammenhang mit dem Schutz personenbezogener Daten eine besonders weitgehende Einschätzungsprärogative zu, weil Art. 8 Abs. 1 GRCh die autonome Entscheidungsgewalt über die Daten gewährleiste.[177]

Frühzeitig hatte der *EuGH* verlangt, dass die EU-Mitgliedstaaten bei der Umsetzung des europäischen Sekundärrechts, darunter der Datenschutz-RL (1995), einen angemessenen Ausgleich zwischen einer Verletzung von Immaterialgüterrechten und dem Schutz des Eigentums und dem Schutz personenbezogener Daten gemäß Art. 8 Abs. 1 GRCh herstellen sollen.[178] In jüngerer Zeit hat der *EuGH* unmissverständlich zum Ausdruck gebracht, dass private Unternehmen die durch Art. 8 GRCh geschützten Interessen in ihre Abwägung einstellen und ihnen eine besondere Bedeutung zumessen müssen.[179]

Dieser starke Einfluss von Art. 8 GRCh auf Streitigkeiten, die das Verhältnis von Privatrechtssubjekten zum Gegenstand haben, geht ebenfalls bereits auf die Datenschutz-RL (1995) zurück. Die Richtlinie selbst differenzierte kaum zwischen staatlichen und privaten Verantwortlichen, sondern etablierte weitgehend einheitliche Vorgaben für die Verarbeitung von personenbezogenen Daten, Art. 2 lit. d Datenschutz-RL. Dies verdeutlicht, dass nicht nur der deutsche, sondern auch der europäische Gesetzgeber von Anfang an einen einheitlichen, horizontalen Ansatz zum Schutz personenbezogener Daten verfolgte.

Die Fortführung dieses Ansatzes war auch deshalb möglich, weil das Problem der Horizontalwirkung vom *Europäischen Grundrechtekonvent* zwar gesehen, aber bewusst nicht diskutiert wurde. Diese Frage sollte dem *EuGH* überlassen bleiben.[180] Für die Etablierung einheitlicher Vorgaben half es, dass nach Ansicht des *EuGH* bereits die Datenschutz-RL von 1995 vollharmonisierend war, unabhängig davon, ob der jeweilige Verantwortliche eine Behörde oder ein privatwirtschaftlich organisiertes Unternehmen ist.[181]

Der europäische Gesetzgeber stellte klar, dass der Schutz von personenbezogenen Daten einheitlichen Vorgaben genügen müsse, unabhängig davon, ob Daten mit oder ohne Hilfe automatisierte Verfahren verarbeitet werden, Art. 2

---

[176] *Herresthal*, ZEuP 2014, 238 (269/275).

[177] *Streinz/Michl*, EuZW 2011, 384 (385: „Jedenfalls soweit die Folgen für den Betroffenen nicht vorhersehbar sind, greifen Einwände gegen den Schutz des privatautonomen Menschen vor sich selbst nicht durch.").

[178] *EuGH*, C-275/06 = EuZW 2008, 113 (Rn. 65/70) – *Promusicae*.

[179] *EuGH*, C-580/13 = EuZW 2015, 747 (Rn. 33) – *Coty Germany GmbH/Stadtsparkasse Magdeburg*; *EuGH*, C-131/12 = NJW 2014, 2257 (Rn. 80) – *Google Spain*.

[180] *Borowsky*, in: Meyer (Hrsg.), Art. 51, Rn. 31; hierzu ausführlich: *Marsch*, Das Europäische Datenschutzgrundrecht, 2018, S. 248 f.

[181] *EuGH*, Urt. v. 06.11.2003, C-101/01 = JZ 2004, 242 ff. (Rn. 96 f.) – *Lindqvist/Schweden*.

lit. b Datenschutz-RL. Grund hierfür war die Überzeugung, dass nur ein umfassender Ansatz in der Lage sei, Umgehungsversuche infolge einer „analogen Lücke" wirksam zu verhindern.[182] Damit hatte der europäische Gesetzgeber implizit auch die letzte Einwendung der deutschen Privatrechtswissenschaften gegen ein einheitliches Konzept von Datenschutz gegenüber staatlichen und privatwirtschaftlichen Verantwortlichen zurückgewiesen.[183]

Dieser Ansatz wurde auf der nächsten Stufe der Vereinheitlichung des europäischen Datenschutzrecht fortgeführt. Mittlerweile sind das Grundrecht auf Schutz personenbezogener Daten aus Art. 8 Abs. 1 GRCh und Art. 16 Abs. 1 AEUV die maßgeblichen Grundlagen der DS-GVO.[184] Wie bereits ausgeführt, wird der Schutz personenbezogener Daten nochmals durch Art. 7 GRCh verstärkt,[185] soweit die personenbezogenen Daten einen Bezug zum Privatleben und insbesondere zur privaten Kommunikation haben. Diese Verstärkung durch das Recht auf Schutz privater Kommunikation ist zusätzliche Grundlage der ePrivacy-RL[186] bzw. der weiterhin geplanten ePrivacy-VO,[187] die im Verhältnis zur DS-GVO spezielle Vorschriften zum Schutz der Privatsphäre[188] in der elektronischen Kommunikation enthält und nicht nur zugunsten natürlicher, sondern ebenfalls zugunsten juristischer Personen Anwendung findet.[189]

bb) Primärrechtlicher Vorrang der Einwilligung

Aus der gemäß Art. 8 Abs. 2 S. 1 GRCh unionsgrundrechtlich vorgesehenen Möglichkeit zur Einwilligung lässt sich eine institutionelle Garantie der informationellen Privatautonomie ableiten. Indem die Möglichkeit zur Einwilligung

---

[182] ErwG 27 Datenschutz-RL (1995).

[183] *Ehmann*, AcP 188 (1988), 230 (289); oben A.II.2.

[184] ErwG 1 und 166 DS-GVO.

[185] *Jarass*, GRCh, 4. Aufl. 2021, Art. 8, Rn. 4.

[186] Richtlinie 2002/58/EG v. 12.06.2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation), ABl. v. 31.07.2002, L 201, S. 37 ff.

[187] *EU-Kommission*, Vorschlag für eine Verordnung über die Achtung des Privatlebens und den Schutz personenbezogener Daten in der elektronischen Kommunikation und zur Aufhebung der Richtlinie 2002/58/EG, COM/2017/010 final.

[188] Darüber hinaus sind gemäß Art. 7 GRCh auch juristische Personen Grundrechtsträger, während Art. 8 GRCh nach h. A. nur natürliche Personen schützt. Für eine Ausweitung auf juristische Personen: *Jarass*, GRCh, 4. Aufl. 2021, Art. 8, Rn. 7. Zum Schutz der informationellen Privatautonomie von gewerblich tätigen juristischen Personen.

[189] Vorschnell für eine Einbeziehung juristischer Personen in den Kreis der Grundrechtsträger aus Art. 8 GRCh und deshalb – insoweit konsequent – mit dem „rechtspolitischen Appell, jedenfalls bei einer Reform der Datenschutzgrundverordnung juristische Personen in den Anwendungsbereich einzubeziehen": *Marsch*, Das Europäische Datenschutzgrundrecht, 2018, S. 276 f. Dieses Vorgehen würde zunächst eine grundlegende Abgrenzung zu den Schutzzwecken der Immaterialgüterrechte, einschließlich des Schutzes von Geschäftsgeheimnissen voraussetzen.

ausdrücklich primärrechtlich gewährleistet wird, ist es dem Gesetzgeber versagt, die Einwilligung durch eine stete Ausweitung oder systematische Bevorzugung von gesetzlichen Erlaubnistatbeständen zurückzudrängen.[190] Einschränkungen der Einwilligungsmöglichkeit sind – und seien sie noch so gut gemeint – Eingriffe in die durch die Einwilligungsmöglichkeit gemäß Art. 8 Abs. 2 S. 1 GRCh gewährleistete informationelle Privatautonomie und deshalb ihrerseits gemäß Art. 52 Abs. 1 S. 2 GRCh rechtfertigungsbedürftig.[191] Insoweit lässt sich von einer unionsgrundrechtlichen Garantie der Einwilligung gemäß Art. 8 Abs. 2 S. 1 GRCh sprechen.

Hieraus folgt ein primärrechtlicher Vorrang der Einwilligung vor anderen Erlaubnistatbeständen und es ist deshalb nicht möglich, lediglich den aus Sicht des Verantwortlichen „speziellsten Erlaubnistatbestand" heranzuziehen[192] oder die mit der Einwilligung aus Sicht des Verantwortlichen verbundene Unsicherheit durch beliebige Rückgriffe auf einen anderen Erlaubnistatbestand zu vermeiden.[193]

Auch das Anliegen, einwilligungsfähige Grundrechtsträger vor den für sie nachteiligen Folgen einer Einwilligung zu schützen, rechtfertigt es deshalb nicht, die Einwilligung durch hohe Anforderungen derart impraktikabel zu machen, dass Datenverarbeitungen zunehmend auf Grundlage von Generalklauseln oder auf Basis einer ständig wachsenden Anzahl von gesetzlichen Erlaubnistatbeständen stattfinden.[194]

---

[190] Jedenfalls für das privatrechtlich Verhältnis ebenso: *Bäcker*, Der Staat 51 (2012), 91 (100); *Marsch*, Das Europäische Datenschutzgrundrecht, 2018, S. 266. Anders im vertikalen Verhältnis: ebda., S. 151 („untergeordnete Auffangfunktion der Einwilligung").

[191] *Grimm*, JZ 2013, 585 (588); *Körber*, NZKart 2016, 348 (350); *Buchner*, Die Informationelle Selbstbestimmung im Privatrecht, 2006, S. 113 f.; *Krönke*, Der Staat 55 (2016), 319 (338); *Klement*, in: Simitis/Hornung/Spiecker gen. Döhmann (Hrsg.), 2019, Art. 7, Rn. 26/33/59. Allgemein zur Einwilligung: *Ohly*, Volenti non fit iniuria, 2002, S. 75 f. 105 ff.; m. w. N. *Neuner*, JuS 2021, 617 (618: „In der Gesamtschau ist die Einwilligung für den Erklärenden ein Medium zur Selbstbestimmung. Sie ist Ausdruck und Gebrauch von Privatautonomie […]").

[192] In diese Richtung: *Leistner/Antoine/Sagstetter*, Big Data, 2021, S. 247 f.

[193] A. A. und für ein Wahlrecht des Verantwortlichen: *Veil*, NJW 2018, 3337 (3338); *Schulz*, in: Gola (Hrsg.), Art. 6, Rn. 10; *Heckmann/Paschke*, in: Ehmann/Selmayr (Hrsg.), DS-GVO, 2017, Art. 7, Rn. 17; *Buchner/Kühling*, in: dies. (Hrsg.), DS-GVO, 2, Aufl. 2018, Art. 7, Rn. 16

[194] *Leistner/Antoine/Sagstetter*, Big Data, 2021, S. 401 („Für den nach heutigem Stand nahezu ubiquitären Bereich der Verarbeitung personenbezogener Daten verlagert sich angesichts des mit der Erfüllung der Einwilligungstatbestände verbundenen Kostenaufwands sowie der diesbezüglichen Schwierigkeiten und insbesondere erheblichen fortbestehenden rechtlichen Unsicherheiten die Bemühungen der Praxis um legitime Datenverarbeitung in vielen Bereichen derzeit zunehmend eher auf die Interessenabwägung"). Dieser Flucht aus der Einwilligung muss also bereits aufgrund von Art. 8 Abs. 2 S. 1 GRCh durch einen Vorrang der Einwilligung entgegengetreten werden. Hierzu unten: Kapitel 5.

III. Schutz der unternehmerischen Freiheit, Art. 16 GRCh

Nach der Rechtsprechung des *EuGH* gewährleistet Art. 16 GRCh das Recht der Person, seine wirtschaftlichen Interessen durch das Angebot von Waren und Dienstleistungen zu verfolgen. Der hierdurch gewährte Schutz umfasst dabei die Freiheit, eine Wirtschafts- oder Geschäftstätigkeit auszuüben, die Vertragsfreiheit und den freien Wettbewerb.[195]

Vom *EuGH* wurde noch nicht eindeutig entschieden, ob Art. 16 GRCh gleichermaßen zugunsten natürlicher wie juristischer Personen Anwendung findet, soweit diese eine Wirtschafts- oder Geschäftstätigkeiten ausüben. Allerdings sprechen der Wortlaut von Art. 16 GRCh („Unternehmen")[196] und die insoweit eindeutige *EuGH*-Rechtsprechung zum Recht auf einen wirksamen Rechtsbehelf (Art. 47 GRCh)[197] für eine Anwendbarkeit auf juristische Personen[198] und zwar unabhängig davon, ob diese ihren Sitz innerhalb oder außerhalb der Europäischen Union haben.[199] Damit können sich auch die datenschutzrechtlich Verantwortlichen auf den Schutz ihrer unternehmerischen Freiheit aus Art. 16 GRCh berufen.[200]

Ebenfalls offen ist, ob und inwieweit Datensubjekte sich – neben Art. 8 und Art. 7 GRCh – selbst auch auf einen Schutz ihrer unternehmerischen Freiheit berufen können. Es ist naheliegend, dass die gemäß Art. 8 Abs. 2 S. 1 GRCh zu gewährleistende Entfaltungsmöglichkeit des Datensubjekts durch Erteilung einer Einwilligung nochmals durch den Schutz der unternehmerischen Freiheit verstärkt wird. Sofern Datensubjekte die Einwilligung nicht nur als Verbraucher dafür einsetzen, um ihr privates Budget für den Konsum von digitalen

---

[195] *EuGH*, EuZW 2013, 347 (Rn. 42) – *Sky Österreich*; *EuGH*, BeckRS 2013, 81980 (Rn. 25) – *Schaible*; *EuGH*, GRUR 2014, 895 (Rn. 81/97) – *Google Spain*; *Everson/Correia Gonçalves*, in: Peers/Hervey/Kenner/Ward (Hrsg.), Art. 16, Rn. 16.34 ff.).

[196] So auch: *BVerfG*, Beschl. v. 06.11.2019, 1 BvR 276/17 = GRUR 2020, 88 (Rn. 104) – *Recht auf Vergessen II*. Diese Auslegung anhand des Wortlauts nimmt das BVerfG selbst vor, obwohl es dies über die Anwendung von Unionsgrundrechten hinausgeht. Insoweit hätte es diese Frage – nach seiner eigenen Differenzierung zwischen Auslegung und Anwendung – eigentlich zunächst dem *EuGH* vorlegen müssen.

[197] *EuGH*, EuZW 2011, 137 (Rn. 38 ff.) – *DEB*.

[198] M.w.N. *Jarass*, in: ders. (Hrsg.), GRCh, 3. Aufl. 2016, Art. 16, Rn. 11.

[199] *EuGH*, EuZW 1996, 595 (Rn. 21 ff.) – *Bosphorus/Minister for Transport, Energy and Communications*; *EuG*, Urt. v. 06.09.2013, T-7/11 = BeckRS 2013, 81654 (Rn. 70) – *Bank Melli Iran/Rat*; *EuG*, Urt. v. 29.04.2015, T-10/13 = BeckRS 2016, 81567 (Rn. 58) – *Bank of Industry and Mine/Rat*; dazu *Sasse*, EuR 2012, 628 (636 ff.); *Jarass*, in: *ders.* (Hrsg.), GRCh, 3. Aufl. 2016, Art. 51, Rn. 52.

[200] Symptomatisch für die Rechtsprechung des EuGH, werden in Google Spain die Interessen des Verantwortlichen bereits verbal abgewertet, nicht grundrechtlich verortet und das Verhalten von Alphabet dem staatlichen Handeln („Eingriff") gleichgestellt: „Wegen seiner potenziellen Schwere kann ein solcher Eingriff nicht allein mit dem wirtschaftlichen Interesse des Suchmaschinenbetreibers an der Verarbeitung der Daten gerechtfertigt werden", *EuGH*, C-362/14 = GRUR 2014, 895 (Rn. 81) – *Google Spain*.

Produkten zu erweitern,[201] sondern um ein (zusätzliches) monetäres Einkommen zu erzielen, kann dieses Verhalten zusätzlich in den Gewährleistungsbereich von Art. 16 GRCh fallen. Jedenfalls Prominente und jene Personen, die ihr überwiegendes Einkommen als Werbeträger für ein Produkt oder als sog. Influencer erzielen, müssen sich auf Art. 16 GRCh berufen können. Diese unternehmerisch handelnden Datensubjekte gestatten die Verarbeitung von personenbezogenen Daten, um im Gegenzug ein monetäres Honorar oder anderweitige materielle Vorteile gewährt zu bekommen.[202]

Insgesamt wirft die Verankerung der Vertragsfreiheit auf Ebene der europäischen Grundrechte weiterhin Fragen auf. Die Vertragsfreiheit ist zwar notwendige Voraussetzung der unternehmerischen Freiheit und wurde vom *EuGH* unter Rückgriff auf die Erläuterungen zur GRCh[203] auch als eine durch Art. 16 GRCh geschützte und gewährleistete Freiheit anerkannt.[204] Es besteht jedoch eine Schwierigkeit, die Gewährleistung der allgemeinen Vertragsfreiheit zugunsten von Datensubjekten zu verorten, die nicht als Unternehmer, sondern als Verbraucher handeln. Abgesehen von den unternehmerisch agierenden Datensubjekten sollen die personenbezogenen Daten von diesen Otto-Normal-Datensubjekten nach ErwG 24 der Richtlinie 2019/770 über bestimmte vertragsrechtliche Aspekte der Bereitstellung digitaler Inhalte und digitaler Dienstleistungen (DID-RL)[205] zwar weder Ware noch Dienstleistung sein, sie werden aber faktisch und rechtlich zunehmend als vertraglicher Leistungsgegenstand behandelt (Art. 3 Abs. 1 S. 2 DID-RL)[206] und auch von Datensubjekten zunehmend bewusst als Substitut für eine Geldzahlung eingesetzt, um das Konsumbudget zu erweitern bzw. das monetäre Konsumbudget zu schonen. Im Rahmen seiner Umsetzung der DID-RL akzeptiert der deutsche Gesetzgeber diese Realität nunmehr zumindest ansatzweise in § 327 Abs. 3 BGB.[207]

Soweit Datensubjekte als Verbraucher lediglich ihr privates Konsumbudget erweitern, indem ihre Einwilligung in die Datenverarbeitung die Zahlung eines Geldbetrags substituiert, handeln sie gerade nicht als Unternehmer. Ein Datensubjekt bleibt auch dann Verbraucher, wenn es in die Verarbeitung von personenbezogenen Daten einwilligt, um dadurch einen Zugang zu Gütern zu be-

---

[201] *Metzger*, in: Lohsse/Schulze/Staudenmayer (Hrsg.), Data as Counter-Performance: Contract Law 2.0?, 2020, S. 25 (41); *Hacker*, Datenprivatrecht, 2020, S. 58.

[202] Zu dieser – in der datenschutzrechtlichen Literatur bislang vernachlässigten – Möglichkeit und ihren Konsequenzen für die Freiwilligkeit und die Widerruflichkeit der Einwilligung: Kapitel 4 B.I.2. bzw. B.II.2. sowie Kapitel 5 C.II.2.b. bzw. III.2.b.

[203] Erläuterungen zur Charta der Grundrechte, ABl. 2007, C 303, S. 17.

[204] *EuGH*, Urt. v. 18.07.2013, C-426/11 = EuZW 2013, 747 (Rn. 32) – *Alemo-Herron*.

[205] ABl. v. 22.05.2019, L 136, S. 1 ff.

[206] Hierzu Kapitel 3 C.III.1.

[207] Gesetz zur Umsetzung der Richtlinie über bestimmte vertragsrechtliche Aspekte der Bereitstellung digitaler Inhalte und digitaler Dienstleistungen, v. 25.06.2021, BGBl. v. 30.06.2021, Teil I Nr. 37, S. 2123 ff.

kommen, der anderenfalls nicht oder jedenfalls nur gegen Geldzahlung eröffnet würde (Budgeterweiterung). Obwohl solche Datensubjekte, die in eine Datenverarbeitung einwilligen, ihre personenbezogene Daten kommerzialisieren, bleiben sie Verbraucher und können sich infolgedessen nicht auf Art. 16 GRCh berufen.

Verpflichtet sich ein Datensubjekt jedoch vertraglich dazu, erkennbar und öffentlichkeitswirksam als Werbeträger für ein bestimmtes (anderes) Unternehmen tätig zu sein, kann es sich bei dieser Verpflichtung auf die Berufsfreiheit gemäß Art. 15 Abs. 1 GRCh berufen, soweit diese Tätigkeit mit einem Beschäftigungsvertrag einhergeht[208] und nicht in Form der unternehmerischen Selbstständigkeit i. S. d. Art. 16 GRCh erfolgt.

Im Ergebnis bestehen auf Ebene der Unionsgrundrechte noch erhebliche Abgrenzungsschwierigkeit zwischen der in Art. 16 GRCh gewährleisteten unternehmerischen Vertragsfreiheit für unternehmerisch handelnde Datensubjekte, der gemäß Art. 15 Abs. 1 GRCh gewährleisteten Freiheit eines Datensubjekts zum Abschluss von Beschäftigungsverträgen und der allgemeinen Vertragsfreiheit solcher Datensubjekten, die ihre personenbezogenen Daten zwar ebenfalls kommerzialisieren, dabei aber dennoch Verbraucher bleiben.

Jedenfalls aus deutscher Perspektive fehlt für letztere ein europäisches Funktionsäquivalent zur allgemeinen Handlungsfreiheit aus Art. 2 Abs. 1 GG (hierzu sogleich), so dass die Gewährleistung der informationellen Privatautonomie von Datensubjekten, die Verbraucher sind, letztlich vorrangig aus der in Art. 8 Abs. 2 S. 1 GRCh verankerten unionsgrundrechtlichen Garantie der Einwilligung folgt.

IV. Schutz der allgemeinen Handlungsfreiheit von Datensubjekten

Die Privatautonomie ist nach deutschem Grundrechtsverständnis normgeprägt. Ohne ihre positive rechtliche Gewährleistung gäbe es weder die Privatautonomie als solche noch ihre spezifischen Ausprägungen, insbesondere die Vertragsfreiheit.[209] Das *BVerfG* hat aus der Privatautonomie die Pflicht des deutschen Gesetzgebers abgeleitet,

„rechtsgeschäftliche Gestaltungsmittel zur Verfügung zu stellen, die als *rechtlich verbindlich* zu behandeln sind und auch im Streitfall *durchsetzbare Positionen begründen*".[210]

---

[208] *Schubert*, in: Franzen/Gallner/Oetker (Hrsg.), Kommentar zum europäischen Arbeitsrecht, 2020, Art. 16, Rn. 10.

[209] *Flume*, FS 100 Jahre Dt. Juristentag, Bd.1, 1960, S. 135; *Höfling*, Vertragsfreiheit, 1991, S. 28 ff.

[210] BVerfGE 89, 214 (321 f.) [Hervorhebung durch den Verfasser]. Zur Bedeutung für die Flexibilisierung der Widerruflichkeit der Einwilligung, unten Kapitel 5.C.III.

Zudem sorgt Art. 2 Abs. 1 GG auch dafür, dass staatliche Einschränkungen der allgemeinen Handlungsfreiheit ihrerseits der Rechtfertigung durch verfassungskonforme Gesetze bedürfen. Kurzum: Eine Privatrechtsgesellschaft[211] basiert darauf, dass die Handlungsfreiheit die Regel und das Verbot die begründungspflichtige Ausnahme bleibt.

Allerdings hat das europäische Recht den im Einklang mit dem Grundgesetz entwickelten Topos der Privatrechtsgesellschaft nicht übernommen und enthält auch keine funktionsäquivalente Gewährleistung der allgemeinen Handlungsfreiheit im Sinne des Art. 2 Abs. 1 GG. Auch in der Rechtsprechung des *EuGH* kommt dem Schutz der Privatautonomie bislang nur geringe explizite Bedeutung zu,[212] wenngleich die Vertragsfreiheit für die Verwirklichung der vier Binnenmarktfreiheiten für Waren, Personen, Dienstleistungen und Kapital fundamental ist. Zudem bezeichnete der *EuGH* ein allgemeines Freiheitsrecht bisweilen als allgemeinen Rechtsgrundsatz.[213] Infolgedessen kann die Vertragsfreiheit, die ein wesentlicher Ausdruck der Privatautonomie ist, als ungeschriebenes Unionsgrundrecht i.S.d. Art. 6 Abs. 3 EUV bezeichnet werden.[214] Dennoch wird die Vertragsfreiheit vom *EuGH* bislang nicht als eigenständiges ungeschriebenes Grundrecht angesprochen, sondern steht regelmäßig im Zusammenhang mit der Berufsfreiheit (Art. 15 GRCh), der freien Wahl des Geschäftspartners[215] oder der unternehmerischen Freiheit (Art. 16 GRCh).[216]

Somit setzt der *EuGH* eine Gewährleistung der Vertragsfreiheit zwar voraus, hat diese jedoch weder näher ausdifferenziert noch – soweit ersichtlich – jemals eine sekundärrechtliche oder nationale Regelung wegen einer Verletzung des allgemeinen unionsrechtlichen Grundrechts der Vertragsfreiheit für nichtig erklärt. Immerhin bedingen sich europäisches Verbraucherschutzrecht und Vertragsfreiheit gegenseitig. Jedenfalls soweit das Unionsrecht den Verbraucherschutz in einem Bereich voll- oder auch nur mindestharmonisiert, muss der europäische Gesetzgeber mittelbar davon ausgehen, dass – gleichsam oberhalb dieser Vollharmonisierung – grundsätzlich Raum für die Vertragsfreiheit verbleibt.

Die fehlende explizite Gewährleistung einer allgemeinen Handlungsfreiheit und ihrer Ausprägung in Form einer allgemeinen Vertragsfreiheit hat zur Folge,

---

[211] *Böhm*, ORDO 117 (1966), 75.

[212] *Herresthal*, ZEuP 2014, 238 (244).

[213] *EuGH*, Urt. v. 21.05.1987, C-133/95, Rn. 15 (19) – *Rau*.

[214] *Ruffert*, in: Ehlers (Hrsg.), Europäische Grundrechte und Grundfreiheiten, 4. Aufl. 2015, § 16.3 Rn. 12; *Calliess/Ruffert/Ruffert*, GRCh Art. 16, Rn. 2; *Schöbener/Stork*, ZEuS 2004, 43 (55 ff.) sowie *Herresthal*, in: Ziegler/Huber (Hrsg.), Current Problems in the Protection of Human Rights, 2013, 97 ff.; *ders*., BeckOGK, (Stand: 01.06.2019) § 311, Rn. 13.

[215] *EuGH*, Urt. v. 10.07.1991, verb. C-90/90 u. C-91/90 = BeckRS 2004, 77886, Rn. 13; *Ruffert*, Vorrang der Verfassung und Eigenständigkeit des Privatrechts, 2001, S. 297 f.

[216] *EuGH* v. 11.01.1977, C- 4/73 = BeckRS 2004, 71093, Rn. 14 – *Nold*; *EuGH*, Urt. v. 07.02. 1985, 240/83 = BeckRS 2004, 72561, Rn. 9 – *ADBHU*.

dass das Privatrecht auf europäischer Ebene mit einer „Phalanx des Grundrechtsschutzes“[217] konfrontiert ist. Dieser muss die Vertragsfreiheit als ungeschriebenes Unionsgrundrecht i. S. d. Art. 6 Abs. 3 EUV aktiv entgegengesetzt werden. Weil die Privatautonomie in den europäischen Grundrechten nur wenige Verankerungen findet und diese zudem – wie Art. 16 GRCh für die unternehmerische Freiheit – bislang kaum durch den *EuGH* präzisiert wurden,[218] ist die Privatautonomie der blinde Fleck des ansonsten detailreich ausdifferenzierten primärrechtlichen Grundrechtskatalogs. Infolgedessen droht eine Konstitutionalisierung des Unionprivatrechts,[219] die mit der Gefahr einer „Hypotrophie der Vertragsfreiheit im Unionsrecht“ einhergeht.[220]

Aufgrund der bislang nur vagen Gewährleistung der Privatautonomie durch den *EuGH*, die durch die Grundfreiheiten auch nicht kompensiert werden kann, ist das Fehlen eines expliziten Unionsgrundrechts als Äquivalent der allgemeinen Handlungsfreiheit nach *Carsten Herresthal* der „schwerwiegende Konstruktionsfehler“[221] der GRCh. Diese primärrechtliche Lücke begünstigt strukturell die Tendenz „eines privatrechtsgefährdenden Grundrechtsaktivismus des *EuGH*“[222] und damit die Gefahr eines „unabgestimmten, hypertrophen Grundrechtschutzes“.[223]

Infolgedessen besteht eine latente Gefahr, dass europäisches Recht gegen die verfassungsrechtlichen Freiheitsgewährleistungen aus Art. 2 Abs. 1 GG verstößt, sofern die Eigenwertungen des Privatrechts auf Ebene der Unionsgrundrechte „entkernt und zu sehr mit abweichenden grundrechtlichen Wertungen aufgeladen“ werden.[224] Sollte das *BVerfG* seine gegenüber dem europäischen Grundrechtsschutz verbleibende Reservefunktion aktivieren müssen oder wollen,[225] so ist eine nach deutschem Maßstab ungenügende primärrechtliche Gewährleistung der Vertragsfreiheit hierfür ein potenzieller Ausgangspunkt.

---

[217] *Herresthal*, ZEuP 2014, 238 (246 f.).

[218] *Herresthal*, ZEuP 2014, 238 (278).

[219] So für das sog. Verbot mit Erlaubnisvorbehalt und den Zweckbindungsgrundsatz: *Marsch*, Das Europäische Datenschutzgrundrecht, 2018, S. 150/258.

[220] *Lüttringhaus*, Vertragsfreiheit, 2018, S. 15; ähnlich: *Wagner*, in: Blaurock/Hager (Hrsg.), Obligationenrecht im 21. Jahrhundert, S. 13 (77).

[221] *Herresthal*, ZEuP 2014, 238 (265); *ders.*, BeckOGK, (Stand: 01.06.2019) § 311 Rn. 15.

[222] *Herresthal*, ZEuP 2014, 238 (246 f.).

[223] *Herresthal*, ZEuP 2014, 238 (277); ähnlich, aber die Kritik auf die Anwendung des speziellen Diskriminierungsverbots aus Art. 21 GRCh beschränkend: *Ruffert*, JuS 2020, 1 (6: „drohen in der unspezifischen unmittelbaren Drittwirkung von Art. 21 GRCh mindestens punktuell nicht legitimierte Freiheitsverluste“).

[224] Maunz/Dürig/*Di Fabio*, GG, 81. EL 09/2017, Art. 2 Abs. 1, Rn. 105.

[225] Im Unterschied dazu, setzt das in *Recht auf Vergessen I* begründete Kooperationsverhältnis gerade voraus, dass der EuGH die wesentlichen Auslegungsfragen und Anwendungsleitlinien eines unionsrechtlichen Grundrechts bereits hinreichend konkretisiert hat: *BVerfG*, Beschl. v. 06.11.2019, 1 BvR 16/13 = NJW 2020, 300 (Rn. 74/154) – *Recht auf Vergessen I*.

V. Informationelle Privatautonomie und gerichtliche Kooperation

Obwohl der *EuGH* zuletzt grundlegende Urteile zu Art. 7 GRCh und Art. 8 GRCh gefällt hat, bleiben der Schutz- und Gewährleistungsbereich dieser Grundrechte – wie ausgeführt – weiterhin vage. Dafür gibt es drei Gründe:

Erstens gerinnt der Schutz- und Gewährleistungsbereich von Grundrechten regelmäßig erst über lange Zeiträume im Wege der Induktion. Der von einem Grundrecht umfasste Schutz- und Gewährleistungsbereich gleicht einem Mosaik. Wie das Mosaikbild durch viele kleine Steine, so setzt sich auch die Definition des Schutz- und Gewährleistungsbereichs erst sukzessive, als Verallgemeinerung der jeweils im Einzelfall festgestellten Eingriffe zusammen. Es braucht eine gewisse Mindestanzahl entschiedener Sachverhalte, bis ein Gesamtmotiv anhand der Einzelfälle allmählich erkennbar wird. Erst retrospektiv, also nach einer Entwicklungsphase, ergibt sich allmählich ein systematischer Zusammenhang, der dann als abstrahierter Schutz- und Gewährleistungsbereich den Ausgangspunkt einer Grundrechtsprüfung bilden kann.

Zweitens sind weder das Vertragsverletzungsverfahren (Art. 258 AEUV) noch die spezifischen Fragen des Vorlageverfahrens gemäß Art. 267 AEUV besonders gut dafür geeignet, solche abstrakten Definitionen der Schutz- und Gewährleistungsbereiche von europäischen Grundrechten hervorzubringen. Sofern der *EuGH* überhaupt zwischen dem Schutz- oder dem Gewährleistungsbereich, dem Eingriff und der Rechtfertigung unterscheidet,[226] liegt der Schwerpunkt meist auf der Feststellung und Begründung eines Eingriffs und den Möglichkeiten, diesen zu rechtfertigen. Für das Privatrechtsverhältnis wird diese Herangehensweise anhand des *Google-Spain* Urteils des *EuGH* deutlich.[227]

Drittens erweckt die Analyse der jüngeren Urteile des *EuGH* den Eindruck, dass der *Gerichtshof* (Große Kammer) es bewusst vermeidet, die Schutz- und Gewährleistungsbereiche und das Verhältnis zwischen Art. 7 und Art. 8 GRCh zu spezifizieren.[228] Weil der *EuGH* auf diesen dritten Gesichtspunkt jedoch Einfluss hat, ist er für diesen mangelnden Willen zur Herausbildung von Systematik und Rechtssicherheit zu kritisieren.[229] Die hieraus resultierende Unbestimmtheit des Schutz- und Gewährleistungsbereichs von Art. 7 und Art. 8

---

[226] Insoweit lehrbuchartig: *EuGH* (Große Kammer), C-293/12, C-594/12 = NJW 2014, 2169 – *Digital Rights Ireland*.

[227] *EuGH*, C-362/14 = GRUR 2014, 895 (Rn. 81) – *Google Spain*: „Wegen seiner potenziellen Schwere kann ein solcher *Eingriff* nicht allein mit dem wirtschaftlichen Interesse des Suchmaschinenbetreibers an der Verarbeitung der Daten *gerechtfertigt* werden" [Hervorhebungen durch den Verfasser].

[228] *EuGH* (Große Kammer), C-293/12, C-594/12 =NJW 2014, 2169 (Rn. 23/29 ff.) – *Digital Rights Ireland*.

[229] A. A. zur EuGH-Entscheidung *Digital Rights Ireland*: *Kühling*, NVwZ 2014, 681 (682: „Der EuGH hat sich durch die teils komplex formulierten und differenzierten Vorlagefragen des irischen High Courts und des Österreichischen Verfassungsgerichts nicht auf Nebenkriegsschauplätze führen lassen […]").

GRCh dürfte das *BVerfG* darin bestärkt haben, seine eigene Rolle im judikativen Gefüge künftig möglicherweise selbstbewusster zu interpretieren.[230]

Ansatzpunkt für die Initiative des *BVerfG* sind Art. 51 Abs. 1 S. 1 GRCh und Art. 6 Abs. 1 EUV. Hiernach binden die GRCh und das Primärrecht nicht nur die Organe, Einrichtungen und Stellen der Union, sondern auch die Mitgliedstaaten und deren Stellen, soweit diese Unionsrecht ausführen. Hieraus leitet das *BVerfG* nicht nur – insoweit unbestritten – ab, dass die Unionsgrundrechte innerstaatlich anwendbar sind, sondern folgert zudem, dass die Grundrechte des Grundgesetzes ein „Funktionsäquivalent" zu den europäischen Grundrechten bilden.[231] Über den Brückenkopf dieser funktionalen Äquivalenz sieht das *BVerfG* sich gemäß Art. 23 Abs. 1 GG dazu verpflichtet und berufen, dem *EuGH* ein Kooperationsverhältnis anzutragen.[232]

Diese Arbeitsteilung soll sich nach Auffassung des *BVerfG* derart vollziehen, dass die letztverbindliche Auslegung des Unionsrechts beim *EuGH* verbleibt.[233] Somit ist nur der *EuGH* für die Auslegung der Grundrechte der Charta und die Entwicklung der aus ihnen abzuleitenden Anwendungsgrundsätze verantwortlich. Allerdings nimmt das *BVerfG* für sich die Kompetenz in Anspruch, die richtige Anwendung der Unionsgrundrechte durch die nationalen Fachgerichte als letzte Instanz zu kontrollieren. Nur sofern die Auslegung der Unionsgrundrechte noch Fragen aufwirft, weil bislang weder die Rechtsprechung des *EuGH* noch diejenige des *EGMR* (Art. 52 Abs. 3, Abs. 4 GRCh) ausreichende Anwendungsgrundsätze bereithalten, müsse das *BVerfG* dem *EuGH* künftig noch Auslegungsfragen vorlegen.[234]

Die vom *BVerfG* in *Recht auf Vergessen II* vorgeschlagene und im Anschluss auch sogleich umgesetzte „Kooperation"[235] leuchtet auf den ersten Blick ein.

---

[230] Mit der Prognose und Forderung diese Entwicklung: *Thym*, JZ 2015, 53 (61); *Bäcker*, EuR 2015, 389 (400 f.); *Marsch*, Das Europäische Datenschutzgrundrecht, 2018, S. 298 ff.

[231] Hierzu ausdrücklich: *BVerfG*, Beschl. v. 06.11.2019, 1 BvR 276/17 = GRUR 2020, 88 (Rn. 59) – *Recht auf Vergessen II*.

[232] Zur Begründung dieses „Kooperativen Grundrechtsschutzes in der EU": *Britz*, NJW 2021, 1489 (1494 f. „Würde es sich in Regelungsmaterien, die durch das Unionsrecht vollständig vereinheitlicht sind, aus dem Grundrechtsschutz herausziehen, könne es die ihm übertragene Aufgabe des Grundrechtsschutzes mit zunehmender Verdichtung des Unionsrechts immer weniger wahrnehmen. Die für die Begründung der Entscheidung bedeutsame Schutzlücke hinsichtlich der fachgerichtlichen und behördlichen Anwendung der Unionsgrundrechte wird nicht durch entsprechende Rechtsbehelfe auf der Ebene des Unionsrechts geschlossen. Denn eine Möglichkeit Einzelner, die Verletzung von Unionsgrundrechten durch die mitgliedstaatlichen Fachgerichte unmittelbar vor dem EuGH geltend zu machen, besteht nicht").

[233] Zu den Schwierigkeiten einer klaren Differenzierung zwischen der Auslegung und Anwendung: *Knauff*, DÖV 2013, 375 (378 f.); *Marsch*, Das Europäische Datenschutzgrundrecht, 2018, S. 356.

[234] Hierzu ausdrücklich: *BVerfG*, Beschl. v. 06.11.2019, 1 BvR 276/17 = GRUR 2020, 88 (Rn. 69 f.) – *Recht auf Vergessen II*.

[235] *BVerfG*, Beschl. v. 06.11.2019, 1 BvR 276/17 = GRUR 2020, 88 (Rn. 98 ff./138 ff.) – *Recht auf Vergessen II*.

Das *BVerfG* hat große Erfahrung darin, die Schutz- und Gewährleistungsbereiche behutsam und systembildend zu entwickeln. Dieser Kooperationsansatz hat aber zwei wesentliche Nachteile.

Erstens muss eine solche Kooperation nicht nur das *BVerfG*, sondern alle nationalen Verfassungsgerichte einbeziehen. Dadurch besteht die Gefahr einer verfassungsgerichtlichen Kakophonie, sofern keine klaren Regeln für die Abgrenzung zwischen Auslegung (einschließlich Anwendungsleitsätzen) und der Anwendung als Grundlage für diese Kooperation gefunden werden.

Zweitens formuliert das *BVerfG* selbst eine Voraussetzung für diese Kooperation. Der *EuGH* muss die europäischen Grundrechte zunächst ausreichend klar und eindeutig definieren. Allenfalls im Anschluss hieran sollen die nationalen Verfassungsgerichte kontrollieren, ob diese Grundsätze des *EuGH* auch durch die nationalen Fachgerichte eingehalten werden.[236] Jedenfalls mit Blick auf den Schutz- und Gewährleistungsbereich von Art. 7 und Art. 8 GRCh und das allgemeine Grundrecht der Vertragsfreiheit (Art. 6 Abs. 3 EUV) fehlt es bereits an dieser ersten Voraussetzung. Der *EuGH* hat die grundrechtliche Dimension des Datenschutzes zwar wiederholt betont. Die normative Basis, die dogmatische Konstruktion dieses Grundrechts[237] und deren Bedeutung für das Privatrechtsverhältnis im Allgemeinen und insbesondere der Zusammenhang zwischen datenschutzrechtlicher Einwilligung (Art. 8 Abs. 2 S. 1 GRCh) und der Vertragsfreiheit sind aber weiterhin vage.[238]

Häufig erschöpft sich die Beschäftigung mit dem durch Art. 8 GRCh gewährleisteten Schutz in einer Wiederholung von dessen Wortlaut.[239] Zuletzt hat der *EuGH*, insbesondere mit Blick auf die Wirkung des Art. 8 GRCh im Rahmen von Streitigkeiten zwischen Privaten, immerhin punktuell einzelne Komponenten des Datenschutzes hervorgehoben und anhand der sekundärrechtlichen Anforderungen konkretisiert.[240] Dennoch fehlt eine klare Definition des Schutz- und Gewährleistungsbereichs von Art. 8 GRCh (ggfs. i. V. m. Art. 7 GRCh).

---

[236] *BVerfG*, Beschl. v. 06.11.2019, 1 BvR 276/17 = GRUR 2020, 88 (Rn. 59) – *Recht auf Vergessen II*.

[237] Hierzu mit dem bislang detailliertesten Vorschlag: *Marsch*, Das Europäische Datenschutzgrundrecht, 2018, S. 124 ff./276 ff.

[238] A. A. (wohl) *Britz*, NJW 2021, 1489 (1495: „Vor allem aber gibt es bei der inhaltlichen Weiterentwicklung der Grundrechte auch jenseits von Vorlageverfahren eine Kooperation zwischen nationalen Verfassungsgerichten und *EuGH* durch intensive wechselseitige Entscheidungsrezeption. So ist aus den Entscheidungen des *Gerichtshofs* zur Vorratsdatenspeicherung die über Jahrzehnte entwickelte Rechtsprechung des *BVerfG* zum Recht auf informationelle Selbstbestimmung ebenso schwer wegzudenken, wie aus der Entscheidung des *BVerfG* Recht auf Vergessen II die vorausgegangene Rechtsprechung des Gerichtshofs".

[239] *EuGH*, GRUR 2008, 241 (Rn. 64) – *Promusicae*; *EuGH*, EuZW 2012, 37 (Rn. 41 f.) – *ASNEF*; *EuGH*, C-92/09 u. a. = EuZW 2010, 939 (Rn. 47) – *Volker und Markus Schecke und Eifert*.

[240] *EuGH* (Große Kammer), verb. C-293/12, C-594/12 = NJW 2014, 2169 (Rn. 37: „das Gefühl zu erzeugen, dass ihr Privatleben Gegenstand einer ständigen Überwachung ist") – *Digital Rights Ireland*; *EuGH*, C-362/14 = GRUR 2014, 895 (Rn. 69 ff.) – *Google Spain*; zu

Ob und inwieweit sich die Auslegung und die Anwendungsgrundsätze des durch Sekundärrecht normgeprägten Art. 8 GRCh nach Anwendbarkeit der DS-GVO geändert hat, lässt sich ebenfalls nur herausfinden, indem dem *EuGH* gemäß Art. 267 Abs. 3 AEUV Auslegungsfragen vorgelegt werden,[241] statt sie als nationales Verfassungsgericht selbst zu beantworten.[242] Zugleich folgt der *EuGH* dieser – theoretisch vorhandenen – Arbeitsteilung zwischen der Auslegung und Anwendung des Unionsrechts nicht. Vielmehr lässt sich mit Blick auf Art. 7 und Art. 8 GRCh eine Tendenz dafür nachweisen, dass der *EuGH* den Begriff der Auslegung i. S. d. Art. 267 AEUV bisweilen sehr weit interpretiert: Handelt es sich bei dem Verantwortlichen um ein global, jedenfalls aber unionsweit tätiges Unternehmen, so beschränkt sich der *EuGH* regelmäßig nicht auf die Bestimmung von Leitlinien. Stattdessen entscheidet er den Sachverhalt anhand der konkreten Tatsachen durch.[243]

Kurzum: Das Kooperationsangebot des *BVerfG* ist möglicherweise gut gemeint. An den Schnittstellen zwischen Datenschutz und Äußerungsrecht fehlen aber die vom *BVerfG* selbst aufgestellten Voraussetzungen. Der Schutz- und Gewährleistungsbereich des Art. 8 GRCh ist bislang zu vage und hat noch keine eigenständige Funktion neben der DS-GVO gefunden. Trotz der Einschätzung, das Urteil *Recht auf Vergessen II* werde zu einer Zunahme von Vorlageverfahren durch das *BVerfG* führen,[244] läuft der vom *BVerfG* verfolgte Kooperationsansatz Gefahr, in einer Auslegung des Sekundärrechts durch das *BVerfG* zu enden. Zudem fehlen – jedenfalls für den hier relevanten Schutz der Datensubjekte vor einer Verarbeitung von personenbezogenen Daten – auf europäischer Ebene bislang auch die Auslegungsregeln und Grundsätze, nach denen ein Ausgleich zwischen dem zu gewährleistenden Schutz von Datensubjekten, der Gewährleistung der unternehmerischen Freiheit und der Gewährleistung der Vertragsfreiheit für Verantwortliche und Datensubjekte gelingen könnte.

Art. 8 Abs. 3 GRCh: *EuGH*, C-362/14 = NJW 2015, 3151 (Rn. 40 ff.) – *Schrems I*; *Reinhardt*, AöR 142 (2017), 564.

[241] So zuletzt: *OLG Düsseldorf*, Vorlagebeschl. v. 24.03.2021, Kart 2/19 (V) = NZKart 2021, 306 ff.; *ÖOGH*, Vorlagebeschl. v. 22.07.2021, 6 Ob 56/21k – *Schrems* [*III*].

[242] *Bernsdorff*, in: Meyer/Hölscheidt (Hrsg.), GRCh, 5. Aufl. 2019, Rn. 19; a. A. *BVerfG*, Beschl. v. 06.11.2019, 1 BvR 276/17 = GRUR 2020, 88 (Rn. 138 ff.) – *Recht auf Vergessen II*. Zur zweiten Entscheidung einer Anwendung der (geklärten) Unionsgrundrechte: *BVerfG* (Zweiter Senat) NJW 2021, 1518 (Rn. 42 ff.) – *Rumänien II*.

[243] Mit abschließender Interessenabwägung: *EuGH*, C-131/12 = NJW 2014, 2257 – *Google Spain*; hierzu: *Marsch*, Das Europäische Datenschutzgrundrecht, 2018, S. 362 f./368.

[244] *Britz*, NJW 2021, 1489 (1495: „In unionsrechtlich vollständig determinierten Konstellationen (Recht auf Vergessen II) werden Vorlagen nach Art. 267 AEUV hingegen vermehrt in Betracht zu ziehen sein, weil dann Unionsgrundrechte und gegebenenfalls auch die diese betreffenden Auslegungsfragen unmittelbar entscheidungserheblich sind. […] Divergierende Auffassungen sind natürlich auch hier nicht ausgeschlossen").

C. Gefährdung der informationellen Privatautonomie

Wie ausgeführt, fanden die Einwände, die aus privatrechtlicher Perspektive gegen ein Verarbeitungsverbot als einheitlichem Ausgangspunkt von Regulierung erhoben wurden,[245] seinerzeit keine politische Unterstützung. Infolgedessen beruhte das deutsche Datenschutzrecht auf einer überschießenden Interpretation des *Volkszählungsurteils* durch den deutschen Gesetzgeber.

Auch der europäische Gesetzgeber übernahm diesen Ansatz in der Datenschutz-RL (1995) und setzte ihn in der DS-GVO fort. Es dürften zunächst primär Hoheitsträger und wenige, dafür aber dominante private Verantwortliche gewesen sein, die dem europäischen Gesetzgeber als Adressaten der DS-GVO vor Augen standen. Eine solche gesetzgeberische Perspektive, die sich aus privatrechtlicher Sicht an den Extremen orientiert, läuft Gefahr, einer Hypertrophie der Grundrechte Vorschub zu leisten und infolgedessen in einen ständigen Konflikt mit dem Verhältnismäßigkeitsgrundsatz zu geraten.

Ausgangspunkt dieser Konfliktlage ist das grundsätzliche Verbot personenbezogene Daten zu verarbeiten. Gemäß Art. 6 Abs. 1 DS-GVO ist eine Verarbeitung von personenbezogenen Daten nur rechtmäßig, wenn mindestens eine der in Art. 6 vorgesehenen Ausnahmen („Bedingungen") erfüllt ist. Damit konkretisiert Art. 6 den bereits in Art. 5 Abs. 1 lit. a DS-GVO erwähnten Grundsatz der Rechtmäßigkeit.

In der Literatur wird diskutiert, ob Art. 6 Abs. 1 DS-GVO – und für besonders sensible personenbezogene Daten: Art. 9 Abs. 1 DS-GVO – ein Verbot mit Erlaubnisvorbehalt[246] oder ein Verbot mit Regelungsvorbehalt[247] enthält (I).[248] Unabhängig von dieser begrifflichen Zuspitzung sind Art. 6 Abs. 1 und Art. 9 Abs. 1 DS-GVO Ausdruck einer Konstitutionalisierung des europäischen Sekundärrechts (II). Das infolgedessen bestehende Spannungsverhältnis zwischen dem staatlich zu gewährleistendem Mindestschutz (Untermaßverbot) und einem Verstoß gegen das Übermaßverbot wird offenkundig, sofern personenbezogene Daten als vertraglicher Leistungsgegenstand vereinbart werden (III).

---

[245] *Zöllner*, RDV 1985, 1; *Meister*, DuD 1986, 173; *Baumann*, RDV 1986, 1; *Ehmann*, AcP 188 (1988), 230 und *Wente*, NJW 1984, 1446. Hierzu oben: A.II.

[246] H.L.: so bereits zu § 4 BDSG a.F.: *Weichert*, DuD 2013, 249 („logische Konsequenz" der Drittwirkung); *Ziegenhorn/von Heckel*, NVwZ 2016, 1585 (1586); *Buchner*, DuD 2016, 155 (157); *Langhanke*, Daten als Leistung, 2018, S. 31; *Veil*, NVwZ 2018, 686 (688); *Golland*, Datenverarbeitung in sozialen Netzwerken, 2019, S. 184 f.; mit Kritik: *Engert*, in: Grundmann/Möslein (Hrsg.), Innovation und Vertragsrecht, 2020, S. 153 (158).

[247] *Roßnagel*, NJW 2019, 1 (4 f.).

[248] Mit einem Verständnis als risikobasierter Ansatz: *Veil*, ZD 2015, 347 ff.

I. Begriffliche Bezeichnung als Zuspitzung

Wenngleich von geringer praktischer Bedeutung, ist die Diskussion über die richtige Bezeichnung von Art. 6 Abs. 1 und Art. 9 Abs. 1 DS-GVO symptomatisch für zwei fundamental unterschiedliche Sichtweisen auf das Datenschutzrecht. Die Bezeichnungen repräsentieren jeweils eine rechtspolitische Auffassung darüber, welche Grenzen das Untermaß- und das Übermaßverbot dem Gesetzgeber für eine Regulierung von Datenverarbeitungen im privatrechtlichen Bereich setzen sollten. Letztlich sind beide Bezeichnungen somit Ausdruck eines unterschiedlichen Vorverständnisses.

Während das Verwaltungsrecht unter einem Erlaubnisvorbehalt die Notwendigkeit einer behördlichen Genehmigung im Sinn einer Zulassung versteht, setzt ein Erlaubnisvorbehalt aus privatrechtlicher Perspektive die Aufhebung eines generellen Handlungsverbots durch eine gesetzliche Erlaubnis oder rechtsgeschäftliche Gestattung voraus. In der Bezeichnung als Verbot mit Erlaubnisvorbehalt klingt aus privatrechtlicher Perspektive bereits der Vorwurf an, dass dieser Regelungsansatz gegen das Übermaßverbot verstoßen könnte, indem er die unternehmerische Freiheit von Verantwortlichen und von unternehmerisch handelnden Datensubjekten (Prominente/Influencer) und die allgemeine Vertragsfreiheit der nicht unternehmerisch handelnden Datensubjekte (Otto-Normal-Datensubjekt/Verbraucher) unverhältnismäßig beeinträchtigt.[249]

Die Bezeichnung als Verbot mit Regelungsvorbehalt[250] legt dagegen nahe, dass durch Art. 6 Abs. 1 bzw. Art. 9 Abs. 1 DS-GVO kein echtes Verbot begründet werden soll und der gewählte Ansatz lediglich Ausdruck der weiten gesetzgeberischen Einschätzungsprärogative ist.[251]

II. Konstitutionalisierung des sekundärrechtlichen Datenschutzes

Schiebt man die schlagwortartigen Abkürzungen zur Seite, so wird deutlich, dass die Rechtmäßigkeit der Verarbeitung davon abhängt, dass der Verantwortliche mindestens einen Erlaubnistatbestand benennen und das Vorliegen seiner Tatbestandsvoraussetzungen beweisen kann. Ob für die Datenverarbeitung im Privatrechtsverhältnis statistisch das Verbot prägend ist, oder die Datenverarbeitung doch zumeist gemäß Art. 6 Abs. 1 lit. a, lit. b und lit. f DS-GVO bzw.

---

[249] In diese Richtung: *Bull*, Sinn und Unsinn des Datenschutzrechts, S. 57; *von Lewinski*, Die Matrix des Datenschutzrechts, 2014, S. 46 ff. („informationelle Fremdbestimmung"); *Giesen*, JZ 2007, 918 (924); *Krönke*, Der Staat 55 (2016), 319 ff.; *Engert*, in: Grundmann/Möslein (Hrsg.), Innovation und Vertragsrecht, 2020, S. 153 (159).

[250] *Roßnagel*, NJW 2019, 1 (4).

[251] *Albrecht/Jotzo*, Das neue Datenschutzrecht der EU, S. 50 f.; *Roßnagel*, in: Simitis/Hornung/Spiecker gen. Döhmann (Hrsg.), Datenschutzrecht, 2019, Art. 5, Rn. 36; *Pötters*, in: Gola (Hrsg.), Art. 5, Rn. 6 („terminologisch unglücklich").

Art. 9 Abs. 2 rechtmäßig ist,[252] kann mangels gefestigter Rechtsprechung zu den Erlaubnistatbeständen derzeit noch nicht abschließend beurteilt werden.

Jedenfalls wird durch die rechtliche Struktur von Art. 6 Abs. 1 und Art. 9 Abs. 1 DS-GVO das Risiko der Unrechtmäßigkeit einer Datenverarbeitung und die Beweislast für das Vorliegen der Rechtsmäßigkeitsvoraussetzungen eindeutig dem jeweiligen Verantwortlichen zugewiesen. Gelingt dem Verantwortlichen dieser Nachweis nicht, so ist die Datenverarbeitung rechtswidrig und es drohen potenziell hohe Bußgeldbescheide der Datenschutzbehörden und – bislang tendenziell geringwertige – Schadensersatzforderungen der Datensubjekte.[253]

Ein solcher Regelungsmechanismus basierend auf einem Verbot mit Erlaubnisvorbehalt ist dem Privatrecht zwar nicht vollkommen fremd. Insbesondere die Zuweisung von Ausschließlichkeitsrechten folgt einer im Ansatz vergleichbaren Systematik, indem andere von der Nutzung eines Gutes im Grundsatz ausgeschlossen werden. Allerdings soll das Datenschutzrecht gerade kein absolutes immaterielles „Recht am eigenen Datum" zugunsten von Datensubjekten etablieren,[254] weil dieses geeignet wäre, die gesellschaftliche Kommunikation zu blockieren.[255]

1. Verarbeitungsverbot als Einhaltung des Untermaßverbots

Mit Art. 6 Abs. 1 und Art. 9 Abs. 1 DS-GVO hat der europäische Gesetzgeber sich dafür entschieden, seine Schutzpflicht zugunsten der Datensubjekte aus Art. 8 Abs. 1 GRCh durch generelle Verarbeitungsverbote für personenbezogene bzw. besonders sensible personenbezogene Daten umzusetzen. Diese Verbote sind im Ausgangspunkt ein Eingriff in die unternehmerische Freiheit, einschließlich der Vertragsfreiheit der Verantwortlichen.[256] Dieser Eingriff kann

---

[252] So: *Roßnagel*, NJW 2019, 1 (5).

[253] Bislang gewähren die Gerichte nur selten einen Schadensersatz. Eine Ausnahme hiervon sind rechtwidrige Datenverarbeitungen von besonders sensiblen Daten oder im Kontext von Arbeitsverhältnissen: *AG Pforzheim*, Urt. v. 25.03.2020, 13 C 160/19 (sensible Gesundheitsdaten: 4.000 Euro) bzw. *ArbG Lübeck*, Beschl. v. 20.06.2019, 1 Ca 538/19 (rechtswidrige Nutzung eines Mitarbeiterfotos: 1.000 Euro; *ArbG Düsseldorf*, Urt. v. 05.03.2020, 9 Ca 6557/18 (Berücksichtigung von Abschreckungseffekt und Umsatz des Schädigers: 5.000 Euro); *LG Darmstadt*, Urt. v. 26.05.2020, 13 O 244/19 (Benachteiligung infolge Fehlsendung einer E-Mail im Bewerbungsprozess: 1.000 Euro; *ArbG Dresden*, Urt. v. 26.08.2020, 13 Ca 1046/20 (Rufschädigung und Kontrollverlust über sensible Gesundheitsdaten: 1.500 Euro + Rechtsverfolgungskosten).

[254] Mit dem (verkürzten) Versuch ein solches zu begründen: *Meister*, Datenschutz im Zivilrecht, 1981, S. 121 ff.; hierzu m. w. N. *Sattler*, in: Bakhoum u. a. (Hrsg.), 2018, Personal Data in Competition, Consumer Protection and Intellectual Property Law, 2018, S. 27 ff.

[255] Hierzu bereits: *BVerfG*, Urt. v. 15.12.1983 – BvR 209/83 u. a. = NJW 1984, 419 (422) – *Volkszählung*; sowie: *BGH*, Urt. v. 23.06.2009, VI ZR 196/08 = NJW 2009, 2888 (Rn. 40 ff.) – *spickmich*.

[256] So auch: *Buchner*, Die Informationelle Selbstbestimmung im Privatrecht, 2006, S. 50 f.

durch die Schutzpflicht aus Art. 8 Abs. 1 GRCh i. V. m. Art. 7 GRCh gerechtfertigt sein, findet seine Schranke aber im Verhältnismäßigkeitsgrundsatz (Art. 52 Abs. 1 S. 2 GRCh) und der Pflicht zur Herstellung eines angemessenen Ausgleichs zwischen dieser staatlichen Schutzpflicht zugunsten von Datensubjekten und den Freiheitsrechten der Verantwortlichen. Dieser Ausgleich wird durch die gesetzlichen Erlaubnistatbestände in Art. 6 Abs. 1 lit. b DS-GVO (vertragsakzessorische Datenverarbeitung) und Art. 6 Abs. 1 lit. f DS-GVO (Interessenabwägung) und die – nach hier vertretener Auffassung im Privatrechtsverhältnis vorrangig anzuwendende – Einwilligung des Datensubjekts (Art. 6 Abs. 1 lit. a i. V. m. Art. 7 f. DS-GVO) erreicht. Sie heben das Verbotsprinzip auf und geben dem Verantwortlichen und dem Datensubjekt damit ihre grundrechtlich geschützten Freiheiten in einer – durch die Tatbestandsvoraussetzungen von Art. 6 ff. DS-GVO – modifizierten Weise lediglich wieder zurück.

Somit dient das Verbotsprinzip dem Gesetzgeber dazu, seine grundrechtlichen Schutzpflichten gegenüber dem Datensubjekt mit den grundrechtlichen Freiheitsrechten der Verantwortlichen in einen angemessenen Ausgleich zu bringen. Der gewählte Mechanismus muss jedoch zusätzlich berücksichtigen, dass die staatliche Schutzpflicht dann reduziert ist, wenn ein Datensubjekt wirksam in die Datenverarbeitung einwilligt. Art. 8 Abs. 2 S. 1 GRCh garantiert die Möglichkeit zur Einwilligung, so dass die Freiheit der Datensubjekte über die Verarbeitung von personenbezogenen Daten zu disponieren, grundsätzlich unbeschränkt ist.

Aufgrund des Ausgestaltungsauftrags gemäß Art. 8 Abs. 2 S. 2 GRCh ist der Gesetzgeber zwar verpflichtet, diese Dispositionsfreiheit *materiell abzustützen*.[257] Dennoch erweitern die in Art. 6 ff. DS-GVO geregelten Voraussetzungen für eine wirksame Einwilligung nicht den Rechtskreis der Datensubjekte, sondern beschränken die Dispositionsfreiheit, im (mutmaßlichem) Eigeninteresse der Datensubjekte.[258]

2. Verstoß gegen das Übermaßverbot (Verhältnismäßigkeit)

Dieser rechtliche Ansatz, die staatliche Schutzpflicht durch ein Verarbeitungsverbot zu gewährleisten, erinnert an den verfassungsrechtlichen Gesetzesvorbehalt und wird auch ähnlich interpretiert, obwohl das datenschutzrechtliche Verbotsprinzip gerade auch im Privatrechtsverhältnis gilt. Nach Ansicht von

[257] Ebenfalls mit dieser Forderung: *Leistner/Antoine/Sagstetter*, Big Data, 2021, S. 333 („materialisierte Privatautonomie") und S. 397 („Ertüchtigung der Einwilligung"). Hierzu unten Kapitel 5 C.II. und III. und Kapitel 6.

[258] So auch mit Blick auf die Frage, ob Datensubjekte in ein herabgesetztes Niveau der Datensicherheit gem. Art. 32 DS-GVO einwilligen können: Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit, Vermerk: Abdingbarkeit von TOMs (Art. 32 DS-GVO), v. 18.02.2021, S. 6; hierzu auch: *Sattler*, in: Ebers/Steinrötter (Hrsg.), Künstliche Intelligenz und smarte Robotik im IT-Sicherheitsrecht, 2021, S. 197 (209 f.).

Alexander Roßnagel folgt diese generelle Geltung des Verbots aus Art. 6 Abs. 1 und Art. 9 Abs. 1 DS-GVO unmittelbar aus Art. 8 Abs. 1 GRCh. Eine Gleichbehandlung von staatlichen und privaten Verantwortlichen sei durch die „Einheitlichkeit der Rechtsordnung" begründet.[259] Der über ein halbes Jahrhundert alte Programmsatz von *Steinmüller u. a.*, wonach „Staat [und] Gesellschaft […] untrennbar zu einem Gemeinwesen verschmolzen"[260] sind, findet in dieser Aussage seinen späten Widerhall.

Tatsächlich beruht dieser Ansatz weiterhin auf einer – meist unausgesprochenen – Gleichsetzung des staatlichen Gewaltmonopols mit der privaten Marktmacht von dominanten IT-Konzernen und Plattformbetreibern.[261] Nach diesem Verständnis sollen den staatlichen und den privat(wirtschaftlich)en potenziellen Gefährdungen für die individuelle Freiheit der Datensubjekte bereits im Vorfeld einheitliche Grenzen gesetzt werden:

„Jede Verarbeitung personenbezogener Daten durch Dritte ist ein Eingriff in die von Art. 7 und 8 GRCh geschützten Grundrechte. […] Für die Bestimmung des Eingriffs kommt es nicht auf die Person an, die den Eingriff vornimmt – auch nicht auf deren Charakterisierung als privat oder staatlich".[262]

Diese – mit der vom *BVerfG* entwickelten Grundrechtsdogmatik unvereinbare – Ansicht kann sich mit Blick auf die Unionsgrundrechte insbesondere auf zwei Argumente berufen.

Erstens findet sie eine gewisse Unterstützung im *Google Spain*-Urteil.[263] Im Kontext der Interessenabwägung gemäß Art. 7 lit. f der Datenschutz-RL von 1995 (mittlerweile: Art. 6 Abs. 1 lit. f DS-GVO) hatte der *EuGH* ausgeführt, dass

---

[259] *Roßnagel*, in: Simitis/Hornung/Spiecker gen. Döhmann (Hrsg.), 2019, Art. 6, Rn. 2.

[260] *Steinmüller u. a.*, Grundfragen des Datenschutzes, Gutachten im Auftrag des Bundesministeriums des Innern, 1971, BT Drs. VI/3826, 35.

[261] Unabhängig von der in der Sache getroffenen rechtlichen Beurteilung, verfügt der *Hamburgische Beauftragte für Datenschutz und Informationsfreiheit* (HmbBfDI) über ein ähnlich verstörendes Verständnis, das weit über die in der DS-GVO tatsächlich angelegten Ziele hinausgeht: „Die Datenschutz-Skandale der letzten Jahre von ‚Cambridge Analytica' bis hin zu dem kürzlich bekannt geworden Datenleck, von dem mehr als 500 Millionen Facebook-Nutzer betroffen waren, zeigen das Ausmaß und die Gefahren, die von einer massenhaften Profilbildung ausgehen. Das betrifft nicht allein die Privatsphäre, sondern auch die Möglichkeit, Profile zur Beeinflussung von Wählerentscheidungen einzusetzen, um demokratische Entscheidungen zu manipulieren. Die Gefahr ist angesichts von fast 60 Millionen Nutzerinnen und Nutzern von WhatsApp mit Blick auf die in Deutschland im September 2021 anstehenden Bundestagswahlen umso konkreter, da diese Begehrlichkeiten nach Beeinflussung der Meinungsbildung seitens der Anzeigekunden von *Facebook* wecken werden." Anordnung des *HmbBfDI* gegen Facebook: Verbot der Weiterverarbeitung von WhatsApp-Nutzerdaten durch *Facebook*, Pressemitteilung v. 11.05.2021: (https://datenschutz-hamburg.de/pressemitteilungen/2021/05/2021-05-11-facebook-anordnung, zuletzt abgerufen am 19.05.2022).

[262] *Roßnagel*, NJW 2019, 1 (2).

[263] Die missglückte Wortwahl wurde bereits durch die Schlussanträge des Generalanwalts *Jääskinen* geprägt, der von einem rechtfertigungsbedürftigen Eingriff *Googles* in Art. 7 GRCh ausging: Schlussanträge, v. 25.06.2013, C-131/12 (Rn. 119) – *Google Spain*.

„[w]egen seiner potenziellen Schwere […] ein solcher *Eingriff* nicht allein mit dem wirtschaftlichen Interesse des Suchmaschinenbetreibers an der Verarbeitung der Daten *gerechtfertigt* werden [kann]".[264]

Mit dieser Wortwahl[265] ist es – jedenfalls nach deutscher Grundrechtsdogmatik – zu einer unmittelbaren Drittwirkung von Art. 7 i. V. m. Art. 8 GRCh nicht mehr weit. [266] Dadurch wird das Handeln von staatlichen Behörden und Privatrechtsubjekten implizit gleichgesetzt, obwohl sie nicht gleich und allenfalls unter der Voraussetzung einer besonderen Marktmacht des Privatrechtsubjekts vergleichbar sind.[267] Grundsätzlich unterscheidet sich das Handeln von staatlichen Behörden und Privatrechtsubjekte weiterhin hinsichtlich der jeweiligen Möglichkeiten zur Rechtsdurchsetzung, insbesondere der Anordnung der sofortigen Vollziehung und der Anwendung unmittelbaren Zwangs (staatliches Gewaltmonopol).[268]

Indem der *EuGH* von einem rechtfertigungsbedürftigen Eingriff in Art. 7 i. V. m. Art. 8 GRCh durch Privatrechtsubjekte spricht, läuft er jedoch Gefahr, einen überschießenden und mit Blick auf die Freiheiten der Verantwortlichen *und* Datensubjekte unverhältnismäßigen Schutz zu etablieren.[269]

Zweitens – und unabhängig von der Kritik an *Google-Spain*[270] – geht auch die (deutsche) verfassungsrechtliche Literatur davon aus, dass durch Art. 8 Abs. 2 GRCh eine vergleichsweise strenge Regulierung von Datenverarbeitungen im

---

[264] *EuGH*, C-362/14 = GRUR 2014, 895 (Rn. 81) – *Google Spain*.

[265] Vgl. auch die Aussage: „[Die Aufnahme in die Ergebnisliste einer Suchmaschine] kann mithin einen stärkeren *Eingriff* in das Grundrecht auf Achtung des Privatlebens der betroffenen Person darstellen als die Veröffentlichung durch den Herausgeber der Internetseite". *EuGH*, C-362/14 = GRUR 2014, 895 (Rn. 87) – *Google Spain*.

[266] In diese Richtung: *Wolff*, BayVBl. 2015, 9 (15: „starke Drittwirkungsdimension, [die] formal wohl noch als mittelbare Drittwirkung bezeichnet werden kann, in ihrer Wirkung aber zumindest sehr nahe an eine unmittelbare Drittwirkung heranreicht"; für eine noch mittelbare Drittwirkung: *Boehme-Neßler*, NVwZ 2014, 825 (828); im Ergebnis unentschieden: *Klement*, Wettbewerbsfreiheit, 2015, S. 88/Fn. 22.

[267] Zur hieraus folgenden kartellrechtsakzessorischen, asymmetrischen Auslegung und Anwendung des Art. 7 Abs. 4 und Abs. 3 DS-GVO: Kapitel 5 C.II.1 und III.2.a.

[268] Zu pauschal und ohne Abgrenzung zum Kartellrecht für eine „Drittwirkung" als logische Reaktion auf die Marktmacht von Unternehmen im digitalen Bereich: *v. Danwitz*, DuD 2015, 581 (584 f.).

[269] Hiervor warnen – jeweils mit Kritik am EuGH: *Masing*, Vorläufige Einschätzung der „Google-Entscheidung" des EuGH, VerfBlog 14.08.2014, 6c („Eine verobjektivierte Kontrolle, wann welche Daten für welchen Zweck noch notwendigerweise veröffentlicht werden müssen, verfehlt den Charakter des Informationsaustauschs zwischen Privaten, der eben auch hinsichtlich des Zwecks maßgeblich von privater Freiheit geprägt ist. Die unterschiedlichen Problemlagen öffentlichen und privaten Datenschutzes werden hier miteinander vermengt"; *Luch/Schulz/Kuhlmann*, EuR 2014, 698 (706); *Marsch*, Das Europäische Datenschutzgrundrecht, 2018, S. 258 f.

[270] *Marsch*, Das Europäische Datenschutzgrundrecht, 2018, S. 253 ff.; zuvor bereits *Bäcker*, Der Staat 51 (2012), 91 (100 ff.).

Privatrechtsverhältnis vorgegeben ist.[271] Nach Ansicht von *Nikolaus Marsch* folgt hieraus eine konkrete unionsgrundrechtliche Ausgestaltungspflicht des Gesetzgebers. Gemeinsam mit der in Art. 8 Abs. 1 GRCh enthaltenen „Strukturierungsermächtigung" an den Gesetzgeber könne das Verbotsprinzips der DS-GVO als ein Eingriff in die Grundrechte der privaten Verantwortlichen gerechtfertigt werden.[272] Hierdurch werde der „Korridor verschoben", der dem Gesetzgeber zur Verfügung steht, um die Interessen von Verantwortlichen und Datensubjekten in einen angemessenen Ausgleich zu bringen.[273] Im Ergebnis lasse sich die *EuGH*-Rechtsprechung und der aus Art. 8 Abs. 2 GRCh entnommene Ausgestaltungsauftrag als Konstitutionalisierung des Sekundärrechts begreifen.[274]

Diese Beschreibung ist sachlich zutreffend. Allerdings vermittelt sie den Eindruck mit einer Vermeidungsstrategie verbunden zu sein. Im Ergebnis bleibt offen, inwieweit diese Konstitutionalisierung des Sekundärrechts sich qualitativ noch von einer unmittelbaren Drittwirkung des europäischen Datenschutzgrundrechts unterscheidet. Berücksichtigt man zudem, dass die DS-GVO das Datenschutzrecht im Grunde vereinheitlicht, weil sie für Datenverarbeitungen im Privatrechtsverhältnis kaum Öffnungsklauseln und zudem eine Vielzahl an unbestimmten Rechtsbegriffen enthält, welche die Anforderungen an das Bestimmtheitsgebot – jedenfalls nach den (nicht-relevanten) deutschen Maßstäben – zumindest bis an die Grenzen beansprucht, so führt diese Konstitutionalisierung des Sekundärrechts aus deutscher Sicht zu einem Paradigmenwechsel.

Indem der *EuGH* dem Schutz der Datensubjekte gemäß Art. 7 i. V. m. Art. 8 GRCh lediglich die „wirtschaftlichen Interessen" des Verantwortlichen gegenüberstellt und letztere nicht einmal grundrechtlich in Art. 16 GRCh verankert,[275] verwirklicht sich mit dieser einseitig an Art. 7 i. V. m. Art. 8 GRCh ausgerichteten Konstitutionalisierung des datenschutzrechtlichen Sekundärrechts[276] gerade jene Gefahr eines „unbestimmten, hypertrophen Grundrechtschutzes",[277] der mit Freiheitsverlusten für die Verantwortlichen und Datensubjekte einhergeht.

---

[271] Gemäß Art. 8 Abs. 2 GRCh dürfen „Daten […] nur nach Treu und Glauben für festgelegte Zwecke und mit Einwilligung der betroffenen Person oder auf einer sonstigen gesetzlich geregelten legitimen Grundlage verarbeitet werden. Jede Person hat das Recht, Auskunft über die sie betreffenden erhobenen Daten zu erhalten und die Berichtigung der Daten zu erwirken".

[272] *Marsch*, Das Europäische Datenschutzgrundrecht, 2018, S. 265/268 f.

[273] *Marsch*, Das Europäische Datenschutzgrundrecht, 2018, S. 269.

[274] *Marsch*, Das Europäische Datenschutzgrundrecht, 2018, S. 150/253 ff. (258).

[275] *EuGH*, C-362/14 = GRUR 2014, 895 (Rn. 81) – *Google Spain*; anders noch Generalanwalt *Jääskinen*, der die wirtschaftlichen Interessen des Betreibers einer Suchmaschine als Bestandteil der gemäß Art. 16 GRCh zu gewährleistenden unternehmerischen Freiheit qualifizierte: Schlussanträge v. 25.06.2013, C-131/12 (Rn. 124.) – *Google Spain*.

[276] Als Beispiel kann die schlechte Begründung des – im Ergebnis dennoch überzeugenden – Beschlusses des VGH München dienen: Hiernach überwog das „schutzwürdige Interesse" des Datensubjekts, einschließlich Art. 8 Abs. 1 GRCh, gegenüber „dem Interesse" des Verantwortlichen: *VGH München*, Beschl. v. 26.09.2018 – 5 CS 18.1157 = NVwZ 2019, 171 (Rn. 27).

[277] *Herresthal*, ZEuP 2014, 238 (277).

Deshalb muss die *EuGH*-Rechtsprechung und die Konstitutionalisierung des Sekundärrechts zukünftig durch eine primärrechtskonforme Auslegung und Anwendung der DS-GVO beschränkt werden, die sich stärker darum bemüht, die staatliche Schutzpflicht und die informationelle Privatautonomie der Verantwortlichen und Datensubjekte in Ausgleich zu bringen.[278]

3. Anerkennung der Kommerzialisierung (Daten als Gegenleistung)

Das Spannungsverhältnis zwischen einem grundsätzlichen Verarbeitungsverbot und der informationellen Privatautonomie wird in der Praxis offenkundig, sobald die Verarbeitung von personenbezogenen Daten Bestandteil einer privatrechtlichen Transaktion ist. Auf Grundlage der hier herausgearbeiteten Entwicklung des Datenschutzrechts ist es wenig überraschend, dass bereits zaghafte Ansätze einer Einordnung von personenbezogenen Daten als vertraglicher Leistungsgegenstand rechtspolitisch sehr umstritten sind.[279] Wie grundlegend dieser Streit ist, wurde deutlich, nachdem die *EU-Kommission* personenbezogene Daten in ihrem Vorschlag für die DID-RL zwischenzeitlich als „Gegenleistung" bezeichnet hatte.

Es lässt sich nicht aufklären, ob diese Einordnung von personenbezogenen Daten als Teil eines vertraglichen Synallagmas als rechtspolitische Evolution gedacht war oder lediglich auf einer naiven Unterschätzung der bestehenden Konfliktlinien beruhte, die sich durch die DS-GVO ziehen. Jedenfalls kam dieser Vorstoß der *EU-Kommission* aus Sicht des damaligen *Europäischen Beauftragten für den Datenschutz* (EDSB), *Giovanni Buttarelli*, einem postmodernen Sakrileg gleich. In seiner Stellungnahme kritisierte er den Vorschlag der *EU-Kommission* mit deutlichen Worten:

> „Es mag wohl einen Markt für personenbezogene Daten geben, so wie es leider auch einen Markt für lebende menschliche Organe gibt, doch bedeutet dies nicht, dass wir diesen Markt mit einem Rechtsinstrument absegnen können oder sollten. Man kann ein Grundrecht nicht zu Geld und zum Gegenstand einer einfachen geschäftlichen Transaktion machen, auch wenn die von den Daten betroffene natürliche Person eine der an der Transaktion beteiligten Parteien ist".[280]

Zwar lässt sich diese Aussage des damaligen *EDSB* mit dem von ihm auszufüllenden Amt legitimieren. Allerdings geht der Vergleich mit einem Organhandel

---

[278] Unten Kapitel 5 C.II. und III.

[279] Hierzu jeweils m. w. N.: *Bräutigam*, MMR 2012, 635; *Langhanke/Schmidt-Kessel*, EuCML 2015, 218; *Metzger*, AcP 216 (2016), 817; *ders.*, in: Lohsse/Schulze/Staudenmayer (Hrsg.), Data as Counter-Performance – Contract Law 2.0, 2020, S. 36; *Härting*, CR 2016, 735; *v. Westphalen/Wendehorst*, BB 2016, 2179; *Specht*, JZ 2017, 763; *Sattler*, JZ 2017, 1031; *ders.*, in: Lohsse/Schulze/Staudenmayer (Hrsg.), Data as Counter-Performance – Contract Law 2.0, 2020, S. 225 ff. ; *Langhanke*, Daten als Leistung, 2018; *Hacker*, ZfPW 2019, 148.

[280] *EDSB*, Stellungnahme 4/2017 zu dem Vorschlag für eine Richtlinie über bestimmte vertragsrechtliche Aspekte der Bereitstellung digitaler Inhalte, 14.03.2017, S. 10/Nr. 17.

auch unter Berücksichtigung dieser institutionell angelegten Verpflichtungen zu weit: Diese Einordnung verkennt jene „soziale Realität", die in der Gemeinschaftsbezogenheit und -gebundenheit der Person zum Ausdruck kommt[281] und offenbart ein mindestens ungewöhnliches Verständnis von der Bedeutung und Funktion von Grundrechten.

Auch grundrechtliche Positionen unterliegen – abgesehen vom sog. Kern der Menschenwürde – ihrerseits Schranken und müssen stets mit den Grundrechten anderer Rechtssubjekte in Ausgleich gebracht werden. Grundrechtlich abgesicherte Rechtspositionen – beispielsweise das Allgemeine Persönlichkeitsrecht aus Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG – werden in den EU-Mitgliedstaaten seit Jahrzehnten auf Grundlage von Verträgen kommerzialisiert. Mit seiner kategorischen Ablehnung von geschäftlichen Transaktionen bleibt der *EDSB* eine Begründung dafür schuldig, warum es einem Prominenten, beispielsweise *Christiano Ronaldo*, aufgrund von Grundrechten nicht möglich sein soll, gegen eine Geldzahlung seine *bindende* Zustimmung dafür zu erteilen, dass „CR7" auf Bekleidungsstücke gedruckt und dafür unter Verarbeitung personenbezogener Daten und unter Verwendung seines Namens und Abbilds multimedial geworben wird.[282]

Obwohl die Aussage in der Stellungnahme des *EDSB* somit offensichtlich falsch ist – mit diesen Worten ließe sich auch jede Verwertung des grundrechtlich geschützten Eigentums ausschließen – stieß die Stellungnahme des *EDSB* unter den Mitgliedern des *EU-Parlaments* auf politische Zustimmung, so dass die Bezeichnung von personenbezogenen Daten als Gegenleistung aus der Endfassung der DID-RL gestrichen wurde.

Seither sind Begriffe wie „Handelsware" oder „Gegenleistung" als Bezeichnung für personenbezogenen Daten auf Ebene der europäischen Gesetzgebung mit einem Tabu belegt. Aus Angst vor grundlegenden Konflikten und einer Blockade von Gesetzgebungsvorhaben vermeidet die europäische Gesetzgebung mittlerweile jede konkrete Aussage.[283] Stattdessen werden politische Kompromisse formuliert, welche die tatsächliche ökonomische Realität nicht benennen dürfen, infolgedessen aber auch nur eine geringe Halbwertzeit haben dürften.

---

[281] Dazu deutlich: *BGH*, Urt. v. 23.06.2009, VI ZR 196/08 = NJW 2009, 2888 (Rn. 40 ff.) – *spickmich*; sowie zuvor: *BVerfGE* 65, 1 (42) = NJW 1984, 419 (422) – *Volkszählung* „Der einzelne […] ist vielmehr eine sich innerhalb der sozialen Gemeinschaft entfaltende, auf Kommunikation angewiesene Persönlichkeit. Information, auch soweit sie personenbezogen ist, stellt ein Abbild sozialer Realität dar, das nicht ausschließlich dem Betroffenen allein zugeordnet werden kann. Das Grundgesetz hat, wie in der Rechtsprechung des BVerfG mehrfach hervorgehoben ist, die Spannung Individuum – Gemeinschaft im Sinne der Gemeinschaftsbezogenheit und Gemeinschaftsgebundenheit der Person entschieden".

[282] Hierzu unten Kapitel 4 B.I.2 und B.II.2. sowie insbesondere Kapitel 5 C.III.2.b.

[283] Mit eindeutiger (persönlicher) Meinung: *Dirk Staudenmayer*: *Lohsse/Schulze/Staudenmayer*, Data as Counter-Performance – Contract Law 2.0?, 2020, S. 9 f.

D. Fazit: Privatrechtssensible Auslegung der DS-GVO

Die Privatrechtswissenschaft ließ das Datenschutzrecht zu viele Jahre links liegen. Erst die DS-GVO hat das Datenschutzrecht infolge der potenziell sehr hohen Bußgelder scharfgestellt und es schlagartig wieder[284] zum privatrechtlichen Forschungsgegenstand gemacht.[285] Infolgedessen stößt das Verbot der Datenverarbeitung in Art. 6 Abs. 1 und Art. 9 Abs. 1 DS-GVO zunehmend auf Kritik.[286] Insbesondere *Andreas Engert* fand dafür zuletzt klare Worte:

„Abgesehen von der Einwilligungsmöglichkeit erscheint der Datenschutz in seiner rechtlichen Struktur als erstaunlicher, ja einzigartiger Übergriff auf die Privatautonomie. Datenverarbeitung durch Private wird umstandslos einem staatlichen Grundrechtseingriff gleichgestellt und einem umfassenden Rechtfertigungsgebot unterworfen […] Strukturell ist das nichts anderes als eine ins Horizontalverhältnis gekippte, unmittelbare Grundrechtsbindung Privater".[287]

Im Anschluss an diese – zuvor bereits weniger prägnant formulierte[288] – Kritik, stellt sich die Frage, welche Optionen zur Verfügung stehen, um die DS-GVO für das im Grundsatz privatrechtlich organisierte Horizontalverhältnis wieder zu sensibilisieren.

Nachdem das Datenschutzrecht über Jahrzehnte durch eine verfassungs- und verwaltungsrechtliche Perspektive geprägt wurde und der *Europäische Grundrechtekonvent* die Frage nach der Wirkung von Art. 8 GRCh im Horizontalverhältnis an die Judikative delegiert hatte,[289] ist es illusorisch und auch nicht erstrebenswert, das Rad der Zeit zurückzudrehen, um das Datenschutzrecht nachträglich wieder aufzuspalten.[290] Eine Trennung der Materie in ein Daten-

---

[284] Frühzeitig: *Mallmann*, Zielfunktionen des Datenschutzes, 1977; *Ebnet*, Der Informationsvertrag, 1995; zwischenzeitlich: *Giesen*, JZ 2007, 918 ff.

[285] *Langhanke/Schmidt-Kessel*, EuCML 2015, 218; *Metzger*, AcP 216 (2016), 817; *ders.*, in: Lohsse/Schulze/Staudenmayer (Hrsg.), Data as Counter-Performance – Contract Law 2.0?, 2020, S. 36; *Härting*, CR 2016, 735; *v. Westphalen/Wendehorst*, BB 2016, 2179; *Specht*, JZ 2017, 763; *Sattler*, JZ 2017, 1031; *ders.*, in: Lohsse/Schulze/Staudenmayer (Hrsg.), Data as Counter-Performance – Contract Law 2.0?, 2020, S. 225 ff. ; *Langhanke*, Daten als Leistung, 2018; *Hacker*, ZfPW 2019, 148; *ders.*, Datenprivatrecht, 2020; *Bunnenberg*, Privates Datenschutzrecht, 2020; *Leistner/Antoine/Sagstetter*, Big Data, 2021, S. 199 ff.

[286] Mit Blick auf die weite Definition von personenbezogenen Daten: *Leistner/Antoine/Sagstetter*, Big Data, 2021, S. 226 („vollkommen ausgeuferte Reichweite datenschutzrechtlicher Regulierung").

[287] *Engert*, in: Grundmann/Möslein (Hrsg.), Innovation und Vertragsrecht, 2020, S. 153 (159).

[288] *Sattler*, JZ 2017, 1031 (1042/1045 f.).

[289] *Borowsky*, in: Meyer (Hrsg.), Art. 51, Rn. 31; hierzu ausführlich: *Marsch*, Das Europäische Datenschutzgrundrecht, 2018, S. 248 f.

[290] Dies – mit unterschiedlichen Ansätzen – fordernd: Ähnlichkeit zum Eigentum („Recht am eigenen Datum"): *Buchner*, Die informationelle Selbstbestimmung im Privatrecht, 2006, S. 313; *Kilian*, CR 2012, 921 (925); für ein Grundrecht auf Datenverarbeitung: *Giesen*, JZ 2007, 918; für eine stärkere Differenzierung des Rechts zwischen staatlichen und privaten Verant-

schutzrecht, das sich auf missbräuchliche Datenverarbeitung durch Privatrechtsubjekte fokussiert und ein Datenschutzrecht für das Verhältnis zwischen Bürger und staatlichen Hoheitsträgern würde viele Redundanzen hervorrufen, wäre unionsweit kaum vermittelbar[291] und birgt das Risiko, die mit dem einheitlichen Regulierungsansatz gemachten Erfahrungen abzuschneiden.

Stattdessen ist es sinnvoll und erforderlich, die weitgehend einheitlichen Vorgaben der DS-GVO teleologisch und primärrechtskonform so auszulegen und anzuwenden, dass die durch Art. 8 Abs. 2 S. 1 GRCh garantierte Möglichkeit zur Einwilligung, die Vertragsfreiheit (Art. 6 Abs. 3 EUV bzw. Art. 16 GRCh), die unternehmerische Freiheit von Verantwortlichen und von unternehmerisch handelnden Datensubjekten (Art. 16 GRCh) und dadurch die informationelle Privatautonomie der Datensubjekte gestärkt werden. Deshalb wird nachfolgend untersucht, inwieweit die datenschutzrechtlichen Erlaubnistatbestände, die im Horizontalverhältnis vorrangig zur Anwendung kommen, für eine Stärkung der informationellen Privatautonomie in Betracht kommen, ohne dabei in Konflikt mit dem durch die DS-GVO zum Ausdruck gebrachten Willen des europäischen Gesetzgebers zu geraten.

Die Erlaubnistatbestände in Art. 6 Abs. 1 lit. a–f DS-GVO differenzieren ansatzweise danach, ob eine staatliche Behörde oder ein Privatrechtssubjekt für die Datenverarbeitung verantwortlich ist; insbesondere steht die flexible Generalklausel einer allgemeinen Interessenabwägung (lit. f) staatlichen Verantwortlichen nicht zur Verfügung, Art. 6 Abs. 1 a. E. DS-GVO. Dennoch hängt das Ausmaß der Ausübung von Privatautonomie durch Verantwortliche und Datensubjekte letztlich davon ab, welche Maßstäbe die Judikative für Art. 6 Abs. 1 lit. a–f DS-GVO entwickelt. Bereits die erste Vermutung und der Wortlaut des Art. 8 Abs. 2 S. 1 GRCh sprechen dafür, dass die Einwilligung derjenige Tatbestand ist, der einer Selbstbestimmung des Datensubjekts den größten Raum einräumt.[292] Allerdings wurde die datenschutzrechtliche Einwilligung insbesondere durch Art. 7 Abs. 3 und Abs. 4 DS-GVO – pauschal für alle Datensubjekte – potentiell so restriktiv ausgestaltet, dass diese Vorschrift Gefahr läuft,

---

wortlichen: *Härting/Schneider*, CRi 2013, Supplement 1, 19ff.; für eine Abkehr vom Verbotsprinzip und hin zur Begrenzung auf missbräuchliche Datenverarbeitung: *dies.*, CR 2015, 819 (820f.).

[291] *Huber*, Staat und Wissenschaft, 2008, S. 29; *Marsch*, Das Europäische Datenschutzgrundrecht, 2018, S. 86/121ff.

[292] Hierzu und zu den alternativen Ansätzen: *Sattler*, in: Lohsse/Schulze/Staudenmayer (Hrsg.), Data as Counter-Performance – Contract Law 2.0?, 2020, S. 225 (238ff.). Wohl mit einer Präferenz für Art. 6 Abs. 1 lit. b DS-GVO (Vertragsakzessorietät), obwohl für diesen jene Defizite gleichermaßen gelten, die gegen die Einwilligung geltend gemacht werden: *Hacker*, Datenprivatrecht, 2020, S. 255ff./260ff. (Wohl) mit Präferenz für Art. 6 Abs. 1 lit. f DS-GVO (Interessenabwägung): *Leistner/Antoine/Sagstetter*, Big Data, 2021, S. 280 („relevanteste Verarbeitungsgrundlage") und S. 402 („verlagert sich […] zunehmend eher auf die Interessenabwägung"), aber andererseits mit Hinweis auf die damit einhergehenden „erhebliche Rechtsunsicherheiten" (S. 201/402) für eine „Ertüchtigung der Einwilligung" (S. 397).

unverhältnismäßig zu sein. Jedenfalls mit Blick auf unternehmerisch handelnde Datensubjekte verstößt Art. 7 DS-GVO – ohne eine unionsgrundrechtskonforme Auslegung und Anwendung – nach hier vertretener Auffassung[293] gegen das Übermaßverbot und damit gegen den Verhältnismäßigkeitsgrundsatz (Art. 52 Abs. 1 S. 2 GRCh).[294]

In diesem Zusammenhang ist es sinnvoll, nochmals den grundrechtlichen Rahmen aufzuspannen, der aus der deutschen Grundrechtsdogmatik bekannt ist. Obwohl dieser Rahmen für das Unionsrecht nicht – jedenfalls gemäß Art. 6 Abs. 3 EUV nicht allein – ausschlaggebend ist, bietet der deutsche Ansatz aber zumindest einen strukturierten und infolgedessen auch besser vorhersehbaren Ansatz. Der *EuGH* hat zwar einen Hang zur argumentativen Abkürzung, indem er nicht das Sekundärrecht im Lichte der Grundrechte auslegt, sondern stattdessen zu einer unmittelbaren Grundrechtsanwendung zwischen Privaten neigt.[295] Allerdings spricht dies nicht dagegen, den aus der deutschen Dogmatik bekannten Rahmen auch für die Auslegung des Privatrechts anhand der europäischen Grundrechte zu übernehmen, solange keine eigenständige stabile Dogmatik für die Prüfung europäischer Grundrechte im Bereich des Privatrechts existiert.[296]

Ein Schutz der Datensubjekte, der über das einzuhaltende grundrechtliche Untermaßverbot hinausgeht, fällt in den großen Bereich, in dem der demokratische Gesetzgeber über eine Einschätzungsprärogative verfügt und in dem er deshalb regulatorisch experimentieren kann. Je weiter der Schutz personenbezogener Daten jedoch über das grundrechtlich zu gewährleistende Untermaß in Form der Wesensgehaltsgarantie hinausgeht,[297] desto intensiver greift der Gesetzgeber wiederum in die Privatautonomie der Verantwortlichen und – paradoxerweise – auch der Datensubjekte ein.[298] Die Regelungen, zumal wenn sie

---

[293] Hierzu unten Kapitel 4 B.I.2. und B.II.2.

[294] Zumindest im Ansatz scheint die EU-Kommission diese Gefahr mittlerweile ebenfalls zu sehen, wenn sie über geringere datenschutzrechtliche Anforderungen für KMU nachdenkt: *Mitteilung der EU-Kommission*, Datenschutz als Grundpfeiler der Teilhabe der Bürgerinnen und Bürger und des Ansatzes der EU für den digitalen Wandel – zwei Jahre Anwendung der Datenschutz-Grundverordnung, 24.06.2020 COM(2020) 264 S. 12/19 ff. (Evaluierung DS-GVO); hierzu grundlegend aus ökonomischer Perspektive: *Gal/Aviv*, Journal of Competition Law and Economics, 2020, S. 349/351 f./386 ff.

[295] *Ruffert*, JuS 2020, 1 (5 f.).

[296] Einen ähnlichen Ansatz verfolgt auch *Riesenhuber* (Hrsg.), Europäische Methodenlehre, 4. Aufl. 2021.

[297] Zur Annahme einer Wesensgehaltsgarantie: *EuGH* (Große Kammer), 08.04.2014, verb. C-293/12 u. C-594/12 = NJW 2014, 2146 (Rn. 40) – *Digital Rights Ireland*, Hierzu: *Bock/Engeler*, DVBl. 2016, 593 (596). Mit Kritik an den fehlenden Maßstäben hierfür: *Classen*, EuR 2014, 441 (443); sowie: *Lepsius*, in: Jestaedt u. a. (Hrsg.), Das entgrenzte Gericht, 2011, S. 159 ff.; *Marsch*, Das Europäische Datenschutzgrundrecht, 2018, S. 187 f.

[298] Insofern überzeugt die von *Hacker* gewählte Unterscheidung zwischen ermöglichenden und regulierenden Strukturen des Datenschutz- und des Privatrechts als methodischer Ansatz und als Beschreibung der jeweiligen gesetzgeberischen Zielsetzung: *Hacker*, Daten-

nahezu unterschiedslos für alle Datensubjekte gelten, kollidieren dann zunehmend mit dem Grundsatz der Verhältnismäßigkeit und es steigt die Gefahr, dass die Gesetzgebung es nicht mehr schafft, die verschiedenen Grundrechtspositionen im Rahmen einer praktischen Konkordanz in einen angemessenen Ausgleich zu bringen, wie er sowohl durch Art. 52 Abs. 1 GRCh vorgegeben ist als auch von ErwG 4 DS-GVO[299] nochmals betont wird. Die Grenzen und Übergänge zwischen dem grundrechtlichen Untermaßverbot (staatliche Schutz- und Gewährleistungspflicht), dem Bereich regulatorischer Experimentierfreiheit (gesetzgeberische Einschätzungsprärogative)[300] und dem grundrechtlichen Übermaßverbot (Verletzung der Verhältnismäßigkeit) sind fließend und Gegenstand kontinuierlicher rechtspolitischer Auseinandersetzungen zwischen Judikative und Legislative.

Der aktuelle Fokus dieser Auseinandersetzung ist der bereits erwähnte Art. 3 Abs. 1 S. 2 DID-RL. Obwohl die Bezeichnung von personenbezogenen Daten als Gegenleistung in dieser Vorschrift nicht mehr enthalten ist, stellt Art. 3 Abs. 1 S. 2 DID-RL klar, dass die Vorgaben der DID-RL auch dann anwendbar sind, wenn der Verbraucher dem Unternehmer keinen Geldbetrag zahlt, sondern stattdessen personenbezogene Daten bereitstellt oder deren Bereitstellung zusagt.[301]

Diese neutrale Formulierung in Art. 3 Abs. 1 S. 2 DID-RL bzw. in § 327 Abs. 3 BGB[302] ist möglich, soweit damit lediglich der Anwendungsbereich der DID-RL bzw. der §§ 327 ff. BGB festgelegt wird. Sobald es jedoch darum geht,

---

privatrecht, 2020, S. 159 ff./343 ff. (Ermöglichung) bzw. S. 270 ff./397 ff. (Regulierung). Allerdings ist dennoch zu beachten, dass die Ermöglichung und die Regulierung janusköpfig sind. Was aus der Perspektive des Datensubjekts eine Ermöglichung bietet, ist aus Perspektive des Verantwortlichen zugleich eine eingreifende Regulierung. Gleiches gilt für die nachfolgend vorgeschlagenen Abstützungen der informationellen Privatautonomie: Kapitel 5 C.II. und III. und Kapitel 6.

[299] ErwG 4 S. 2 und S. 3 DS-GVO lauten auszugsweise: „Das Recht auf Schutz der personenbezogenen Daten ist kein uneingeschränktes Recht; es muss im Hinblick auf seine gesellschaftliche Funktion gesehen und unter Wahrung des Verhältnismäßigkeitsprinzips gegen andere Grundrechte abgewogen werden. Diese Verordnung steht im Einklang mit allen Grundrechten und achtet alle Freiheiten und Grundsätze, die mit der Charta anerkannt wurden und in den Europäischen Verträgen verankert sind, insbesondere […] Freiheit der Meinungsäußerung und Informationsfreiheit, unternehmerische Freiheit, […]."

[300] Zum gesetzgeberischen Gestaltungsspielraum grundlegend: *BVerfG*, Urt. v. 07.02.1990 – 1 BvR 26/84, BVerfGE 81, 242 (255); *BVerfG*, Urt. v. 11.08.1999 – 1 BvR 2181/98, 1 BvR 2182/98, 1 BvR 2183/98 = NJW 1999, 3399 (3401) – *Organentnahme*.

[301] Art. 3 Abs. 1 S. 2 DID-RL lautet auszugsweise: „Diese Richtlinie gilt auch, wenn der Unternehmer dem Verbraucher digitale Inhalte oder digitale Dienstleistungen bereitstellt oder deren Bereitstellung zusagt und der Verbraucher dem Unternehmer personenbezogene Daten bereitstellt oder deren Bereitstellung zusagt, […]".

[302] § 327 Abs. 3 BGB lautet: „Die Vorschriften dieses Untertitels sind auch auf Verbraucherverträge über die Bereitstellung digitaler Produkte anzuwenden, bei denen der Verbraucher dem Unternehmer personenbezogene Daten bereitstellt oder sich zu deren Bereitstellung verpflichtet, […]".

materielle Rechte und Pflichten zu konkretisieren, stellt sich die Frage nach der richtigen vertragsrechtlichen Einordnung von personenbezogenen Daten erneut und mit gesteigerter Brisanz.[303] Der zugrundeliegende Konflikt, inwieweit personenbezogene Daten als Leistungsgegenstand vereinbart werden können, bricht bei nächster Gelegenheit, insbesondere bei der Auslegung der Gesetze zur Umsetzung der DID-RL ins nationale Recht wieder auf.

Die derzeitigen verbalen Ausweichmanöver der Gesetzgebung – für Deutschland in §§ 327 Abs. 3, 327q Abs. 1–3 und § 516a Abs. 1 BGB[304] – delegieren die privatrechtliche Einordnung von personenbezogenen Daten im Ergebnis an die Judikative und damit letztlich an den *EuGH*.[305] Allerdings verfügt der *EuGH* bislang weder über die erforderlichen Ressourcen, um dieser Aufgabe gerecht werden zu können,[306] noch über das erforderliche Bewusstsein, dass er sich mit dem Begriff der „Gegenleistung" auf rechtspolitisch vermintes Terrain wagt.[307]

Dennoch werden weder der *EuGH* noch die nationalen Fachgerichte umhinkommen, das *tatsächliche* Verhalten von Verantwortlichen und Datensubjekten auch *rechtlich* einzuordnen. Infolgedessen ist es notwendig, einen Ausgleich zwischen einem Schutz der Datensubjekte und der Ermöglichung von informationeller Privatautonomie herbeizuführen. Grundlage hierfür ist eine primärrechtskonforme Auslegung derjenigen wesentlichen datenschutzrechtlichen Erlaubnistatbestände,[308] die im Privatrechtsverhältnis Anwendung finden.[309]

Die Analyse der Interessenabwägung (Kapitel 2), der vertragsakzessorischen Datenverarbeitung (Kapitel 3) und der – nach hier vertretener Ansicht vorrangig anzuwendenden – Einwilligung (Kapitel 4) mündet in ein doppeltes Stufen-

---

[303] Vgl. nur die Stellungnahmen: *BITKOM*, v. 30.11.2020, S. 3 und *VDA*, v. 01.12.2020, S. 11 zum des Referentenentwurfs eines Gesetzes zur Umsetzung der Richtlinie über bestimmte vertragsrechtliche Aspekte der Bereitstellung digitaler Inhalte und digitaler Dienstleistungen v. 03.11.2020.

[304] Hierzu unten: Kapitel 4 C.III. sowie Kapitel 5 C.III.1.b.

[305] Hierzu: *Sattler*, NJW 2020, 3623 (3627 ff.); für Datenverarbeitungen im Privatrechtsverhältnis verbleibt dem *BVerfG* allenfalls noch Spielraum, sofern diese in den Anwendungsbereich einer der Öffnungsklauseln – insbesondere Art. 85 Abs. 1 und Art. 88 DS-GVO – fallen: Hierzu detailliert: *Marsch*, Das Europäische Datenschutzgrundrecht, 2018, S. 352–366.

[306] Mit dem Hinweis, dass der EuGH hoffnungslos überlastet würde, sollten die mitgliedstaatlichen Gerichte die Vorlagepflicht des Art. 267 Abs. 3 AEUV in Gestalt der CILFIT-Rechtsprechung auch im Bereich des Datenschutzrechts ernst nehmen: *Masing*, JZ 2015, 477 (484).

[307] *EuGH*, Urt. v. 29.07.2019, C-40/17 = GRUR 2019, 977 (Rn. 80) – *Fashion ID* (m. Anm. *Sattler*); ähnlich: *BGH*, Urt. v. 14.03.2017, VI ZR 721/15= GRUR 2017, 748 (Rn. 22) – *Robinson Liste*.

[308] Obwohl eine Datenverarbeitung im Privatrechtsverhältnis auch auf Grundlage von Art. 6 Abs. 2 lit. c (Erfüllung einer gesetzlichen Verpflichtung) und lit. d DS-GVO (Schutz lebenswichtiger Interessen) möglich ist, spielen beide Erlaubnistatbestände für die Gestaltung von Rechtsbeziehungen im Privatrechtsverhältnis keine Rolle.

[309] Mit einer ersten wichtigen Gelegenheit zur Abgrenzung der Erlaubnistatbestände durch den EuGH: *OLG Düsseldorf*, Vorlagebeschl. v. 24.03.2021, Kart 2/19 (V) = NZKart 2021, 306 ff.; *ÖOGH*, Vorlagebeschl. v. 22.07.2021, 6 Ob 56/21k – *Schrems* [*III*].

modell der Erlaubnistatbestände (unten: Kapitel 5), das – jedenfalls bei einer Verbesserung der Entscheidungsgrundlage und Entscheidungsumsetzung für Datensubjekte (Kapitel 6) – eine abgestützte informationelle Privatautonomie ermöglicht, ohne dabei gegen das gemäß Art. 8 Abs. 1 GRCh und gemäß Art. 7 GRCh zu gewährleistende Untermaßverbot zu verstoßen.

2. Kapitel

Subsidiarität der Interessenabwägung

Ausgangspunkt aller Optionen, die der Judikative derzeit zur Verfügung stehen, um die informationelle Privatautonomie zu stärken, sind die Verarbeitungsverbote in Art. 6 Abs. 1 DS-GVO und Art. 9 Abs. 1 DS-GVO. Infolgedessen setzt jede Verarbeitung von personenbezogenen Daten, insbesondere im Austausch zu einem Zugang zu digitalen Produkten, eine datenschutzrechtliche Grundlage voraus. In diesem Fall ist der Anbieter digitaler Produkte im Sinne der DID-RL zugleich Verantwortlicher im Sinne der DS-GVO.

Obwohl Art. 3 Abs. 1 S. 2 DID-RL und im Anschluss hieran § 327 Abs. 3 BGB personenbezogene Daten als Leistungsgegenstand anerkennen, haben weder der europäische noch der deutsche Gesetzgeber versucht, das Schuldrecht mit der DS-GVO zu synchronisieren. Gemäß Art. 3 Abs. 8 DID-RL bleibt die DS-GVO „unberührt". Gemäß § 327q Abs. 1 BGB lassen die Ausübung von Betroffenenrechten und die Abgabe datenschutzrechtlicher Erklärungen eines Verbrauchers die Wirksamkeit des Vertrags über die Bereitstellung digitaler Produkte „unberührt".[1]

Sofern die Verarbeitung von personenbezogenen Daten Bestandteil eines Vertragsverhältnisses zwischen Datensubjekt und Verantwortlichem ist, kommen für eine rechtmäßige Datenverarbeitung grundsätzlich[2] drei Optionen in Betracht: Die Datenverarbeitung kann entweder aufgrund einer Einwilligung des Datensubjekts (Art. 4 Nr. 11, Art. 6 lit. a, Art. 7 ff. DS-GVO), akzessorisch zu einem Vertrag (Art. 6 Abs. 1 lit. b DS-GVO) oder auf Grundlage einer zugunsten des Verantwortlichen ausfallenden Interessenabwägung (Art. 6 Abs. 1 lit. f. DS-GVO) rechtmäßig sein.

---

[1] Allerdings hat der deutsche Gesetzgeber – abweichend vom Grundsatz in § 327q Abs. 1 BGB – in Abs. 2 dennoch die Möglichkeit eines abwägungsoffenen Kündigungsrechts durch den unternehmerischen Anbieter digitaler Produkte vorgesehen, sofern diese im Austausch gegen personenbezogene Daten zur Verfügung gestellt werden. Hierzu: *Sattler*, NJW 2020, 3623 (3628).

[2] Die darüber hinaus bestehen Möglichkeiten einer Datenverarbeitung sind unabhängig vom Willen des Datensubjekts und haben deshalb für eine abgestützte informationelle Privatautonomie keine Bedeutung: Art. 6 Abs. 1 lit. c DS-GVO (Erfüllung einer rechtlichen Verpflichtung des Verantwortlichen), Art. 6 Abs. 1 lit. d DS-GVO (Schutz von lebenswichtige Interessen) und Art. 6 Abs. 1 lit. e DS-GVO (Wahrnehmung einer von der öffentlichen Hand übertragenen Aufgabe). Zu weiteren wesentlichen Öffnungsklauseln: Art. 88 DS-GVO i. V. m. § 26 BDSG (Beschäftigungsverhältnis) und Art. 89 DS-GVO i. V. m. § 27 BDSG (wissenschaftliche Forschungszwecke).

Allerdings ist zu beachten, dass diese Optionen sich im privatrechtlichen Bereich gemäß Art. 9 Abs. 2 lit. a DS-GVO regelmäßig auf eine Einwilligung verengen, soweit besonders sensible personenbezogene Daten i. S. d. Art. 9 Abs. 1 DS-GVO verarbeitet werden. Während für eine Verarbeitung solcher besonders sensibler personenbezogener Daten weder eine vertragsakzessorische Datenverarbeitung (Art. 6 Abs. 1 lit. b DS-GVO) noch eine Datenverarbeitung auf Grundlage einer einfachen Interessenabwägung (Art. 6 Abs. 1 lit. f DS-GVO) in Betracht kommt, erweitert § 22 Abs. 1 BDSG eine rechtmäßige Verarbeitung von besonders sensiblen personenbezogenen Daten durch Privatrechtssubjekte („nicht-öffentliche Stellen") für mehrere spezifische Anwendungsfälle.

Hiernach kann die Datenverarbeitung rechtmäßig sein, soweit sie für die Bereiche des *Sozialrechts* (lit. a), der *Gesundheitsvorsorge* und *-versorgung*, einschließlich aufgrund eines Vertrags mit einem Angehörigen eines Gesundheitsberufs (lit. b), aus Gründen des öffentlichen Interesses im Bereich der *öffentlichen Gesundheit*, einschließlich zur Gewährleistung hoher Standards bei der Gesundheitsversorgung, bei Arzneimitteln und Medizinprodukten (lit. c) und soweit sie aus Gründen eines *erheblichen öffentlichen Interesses* zwingend erforderlich ist (lit. d).

Wie diese Erlaubnistatbestände verdeutlichen, können privatrechtlich konstituierte Verantwortliche besonders sensible personenbezogene Daten zu eigenen kommerziellen Zwecken nur auf Grundlage einer ausdrücklichen Einwilligung des Datensubjekts verarbeiten, Art. 9 Abs. 2 lit. a DS-GVO.

Somit ist Art. 9 Abs. 2 DS-GVO im Ergebnis eine gravierende Einschränkung des Anwendungsbereichs von Art. 6 Abs. 1 lit. b (vertragsakzessorische Datenverarbeitung) und Art. 6 Abs. 1 lit. f DS-GVO (Interessenabwägung), weil bereits die Verarbeitung von Abbildungen von Datensubjekten den Anwendungsbereich des Art. 9 Abs. 1 DS-GVO eröffnen kann. Selbst unter Ausblendung der rasanten Fortschritte im Bereich der biometrischen Bildanalyse und der angeblichen Möglichkeit von *Facebook*, anhand von wenigen Daten und deren Kontext die sexuelle Orientierung von Personen – ein besonders sensibles personenbezogenes Datum – ableiten zu können,[3] genügt im Einzelfall bereits die Hautfarbe (Möglichkeit zu Rückschlüssen auf eine rassische oder ethnische Herkunft) oder das Tragen einer Brille oder eines Hörgeräts (Gesundheitsdatum), um eine Abbildung als sensibles personenbezogenes Datum zu qualifizieren. Jedenfalls aus Sicht eines risikoaversen Verantwortlichen bleibt somit nur der Rückgriff auf eine ausdrückliche Einwilligung des Datensubjekts.[4] Somit scheiden Art. 6

[3] *Choi/Jeon/Kim*, Journal of Public Economics 2019, 113 (115 f.); zu dieser statistischen Drittwirkung als einer Form von Externalitäten bereits: *MacCarthy*, I/S: A Journal of Law and Policy for the Information Society 2011, 425 (453/457); hierzu ausführlich *Hermstrüwer*, Informationelle Selbstgefährdung, 2016, S. 163 ff.

[4] Obwohl die Einwilligung gemäß Art. 7 Abs. 3 S. 1 und Abs. 4 DS-GVO ihrerseits riskant ist. Hierzu: Kapitel 4 A.II.4. und 5.

Abs. 1 lit. b und lit. f DS-GVO für Fälle aus, in denen eine (bekannte) natürliche Person beispielsweise ihr Recht am eigenen Bild (§ 22 KUG) einsetzt, um als Werbeträger für ein Unternehmen tätig zu werden.

Weil die Abgrenzung zwischen personenbezogenen und besonders sensiblen personenbezogenen Daten schwierig ist und zugleich als Weichenstellung für die Anforderungen an eine rechtmäßige Datenverarbeitung grundsätzliche Bedeutung hat, hat das *OLG-Düsseldorf* dem *EuGH* diese Frage zur Klärung vorgelegt und will wissen, ob bereits die Protokollierung des Besuchs eines Datensubjekts auf einer Webseite für Gesundheitsfragen oder einer Webseite für gleichgeschlechtliche Partnervermittlung als ein besonders sensibles personenbezogenes Datum zu beurteilen ist.[5] Auf die Nichtanwendbarkeit der Interessenabwägung für eine Verarbeitung von besonders sensiblen personenbezogenen Daten wird später eingegangen.[6]

Bereits anhand des Wortlauts von Art. 6 Abs. 1 lit. f DS-GVO wird sein Charakter als datenschutzrechtliche Generalklausel deutlich (A). Infolgedessen ist die Flexibilität und Entwicklungsoffenheit der wesentliche Vorteil dieses Erlaubnistatbestands (B). Kehrseite dieser Flexibilität ist jedoch die große Rechtsunsicherheit, die mit der Anwendung von Art. 6 Abs. 1 lit. f DS-GVO einhergeht und die von Verantwortlichen potenziell dazu genutzt werden könnte, um die datenschutzrechtlichen Anforderungen der Einwilligung zu umgehen (C). Deshalb sollte Art. 6 Abs. 1 lit. f DS-GVO nach hier vertretener Auffassung restriktiv ausgelegt und *grundsätzlich* nur subsidiär zur Einwilligung angewendet werden (D).

A. Die Interessenabwägung als Generalklausel

Der Tatbestand des Art. 6 Abs. 1 lit. f DS-GVO ist – wie seine Vorgängernorm in Art. 7 lit. f Datenschutz-RL (1995) – als offene Generalklausel konzipiert. Hiernach ist die Verarbeitung unter drei materiellen Voraussetzungen rechtmäßig.[7] *Erstens* muss sie der Wahrung von berechtigten Interessen des Verantwortlichen oder eines Dritten dienen (I). *Zweitens* ist die Datenverarbeitung nur rechtmäßig, soweit sie zur Wahrung dieser Interessen auch erforderlich ist (II). *Drittens* dürfen die Interessen oder Grundrechte und Grundfreiheiten des Datensubjekts nicht überwiegen (III). Zuletzt wird die Interessenabwägung je-

---

[5] Vorlagefrage 2a des *OLG Düsseldorf*, Vorlagebeschl. v. 24.03.2021, Kart 2/19 (V), GRUR-RS 2011 8370; sowie die Vorlagefrage 3 des *ÖOGH*, Vorlagebeschl. v. 22.07.2021, 6 Ob 56/21k (Rn. 24 ff.) – *Schrems* [*III*].

[6] Unten C.I.3.

[7] So bereits für Art. 7 lit. f Datenschutz-RL: *EuGH*, Urt. v. 04.05.2017, C-13/16 = EuZW 2017, 912 (Rn. 28) – *Rīgas satiksme*; *EuGH*, Urt. v. 29.07.2019, C-40/17 = GRUR 2019, 958 (Rn. 130) – *Fashion ID*.

doch beschränkt, indem das Datensubjekt seine Entscheidungszuständigkeit durch einen Widerspruch gegen die Datenverarbeitung herstellen kann (IV).

I. Berechtigte Interessen des Verantwortlichen oder Dritter

Als berechtigte Interessen kommen zunächst alle rechtlich gebilligten[8] und damit grundsätzlich auch lediglich wirtschaftliche[9] oder ideelle[10] Interessen des Verantwortlichen oder eines Dritten, einschließlich der Meinungs-[11] und der Informationsfreiheit,[12] des Schutzes des Eigentums[13] und der unternehmerischen Freiheit[14] in Betracht.[15]

Weil es über Art. 6 Abs. 1 lit. f DS-GVO möglich sein muss, die einfachgesetzlich anerkannten und die (unions-)grundrechtlich zu gewährleistenden Positionen von Privatrechtssubjekten zum Ausgleich zu bringen, ist eine möglichst weite Auslegung des berechtigten Interesses erforderlich. Infolgedessen grenzt das berechtigte Interesse den Anwendungsbereich von Art. 6 Abs. 1 lit. f DS-GVO allenfalls ein, soweit ein Interesse als solches ausschließlich Zwecken dient, die von der Rechtsordnung unter keinen Umständen anerkannt werden (sollen).

Weil die gegenläufigen Interessen des Datensubjekts auf der zweiten Ebene und damit im Rahmen der eigentlichen Interessenabwägung vollständig zu berücksichtigen sind, kann das berechtigte Interesses des Verantwortlichen auf der ersten Ebene nicht eingegrenzt werden, indem auf entgegenstehende Schutzinteressen, Grundrechte und Grundfreiheiten der Datensubjekte verwiesen wird.[16] Entsprechend der Funktion als Generalklausel lässt sich der Begriff des berechtigten Interesses allenfalls negativ begrenzen, so dass nur eindeutig verbotene und strafbare Datenverarbeitungen *per se* ausgeschlossen sind.[17]

In ihrer Stellungnahme zum Begriff des berechtigten Interesses in Art. 7 lit. f Datenschutz-RL (1995)[18] führt die *Artikel-29-Datenschutzgruppe* die Wahrnehmung des Rechts auf Meinungs- und Informationsfreiheit, die Durchset-

---

[8] Ausdrücklich weit: *GA Bobek*, Schlussanträge v. 19.12.2018, C-40/17 (Rn. 122) – *Fashion ID*.

[9] *EuGH*, Urt. v. 13.05.2014, C-131/12 = NJW 2014, 2257 (Rn. 81/97/99) – *Google Spain*.

[10] *Buchner/Petri*, in: Kühling/Buchner (Hrsg.), DS-GVO, 3 Aufl. 2020, Art. 6, Rn. 146.

[11] *EuGH*, Urt. v. 06.11.2003, C-101/01 = EuZW 2004, 245 (Rn. 87) – *Lindquist*.

[12] *EuGH*, Urt. v. 13.05.2014, C-131/12 = NJW 2014, 2257 (Rn. 81/97/99) – *Google Spain*.

[13] *EuGH*, Urt. v. 11.12.2014, C-212/13 = NJW 2015, 4673 (Rn. 34) – *Ryneš*.

[14] *EuGH*, Urt. v. 24.11.2011, C-468/10 u. C-469/10 = ZD 2012, 33 (Rn. 43) – *ASNEF*.

[15] Zum Interesse des Erben (und Vaters) eines Erblassers: *BGH*, Urt. v. 12.07.2018, III ZR 183/17 = NJW 2018, 3178 (Rn. 74 ff.) – *Digitaler Nachlass*.

[16] *Albers/Veit*, in: Wolff/Brink (Hrsg.), BeckOK Datenschutzrecht, 36. Ed., Stand: 01.05. 2020, Art. 6, Rn. 49.

[17] Beispielsweise kann eine Interessenabwägung das Ausspähen von Daten (§ 202a StGB) – im Privatrechtsverhältnis – nicht rechtfertigen, weil insoweit das Einverständnis oder eine mutmaßliche Einwilligung erforderlich sind: *Graf*, in: MK/StGB, 4. Aufl. 2021, § 202a, Rn. 70 f.

[18] *Artikel-29-Datenschutzgruppe*, Stellungnahme 06/2014 zum Begriff des berechtigten

zung von Rechtsansprüchen über außergerichtliche Verfahren, die Verhütung von Betrug, den Leistungsmissbrauch oder die Geldwäsche, die persönliche Sicherheit, die IT- und Netzsicherheit, die herkömmliche Direktwerbung und andere Formen des Marketings oder der Werbung auf.

Wie sich aus einem Umkehrschluss zu Art. 21 Abs. 1 S. 1 Hs. 2 DS-GVO ergibt, kann auch ein Profiling, beispielsweise als Voraussetzung für eine personalisierte Direktwerbung, grundsätzlich auf eine Interessenabwägung gemäß Art. 6 Abs. 1 lit. f DS-GVO gestützt werden.[19] Gemäß Art. 4 Nr. 4 DS-GVO ist das Profiling definiert als jede Art der automatisierten Verarbeitung personenbezogener Daten, um diese anschließend dazu zu verwenden, bestimmte persönliche Aspekte eines Datensubjekts zu bewerten, insbesondere um die Arbeitsleistung, wirtschaftliche Lage, Gesundheit, persönlichen Vorlieben, Interessen, die Zuverlässigkeit, das Verhalten, den Aufenthaltsort oder einen Ortswechsel dieses Datensubjekts zu analysieren oder vorherzusagen.

Soweit Art. 6 Abs. 1 lit. f DS-GVO auch Drittinteressen als berechtigte Interessen ausdrücklich einbezieht, ist zu beachten, dass diese gerade in Bezug auf personalisierte Werbung kaum Auswirkungen zugunsten einer Datenverarbeitung entfalten (1). Umgekehrt gilt, dass Drittinteressen, die gegen eine Datenverarbeitung sprechen, dieser nicht entgegengehalten werden können, weil der Schutz von Datensubjekten vor einer Verarbeitung personenbezogener Daten auf einem individualrechtlichen Ansatz beruht (2).

1. Begrenzung des Drittinteresses zugunsten einer Datenverarbeitung

Weil Art. 6 Abs. 1 lit. f DS-GVO auch Drittinteressen als berechtigte Interessen ausdrücklich einbezieht, ist eine Datenverarbeitung auf Grundlage einer Interessenabwägung insbesondere für Verantwortliche attraktiv, die personenbezogene Daten erheben und anschließend Dritten einen direkten Zugang zu diesen Daten eröffnen, oder die Daten zunächst selbst analysieren und Dritten anschließend einen Zugang zu den aufbereiteten Daten oder Datenderivaten eröffnen.[20]

Auf den ersten, oberflächlichen Blick erscheint es möglich, dass die Verwertung personenbezogener Daten als Voraussetzung für (personalisierte) Werbung sowohl für Produkte des Verantwortlichen als auch Dritter gemäß Art. 6 Abs. 1 lit. f DS-GVO rechtmäßig sein könnte.[21] Allerdings täuscht dieser auch

---

Interesses des für die Verarbeitung Verantwortlichen gemäß Artikel 7 der Richtlinie 95/46/EG, WP217, 09.04.2014, S. 31 f.

[19] Zur Notwendigkeit den Begriff der Direktwerbung im Anwendungsbereich des Art. 6 Abs. 1 lit. f DS-GVO eng auszulegen: unten C.I.2.

[20] Zu den Geschäftsmodellen der Datenverwertung – einschließlich personenbezogener Daten: *Peitz/Schweitzer*, NJW 2018, 275 (277 f.); sowie zu möglichen Varianten des Datenhandels: *Sattler*, in: Pertot (Hrsg.), Rechte an Daten, 2020, S. 49 (57 ff.).

[21] In diese Richtung: *GA Bobek*, Schlussanträge, v. 19.12.2018, C-40/17 (Rn. 123) – *Fashion ID*; *Drewes*, ZD 2019, 296 (300).

durch ErwG 47 S. 7 DS-GVO (Direktwerbung als berechtigtes Interesse) vermittelte erste Eindruck in mehrfacher Hinsicht.

Obwohl die Möglichkeiten und Grenzen einer Datenverarbeitung für personalisierte Werbung noch ausführlich untersucht werden,[22] folgt bereits aus Art. 13 Abs. 1 und Abs. 2 der ePrivacy-RL (2002),[23] dass jedenfalls eine Werbung unter Verwendung von elektronischer Post[24] nur dann keine Einwilligung voraussetzt, wenn der Werbende die Daten von dem Datensubjekt im *Kontext einer bestehenden Kundenbeziehung* erhalten hat und diese nur zur Direktwerbung für *eigene ähnliche Produkte* des Werbenden verwendet werden. Wie nachfolgend noch ausführlich begründet wird, lässt sich aus der Übernahme des Begriffs der Direktwerbung aus Art. 13 ePrivacy-RL und mit Blick auf die weiteren Ausführungen in ErwG 47 DS-GVO ableiten, dass eine Direktwerbung des Verantwortlichen *für Produkte Dritter* und eine *Direktwerbung durch Dritte* keine berechtigten Interessen i. S. d. Art. 6 Abs. 1 lit. f DS-GVO sind.

Zudem hat der *EuGH* den Anwendungsbereich des Art. 6 Abs. 1 lit. f DS-GVO für eine Datenverarbeitung zugunsten von Drittinteressen mittelbar stark eingeschränkt. Zwar entschied der *EuGH* in *Fashion-ID* nicht darüber, ob auch das Interesse eines Dritten an einer Datenverarbeitung zur Ermöglichung von Werbung ein berechtigtes Interesse i. S. d. Art. 7 lit. f Datenschutz-RL (1995) bzw. Art. 6 Abs. 1 lit. f DS-GVO ist. Dennoch erschwert das Urteil *Fashion-ID* die Rechtfertigung einer Datenverarbeitung zugunsten von Drittinteressen, weil der *EuGH* den Begriff des Verantwortlichen sehr weit interpretiert hat. Hiernach sind sowohl der Betreiber der Webseite *Fashion ID* als auch *Facebook* als Betreiber des in die Webseite eingebundenen „*Gefällt mir-Button*" (*social plug-in)* jeweils als (gemeinsam) Verantwortliche zu betrachten.[25]

Dies hat zur Folge, dass beide als Verantwortliche jeweils einen eigenen Erlaubnistatbestand und im Fall des Art. 6 Abs. 1 lit. f DS-GVO jeweils ein eigenes berechtigtes Interesse nachweisen müssen.[26] Aufgrund dieser weiten Definition der (gemeinsamen) Verantwortlichkeit wird der Anwendungsbereich für Fälle eines Drittinteresses im Rahmen von Art. 6 Abs. 1 lit. f DS-GVO erheblich reduziert, weil ein vermeintlich Dritter bereits dann selbst zum Verantwort-

---

[22] Unten: C.I.2.b.

[23] Richtlinie 2002/58/EG v. 12.07.2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (ePrivacy-RL), ABl. v. 31.07.2002, Nr. L 201, S. 37 ff. Art. 13 Abs. 1 und Abs. 2 ePrivacy-RL wurden in in § 7 Abs. 2 Nr. 3, Abs. 3 UWG umgesetzt.

[24] Die Definition von „elektronischer Post" in Art. 2 lit. h ePrivacy-RL (2002/58/EG) stellt noch auf ein öffentliches Kommunikationsnetz ab, so dass die Anbieter von internetbasierten sog. over the top (OTT) Diensten – beispielsweise die üblichen Nachrichtendiente *Whatsapp*, *Telegram* und *Signal* – aber auch die in der Betriebssoftware von Android und IoS integrierten Nachrichten-Apps von dieser Definition nicht erfasst werden und erst nach in Kraft treten der ePrivacyVO einbezogen sind.

[25] *EuGH*, Urt. v. 29.07.2019, C-40/17 = GRUR 2019, 958 (Rn. 132 f.) – *Fashion ID*.

[26] Hierzu *Sattler*, GRUR 2019, 1023 f.

lichen wird, wenn er die Datenverarbeitung (mit)veranlasst hat und wirtschaftlich von dieser profitiert.

Eine Kooperation in den Werbenetzwerken von *Facebook* (beispielsweise *Custom Audience*) oder *Google* (beispielsweise *AdX/Ad Manager*) hat deshalb regelmäßig zur Folge, dass die Beteiligten jeweils (gemeinsam) Verantwortliche und nicht lediglich Dritte sind. Infolgedessen müssen alle Verantwortlichen sich jeweils auf einen eigenen Erlaubnistatbestand für die Datenverarbeitung berufen können und es ist nicht möglich, lediglich eine summarische Interessensabwägung vorzunehmen, in der die Interessen der werbenden Unternehmen eines solchen Werbenetzwerks als berechtigte Drittinteressen zugunsten einer Datenverarbeitung berücksichtigt werden.

Somit ist das berechtigte Interesse i. S. d. Art. 6 Abs. 1 lit. f DS-GVO zwar generalklauselartig weit gefasst und es können Drittinteressen zugunsten einer Datenverarbeitung berücksichtigt werden. Allerdings besteht im Anschluss an *Fashion-ID* die Notwendigkeit, zu differenzieren, ob ein berücksichtigungsfähiges Drittinteressen an der Datenverarbeitung vorliegt oder, ob der Dritte diese Datenverarbeitung mitveranlasst hat und tatsächlich eigene Verarbeitungszwecke verfolgt, so dass er seinerseits (gemeinsam) Verantwortlicher ist und für seine Datenverarbeitung einen eigenständigen Erlaubnistatbestand benötigt.

2. Irrelevanz von Drittinteressen zulasten einer Datenverarbeitung

Soweit vertreten wird, dass im Rahmen von Art. 6 Abs. 1 lit. f DS-GVO Drittinteressen nicht nur zugunsten einer Verarbeitung berücksichtigt werden müssen, sondern auch solche, die gegen eine Datenverarbeitung sprechen,[27] sprengt diese Herangehensweise den Wortlaut von Art. 6 Abs. 1 lit. f DS-GVO („Interessen […] der betroffenen Person")[28] und den individualrechtlichen Ansatz der DS-GVO. Auch wenn die Summe der Interessen aller betroffenen Datensubjekte größer sein kann als ihre einzelnen Teile, kann dieser Summeneffekt aufgrund des individualrechtlichen Ansatzes der DS-GVO nicht in Art. 6 Abs. 1 lit. f DS-GVO berücksichtigt werden.[29] Im Unterschied zum IT-Sicherheitsrecht[30] dient die DS-GVO grundsätzlich keinen Kollektivinteressen.[31]

---

[27] *Hacker*, Datenprivatrecht, 2020, S. 274.

[28] Gemäß Art. 4 Nr. 1 DS-GVO definiert als „eine identifizierte oder identifizierbare natürliche Person".

[29] Eine hiervon zu trennende Frage ist, inwieweit solche Summeneffekte zu einem öffentlichen Interesse an stärkerem Datenschutz führen können. Hierzu: *Klement*, JZ 2017, 161 (170).

[30] Hierzu *Sattler*, in: Ebers/Steinrötter (Hrsg.), Künstliche Intelligenz und smarte Robotik im IT-Sicherheitsrecht, 2021, S. 197 (198 ff.).

[31] A. A. *Schweitzer*, in: Körber/Kühling (Hrsg.), Regulierung-Wettbewerb-Innovation, 2017, S. 269 (282).

Allerdings ist zu beachten, dass aufgrund der weiten Auslegung des Personenbezugs gemäß Art. 4 Nr. 1 DS-GVO durch den *EuGH* ein solcher Personenbezug bereits dann besteht, wenn eine Datenverarbeitung Konsequenzen für eine (andere) identifizierbare natürliche Person hat.[32] Abgesehen von den Fällen einer mittelbaren Auswirkung in Form eines wirtschaftlichen oder gesellschaftlichen Drucks zur Offenbarung personenbezogener Daten und den potenziell negativen Konsequenzen einer Nicht-Offenlegung (sog. *unravelling*),[33] bleiben damit faktisch kaum Anwendungsfälle, in denen ein echtes Drittinteresse gegen eine Verarbeitung spricht. Vielmehr dürfte es sich regelmäßig gerade nicht um Drittinteressen, sondern um die unmittelbaren Interessen anderer Datensubjekte handeln.[34] Infolgedessen fällt eine Verarbeitung von (multi-relationalen) personenbezogenen Daten im Verhältnis zu jedem betroffenen Datensubjekt unter das Verarbeitungsverbot und der Verantwortliche muss sich für die Verarbeitung gegenüber jedem Datensubjekt jeweils auf einen (unterschiedlichen) Erlaubnistatbestand berufen können. So sind die wichtigsten Anwendungsfälle des Art. 6 Abs. 1 lit. f DS-GVO gerade solche, in denen entweder viele Datensubjekte nur leicht betroffen sind, so dass die (vorrangige) Einholung einer Vielzahl von Einwilligungen mit Blick auf die für das individuelle Datensubjekt jeweils geringen Risiken unverhältnismäßig aufwändig wäre. Zudem kommt Art. 6 Abs. 1 lit. f DS-GVO in Konstellationen in Betracht, in denen zwar vom primär betroffenen Datensubjekt eine Einwilligung eingeholt werden muss, andere Datensubjekte jedoch aufgrund der Multi-Relationalität der Daten lediglich ganz peripher von der Datenverarbeitung betroffen sind.[35]

II. Erforderlichkeit der Datenverarbeitung zur Interessenwahrung

Weil das berechtigte Interesse noch nicht einmal ein rechtlich anerkanntes Interesse sein muss, wird der Anwendungsbereich der Interessenabwägung regelmäßig erst durch die zweite Tatbestandsvoraussetzung etwas eingegrenzt. Hiernach muss eine Datenverarbeitung auf Grundlage von Art. 6 Abs. 1 lit. f DS-GVO zur Wahrung der berechtigten Interessen des jeweiligen (gemeinsam) Verantwortlichen *erforderlich* sein. Diese Voraussetzung folgt im Grunde bereits aus dem allgemeinen datenschutzrechtlichen Grundsatz der Datenmini-

---

[32] *EuGH*, Urt. v. 19.10.2016, C-582/14 = NJW 2016, 3579 (Rn. 40 ff.) – *Breyer*.

[33] *Choi/Jeon/Kim*, Journal of Public Economics 2019, 113 (115 f.); zu dieser statistischen Drittwirkung als eine Form von Externalitäten bereits: *MacCarthy*, I/S: A Journal of Law and Policy for the Information Society 2011, 425 (453/457); hierzu ausführlich: *Hermstrüwer*, Informationelle Selbstgefährdung, 2016, S. 163 ff.

[34] *Hoffmann-Riem*, AöR 142 (2017), 1 (38 f.); *Schantz*, in: Simitis/Hornung/Spiecker gen. Döhmann (Hrsg.), Datenschutzrecht, 2019, Art. 6, Rn. 102.

[35] Insoweit entscheidet die Auslegung und Anwendung von Art. 6 Abs. 1 lit. f DS-GVO auch über das gesellschaftlich zu akzeptierende Mindestmaß an Datenverarbeitung.

mierung (Art. 5 Abs. 1 lit. c DS-GVO).[36] Infolgedessen ist eine Datenverarbeitung nicht auf Grundlage einer Interessenabwägung rechtmäßig, soweit diese berechtigten Interessen auch ohne eine Verarbeitung von personenbezogenen Daten oder zumindest durch eine Datenverarbeitung geringeren Umfangs gewahrt werden können.[37]

Nach dem Wortlaut muss der Verantwortliche deshalb im Rahmen der Erforderlichkeit eine erste Verhältnismäßigkeitsprüfung *in Relation* zum berechtigten Interesse anstellen. Danach würde es nicht genügen, festzustellen, dass die Verarbeitung lediglich dazu geeignet ist, das berechtigte Interesse zu wahren. Vielmehr setzt eine Erforderlichkeit unter Berücksichtigung des Grundsatzes der Datenminimierung gerade voraus, dass diese Datenverarbeitung das mildeste dem Verantwortlichen zur Verfügung stehende Mittel ist, um das berechtigte Interesse zu wahren.

Allerdings könnten sich Zweifel an dieser strengen Auslegung anhand des Wortlauts ergeben, weil diese den Anwendungsbereich des Art. 6 Abs. 1 lit. f DS-GVO auf den ersten Blick ganz erheblich einschränken würde. Infolgedessen könnte seine Funktion als Auffangtatbestand gefährdet sein. Zudem spricht gegen eine derart strenge Auslegung der Erforderlichkeit, dass dadurch die Bedeutung der – den Tatbestand des Art. 6 Abs. 1 lit. f DS-GVO eigentlich prägenden – Abwägung der Interessen des Verantwortlichen und des Datensubjekts sehr reduziert würde. Auf eine Interessenabwägung käme es nur noch an, sofern eine an für sich erforderliche Datenverarbeitung dennoch ausnahmsweise an den überwiegenden Interessen des Datensubjekts scheitert.

Diese Zweifel an einer engen Auslegung der Erforderlichkeit lassen sich jedoch ausräumen. Selbst wenn das Kriterium der Erforderlichkeit streng ausgelegt wird, hat der Verantwortliche aufgrund der vergleichsweise weiten Anerkennung von berechtigten Interessen stets die Möglichkeit, diese berechtigten Interessen detailliert und ausführlich zu beschreiben. In der Folge ist es dem Verantwortlichen regelmäßig möglich, die Erforderlichkeit einer sehr umfassenden Datenverarbeitung *in Relation* zu dieser Vielzahl an berechtigten Interessen zu begründen.

Zusammengefasst: Je umfangreicher die verfolgten berechtigten Interessen sind und je umfangreicher diese beschrieben und dokumentiert werden, desto umfangreicher ist regelmäßig auch die Datenverarbeitung, die erforderlich ist, um diese Interessen zu wahren.

---

[36] *Ehmann*, in: Simitis/Hornung/Spiecker gen. Döhmann (Hrsg.), Datenschutzrecht, 2019, Anhang 3 zu Artikel 6, Rn. 28.

[37] So zum BDSG: *BGH*, Urt. v. 15.05.2018, VI ZR 233/17 = NJW 2018, 2883 (Rn. 30) – *Dashcam*; m. w. N. *Schantz*, in: Simitis/Hornung/Spiecker gen. Döhmann (Hrsg.), Datenschutzrecht, 2019, Art. 5, Rn. 100.

III. Kein Überwiegen der Interessen des Datensubjekts

Nachdem die ersten beiden Voraussetzungen des Art. 6 Abs. 1 lit. f DS-GVO, also die berechtigten Interessen und die Erforderlichkeit der Datenverarbeitung zur Wahrung dieser berechtigten Interessen aus der Perspektive des Verantwortlichen beurteilt werden, wechselt die Perspektive für die dritte Voraussetzung. Nunmehr muss der Verantwortliche – dieser entscheidet im Ausgangpunkt selbst über die Voraussetzungen des Art. 6 Abs. 1 lit. f DS-GVO – seine berechtigten Interessen mit den Interessen, Grundrechten und Grundfreiheiten des Datensubjekts abwägen. Dabei ist neben dem offensichtlich relevanten Grundrecht auf Schutz des Datensubjekts vor einer Verarbeitung personenbezogener Daten aus Art. 8 GRCh ebenfalls das Grundrecht auf Achtung der Privatsphäre gemäß Art. 7 GRCh einzustellen.[38] Zu berücksichtigen sind auch potenzielle wirtschaftliche Nachteile für das Datensubjekt.[39]

Diese Interessenabwägung verursacht in der Praxis mehrere Schwierigkeiten. Gründe dafür sind – neben den anderen Nachteilen (unten C) –, die in Art. 6 Abs. 1 lit. f DS-GVO angelegte Dichotomie der Interessen (1), die negative Formulierung, die sich tendenziell zugunsten einer Datenverarbeitung auswirkt (2) und das Fehlen von konkreten Kriterien für die Interessenabwägung (3).

1. Dichotomie der Interessen

Die Systematik des Art. 6 Abs. 1 lit. f DS-GVO geht grundsätzlich von einem antagonistischen Verhältnis zwischen Verantwortlichem und Datensubjekt aus. Weil es sich bei der Interessenabwägung im Ausgangspunkt um einen internen Vorgang des Verantwortlichen handelt, ist fraglich, ob und wie in dieser Interessenabwägung berücksichtigt werden kann, dass die Datenverarbeitung womöglich auch teilweise im Interesse des Datensubjekts erfolgt.

Zunächst erscheint es logisch, dass nicht nur die Interessen des Verantwortlichen und Dritter, sondern auch die mutmaßlichen oder gemutmaßten Interesse der Datensubjekte *zugunsten* einer Datenverarbeitung im Rahmen der Abwägung berücksichtigt werden können. Eindeutig ist diese Möglichkeit aber deshalb nicht, weil als erste Voraussetzung nur die berechtigten Interessen des Verantwortlichen und der Dritten berücksichtigt werden dürfen.

Indem ErwG 47 S. 7 DS-GVO ein berechtigtes Interesse an einer Direktwerbung für ähnliche Produkte jedenfalls dann gegenüber einem Datensubjekt anerkennt, wenn das Datensubjekt bereits ein Kunde des Verantwortlichen ist (ErwG 47 S. 2 DS-GVO), scheint der europäische Gesetzgeber implizit davon

[38] Zum Verhältnis zwischen Art. 8 und Art. 7 GRCh, oben: Kapitel 1 B.II.

[39] *Hacker*, Datenprivatrecht, 2020, S. 275; *Buchner/Petri*, in: Kühling/Buchner (Hrsg.), DS-GVO/BDSG, 3. Aufl. 2020, Art. 6, Rn. 148; *DSK*, Orientierungshilfe der Aufsichtsbehörden für Anbieter von Telemedien, 2019, S. 13.

auszugehen, dass ein Datensubjekt, das zugleich Kunde des Verantwortlichen ist, entweder weniger schutzwürdig ist oder aber – und dies ist plausibler – an dieser Werbung mutmaßlich ebenfalls ein eigenes Interesse haben könnte.

Somit illustrieren ErwG 47 S. 2 i. V. m. S. 7 DS-GVO exemplarisch, dass zwischen den *berechtigten* Interessen des Verantwortlichen (1. Voraussetzung) und den Interessen des Datensubjekts (Bestandteil der 3. Voraussetzung) eine Dichotomie besteht, die im Wortlaut des Art. 6 Abs. 1 lit. f DS-GVO nicht eindeutig aufgelöst wird.

Diese Dichotomie hat Folgen für die praktische Anwendung von Art. 6 Abs. 1 lit. f DS-GVO, weil sie es dem Verantwortlichen erleichtert, bestehende Interessenwidersprüche sprachlich aufzuweichen. In der Praxis wird das Interesse des Verantwortlichen daran, den eigenen Absatz zu steigern, bisweilen als „professionelle Kundenansprache" oder als „Ermöglichung eines besonderen und persönlichen Kundenerlebnisses" verklausuliert. Dadurch soll offenkundig versucht werden, die vorrangig eigenen kommerziellen Interessen des Verantwortlichen ebenfalls als Interesse des Datensubjekts darzustellen.[40] Im Ergebnis fällt die (interne) Interessenabwägung des Verantwortlichen weniger antagonistisch aus und die Datenverarbeitung lässt sich aus Sicht des Verantwortlichen leichter gemäß Art. 6 Abs. 1 lit. f DS-GVO legitimieren. Bei diesem Vorgehen können die Verantwortlichen sich deshalb auf das Vorbild der Direktwerbung in ErwG 47 S. 2 und S. 7 berufen, weil auch dieses – ausdrücklich anerkannte berechtigte Interesse des Verantwortlichen – zwar vorrangig dessen Absatzsteigerung dient, aber nach Ansicht des europäischen Gesetzgebers in einer bereits bestehenden Kundenbeziehung (angeblich) auch dem Interesse des Datensubjekts zu dienen scheint.[41]

2. Formulierung zugunsten der Rechtmäßigkeit

Gemäß Art. 6 Abs. 1 lit. f DS-GVO ist eine Datenverarbeitung auf Grundlage einer Interessenabwägung rechtmäßig, soweit die Interessen des Datensubjekts, die den Schutz personenbezogener Daten erfordern, nicht überwiegen. Diese negative Formulierung begründet zwar keine grundsätzliche Vermutung für die Rechtmäßigkeit der Datenverarbeitung. Allerdings folgt hieraus prozessual, dass die Datenverarbeitung im Fall eines *non liquet* rechtmäßig ist.[42]

Weil die Interessenabwägung im Ausgangspunkt regelmäßig eine interne Angelegenheit des Verantwortlichen ist, dürfte diese negative Formulierung eine

---

[40] Mit weiteren Beispielen: *Metzger*, GRUR 2019, 129 (133 ff.).

[41] Hierzu noch unten C.I.2.

[42] *Schulz*, in: Gola (Hrsg.), DS-GVO, 2. Aufl. 2018, Art. 6, Rn. 58; *Tavanti*, RDV 2016, 295 (298); *Hacker*, Datenprivatrecht, 2020, S. 276; ohne Begründung a. A. *Ehmann*, in: Simitis/Hornung/Spiecker gen. Döhmann (Hrsg.), Datenschutzrecht, 2019, Anhang 3 zu Artikel 6, Rn. 35.

(über)optimistische Beurteilung des Erlaubnistatbestands durch den Verantwortlichen zugunsten einer Datenverarbeitung begünstigen.

Obwohl eine allzu optimistische Interessenabwägung wegen eines potenziell sehr hohen Bußgelds und eines möglichen Reputationsverlust auch aus Sicht des Verantwortlichen riskant ist, lässt sich dieses Risiko vertreten, weil insoweit kaum Erfahrungswerte vorhanden sind, die Kontrolldichte – je nach Branche – bislang gering ist und eine umfangreiche Dokumentation des Abwägungsprozesses dem Verantwortlichen eine gute argumentative Grundlage für die Verteidigung seiner Entscheidung zugunsten einer Datenverarbeitung bieten kann.

3. Fehlen von Abwägungskriterien

Weder Art. 6 Abs. 1 lit. f DS-GVO noch die ErwG 47–49 DS-GVO sind besonders ergiebig, wenn es darum geht, diese datenschutzrechtliche Generalklausel zu konkretisieren. Immerhin lässt sich ErwG 47 DS-GVO entnehmen, dass der Zeitpunkt (S. 3) und die situativen Umstände (S. 4) Einfluss auf die relevanten vernünftigen Erwartungen (S. 1 und S. 3) des Datensubjekts haben sollen. Zudem ist das Bestehen und die Art einer bereits vorhandenen Kundenbeziehung (S. 1 und S. 2) zwischen Datensubjekt und Verantwortlichem zu berücksichtigen. Zuletzt wirkt es sich im Rahmen der Interessenabwägung zugunsten des Verantwortlichen aus, wenn pseudonymisierte Daten[43] verarbeitet und Verschlüsselungstechniken verwendet werden.[44] Letzteres ist Ausdruck und Konsequenz des risikoorientierten Ansatzes der DS-GVO.[45]

Dagegen sollen die Interessen der Datensubjekte insbesondere dann überwiegen, wenn die Datenverarbeitung das Risiko einer Diskriminierung birgt oder die derzeitige Risikoprognose des Verantwortlichen aufgrund einer geplanten langen Speicherdauer sowie einer Weiterleitung ins EU-Ausland besonders vage und unzuverlässig bleiben muss.[46]

Auch die Quantität der zu verarbeitenden Daten soll im Rahmen der Interessenabwägung eine Rolle spielen können.[47] Hierbei ist allerdings Vorsicht geboten. Weil die zweite Voraussetzung (Erforderlichkeit zur Interessenwahrung) die Quantität der zu verarbeitenden Daten bereits auf das in Relation zu den

---

[43] Definiert in Art. 4 Nr. 5 DS-GVO. Instruktiv: *ENISA*, Pseudonymization Techniques and best Practices, 03.12.2019, S. 21 ff.

[44] *Herfurth*, ZD 2018, 514 (516); *Hanloser*, ZD 2019, 287 (289); *Schantz*, in: Simitis/Hornung/Spiecker gen. Döhmann (Hrsg.), Datenschutzrecht, 2019, Art. 6, Rn. 114; *Artikel-29-Datenschutzgruppe*, Stellungnahme 06/2014 zum Begriff des berechtigten Interesses des für die Verarbeitung Verantwortlichen gemäß Artikel 7 der Richtlinie 95/46/EG, WP 217, 2014, S. 54.

[45] *Veil*, ZD 2015, 347.

[46] *Schantz*, in: Simitis/Hornung/Spiecker gen. Döhmann (Hrsg.), Datenschutzrecht, 2019, Art. 6, Rn. 105 f.; *Herfurth*, ZD 2018, 514 (518 f.); *DSK*, Orientierungshilfe der Aufsichtsbehörden für Anbieter von Telemedien, 2019, S. 19.

[47] *Herfurth*, ZD 2018, 514 (516); *DSK*, Orientierungshilfe der Aufsichtsbehörden für Anbieter von Telemedien, 2019, S. 20.

berechtigten Interessen notwendige Maß reduziert hat, wäre es widersprüchlich, wenn die zuvor zur Wahrung des berechtigten Interesses für erforderlich gehaltene Quantität der zu verarbeitenden Daten anschließend als maßgeblicher Grund für das Überwiegen der Interessen des Datensubjekts angeführt wird.[48]

Obwohl die DS-GVO kaum konkrete Kriterien für die Interessenabwägung i. R. v. Art. 6 Abs. 1 lit. f DS-GVO vorgibt, lassen sich aus der Systematik der DS-GVO dennoch zwei wesentliche Kriterien ableiten. Zunächst muss die Person des Datensubjekts berücksichtigt werden (a), zudem bietet der vernünftige Erwartungshorizont ein zwar vages, aber für die Steuerung des Mindestmaßes an Datenverarbeitung dennoch geeignetes Kriterium (b). Zuletzt ist eine Gegenausnahme zu beachten. Hat das Datensubjekt die Daten öffentlich verfügbar gemacht, so sind die Interessen des Datensubjekts nicht oder jedenfalls weniger schutzwürdig (c).

a) Persönliche Eigenschaften von Datensubjekten

Weil es gemäß Art. 6 Abs. 1 lit. f DS-GVO ausdrücklich zu berücksichtigen ist, wenn das Datensubjekt ein Kind ist, liegt es nahe, im Rahmen der Interessenabwägung stets auf die konkret betroffenen Datensubjekte einzugehen, sofern diese sich typisieren lassen. Hierfür spricht zudem, dass die Erwähnung von Kindern in Art. 6 Abs. 1 lit. f DS-GVO lediglich beispielhaft ist („insbesondere"), wenngleich die DS-GVO – im Unterschied zu anderen sekundärrechtlichen Rechtsakten[49] – selbst keine weiteren Kategorien von Datensubjekten kennt (Art. 8/ErwG 38 DS-GVO). Im Unterschied zur Einwilligung kommt es für Art. 6 Abs. 1 lit. f DS-GVO – als gesetzlichem Erlaubnistatbestand – zwar nicht auf besondere geistige Fähigkeiten oder die geistige Reife des Datensubjekts an. Allerdings setzt jedenfalls die mit einer Datenverarbeitung auf Grundlage der Interessenabwägung anschließend einhergehende Möglichkeit zur Ausübung des *Widerspruchsrechts* gemäß Art. 21 Abs. 1 DS-GVO (hierzu sogleich) die geschäftliche Entscheidungsfähigkeit voraus. Inwieweit das typischerweise von einer bestimmten Datenverarbeitung betroffene Datensubjekt künftig in der Lage ist, die eigene Entscheidungszuständigkeit durch Erklärung

[48] Dies aber für möglich haltend („Umfang der Daten"): *Schantz*, in: Simitis/Hornung/Spiecker gen. Döhmann (Hrsg.), Datenschutzrecht, 2019, Art. 6, Rn. 105.

[49] Insofern liegt es jedoch nahe, im Rahmen der Interessenabwägung auch zu berücksichtigen, ob die Datenverarbeitung ausschließlich oder weit überwiegend die Interessen bestimmter Datensubjekte betrifft. Wie sich aus Art. 5 Abs. 3 der Richtlinie 2005/29/EG vom 11.05.2005 über unlautere Geschäftspraktiken zwischen Unternehmen und Verbrauchern (UGP-RL) ergibt, ist dieser Gedanke dem EU-Recht jedenfalls im Bereich des Verbraucherrechts nicht fremd. Hierzu auch RL 2019/2161 zur Änderung der Richtlinie 93/13/EWG des Rates und der Richtlinien 98/6/EG, 2005/29/EG und 2011/83/EU des Europäischen Parlaments und des Rates zur besseren Durchsetzung und Modernisierung der Verbraucherschutzvorschriften der Union v. 27.11.2019 (Omnibus-RL), ABl. v. 18.12.2019, L 328, S. 7 ff.

eines Widerspruchs herzustellen, ist infolgedessen ein Kriterium, dass bereits im Rahmen der ursprünglichen Interessenabwägung zu berücksichtigen ist.

Für die Datenverarbeitung auf Grundlage einer Interessenabwägung ist – im Unterschied zur Einwilligung – stets eine Entscheidung anhand von (typisierten) Einzelfällen erforderlich. Deshalb ist es überzeugend, dass Art. 6 Abs. 1 lit. f DS-GVO zwar lediglich die aus dem Kontext der Einwilligung (Art. 8 DS-GVO) bekannte Kategorie der „Kinder" als ein Beispiel anführt („insbesondere"). Dies verbietet es jedoch nicht, im Rahmen der Interessenabwägung die konkreten Umstände des Einzelfalls zu berücksichtigen, so dass andere, für den Verantwortlichen erkennbare Umstände – ebenso wie gemäß § 3 Abs. 4 S. 2 UWG[50] – einzubeziehen sind. Anders als die Definition der Einwilligungsfähigkeit, die dazu dient, die datenschutzrechtliche Einwilligung durch eine eindeutige – gegenüber der Geschäftsfähigkeit herabgesetzte – Altersgrenze mit einem gewissen Verkehrsschutz auszustatten,[51] bietet die Interessenabwägung als datenschutzrechtliche Generalklausel keinen solchen Verkehrsschutz, wenngleich eine künftige Bildung von Fallgruppen zur Wahrung der Rechtssicherheit sinnvoll und notwendig ist.

b) Erwartungshorizont der Datensubjekte

Soweit die vernünftigen Erwartungen der Datensubjekte ausschlagend sein sollen,[52] liegt es nach hier vertretener Auffassung nahe, diesen Erwartungshorizont normativ auszulegen,[53] ohne dass dem Verantwortlichen die Möglichkeit genommen wird, empirische Studien vorzulegen, die das Ergebnis seiner Interessenabwägung unterstützen. Soweit *Philipp Hacker* dafür plädiert, stets die mutmaßlichen Datenschutzpräferenzen derjenigen Datensubjekte einzubeziehen, die typischerweise von der Datenverarbeitung betroffen sind,[54] ist Vor-

[50] Gemäß § 3 Abs. 4 S. 2 UWG sind solche geschäftlichen Handlungen, „die für den Unternehmer vorhersehbar das wirtschaftliche Verhalten nur einer eindeutig identifizierbaren Gruppe von Verbrauchern wesentlich beeinflussen, die auf Grund von geistigen oder körperlichen Beeinträchtigungen, Alter oder Leichtgläubigkeit […] besonders schutzbedürftig sind, […] aus der Sicht eines durchschnittlichen Mitglieds dieser Gruppe zu beurteilen". Hierzu: *BGH*, Urt. v. 07.05.1998 – I ZR 85/96 = GRUR 1998, 1041 (1042) – *Verkaufsveranstaltung in Aussiedlerwohnheim*. Zur Erkennbarkeit dieser besonderen Gruppe von Verbrauchern: *BGH*, Urt. v. 12.12.2013, I ZR 192/12 = GRUR 2014, 686 (Rn. 16) – *Goldbärenbarren*.

[51] Zur Berücksichtigungsfähigkeit der geschäftlichen Unerfahrenheit im Kontext der Einwilligung unten Kapitel 5 C.III.3.d.bb.

[52] Zugunsten einer Datenverarbeitung: ErwG 47 S. 1, S. 3 DS-GVO und zulasten einer Datenverarbeitung: ErwG 47 S. 4 DS-GVO.

[53] Für eine gemischt normativ-empirische Analyse: m. w. N. *Hacker*, Datenprivatrecht, 2020, S. 277; für eine weder durch die Verantwortlichen noch Behörden und Gerichte praktisch leistbare Empirie, die gemäß ErwG 47 zumindest den Zeitpunkt, die Beziehung zwischen Datensubjekt und Verantwortlichem, die Umstände und die Situation des jeweiligen Einzelfalls berücksichtigen müsste: *Hanloser*, ZD 2019, 287 (290).

[54] In diese Richtung: *Hacker*, Datenprivatrecht, 2020, S. 281.

sicht geboten. Zunächst gelingt es selten, eine Gruppe von Datensubjekten klar abzugrenzen und ausschließlich deren Daten zu verarbeiten. Darüber hinaus sind kundgetane Datenschutzpräferenzen sehr dynamisch und angesichts des empirisch belegten sog. *privacy paradoxon*[55] nicht sonderlich belastbar. Hiernach besteht eine paradoxe Diskrepanz zwischen der hohen Bedeutung, die Datensubjekte dem Datenschutz auf Nachfrage beimessen und der tatsächlichen Bereitschaft, personenbezogene Daten bereitzustellen (Telefonnummer/Wohnadresse), um im Gegenzug eine kleine Reduktion des monetären Preises für ein Produkt zu erhalten.[56] Weil belastbare empirische Studien sehr aufwendig sind und die Gefahr besteht, dass die daraus jeweils abgeleiteten aktuellen Präfenzen von Datensubjekten wegen des sog. *privacy paradoxon* in eine Anmaßung von tatsächlich nicht vorhandenem Wissen münden, sollte die Interessenabwägung in Art. 6 Abs. 1 lit. f DS-GVO vorrangig normativ erfolgen.

Während die datenschutzrechtliche Einwilligung – trotz der an ihr berechtigter Weise geübten Kritik[57] – Ausdruck der tatsächlichen subjektiven Einstellungen und Präferenzen ist, bietet der Auffangtatbestand in Art. 6 Abs. 1 lit. f DS-GVO einen normativen Rahmen für die Datenverarbeitung, so dass selbst eine ubiquitäre Datenverarbeitung und eine dementsprechende Anpassung des Erwartungshorizonts der Datensubjekte nicht in der Lage sind, eine Abwärtsspirale auszulösen, nur weil sich empirisch nachweisen lässt, dass sich ein insoweit angepasster „vernünftiger" datenschutzrechtlicher Fatalismus verbreitet hat.[58] Die primär normative Beurteilung des vernünftigen Erwartungshorizonts verhindert, dass Gerichte einer tatsächlichen Erosion der echten oder behaupteten Datenschutzpräferenzen im Sinne einer normativen Kraft des Faktischen lediglich ohnmächtig zusehen müssen.

c) Öffentlich zugängliche personenbezogene Daten

Sofern personenbezogene Daten öffentlich zugänglich sind, reduziert diese Tatsache das Interesse des Datensubjekts im Rahmen der Abwägung grundlegend.[59]

---

[55] *Brandimarte/Acquisti/Loewenstein*, 4 Social Psychological and Personality Science, 2013, 340 ff.

[56] *Preibusch/Kübler/Beresford*, 13 Electronic Commerce Research (2013), S. 423 (441/444 f.).

[57] *Simitis*, NJW 1998, 2573 (2476); sowie jeweils m. w. N.: *Rogosch*, Die Einwilligung im Datenschutzrecht, 2013, S. 17 f.; *Radlanski*, Das Konzept der Einwilligung in der datenschutzrechtlichen Realität, 2016, S. 147/212/239; *Buchner/Kühling*, in: Kühling/Buchner (Hrsg.), DS-GVO, 3. Aufl. 2020, Art. 7, Rn. 10; ähnlich: *Veil*, NJW 2018, 3337 (3344).

[58] Anderenfalls könnten die faktisch weitverbreitete abstrakte Kenntnis über die derzeitige Praxis „personalisierte Werbung" (*DIVSI*, Daten – Ware und Währung, 2014, S. 16) und das Desinteresse der Mehrheit der Datensubjekte an diesen Formen der Datenverarbeitung zur normativen Grundlage für eine solche Praxis werden. Zu dieser Gefahr, sofern im Rahmen von Art. 6 Abs. 1 lit. b DS-GVO lediglich auf die subjektiven Erwartungen abgestellt wird: *Leistner/Antoine/Sagstetter*, Big Data, 2021, S. 256 f.

[59] *Herfurth*, ZD 2018, 514 (517); *Ehmann*, in: Simitis/Hornung/Spiecker gen. Döhmann

Soweit man den Schutz personenbezogener Daten auch mit Blick auf den Schutz der Privatsphäre versteht, reduziert eine solche öffentliche Zugänglichkeit das Interesse am Schutz der Privatsphäre (Art. 7 GRCh). Dennoch erfolgt die Interessenabwägung gemäß Art. 6 Abs. 1 lit. f DS-GVO stets für bestimmte Verarbeitungszwecke (Art. 5 Abs. 1 lit. b DS-GVO) und aufgrund des risikoorientierten Ansatzes der Interessenabwägung[60] kann aus der öffentlichen Verfügbarkeit von Daten nicht automatisch geschlossen werden, das Datensubjekt habe – sofern es um die öffentliche Verfügbarkeit weiß – vernünftigerweise den Erwartungshorizont, dass es damit alle Interessen und Rechte an den personenbezogenen Daten verloren hat und diese Daten für jeden Zweck beliebig einsetzbar werden. Vielmehr müssen die „vernünftigen Erwartungen" (ErwG 47 DS-GVO) auch berücksichtigen, zu welchem Zeitpunkt und unter welchen Umständen die Daten öffentlich zugänglich gemacht wurden. Wann und in welchem Kontext personenbezogene Daten öffentlich verfügbar gemacht wurden, hat Auswirkungen darauf, welche Arten von Datenverarbeitung zu diesem Zeitpunkt vernünftigerweise absehbar waren.

Abweichend ist eine Konstellation zu beurteilen, in der das Datensubjekt die Daten selbst offensichtlich öffentlich gemacht hat. In diesem Fall ist gemäß Art. 9 Abs. 2 lit. e DS-GVO sogar die Verarbeitung von besonders sensiblen personenbezogenen Daten rechtmäßig.[61] Soweit für ein solches öffentliches Zugänglichmachen ein bewusster Willensakt des Datensubjekts gefordert wird,[62] handelt es sich dabei um eine im Gesetz nicht vorgesehene Beschränkung, weil es für Art. 9 Abs. 2 lit. e DS-GVO genügt, dass die Daten offensichtlich vom Datensubjekt öffentlich gemacht wurden. Auf subjektive Voraussetzung kommt es nach dem Wortlaut nicht an. Dieser Verzicht auf ein subjektives

(Hrsg.), Datenschutzrecht, 2019, Anhang 3 zu Artikel 6, Rn. 36; wie hier *Tavanti*, RDV 2016, 295 (297). Auf eine analoge Anwendung des Art. 9 Abs. 2 lit. e DS-GVO kommt es aufgrund der gemäß Art. 6 Abs. 1 lit. f DS-GVO ohnehin bestehenden, offenen Interessenabwägung nicht an; diesbezüglich a. A. *Golland*, MMR 2018, 130 (133).

[60] Dieser ergibt sich bereits aus dem Erfordernis einer Risikofolgenabschätzung gemäß Art. 35 Abs. 1 S. 1 DS-GVO, sofern eine Datenverarbeitung risikoreich erscheint.

[61] Hierzu die Vorlagefrage 4 des *ÖOGH*, Vorlagebeschl. v. 22.07.2021, 6 Ob 56/21k – *Schrems* [*III*]. Der ÖOGH legt dem EuGH damit u. a. Frage vor, ob die auf einer (öffentlichen) Podiumsdiskussion erwähnte eigene sexuelle Orientierung anschließend durch Facebook auf Grundlage von Art. 9 Abs. 2 lit. e DS-GVO für ein Profiling genutzt werden kann. Dass die Daten offensichtlich vom Datensubjekt öffentlich gemacht worden sein müssen, schränkt die praktische Bedeutung von Art. 9 Abs. 2 lit. e DS-GVO ein. Zwar ist die Offensichtlichkeit am Maßstab des objektiven Empfängerhorizonts zu messen und es genügt, wenn das Datensubjekt das Öffentlichmachen selbst veranlasst hat. Insoweit kann beispielsweise für Daten auf einer vom Datensubjekt betriebenen Webseite von einer solchen Offensichtlichkeit grundsätzlich ausgegangen werden. Weil aber kein genereller Schutz des guten Glaubens an das Öffentlichmachen durch das Datensubjekt existiert, ist eine Datenverarbeitung auf Grundlage von Art. 9 Abs. 2 lit. e DS-GVO riskant.

[62] *Petri*, in: Simitis/Hornung/Spiecker gen. Döhmann (Hrsg.), Datenschutzrecht, 2019, Art. 9, Rn. 57.

Element ist deshalb konsequent, weil anderenfalls das Erfordernis eines nachweisbaren bewussten Willensakts erhebliche Abgrenzungsschwierigkeiten zu einer Einwilligung gegenüber der Allgemeinheit[63] verursachen würde.

Grundsätzlich sind Daten öffentlich, wenn sie einem unbestimmten, also individuell nicht bestimmbaren Personenkreis zugänglich gemacht wurden. Somit sind Daten, die über Plattformen und Kommunikationsnetzwerke zugänglich sind, nur dann öffentlich, wenn jedermann Kunde dieser Plattform werden kann. Ist es dagegen zusätzlich erforderlich, Mitglied einer – gegebenenfalls auch sehr großen – Gruppe innerhalb eines Netzwerks zu sein, um Zugang zu den Daten zu erhalten, schließt diese Voraussetzung regelmäßig aus, dass die Daten öffentlich zugänglich sind.

Anders als der Begriff der Öffentlichkeit auf den ersten Blick suggeriert, ist jedoch auch eine allgemeine Verfügbarkeit über das Internet nicht notwendig mit einem Öffentlichmachen verbunden. Ergibt sich aus den konkreten situativen und zeitlichen Umständen und der Technik, die zum Öffentlichmachen verwendet wurde, welchen mutmaßlichen Zweck das Datensubjekt damit verfolgte, so können diese Daten anschließend nicht durch jeden Verantwortlichen für jeden beliebigen Zweck, beispielsweise für eine Datenanalysen auf Grundlage von maschinellem Lernen, zur Profilbildung und anschließendem entgeltlichen Angebot dieses Profils an Arbeit- oder Versicherungsgeber verarbeitet werden.[64] Vielmehr können auch grundsätzlich allgemein zugängliche Plattformen bestimmten erkennbaren Kommunikationsinteressen des Datensubjekts dienen. Daraus können sich über den vernünftigen Erwartungshorizont der Datensubjekte Beschränkungen für eine spätere, anderweitige Datenverarbeitung ergeben, sofern diese eine neue, abweichende Öffentlichkeit eröffnet, eine grundlegend andere Technik verwendet und eine neue Verwertungsart ermöglicht, die im Zeitpunkt des erstmaligen Öffentlichmachens noch nicht abzusehen war.[65]

IV. Option zur Herstellung der Entscheidungszuständigkeit

Sofern eine Datenverarbeitung auf einer Einwilligung beruht, hat das Datensubjekt – trotz der weitverbreiteten Skepsis gegenüber der Einwilligung – zumindest formal zugunsten dieser Verarbeitung entschieden. Zudem verfügt das

---

[63] Mit der Annahme einer konkludenten Einwilligung gegenüber der Allgemeinheit für das Urheberrecht: *Ohly*, GRUR 2012, 983 (987 f.).

[64] Ebenso *Hacker*, Datenprivatrecht, 2020, S. 278.

[65] Mit der Frage, ob die auf einer (öffentlichen) Podiumsdiskussion erwähnte eigene sexuelle Orientierung anschließend durch Facebook auf Grundlage von Art. 9 Abs. 2 lit. e DS-GVO für ein Profiling genutzt werden kann: *ÖOGH*, Vorlagebeschl. v. 22.07.2021, 6 Ob 56/21k – *Schrems* [*III*] (Vorlagefrage 4/Rn. 25 ff.). Hierzu auch unten: C.I.3.a.

Datensubjekt mit dem Einwilligungswiderruf gemäß Art. 7 Abs. 3 S. 1 DS-GVO regelmäßig über eine Möglichkeit, seine eigene Entscheidung wieder zu ändern. Obwohl der *Widerruf* infolge seiner *ex nunc*-Wirkung keine Rückkehr zum *ex ante*-Zustand ermöglicht, kann der Widerruf als Instrument zur Wiederherstellung der Entscheidungszuständigkeit durch das Datensubjekt bezeichnet werden.

Im Gegensatz zum Einwilligungswiderruf, führt der gemäß Art. 21 Abs. 1 DS-GVO vorgesehene *Widerspruch* gegen eine Datenverarbeitung, die bis zu diesem Zeitpunkt auf Grundlage einer Interessenabwägung gemäß Art. 6 Abs. 1 lit. f DS-GVO erfolgte, zu einer erstmaligen Herstellung der Entscheidungszuständigkeit des Datensubjekts. Dieses Widerspruchsrecht wird zunächst allgemein in den datenschutzrechtlichen Kontext eingeordnet (1). Anschließend liegt der Fokus auf dem komplexen Verhältnis zwischen dem Widerrufs- und dem Widerspruchsrecht des Datensubjekts (2). Bereits in diesem Kontext wird deutlich, warum der Einwilligung als Rechtsgrundlage für eine Datenverarbeitung gegenüber der Interessenabwägung – im Grundsatz – ein Vorrang einzuräumen ist (unten D).

1. Einordnung des Widerspruchsrechts

Gemäß Art. 21 Abs. 1 S. 1 DS-GVO haben Datensubjekte das Recht, aus Gründen, die sich aus ihrer besonderen Situation ergeben, jederzeit Widerspruch gegen solche Datenverarbeitungen einzulegen, die infolge einer Interessenabwägung des Verantwortlichen (Art. 6 Abs. 1 lit. f DS-GVO) rechtmäßig sind.

Wesentliche Besonderheit der Interessenabwägung ist, dass das Datensubjekt zunächst nicht an der Entscheidung über die Datenverarbeitung beteiligt ist, sondern regelmäßig lediglich im Rahmen der Erklärungen zum Datenschutz über die Verarbeitungsgrundlage, die berechtigten Interessen an der Verarbeitung (Art. 13 Abs. 1 lit. d DS-GVO bzw. Art. 14 Abs. 2 lit. b DS-GVO) und das Widerspruchsrecht informiert wird (Art. 21 Abs. 4 DS-GVO). Soweit die Verarbeitung auf Art. 6 Abs. 1 lit. f DS-GVO beruht, entscheidet somit der jeweilige Verantwortliche im Rahmen einer eigenen, internen Abwägung darüber, ob und inwieweit die Interessen des Datensubjekts am Unterbleiben einer Datenverarbeitung gegenüber seinen eigenen Interessen an der Verarbeitung nicht überwiegen.

Erst durch den Widerspruch gemäß Art. 21 Abs. 1 DS-GVO kann das Datensubjekt dem Verantwortlichen die Entscheidungszuständigkeit erstmals entziehen. Allerdings lebt das Verarbeitungsverbot aus Art. 6 Abs. 1 DS-GVO mit dem Zugang der Widerspruchserklärung nicht generell und automatisch wieder auf. Nur soweit die Datenverarbeitung für Zwecke der Direktwerbung erfolgte, gilt mit der Widerspruchserklärung das ursprüngliche Verarbeitungsverbot wieder, Art. 21 Abs. 3 DS-GVO.

Abgesehen von diesem engen Sonderfall der Direktwerbung löst ein Widerspruch zunächst eine erneute Prüfung aus. Weil in dieser Prüfung die Widerspruchsbegründung des Datensubjekts berücksichtigt werden muss (a), handelt es sich dabei um eine qualifizierte Interessenabwägung (b). Bis zum Abschluss dieser Prüfung hat das Datensubjekt gemäß Art. 18 Abs. 1 lit. d DS-GVO lediglich das Recht, eine interimistische Einschränkung der Datenverarbeitung zu verlangen.

a) Widerspruchsbegründung

Gemäß Art. 21 Abs. 1 S. 1 DS-GVO müssen für den Widerspruch Gründe existieren, die sich aus der besonderen Situation des Datensubjekts ergeben. Anders als der sog. *freie Widerruf* der Einwilligung gemäß Art. 7 Abs. 3 S. 1 DS-GVO handelt es sich bei Art. 21 Abs. 1 S. 1 DS-GVO um einen *qualifizierten Widerspruch*. Der Wortlaut spricht zunächst dafür, dass sich diese Gründe für einen Widerspruch aus der besonderen Situation des Datensubjekts ergeben müssen und es nicht genügt, wenn diese Gründe ausschließlich mit den Umständen der Datenverarbeitung zusammenhängen. Nur in Verbindung mit der besonderen Situation des Datensubjekts kann eine (bislang rechtmäßige) Datenverarbeitung infolge eines Widerspruchs nicht mehr in rechtmäßiger Weise fortgesetzt werden.[66]

Obwohl der Konnex zur besonderen Situation des Datensubjekts zunächst den Eindruck einer gewissen, persönlichkeitsrechtlich geprägten Schwelle vermittelt, sprechen mehrere systematische Argumente dagegen, hohe Anforderungen an die Widerspruchsbegründung zu stellen.[67] Zunächst stehen das gesetzliche Verbot der Datenverarbeitung und die Rechtmäßigkeit der Verarbeitung nach der Gesetzessystematik in einem Verhältnis von Regel und Ausnahme, Art. 6 Abs. 1 DS-GVO.

Zudem spricht die Tatsache, dass die Einwilligung gemäß Art. 7 Abs. 3 S. 1 DS-GVO grundlos widerrufen werden kann, dafür, keine hohen Anforderungen an die Begründung des Widerspruchs zu stellen. Immerhin hatte das Datensubjekt im Rahmen der Einwilligung die Möglichkeit, seinen Willen vor Beginn der Datenverarbeitung mitzuteilen. Beruht die Datenverarbeitung dagegen auf einer internen Interessenabwägung des Verantwortlichen, dann bietet das Widerspruchsrecht dem Datensubjekt – im Unterscheid zum Widerruf einer vorher erteilten Einwilligung – die erste und einzige Möglichkeit seinem der Datenverarbeitung entgegenstehenden Willen Ausdruck zu verleihen. Aller-

[66] *Kamann/Braun*, in: Ehmann/Selmayr (Hrsg.), DS-GVO, Art. 21, Rn. 35.

[67] Das LG Frankfurt a. M. sah einen besonderen Grund bereits dann gegeben, wenn ein Datensubjekt aufgrund der Weitergabe von Daten über seine Restschuldbefreiung Schwierigkeiten bei der Wohnungssuche und Aufnahme einer selbständigen Tätigkeit hat: *LG Frankfurt a. M.,* NZI 2019, 342; kritisch hierzu: *Heyer*, NZI 2019, 342.

dings muss die Begründung des Widerspruchs so spezifisch ausfallen, dass sie es dem Verantwortlichen ermöglicht, auf dieser Grundlage anschließend eine qualifizierte Interessenabwägung vorzunehmen.

b) Rechtsfolge: Qualifizierte Interessenabwägung

Auch für die qualifizierte Interessenabwägung bietet die DS-GVO leider keine konkreten Kriterien. Weil für eine Fortsetzung der Datenverarbeitung nach dem Widerspruch lediglich berechtigte Interessen nicht mehr ausreichen, sondern zwingende Gründe erforderlich sind, müssen die Anforderungen i. R. v. Art. 21 Abs. 1 S. 2 DS-GVO deutlich höher liegen, als diejenigen der ursprünglichen Datenverarbeitung, der das Datensubjekt mittlerweile widersprochen hat. Der Verantwortliche möchte ab diesem Zeitpunkt personenbezogene Daten im eigenen Interesse oder im Interessen eines Dritten verarbeiten, obwohl dies gegen den ausdrücklichen Willen des Datensubjekts geschieht. Eine Einwilligung wäre für eine solche Datenverarbeitung aufgrund des entgegenstehenden Willens nicht mehr zu erreichen.

Infolgedessen kann es für die Annahme von zwingenden Gründen nicht genügen, dass dem Verantwortlichen ohne die Fortsetzung der Datenverarbeitung lediglich Unannehmlichkeiten oder wirtschaftliche Nachteile drohen. Nicht überzeugen kann es zudem, dass es als zwingender Grund ausreichen soll, wenn der Verantwortliche anderenfalls gegenüber Dritten seine vertraglichen Pflichten nicht mehr erfüllen kann.[68] In diesem Fall würde der Vertrag zwischen dem Verantwortlichen und dem Dritten nachträglich zu einem Vertrag zulasten des Datensubjekts und das, obwohl weder der gute Glaube an eine wirksame Einwilligung noch derjenige an das Bestehen eines gesetzlichen Erlaubnistatbestands geschützt werden.

Zudem spricht der aufgrund des Widerspruchs offenkundig entgegenstehende Wille des Datensubjekts dafür, auch die gesetzliche Ausnahme zugunsten einer Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen gemäß Art. 21 Abs. 1 S. 2 a. E. DS-GVO eher restriktiv auszulegen. Während der Verantwortliche die Daten zweifelsfrei weiterhin verarbeiten darf, soweit sich die gerichtliche und außergerichtliche Verfolgung von Rechtsansprüchen gegen das Datensubjekt selbst richten, kommt eine Verarbeitung personenbezogener Daten zur Verfolgung von Rechtsansprüche gegenüber Dritten im Grundsatz nur in Betracht, sofern das Datensubjekt gesetzliche oder rechtsgeschäft(sähn)liche Mitwirkungspflichten treffen.[69]

---

[68] So: *Munz*, in: Taeger/Gabel (Hrsg.), DS-GVO/BDSG, 3. Aufl. 2019, Art. 21, Rn. 25.

[69] A. A., also für eine rechtmäßige Datenverarbeitung zur Verfolgung von Rechtsansprüchen gegenüber Dritten: *Kamann/Braun*, in: Ehmann/Selmayr (Hrsg.), DS-GVO, 2018, Art. 21, Rn. 28.

Die ausdrückliche Nennung der Rechtsverfolgung als qualifiziertes Verarbeitungsinteresse macht deutlich, dass die sonstigen zwingenden Gründe von vergleichbarer Bedeutung sein müssen. Insoweit liegen die zwingenden Gründe im Graubereich zwischen den (niedrigeren) berechtigten Interessen der ursprünglichen, unwidersprochenen Interessenabwägung (Art. 6 Abs. 1 lit. f DS-GVO) und den durch Unionsrecht oder nationales Recht etablierten (höheren) rechtlichen Verpflichtungen des Verantwortlichen gemäß Art. 6 Abs. 1 lit. c DS-GVO.[70] Ist eine Datenverarbeitung in öffentlichem Interesse, so kann gegen diese kein Widerspruch erhoben werden und es kommt gerade nicht auf eine (qualifizierte) Interessenabwägung an.[71]

Gegen eine allzu enge Auslegung dieser zwingenden Gründe spricht die Notwendigkeit, anschließend erneut zwischen diesen zwingenden Gründen des Verantwortlichen und den Interessen, Rechten und Freiheiten des Datensubjekts abwägen zu müssen. Insofern ist der Wortlaut des Art. 21 Abs. 1 S. 2 DS-GVO etwas paradox, wenn zunächst zwingende Gründe für eine Datenverarbeitung vorliegen müssen, diese sich aber anschließend im Rahmen der Abwägung mit den Interessen, Rechten und Freiheiten des Datensubjekts gerade als nicht zwingend herausstellen können.

Im Vergleich zur einfachen Interessenabwägung gemäß Art. 6 Abs. 1 lit. f DS-GVO folgt aus der Formulierung des Art. 21 Abs. 1 S. 2 DS-GVO immerhin, dass für diese qualifizierte Interessenabwägung eine Umkehr der Darlegungs- und Beweislast gilt („nachweisen"): Ein *non liquet* wirkt sich nunmehr – anders als in der ursprünglichen Interessenabwägung gemäß Art. 6 Abs. 1 lit. f DS-GVO – zulasten des Verantwortlichen aus.[72] In Kombination mit einem potenziell sehr hohen Bußgeld, dürfte eine allzu sorglose Fortsetzung der Datenverarbeitung durch den Verantwortlichen infolgedessen begrenzt sein.

Ist der Widerspruch erfolgreich, dürfen die personenbezogenen Daten, soweit sie vom Widerspruch erfasst sind, nicht mehr verarbeitet werden. Zudem ist der Verantwortliche gemäß Art. 17 Abs. 1 Hs. 2 lit. c DS-GVO grundsätzlich dazu verpflichtet,[73] die vorhandenen Daten selbstständig zu löschen.

2. Kollision mit der Widerruflichkeit der Einwilligung

Weil eine Einwilligung gemäß Art. 6 Abs. 1 lit. a DS-GVO und die Interessenabwägung gemäß Art. 6 Abs. 1 lit. f DS-GVO sich nicht gegenseitig als Erlaub-

[70] Vgl. ErwG 45 DS-GVO.

[71] Dies gilt gemäß Art. 6 Abs. 1 lit. d DS-GVO erst recht zur Wahrung von lebenswichtigen Interessen des Datensubjekts oder Dritter; hierzu ErwG 46 DS-GVO.

[72] ErwG 69 S. 2 DS-GVO ist insoweit etwas undeutlich. Hiernach sollte der Verantwortliche „*darlegen* müssen, dass seine zwingenden berechtigten Interessen Vorrang vor den Interessen oder Grundrechten und Grundfreiheiten der betroffenen Person haben." [Hervorhebung durch den Verfasser].

[73] Zu den Ausnahmen: Art. 17 Abs. 3 DS-GVO.

nistatbestand ausschließen,[74] ist das Verhältnis zwischen einem Einwilligungswiderruf gemäß Art. 7 Abs. 3 S. 1 DS-GVO und einem Widerspruch gemäß Art. 21 Abs. 1 S. 1 DS-GVO komplex und bedarf einer Synchronisierung.[75] Diese Komplexität hat zudem Auswirkungen auf die Gestaltung von solchen technischen Mitteln, die es den Datensubjekten erleichtern sollen, datenschutzrechtliche Erklärungen abzugeben, ihre Ansprüche gegenüber Verantwortlichen geltend zu machen und die deshalb dazu dienen, die informationelle Privatautonomie der Datensubjekte abzustützen.[76]

Dem Wortlaut des Art. 6 Abs. 1 DS-GVO lässt sich keine offenkundige Reihenfolge zwischen den Erlaubnistatbeständen entnehmen. Er lässt es ausdrücklich genügen, dass „*mindestens* eine der nachstehenden Bedingungen erfüllt ist".[77] Infolgedessen kommt der Einwilligung kein formeller Vorrang gegenüber der Interessenabwägung zu. Dennoch offenbart der systematische Zusammenhang von Einwilligung und Interessenabwägung, dass der Einwilligung im Privatrechtsverhältnis aus materiell-rechtlichen Gründen ein Vorrang einzuräumen ist,[78] weil sie eine besondere Bedeutung für die Verwirklichung informationeller Privatautonomie hat[79] und eine umfangreiche Anwendung der Interessenabwägung die speziellen Voraussetzungen an eine wirksame Einwilligung unterlaufen würde.[80]

Sofern keine besonders sensiblen Daten verarbeitet werden – dann ist eine Verarbeitung auf Grundlage von Art. 6 Abs. 1 lit. f DS-GVO derzeit von vornherein ausgeschlossen[81] – ist ein Widerruf der Einwilligung regelmäßig zugleich als Widerspruch im Sinne des Art. 21 Abs. 1 S. 1 DS-GVO auszulegen.[82]

---

[74] Mit Blick auf den Wortlaut von Art. 6 Abs. 1 DS-GVO („mindestens" ein Erlaubnistatbestand) sowie Art. 17 Abs. 1 lit. b DS-GVO (kein Löschungsanspruch, bei anderweitiger Rechtmäßigkeit) ist diese Auffassung zwingend.

[75] Mangels klarer Abgrenzbarkeit in der Praxis, ist es legitim – vorsorglich – auch eine Einwilligung einzuholen, wobei der Widerruf der Einwilligung – jedenfalls bei Begründung durch das Datensubjekt – ebenfalls als Widerspruch gemäß Art. 21 Abs. 1 S. 1 DS-GVO zu werten ist.

[76] Zu den Konsequenzen: Kapitel 6 B.II.1.b.cc.

[77] [Hervorhebung durch den Verfasser].

[78] A. A. *Radlanski*, Das Konzept der Einwilligung in der datenschutzrechtlichen Realität, 2016, S. 205; *Simitis*, NJW 1998, 2472 (2476) und (wohl) *Schantz*, in: Simitis/Hornung/Spiecker gen. Döhmann (Hrsg.), Datenschutzrecht, 2019, Art. 6, Rn. 11/88.

[79] *Bunnenberg*, Privates Datenschutzrecht, 2020, S. 68; ebenso zum BDSG a. F. *Roßnagel/Pfitzmann/Garska*, Modernisierung des Datenschutzrechts, Gutachten für das BMI, 2001, S. 72.

[80] Ebenso: *Buchner*, DuD 2016, 155 (157); *Engeler*, ZD 2018, 55 (56); *Richter*, PinG 2018, 6. Hierzu unten: C.II.

[81] Zur Möglichkeit von Ausnahmen durch das Hineinlesen der ungeschriebenen Tatbestandsvoraussetzung der „Verwendungsabsicht" in Art. 9 Abs. 1 DS-GVO und zur hier stattdessen bevorzugten Notwendigkeit, *de lege ferenda* einen Tatbestand der Interessenabwägung in Art. 9 Abs. 2 DS-GVO einzuführen: Unten C.I.3.

[82] Ebenso *Schantz*, in: Simitis/Hornung/Spiecker gen. Döhmann (Hrsg.), Datenschutzrecht, 2019, Art. 6, Rn. 89.

Es wäre mit dem Grundrecht auf Schutz personenbezogener Daten nicht vereinbar, wenn dieselbe Datenverarbeitung nach einem Widerruf der Einwilligung stattdessen auf Grundlage der schlichten Interessenabwägung gemäß Art. 6 Abs. 1 lit. f DS-GVO *nahtlos* fortgesetzt werden könnte.[83] Die Anforderung, dass der Widerspruch gemäß Art. 21 Abs. 1 S. 1 DS-GVO – anders als der Widerruf gemäß Art. 7 Abs. 3 S. 1 DS-GVO – aus Gründen erfolgt, die sich aus der besonderen Situation des Datensubjekts ergeben, ist in diesem Fall – sofern er überhaupt ein Hindernis darstellt – entweder teleologisch zu reduzieren oder der Verantwortliche muss das Datensubjekt anlässlich des Einwilligungswiderrufs – erneut und qualifiziert – auf die Möglichkeit zum begründeten Widerspruch hinweisen.[84]

Für eine teleologische Reduktion der Begründungspflicht spricht, dass diese Vorrausetzung schon bei der vergleichsweise risikoarmen Datenverarbeitung für eine Direktwerbung des Verantwortlichen gemäß Art. 21 Abs. 2, Abs. 3 DS-GVO entfällt. Der Vergleich mit der Direktwerbung spricht dafür, dass die Begründungspflicht erst recht entfallen kann, wenn für eine Datenverarbeitung ursprünglich (auch) eine Einwilligung eingeholt wurde. Infolgedessen hat der Widerruf der Einwilligung regelmäßig auch Auswirkungen auf die Rechtmäßigkeit einer (fortgesetzten) Datenverarbeitung auf Grundlage von Art. 6 Abs. 1 lit. f i. V. m. Art. 21 Abs. 1 DS-GVO.

Sofern eine Verarbeitung gemäß Art. 6 Abs. 1 lit. a DS-GVO rechtmäßig war, diese Rechtmäßigkeit jedoch infolge eines Einwilligungswiderrufs entfällt, spricht dies dafür, dass eine anschließende zweckidentische Verarbeitung auf Grundlage von Art. 6 Abs. 1 lit. f DS-GVO nur möglich ist, sofern zwingend schutzwürdige Gründe gemäß Art. 21 Abs. 1 S. 2 DS-GVO überwiegen.[85]

Aus diesem systematischen Vergleich von Art. 7 Abs. 3 S. 1 und Art. 21 DS-GVO folgt zudem, dass der Verantwortliche nach Zugang des Einwilligungswiderrufs keine zeitliche Zäsur in dem Sinne vornehmen kann, dass er eine identische Datenverarbeitung zu einem identischen Zweck kurze Zeit nach dem Einwilligungswiderruf erneut beginnt, sich für die Zukunft nun aber auf ein (einfaches) berechtigtes Interesse an der Verarbeitung gemäß Art. 6 Abs. 1 lit. f DS-GVO beruft und in diesem Zusammenhang den erst kürzlich erfolgten Einwilligungswiderruf des Datensubjekts als abgeschlossenen Sachverhalt der Vergangenheit unberücksichtigt lässt. Nach einem durch den Verantwortlichen unbeanstandet gebliebenen oder sogar automatisch bestätigten Widerruf kann ein Datensubjekt unter Zugrundelegung eines vernünftigen Erwartungshori-

---

[83] *Robrahn/Bremert*, ZD 2018, 291 (296).

[84] Hierzu unten C.II. und zu den Folgen für die Gestaltung eines Kontroll-Cockpits: Kapitel 6 B.II.2.a.

[85] A. A. *Leistner/Antoine/Sagstetter*, Big Data, 2021, S. 270 (Es muss „ein gänzlich neuer Verarbeitungsprozess auf neuer Grundlage initiiert werden"). Hiergegen spricht der Wortlaut des Art. 6 Abs. 1 DS-GVO („mindestens") und des Art. 17 Abs. 1 lit. b a. E. DS-GVO.

zonts davon ausgehen, dass keine Fortsetzung dieser Datenverarbeitung – nunmehr auf Grundlage einer Interessenabwägung – möglich ist, ohne dass das Datensubjekt hierauf ausdrücklich hingewiesen wurde.

Allenfalls nach einem längeren Zeitraum oder nach dem ausdrücklichen und qualifizierten Hinweis gegenüber dem Datensubjekt, künftig auf Grundlage einer einfachen Interessenabwägung gemäß Art. 6 Abs. 1 lit. f DS-GVO Daten zu verarbeiten, kann eine solche Datenverarbeitung rechtmäßig sein.[86] Voraussetzung ist jedoch, dass diese qualifizierte Information dem Datensubjekt deutlich macht, dass diese Verarbeitung in Art, Umfang und Zweck derjenigen entspricht oder ähnelt, für die das Datensubjekt zuvor seine Einwilligung widerrufen hat.

Je großzügiger die einfache und qualifizierte Interessenabwägung ausgelegt und angewendet werden, desto seltener ist der Verantwortliche auf die Einwilligung des Datensubjekts angewiesen. Weil der Widerspruch gemäß Art. 21 Abs. 1 S. 1 DS-GVO aus Sicht der Datensubjekte aber nur einen *Opt-Out* ermöglicht, während Art. 6 Abs. 1 lit. a i. V. m. Art. 7 DS-GVO detaillierte Anforderungen an einen *Opt-In* formuliert, wird bereits an dieser Stelle deutlich, warum zwischen der Interessenabwägung und der Einwilligung ein Stufenverhältnis besteht und der Einwilligung als Ausdruck der informationellen Privatautonomie der Vorrang einzuräumen ist.[87]

B. Erleichterung der Datenverarbeitung durch eine Interessenabwägung

Der Erlaubnistatbestand des Art. 6 Abs. 1 lit. f DS-GVO verfügt im Vergleich zu den anderen Erlaubnistatbeständen über mehrere Mechanismen, die eine rechtmäßige Datenverarbeitung ermöglichen. Zunächst verschafft der offene Tatbestand der Interessenabwägung die notwendige Flexibilität, um rechtlich auf das rasant zunehmende Ausmaß und die ökonomischen und technologischen Entwicklungen der Datenverarbeitung reagieren zu können (I). Zudem bietet die Interessenabwägung eine Lösung an, sofern Daten potenziell einen multi-relationalen Personenbezug aufweisen. In diesem Fall kann die Einholung einer entsprechenden Vielzahl an Einwilligungen schwierig sein oder mit Blick auf den Zweck der Datenverarbeitung und die Risiken für die Datensubjekte aufgrund des damit verbundenen Aufwands unverhältnismäßig und deshalb unzumutbar sein (II).

[86] Zudem müsste dann inzident innerhalb von Art. 6 Abs. 1 lit. f. DS-GVO zusätzlich geprüft werden, ob die sonstigen Wirksamkeitsvoraussetzungen der – mittlerweile widerrufenen – Einwilligung ursprünglich vorlagen. So insbesondere für die Freiwilligkeit gemäß Art. 7 Abs. 4 DS-GVO: *Hacker*, Datenprivatrecht, 2020, S. 279.

[87] Unten: Kapitel 4 A.I. und Kapitel 5 A.

I. Erleichterung: Flexible Reaktion auf die ubiquitäre Datenverarbeitung

Die ökonomischen und technologischen Entwicklungen im Bereich der Datenverarbeitung machen es bereits seit mehreren Jahrzehnten erforderlich, auf die zunehmend ubiquitäre Datenverarbeitung rechtlich reagieren zu können.[88]

Bereits die Erfahrungen mit dem *BDSG* a. F. hatten zu der Einsicht geführt, dass die Kombination aus einem Verarbeitungsverbot und technischem Fortschritt immer wieder erneuten Reformbedarf auslöst, sobald sich neue technologische Möglichkeiten zur Datenverarbeitung entwickeln.[89] Um diesen Reformdruck zu reduzieren, entschied sich der deutsche Gesetzgeber, eine Interessenabwägung durch den Verantwortlichen als mögliche Rechtsgrundlage für eine Verarbeitung einzuführen.[90] Der europäische Gesetzgeber übernahm diesen Ansatz zunächst in Art. 7 lit. f der Datenschutz-RL (1995). Nunmehr bringt Art. 6 Abs. 1 lit. f DS-GVO diese angestrebte Technikneutralität[91] zum Ausdruck und bietet – für die Verarbeitung von personenbezogenen Daten[92] – einen entwicklungsoffenen Erlaubnistatbestand.[93] Je restriktiver die Voraussetzungen der Einwilligung künftig ausgelegt werden, desto wichtiger dürfte Art. 6 Abs. 1 lit. f DS-GVO als „Schrittmacher" für Datenverarbeitungen werden. Je häufiger Verantwortliche eine Datenverarbeitung auf Grundlage einer Interessenabwägung vornehmen, desto wichtiger wird es, dass zunächst die Judikative zeitnah klare Fallgruppen herausbildet und die Legislative diese mittel- und langfristig als Regelbeispiele oder als zusätzliche, spezifischere Erlaubnistatbestände in der DS-GVO kodifiziert.

Jedenfalls solange keine effektiven Assistenzsysteme für die Einwilligung verfügbar sind,[94] die detaillierte und scharf abgrenzbare Einwilligungen auf Grundlage der tatsächlichen Präferenzen des jeweiligen Datensubjekts ermöglichen, bleibt als Antwort auf die Kombination aus Verarbeitungsverbot und ubiquitärer Datenverarbeitung bisweilen nur ein Rückgriff auf die Interessenabwägung.[95]

---

[88] *Leistner/Antoine/Sagstetter*, Big Data, 2021, S. 199 ff.

[89] *Simitis*, Kommentar zum BDSG (2014), Einleitung, Rn. 92 („Regelungskonzept fehlte").

[90] Mit Kritik an diesem Ansatz: *Simitis*, Kommentar zum BDSG (2014), Einleitung, Rn. 141.

[91] ErwG 15 S. 1 DS-GVO. Mit Kritik an der Technologieneutralität: *Sydow/Krings*, ZD 2014, S. 271 ff.

[92] Dieser Schrittmacher fehlt der DS-GVO jedoch, soweit besonders sensible personenbezogene Daten verarbeitet werden: hierzu unten C.I.3.b. und c.

[93] *Albers/Veit*, in: Wolff/Brink (Hrsg.), BeckOK Datenschutzrecht, 36. Ed. 2020, Art. 6, Rn. 14.

[94] Hierzu der Vorschlag für ein Kontroll-Cockpit: Kapitel 6 B.

[95] Noch deutlicher in diese Richtung: *Leistner/Antoine/Sagstetter*, Big Data, 2021, S. 280 („relevanteste Verarbeitungsgrundlage").

II. Erleichterung: Reagibilität auf die Multi-Relationalität

Es existieren zahlreiche Konstellationen, in denen eine Datenverarbeitung eine Vielzahl von Datensubjekten betrifft. Ein wesentlicher Vorteil von Art. 6 Abs. 1 lit. f DS-GVO ist es, dass er im Unterschied zur Einwilligung (Art. 6 Abs. 1 lit. a DS-GVO) und zur vertragsakzessorischen Datenverarbeitung (Art. 6 Abs. 1 lit. b DS-GVO) eine Möglichkeit eröffnet, auch die Interessen von Datensubjekten zu berücksichtigen, für die eine solche Datenverarbeitung lediglich geringe Risiken birgt. Während von denjenigen Datensubjekten, deren Risiko erhöht ist, eine Einwilligung eingeholt werden muss, selbst wenn diese mit großem Aufwand verbunden ist, kann die Verarbeitung der Daten derjenigen Datensubjekte, die von der Datenverarbeitung lediglich am Rande tangiert werden, möglicherweise auf Grundlage einer Interessenabwägung rechtmäßig sein.

Wird beispielsweise der Fahrer eines Leasing-Fahrzeugs identifiziert und werden während der Nutzung des Fahrzeugs solche Daten verarbeitet, die Aussagen über das Verhalten des Fahrers ermöglichen, so ist diese Datenverarbeitung zwar entweder für die Erfüllung des Leasingvertrags erforderlich (Art. 6 Abs. 1 lit. b DS-GVO) oder – soweit die Verarbeitung darüber hinausgeht[96] – von einer Einwilligung des Fahrers abhängig. Soweit das Fahrzeug jedoch zusätzlich Daten erfasst, beispielsweise über die jeweilige Nutzung des Infotainment-Systems durch die Fahrzeuginsassen oder mittels eingearbeiteten Sensoren, einschließlich Innenraumkamera,[97] welche die Insassen erfassen, können auch diese Daten personenbezogene Daten sein, sofern der Verantwortliche beispielsweise über die Möglichkeit verfügt, diese Daten über Schnittstellen mit dem Smartphone der Insassen oder als einzelne Familienmitglieder des Fahrers zu identifizieren. Solange diese Daten über die sonstigen Insassen jedoch nicht gezielt kommerziell und mittels Profiling ausgewertet werden, kann für deren periphere und lokal begrenzte Verarbeitung durch die Kfz-Software und für Zwecke der Fahrsicherheit eine Rechtfertigung gemäß Art. 6 Abs. 1 lit. f DS-GVO ausreichend sein.

Ein weiteres Beispiel sind sog. Assistenzsysteme oder anderweitige Anwendungsfälle des IoT. Sofern beispielsweise *Alexa* (Alphabet) oder *Echo* (Amazon) kurze Sprachsequenzen von Dritten – beispielweise Gästen oder Nachbarn – verarbeiten, um dadurch ausschließlich sicherzustellen, dass nur die Sprachbefehle der jeweiligen Kunden und Vertragspartner aufgenommen, analysiert und ausgeführt werden, kann diese kurze Datenverarbeitung, die lediglich dazu dient, einen negativen Abgleich mit den Stimmen Dritter durchzuführen gemäß

---

[96] Hierzu unten Kapitel 3.

[97] *Smans*, Unter Beobachtung – Tesla-Autopilot: Innenraum-Kamera überwacht nun den Fahrer, Computerbild, 28.05.2021 (https://www.computerbild.de/artikel/cb-News-Connected-Car-Tesla-Autopilot-Innenraum-Kamera-ueberwacht-nun-den-Fahrer-30241287.html, zuletzt abgerufen am 19.05.2022).

Art. 6 Abs. 1 lit. f DS-GVO rechtmäßig sein,[98] sofern die Datenverarbeitung sich auf diesen Zweck („Verifizierung der Nutzungsberechtigung") beschränkt.[99]

C. Herausforderungen einer Datenverarbeitung auf Grundlage der Interessenabwägung

Neben dem Vorteil der Flexibilität und Entwicklungsoffenheit einer Interessenabwägung teilt Art. 6 Abs. 1 lit. f DS-GVO einige Nachteile, die Generalklauseln typischerweise zu eigen sind. Eine Analyse von Art. 6 Abs. 1 lit. f DS-GVO legt ein Paradoxon offen. Obwohl Art. 6 Abs. 1 lit. f DS-GVO als Generalklausel einerseits eine Gefahr für die Rechtssicherheit bedeutet, ist der Anwendungsbereich der Interessenabwägung zugleich dennoch zu eng geraten (I). Eine wesentliche Herausforderung ist, dass sie vom Verantwortlichen strategisch als Erlaubnistatbestand herangezogen werden kann, um die detaillierteren und aufwendigeren Voraussetzungen einer Einwilligung zu vermeiden (II). Weil es sich bei der Interessenabwägung im Ausgangspunkt lediglich um einen internen Prozess des Verantwortlichen handelt, besteht zudem die Befürchtung, dass die behördliche und gerichtliche Kontrolldichte von Art. 6 Abs. 1 lit. f DS-GVO gering ausfällt (III).

I. Herausforderung: Paradoxon aus Unsicherheit und geringer Flexibilität

Mit der doppelten Interessenabwägung in Art. 6 Abs. 1 lit. f und Art. 21 Abs. 1 S. 2 DS-GVO räumt der europäische Gesetzgeber der Judikative große Gestaltungsfreiheit ein, delegiert aber auch ganz wesentliche Entscheidungen über das Niveau des europäischen Datenschutzes im Privatrechtsverhältnis an die Gerichte, ohne diesen Leitlinien mit auf den Weg zu geben. Infolgedessen hat der europäische Gesetzgeber sein mit Art. 6 Abs. 1 lit. f DS-GVO verfolgtes Ziel teilweise verfehlt. Es besteht die Gefahr, dass die Anwendung von Art. 6 Abs. 1 lit. f und Art. 21 Abs. 1 S. 2 DS-GVO durch die nationalen Gerichte in einem Flickenteppich endet, für Verantwortliche und Datensubjekte kaum vorherseh-

[98] Sofern der Abgleich lediglich in negativer Hinsicht („Dies ist nicht die Stimme/das Gesicht des berechtigten Endnutzers") auf dem Endgerät selbst vorgenommen wird, handelt es sich gegebenenfalls nicht um ein personenbezogenes Datum, soweit der Anbieter – im Sinne von *Breyer* (*EuGH*, Urt. v. 19.10.2016, C-582/14 = NJW 2017, 2416, Rn. 26/49) keinerlei Möglichkeit hat, auf diese Daten anderweitig zuzugreifen und diese mit einer Datenbank der Stimmen/Gesichter aller seiner Kunden oder sogar mit Datenbanken Dritter abzugleichen.

[99] Hierzu detailliert und zu den Herausforderungen, sofern besonders sensible personenbezogene Daten verarbeitet werden: unten C.I.3.b.

bar ist und dabei zugleich das Ziel eines freien Verkehrs personenbezogener Daten im Binnenmarkt gefährdet (1).

Obwohl gerade die Unbestimmtheit der Interessenabwägung eine wesentliche Herausforderung für die Anwendung des Erlaubnistatbestands ist und Anlass zur Kritik gibt, ist Art. 6 Abs. 1 lit. f DS-GVO mit Blick auf den einzigen explizit erwähnten Anwendungsfall der Direktwerbung wiederum potenziell zu weit geraten (2).

Zudem besteht das Paradoxon, dass der Anwendungsbereich der Interessenabwägung insgesamt zu eng ausgestaltet wurde. Es wird zunehmend deutlich, dass auch für die Verarbeitungen von besonders sensiblen personenbezogenen Daten ein Rückgriff auf eine (qualifizierte) Interessenabwägung erforderlich ist. Daraus folgt die Notwendigkeit, den Erlaubnistatbestand der Interessenabwägung nicht nur durch Regelbeispiele zu konkretisieren, sondern seinen Anwendungsbereich *de lege ferenda* zu erweitern, um seine Funktion als Schrittmacher zu nutzen (3).

1. Fehlende Konkretisierung der Interessenabwägung

Die wesentlichen Vorzüge von Generalklauseln sind bekannt und unbestritten.[100] Sie liegen in deren Flexibilität, indem sie der Judikative eine Möglichkeit zum interessengerechten Ausgleich im Einzelfall eröffnen. Die Kehrseite der Einzelfallgerechtigkeit ist eine gewisse, im Idealfall jedoch lediglich vorübergehende Rechtsunsicherheit. Diese Rechtsunsicherheit lässt sich jedoch von Anfang an reduzieren, sofern eine Generalklausel durch Regelbeispiele ergänzt wird.

Weil der europäische Gesetzgeber Art. 6 Abs. 1 lit. f DS-GVO weder durch Regelbeispiele noch konkretisierende Kriterien flankiert hat, handelt sich um eine missglückte Vorschrift, die jedenfalls im Vergleich zum BDSG a. F. einen Rückschritt bedeutet (a). Noch schwerer als dieser Rückschritt wiegt jedoch, dass sich die Vorteile, die mit einer Generalklausel grundsätzlich einhergehen, im europäischen Mehrebenensystem aus nationalen Gerichten und *EuGH* weniger effektiv entfalten können (b). Zudem ist es zweifelhaft, ob die Datenschutzbehörden und damit letztlich der Europäische Datenschutzausschuss (EDSA) interimistische Lösungen entwickeln und anbieten können, um ein Mindestmaß an einheitlicher Rechtsanwendung in der Union sicherzustellen (c).

---

[100] Grundlegend: *Beater*, AcP 194 (1994), S. 82 ff.; *Ohly*, Richterrecht und Generalklausel im Recht des unlauteren Wettbewerbs, 1997; *Auer*, Materialisierung, Flexibilisierung, Richterfreiheit. Generalklauseln im Spiegel der Antinomien des Privatrechtsdenkens, 2005.

a) Art. 6 Abs. 1 lit. f DS-GVO als missglückte Generalklausel

Die Vorteile einer Generalklausel überkompensieren deren Nachteile, solange eine detaillierte gesetzliche Regelung scheitert, weil die tatsächlichen Entwicklungen noch zu vage und/oder die Interessen im Einzelfall zu diffus sind, so dass der Gesetzgeber sie nicht eindeutig bewerten und bestimmten Interessen typisiert den Vorrang einräumen kann. Allerdings muss für diese Flexibilität der Preis einer gewissen Rechtsunsicherheit gezahlt werden. Mit Blick auf Art. 6 Abs. 1 lit. f DS-GVO ist dieser Preis ungewöhnlich und unnötig hoch ausgefallen.

Die Möglichkeit, eine Generalklausel mit Hilfe von Regelbeispielen zu konkretisieren und durch schwarze, graue und gegebenenfalls sogar weiße Listen zu flankieren,[101] ist mittlerweile keine gesetzgeberische Innovation mehr. Mittels solcher Listen hätte der Gesetzgeber diejenigen Sachverhalte erfassen können, die auf Grundlage einer Interessenabwägung nicht gerechtfertigt werden können (schwarze Liste),[102] solche Datenverarbeitungen, die – zumindest typischerweise – im Rahmen einer Interessenabwägung rechtmäßig sind (weiße Liste) und solche Sachverhalte, für die Art. 6 Abs. 1 lit. f DS-GVO zwar als Grundlage in Betracht kommt, die jedoch stets einer detaillierten Abwägung der beteiligten Interessen im Einzelfall bedürfen (graue Liste). Die Notwendigkeit solcher Konkretisierungen besteht insbesondere deshalb, weil die Anwendung des Art. 6 Abs. 1 lit. f DS-GVO zunächst dezentral durch die jeweils zuständigen Datenschutzbehörden und durch hunderte mitgliedstaatliche Gerichte erfolgt. Leider ist der europäische Gesetzgeber mit Art. 6 Abs. 1 lit. f DS-GVO von dieser – beispielsweise im Lauterkeits- und Kartellrecht erfolgreich erprobten[103] – arbeits-

---

[101] Ebenfalls mit diesem Gedanken– allerdings in Bezug auf besonderes unangemessene Vertragsklauseln für eine spezielle AGB-Kontrolle: *Wendehorst*, in: Lohsse/Schulze/Staudenmayer (Hrsg.), Data as Counter-Performance – Contract Law 2.0?, 2020, S. 193 (219); *Hacker*, Datenprivatrecht, 2020, S. 285 f.

[102] Hierfür existieren bereits potenzielle Datenverarbeitungsprozesse, die jedoch ebenfalls das Konfliktpotential im Einzelfall aufzeigen: Dazu zählt die *Policy and Research Group of the Office of the Privacy Commissioner of Canada*, das Abspeichern und Abgleichen von Fingerabdrücken, ohne ausdrückliche Information des Datensubjekts; das Tracking von Minderjährigen und die Nutzung von genetischen Analyseergebnisse für nicht-medizinische Dienstleistungen: *Policy and Research Group of the Office of the Privacy Commissioner of Canada*, Consent and privacy – A discussion paper exploring potential enhancements to consent under the Personal Information Protection and Electronic Documents Act, 2016, S. 17. Hierzu auch *Hacker*, Datenprivatrecht, 2020, S. 286.

[103] Vgl. Anhang I der RL 2005/29/EG v. 11.05.2005 über unlautere Geschäftspraktiken im binnenmarktinternen Geschäftsverkehr zwischen Unternehmen und Verbrauchern (UGP-RL), ABl. v. 11.06.2005, L 149/22 (S. 35) sowie deren Erweiterung durch Art. 3 Nr. 7 der RL (EU) 2019/2161 v. 27.11.2019 zur besseren Durchsetzung und Modernisierung der Verbraucherschutzvorschriften der Union („Fair Deal for Consumers-RL"), ABl. v. 18.12.2019, L 328, S. 7 (21); beide umgesetzt im Anhang zu § 3 Abs. 3 UWG als stets unzulässige Handlungen (sog. schwarze Liste); sowie VO (EU) 2022/720 v. 10.05.2022 über die Anwendung des

teiligen Vorgehensweise zwischen Legislative und Judikative abgewichen,[104] obwohl beispielsweise die in Deutschland bereits zuvor stärker ausdifferenzierten Fallgruppen[105] als ein Anhaltspunkt zur Verfügung gestanden hätten. Infolgedessen fallen diese in Deutschland bereits erreichten Konkretisierungen wieder in den allgemeinen Anwendungsbereich der Generalklausel zurück.

Leider unterlag die *EU-Kommission* der Fehleinschätzung, derartige Konkretisierung zu einem späteren Zeitpunkt selbst vornehmen zu können.[106] Trotz vorhandener Erfahrungen mit der Vorgänger-Vorschrift in Art. 7 lit. f Datenschutz-RL (1995) verfolgte die *EU-Kommission* den Plan, zunächst erste Erfahrungen mit der DS-GVO zu sammeln und Art. 6 Abs. 1 lit. f DS-GVO anschließend selbst mit Hilfe von delegierten Rechtsakten zu konkretisieren.[107] Dieses Vorgehen ist konzeptionell plausibel. Allerdings wären dadurch wesentliche Regelungen der DS-GVO erst nachträglich und außerhalb des ordentlichen Gesetzgebungsverfahrens bestimmt worden. Aus diesem Grund lehnte das *EU-Parlament* diesen Vorschlag ab.

Tatsächlich lässt sich dieser Vorschlag der *EU-Kommission* wegen einer „undemokratische[n], zentralistische[n] Note" kritisieren.[108] Allerdings ist es dem *EU-Parlament* anschließend ebenfalls nicht gelungen, den Tatbestand der Interessenabwägung inhaltlich zu konkretisieren,[109] obwohl Art. 6 Abs. 1 lit. f DS-GVO nach h. A. weiterhin als zentraler Erlaubnisgrund für die Datenverarbeitung durch Private fungieren soll.[110] Infolgedessen fällt diese Rolle nun den jeweils berufenen Institutionen der 27 Mitgliedstaaten zu. Diesen stehen dafür einstweilen kaum Kriterien zur Verfügung,[111] sie müssen aber dennoch über die Zulässigkeit zahlreicher Geschäftsmodelle entscheiden.[112]

Art. 101 Abs. 3 des AEUV auf Gruppen von vertikalen Vereinbarungen und abgestimmten Verhaltensweisen, ABl. 2022 L 134, S. 4 ff.

[104] Zur richterrechtlichen Ausdifferenzierung und anschließenden gesetzlichen Übernahme von Fallgruppen auf Grundlage der lauterkeitsrechtlichen Generalklausel: *Ohly/Sattler*, GRUR 2016, 1229 (1234 f.).

[105] §§ 28, 28a, 30a BDSG a. F. enthielten spezifischere Tatbestände für die Interessenabwägung als Art. 6 Abs. 1 lit. f DS-GVO. Hierzu: *Buchner/Petri*, in: Kühling/Buchner (Hrsg.), DS-GVO/BDSG, 3. Aufl. 2020, Art. 6, Rn. 145.

[106] *Frenzel*, in: Paal/Pauly (Hrsg.), DS-GVO, 2021, Art. 6, Rn. 26.

[107] Vgl. Art. 6 Abs. 5 i. V. m. Art. 86 Abs. 1 des Vorschlags der EU-Kommission für die DS-GVO v. 25.01.2012, DOK. KOM(2012) 11 endgültig.

[108] *Roßnagel/Nebel/Richter*, ZD 2015, 455 (460); in diese Richtung auch: *Schild/Tinnefeld*, DuD 2012, 312 (316 f.).

[109] *Albrecht*, CR 2016, 88 (92).

[110] M.w.N. *Leistner/Antoine/Sagstetter*, Big Data, 2020, S. 280.

[111] Mit Kritik an der fehlenden Konkretisierung: *Marsch*, Das Europäische Datenschutzgrundrecht, 2018, S. 267/372.

[112] Die Regelung enthält abgesehen von der Direktwerbung (Art. 21 Abs. 2 DS-GVO) und der Privilegierung der Rechtsverfolgung (Art. 21 Abs. 1 S. 2 DS-GVO) keine rechtlichen Anhaltspunkte, unterstellt den Beurteilungsspielraum des Verantwortlichen aber vollständig der gerichtlichen Überprüfung. Hierzu *Dammann*, ZD 2016, 307 (312).

b) Nachteile einer Typisierung durch Richterrecht

Als Konsequenz des missglückten Gesetzgebungsverfahrens muss der *EuGH* versuchen, die unionsweite Einheitlichkeit der Auslegung von Art. 6 Abs. 1 lit. f DS-GVO sicherzustellen. Hierfür ist der *EuGH* auf vorlagefreudige nationale Gerichte angewiesen; nur dann hat er überhaupt die Möglichkeit, harmonisierend auf die nationale Anwendung dieses Auffangtatbestands einzuwirken. Allerdings dürfte der *EuGH* mit dieser Aufgabe gerade dann schnell überfordert sein, wenn die nationalen Gerichte von Art. 267 AEUV rege Gebrauch machen.[113]

Selbst wenn der *EuGH* die Gefahr erkennen sollte, die von Art. 6 Abs. 1 lit. f DS-GVO für die unionsweite Einheitlichkeit der Auslegung und Anwendung des Datenschutzrechts im Verhältnis zwischen Privatrechtsubjekten ausgeht, sind seine Möglichkeiten unionsgrundrechtlich und institutionell beschränkt. Aus unionsgrundrechtlicher Perspektive lässt sich aus Art. 8 GRCh wenig für die konkrete Interessenabwägung gewinnen. Der ohnehin weite Ausgestaltungsspielraum gemäß Art. 8 Abs. 2 GRCh bietet keine Maßstäbe für die konkretisierende Auslegung von Art. 6 Abs. 1 lit. f DS-GVO.[114] Die Interessen privater Verantwortlicher entziehen sich eben nicht nur

> „einer abstrakten ex-ante-Beurteilung [durch den Gesetzgeber], da [private Verantwortliche] keine ihnen zugewiesenen Aufgaben erfüllen, sondern ihre grundrechtlich geschützte Freiheit betätigen".[115]

Vielmehr bleibt diese Lückenhaftigkeit auf der primär- und sekundärrechtlichen Ebene auch für die gerichtliche Anwendung im Einzelfall folgenschwer.

Weil der europäische Gesetzgeber die DS-GVO nicht genutzt hat, um bereichsspezifische und ausdifferenzierte Typisierungen zu entwickeln, stehen infolgedessen auch der Judikative einstweilen kaum Kriterien für die Anwendung von Art. 6 Abs. 1 lit. f DS-GVO zur Verfügung. Dennoch müssen die Gerichte im Rahmen von Interessenabwägungen *ex post* über die Zulässigkeit zahlreicher Geschäftsmodellen entscheiden, die – zumindest teilweise – auf der Verarbeitung von personenbezogenen Daten basieren.

Erschwerend kommt hinzu, dass das Verfahren gemäß Art. 267 AEUV aus institutioneller Perspektive kaum für eine einheitliche und unionsweite Herausbildung von Fallgruppen geeignet ist. Der *EuGH* kann allenfalls Fragen zur unions(grund)rechtskonformen Auslegung und auch diese regelmäßig nur abstrakt beantworten. Zwar ist eine klare Abgrenzung zwischen der Auslegung des Sekundärrechts – gegebenenfalls unter Heranziehung der europäischen

---

[113] Mit dem Hinweis, dass der EuGH durch diese Aufgabe hoffnungslos überlastet würde, sofern die mitgliedstaatlichen Gerichte die Vorlagepflicht des Art. 267 Abs. 3 AEUV in Gestalt der CILFIT-Rechtsprechung ernst nehmen: *Masing*, JZ 2015, 477 (484).

[114] *Kühling*, DV 40 (2007), 153 (166); *Klement*, JZ 2017, 161 (162).

[115] *Marsch*, Das Europäische Datenschutzgrundrecht, 2018, S. 266.

Grundrechte – und dessen Anwendung im Einzelfall schwierig. Der *EuGH* könnte deshalb zumindest indirekt zur Fallgruppenbildung im Rahmen von Art. 6 Abs. 1 lit. f DS-GVO beitragen. Allerdings ist noch offen, ob bzw. inwieweit der *EuGH* bereit und gewillt ist, diese Aufgabe zur Konkretisierung wahrzunehmen,[116] obwohl der europäische Gesetzgeber ihm wissentlich kaum Wertungskriterien zur Verfügung gestellt hat.

Darüber hinaus erschweren die dem Vorlageverfahren intrinsischen Beschränkungen eine Typisierung, die über das jeweilige Vorlageverfahren hinaus Geltung beanspruchen kann. Die konkrete Sachentscheidung muss der *EuGH* regelmäßig dem vorlegenden Gericht überlassen. So hat der *EuGH* beispielsweise dem vorlegenden *OLG Düsseldorf* in *Fashion-ID* die wesentliche Entscheidung darüber überlassen, welcher Erlaubnistatbestand anzuwenden ist,[117] obwohl der Sachverhalt gut aufbereitet worden war. Mit Beschluss vom 24.03. 2021 hat – nun der Kartellsenat des *OLG Düsseldorf* – einen erneuten Versuch gestartet, um den *EuGH* zumindest inzident zu einer Konkretisierung des Art. 6 Abs. 1 lit. f DS-GVO zu veranlassen.[118] Sieht auch der *EuGH* sich nicht in der Lage, eine unionsweit einheitliche Konkretisierung vorzunehmen, so müssen die nationalen Gerichte anhand einer sehr abstrakten Interessenabwägung über die Rechtmäßigkeit aktueller Geschäftsmodelle entscheiden.

Anhand eines Beschlusses des *VGH München*,[119] der noch zum BDSG a. F. erging, lassen sich die potenziellen Folgen illustrieren. Dem Beschluss liegt ein Beschwerdeantrag eines Online-Händlers gegen den Beschluss des *VG Bayreuth* zugrunde, in dem letzteres die sofortige Vollziehung einer Anordnung des *Bayerischen Landesamts für Datenschutzaufsicht* bestätigt hat, wonach der Online-Händler binnen zwei Wochen nach Zustellung des Bescheids die unter seinem *Facebook*-Konto im Rahmen von „*Facebook Custom Audiences*" erstellten personenbezogenen (Kunden-)Daten zu löschen hat.

Die Dienstleistung „*Custom Audience*" von *Facebook* ermöglicht es Unternehmen, ihre Kunden (auch) innerhalb der Kommunikationsnetzwerke von *Facebook* gezielt zu bewerben. Um abzugleichen, ob der zu bewerbende Kunde des Unternehmens zugleich Nutzer der Kommunikationsnetzwerke von *Facebook* ist, gleicht *Facebook* die jeweiligen E-Mail-Adressen der jeweiligen Kun-

---

[116] Noch zurückhaltend: *EuGH*, Urt. v. 20.05.2003, verb. C-465/00 u. a. (Rn. 84 ff.) – *Österreichischer Rundfunk*; *EuGH*, Urt. v. 06.11.2003, C-101/01 = EuZW 2004, 245 (Rn. 85 ff.) – *Lindqvist*. Dagegen mit abschließender Interessenabwägung: *EuGH*, Rs. C-131/12 = NJW 2014, 2257 – *Google Spain*; hierzu: *Marsch*, Das Europäische Datenschutzgrundrecht, 2018, S. 368 („Es ist jedoch schon aus Gründen knapper Ressourcen davon auszugehen, dass der EuGH nicht zu jeder Konstellation einer Interessenabwägung im Datenschutzrecht Stellung nehmen wird").

[117] *EuGH*, Urt. v. 29.06.2019, C-40/17 = GRUR 2019, 958 (Rn. 90 f.).

[118] Vorlagefrage 4 des *OLG Düsseldorf*, Vorlagebeschl. v. 24.03.2021, Kart 2/19 (V) = GRURRS 2021 8370 (Rn. 54 ff.).

[119] *VGH München*, Beschl. v. 26.09.2018 – 5 CS 18.1157 = NVwZ 2019, 171 ff.

den ab (sog. Überschneidungsanalyse). Die im Anschluss hieran erstellten Kundenlisten (Custom Audience), ggfs. einschließlich persönlicher Präferenzen und Kaufgewohnheiten der Kunden, sind Grundlage und Voraussetzung für die vertraglich vereinbarte, zielgerichtete Werbung durch *Facebook*.[120]

Mangels Einwilligung der Kunden in diese Datenverarbeitungen (E-Mail-Abgleich, Erstellung und Speicherung von Kundenlisten), kam als Rechtsgrundlage lediglich eine Interessenabwägung gemäß § 28 Abs. 1 S. 1 Nr. 2 BDSG a. F. in Betracht. Obwohl die Begründung der Löschungsanordnung und deren Bestätigung durch das *VG Bayreuth* und durch den *VGH München* im Ergebnis überzeugen, hat es sich der *VGH München* in seiner Begründung sehr leicht gemacht. Ohne die Interessen der Beteiligten auszuarbeiten, die Erforderlichkeit der Datenverarbeitung zur Erreichung dieser Interessen zu beurteilen und ohne eine echte Abwägung vorzunehmen, entschied letztlich das in § 28 Abs. 1 Nr. 1 BDSG a. F. noch enthaltene unbestimmte und wertende Adjektiv darüber, dass die „*schutzwürdigen* Interessen" der Datensubjekte in der Abwägung gegenüber den bloßen „Interessen" der Verantwortlichen überwiegen.[121]

Der Beschluss verdeutlicht die Gefahren, die von dem unbestimmten Tatbestand des Art. 6 Abs. 1 lit. f DS-GVO ausgehen, weil er den jeweiligen nationalen Gerichten keine Leitlinien an die Hand gibt. Ein rechtssicherer freier Verkehr personenbezogener Daten im europäischen Binnenmarkt i. S. d. Art. 1 Abs. 3 DS-GVO lässt sich auf diesem Weg nicht verwirklichen.

c) Interimistische Maßnahmen zur Konkretisierung

Weil eine künftige Ausdifferenzierung der Interessenabwägung durch den europäischen Gesetzgeber ungewiss und eine verlässliche Typisierung durch die Judikative allenfalls mittel- bis langfristig zu erwarten ist, rücken zwei Möglichkeiten für eine zwischenzeitliche Konkretisierung der Interessenabwägung in den Fokus.

Erstens könnte der Europäische Datenschutzausschuss (*EDSA*) gemäß Art. 70 Abs. 1 S. 2 lit. e DS-GVO Leitlinien verabschieden, die Kriterien und Anhaltspunkte für die Auslegung von Art. 6 Abs. 1 lit. f DS-GVO enthalten. Diese würden immerhin einen offiziellen Standpunkt und damit eine Orientierungshilfe bieten.[122] Allerdings führen auch die institutionellen und personellen Rahmenbedingungen des *EDSA*, die demjenigen des Europäischen Datenschutzbeauftragten (EDSB) ähneln, zu einer Unwucht zugunsten einer kontinuierlichen Stärkung des Datenschutzes. Die privatrechtliche Perspektive und das (volks)wirt-

---

[120] *VGH München*, Beschl. v. 26.09.2018 – 5 CS 18.1157 = NVwZ 2019, 171 (Rn. 19).

[121] *VGH München*, Beschl. v. 26.09.2018 – 5 CS 18.1157, (Rn. 32) = NVwZ 2019, 171 (Rn. 27).

[122] *Hacker*, Datenprivatrecht, 2020, S. 286; *Buchner/Petri*, in: Kühling/Buchner (Hrsg.), DS-GVO/BDSG, 3. Aufl. 2020, Art. 6, Rn. 145.

schaftliche Allgemeininteresse kommen in den Stellungnahmen des *EDSA* regelmäßig zu kurz. Gleichzeitig offenbaren die bereits verabschiedeten Leitlinien zur Einwilligung[123] und zur Datenverarbeitung auf Grundlage von Art. 6 Abs. 1 lit. b DS-GVO[124] eine Tendenz des *EDSA*, die besonders umstrittenen Datenverarbeitungsprozesse durch *GAFAM* in den verwendeten Beispielen nicht zu erwähnen. Aus privatrechtlicher Perspektive ist jedenfalls zu hoffen, dass die Judikative sich die bisherigen – nicht verbindlichen – Leitlinien des *EDSA* nicht, oder allenfalls nach einer kritischen Analyse argumentativ zu eigen macht.[125]

Zweitens besteht eine Möglichkeit, die Auslegung und Anwendung dieses Erlaubnistatbestands mit Hilfe von Verhaltensregeln zu konkretisieren. Die Datenverarbeitung auf Grundlage einer Interessenabwägung ist zunächst eine Entscheidung des jeweiligen Verantwortlichen. Deshalb könnten solche Verhaltensregeln durchaus zu einer Konkretisierung führen, sofern sich eine große Zahl von Verantwortlichen zur Einhaltung solcher Verhaltensregeln verpflichtet. Gemäß Art. 40 Abs. 2 lit. b DS-GVO können Vereinigungen, die Verantwortliche repräsentieren, Verhaltensregeln ausarbeiten, mit denen die berechtigten Interessen des Verantwortlichen in bestimmten Zusammenhängen präzisiert werden. Anschließend wird der Entwurf der Verhaltensregeln den gemäß Art. 55 DS-GVO zuständigen nationalen Aufsichtsbehörde (Art. 40 Abs. 5 DS-GVO) zur Stellungnahme und Genehmigung vorgelegt. Hat der Entwurf von Verhaltensregeln Bedeutung für den freien Verkehr von personenbezogenen Daten im Binnenmarkt, so legt die nationale Aufsichtsbehörde diesen wiederum dem *EDSA* (Art. 40 Abs. 7 DS-GVO) zur Stellungnahme vor. Hält der *EDSA* den Entwurf für mit der DS-GVO vereinbar, so übermittelt er ihn an die *EU-Kommission*. Letztere kann Verfahren zur Verabschiedung von Durchführungsrechtsakten beschließen, so dass die ihr übermittelten und genehmigten Verhaltensregeln in der Union allgemein gültig werden.

Dieses Verfahren aus sektorspezifischen Verhaltensregeln durch freiwillige Selbstverpflichtung bietet eine theoretische Möglichkeit, zumindest zu konkretisieren, welche Interessen des Verantwortlichen sich im Rahmen einer Interessenabwägung typischerweise durchsetzen. Dennoch sind die Erfolgsaussichten dieser Option – abgesehen vom damit verbundenen Aufwand – aus drei Gründen gering.[126]

Erstens können in solchen Verhaltensregeln allenfalls die berechtigten Interessen des Verantwortlichen und damit nur die eine Seite der Interessenabwä-

---

[123] *EDSA*, Leitlinien 05/2020 zur Einwilligung gemäß Verordnung 2016/679, v. 04.05.2020.

[124] *EDSA*, Leitlinien 2/2019 für die Verarbeitung personenbezogener Daten gemäß Artikel 6 Absatz 1 Buchstabe b DSGVO im Zusammenhang mit der Erbringung von Online-Diensten für betroffene Personen, v. 08.10.2019.

[125] Ebenfalls kritisch: *Leistner/Antoine/Sagstetter*, Big Data, 2021, S. 401 („nicht stets in jeder Hinsicht ausgewogener Vorgaben").

[126] A. A. *Bergt*, CR 2016, 670 (671); *Schweitzer/Peitz*, in: Körber/Kühling (Hrsg.), Regulierung-Wettbewerb-Innovation, 2017, S. 282 f.; *Leistner/Antoine/Sagsteter*, Big Data, 2021, S. 280.

gung aus Art. 6 Abs. 1 lit. f DS-GVO konkretisiert werden. Daraus lassen sich noch keine typisierten Abwägungen ableiten.

Zweitens besteht die Gefahr, dass die berufenen nationalen Aufsichtsbehörden und der *EDSA* ihre Aufgabe primär als Wahrer des Regelungsziels aus Art. 1 Abs. 2 DS-GVO (Schutzes des Grundrechts gem. Art. 8 GRCh) interpretieren. Der freie Verkehr personenbezogener Daten im Binnenmarkt (Art. 1 Abs. 3 DS-GVO) wird von diesen Institutionen zwar als Konsequenz eines einheitlich hohen Schutzes akzeptiert, aber nicht als eigenständiges Ziel gefördert, obwohl die Kompetenz für die Verabschiedung der DS-GVO maßgeblich aus dem Binnenmarkt abgeleitet wurde, Art. 16 Abs. 2 S. 1 AEUV. Der institutionelle und personelle Rahmen und das bisherige Selbstverständnis vieler Datenschutzbehörden legen nahe, dass die auf Grundlage von Art. 40 Abs. 2 lit. b DS-GVO für bestimmte Situationen und Sektoren genehmigungsfähigen berechtigten Interessen jedenfalls nicht einmal im Ansatz in die Nähe dessen gelangen, was die Verantwortlichen darunter verstehen. Sofern Verhaltensregeln also tatsächlich genehmigt werden, werden sich allenfalls solche Verantwortlichen zu deren Einhaltung verpflichten, deren Geschäftsmodell bislang und künftig nicht maßgeblich von einer Verarbeitung personenbezogener Daten abhängt. Je geringer die Anzahl der selbstverpflichteten Verantwortlichen ist, desto geringer ist die harmonisierende Wirkung solcher Verhaltensregeln. Sofern Datenschutzbehörden und Gerichte diese Verhaltensregeln unmittelbar oder mittelbar auch gegenüber solchen Verantwortlichen heranziehen, die keine Selbstverpflichtung abgegeben haben, würde das Instrument der selbstverpflichtenden Verhaltensregeln *ad absurdum* geführt.

Drittens hängt eine echte, unionsweite Konkretisierung der Interessenabwägung in bestimmten Sektoren letztlich davon ab, dass die *EU-Kommission* von ihrem Ermessen gemäß Art. 40 Abs. 9 DS-GVO wirklich Gebrauch macht und diese Verhaltensregeln für verbindlich erklärt.[127] Der Vorschlag der *EU-Kommission*, personenbezogene Daten in der DID-RL ausdrücklich als Gegenleistung anzuerkennen und die Reaktion des *EDSB* hierauf lassen jedoch vermuten, dass auch die Vorstellungen über solche Verhaltensregeln sehr weit auseinanderliegen. Es ist unrealistisch, dass die *EU-Kommission* solche Verhaltensregeln für verbindlich erklärt, die auch der *EDSA* für gut befunden hat.

2. Restriktive Anwendung für personalisierte Direktwerbung

Besonders wichtig und aktuell zugleich sehr umstritten ist die Anwendung der Interessenabwägung für personalisierte Direktwerbung. Nach einer kurzen Erläuterung der wesentlichen technischen Grundlagen der automatisierten perso-

[127] Insoweit optimistisch: *Schweitzer/Peitz*, Datenmärkte in der digitalisierten Wirtschaft: Funktionsdefizite und Regelungsbedarf, ZEW Discussion Paper No. 17–043, 2017, S. 43; *Buchner/Petri*, in: Kühling/Buchner (Hrsg.), DS-GVO, 3. Aufl. 2020, Art. 6, Rn. 145.

nalisierten Direktwerbung (a), wird begründet, warum der Begriff der Direktwerbung in der DS-GVO restriktiv ausgelegt werden sollte (b).

a) Technische Grundlagen automatisierter personalisierter Werbung

Die automatisierte Personalisierung von Werbung beruht auf einer softwarebasierten Analyse des möglichst umfassend beobachtbaren Verhaltens von Datensubjekten. Je umfangreicher und ausdifferenzierter die über ein Datensubjekt erhobenen Daten sind, desto granularer ist das Persönlichkeitsbild, das mit Hilfe der Datenanalyse erstellt und anschließend für eine möglichst interessen- und bedürfnisspezifische Werbeansprache genutzt werden kann.

Der Erfolg dieser Werbeansprache lässt sich unterschiedlich messen.[128] Je genauer eine interessen- und bedürfnisspezifische Werbeansprache gelingt, desto wahrscheinlicher ist es, dass die Werbung nicht nur durch das Datensubjekt wahrgenommen wird, sondern auch eine geschäftliche Transaktion zwischen Datensubjekt und werbendem Unternehmen zustande kommt. Je erfolgreicher ein Vermittler von personalisierter Werbung ist, desto höhere Preise kann er von den Werbekunden für seine Profile und das Ausspielen der personalisierten Werbung verlangen. Hierbei werden die Profile der Nutzer regelmäßig zur Grundlage einer sog. Echtzeit-Versteigerung von Werbeplätzen (sog. *real time bidding*) herangezogen. Infolgedessen bekommt der Besucher einer Webseite oder der Nutzer einer App die Werbung desjenigen Unternehmens angezeigt, das auf Grundlage des Profils den höchsten Preis für den digitalen Werbeplatz angeboten hat.[129]

Grundlage der automatisiert personalisierten bzw. stratifizierten (gruppenspezifischen) Werbeansprache ist somit immer ein Profiling. [130] Gemäß Art. 4 Nr. 4 DS-GVO ist dieses definiert als

„jede Art der automatisierten Verarbeitung personenbezogener Daten, die darin besteht, dass diese personenbezogenen Daten verwendet werden, um bestimmte persönliche

[128] Wichtig ist jedoch vor allem, dass dieser Erfolgsmessung ihrerseits regelmäßig unter erheblichen Informationsasymmetrien zwischen dem Werbenden und dem Anbieter der Werbeplattform leiden: *UK Competition and Marktes Authority* (CMA), Online platforms and digital advertising Market study final report, 1.7.2020, S. 297 ff. (https://assets.publishing.service.gov.uk/media/5fa557668fa8f5788db46efc/Final_report_Digital_ALT_TEXT.pdf, zuletzt abgerufen am 19.05.2022); *Cabral/Haucap/Parker/Petropoulos/Valletti/Van Alstyne*, The EU Digital Markets Act – A Report from a Panel of Economic Experts, 2021, S. 15; *Srinivasan*, 24 Stanford Technology Law Review, 2020, 55 ff.

[129] *Arning/Moos*, ZD 2014, 242 (242 f.).

[130] Für die Annahme des Personenbezugs reicht es jedoch schon aus, wenn eine Identifizierungsmöglichkeit auch nur abstrakt besteht, eine solche Identifikation hinreichend wahrscheinlich ist, selbst wenn diese erst durch Einbeziehung eines zur Mithilfe verpflichteten Dritten erfolgt: *EuGH*, Urt. v. 19.10.2016, C-582/14 = NJW 2017, 2416 (Rn. 26/49) – *Breyer*; mit ebenfalls weitem Verständnis: *GA Bobek*, Schlussanträge, v. 19.12.2018,C-40/17 (Rn. 58) – *FashionID*.

Aspekte, die sich auf eine natürliche Person beziehen, zu bewerten, insbesondere um Aspekte bezüglich Arbeitsleistung, wirtschaftliche Lage, Gesundheit, persönliche Vorlieben, Interessen, Zuverlässigkeit, Verhalten, Aufenthaltsort oder Ortswechsel dieser natürlichen Person zu analysieren oder vorherzusagen".

Um eine möglichst umfassende und aktuelle Datenbasis für das Profiling zu erhalten, werden personenbezogene Daten über das Verhalten von Datensubjekten erhoben. Um das Verhalten der Datensubjekte möglichst umfassend zu protokollieren (sog. *tracking*) wird versucht, die Grenzen von Webseiten (*cross domain*), von Endeinrichtungen wie Notebooks, Smartphones, Smartwatches oder Smart-Home-Geräten (*cross device*) und zwischen virtuellem und physischem Raum (*geo-tracking*) zu überwinden.

Besonders erfolgreich hierbei sind die mehrseitigen Plattformen von *GAFAM* und *BAT*, zumal diese – jedenfalls in der Vergangenheit – teilweise miteinander kooperierten und sich reziprok partielle Zugänge zu personenbezogenen Daten eröffneten.[131] Die Werkzeuge, die für ein *tracking* eingesetzt werden, können für das Datensubjekt sichtbar sein – beispielsweise das sog. *social plug-in* „Gefällt mir" von *Facebook* – oder schwer einsehbar sein – beispielsweise die jeweilige Werbe-ID von *Apple* oder *Google* (sog. *identifier for advertisers* – (IDFA). *Meta Platforms* (ehemals: *Facebook*) soll es gelungen sein, auf 75 % der 130 untersuchten deutschen Nachrichtenseiten das Nutzungsverhalten der Besucher dieser Webseiten zu beobachten,[132] für das eigene Profiling zu nutzen und im Rahmen seiner Angebote für Werbekunden (insbesondere im Rahmen von *Facebook Custom Audience*) zu verwerten.

Die Werkzeuge zur Verhaltensbeobachtung werden regelmäßig danach unterschieden, ob diese von demjenigen Verantwortlichen eingesetzt werden, mit dem das Datensubjekt ein primäres Nutzungsverhältnis eingegangen ist (*first party tracking*) – beispielsweise der Betreiber einer Nachrichten-Webseite oder der Anbieter einer App auf einer Endeinrichtung – oder durch ein Drittunter-

---

[131] Weil *Apple* sich entschlossen hat, vor einem solchen Tracking durch Dritte künftig die Datensubjekte um Einwilligung zu bitten, ist es zum öffentlichen Konflikt zwischen *Apple* und *Facebook* und zwischen *Apple* und der *Chinesischen Regierung* gekommen. Zudem mahnte die EU-Wettbewerbskommissarin *Apple* bereits davor, sich dadurch einen Wettbewerbsvorteil zu verschaffen, indem die eigene Datenerhebung unter anderen, leichtere Bedingungen – also insbesondere ohne getrennte Einwilligung – ermöglicht wird: *Der Standard,* EU-Kommission warnt Apple im Streit mit Facebook, 09.02.2021 (https://www.derstandard.de/story/2000123988050/eu-kommission-warnt-apple-im-streit-mit-facebook, zuletzt abgerufen am 19.05.2022). Das *BundesKartA* hat nach der Aufnahme von Ermittlungen gegen *Facebook* (Pressemitteilung v. 28.01.2021), gegen *Amazon* (Pressemitteilung v. 18.05.2021) und gegen *Google* (Pressemitteilung v. 25.05.2021) ein Verfahren zur Überprüfung einer marktübergreifenden Bedeutung von Apple für den Wettbewerb nach (§ 19a Abs. 1 GWB) eröffnet (Pressemeldung v. 21.06.2021).

[132] *Eberl*, Konzern liest mit: FB trackt Nutzer auf drei Viertel aller deutschen Nachrichtenseiten, 03.06.2019 (https://netzpolitik.org/2019/konzern-liest-mit-facebook-trackt-nutzer-auf-drei-viertel-aller-deutschen-nachrichtenseiten/, zuletzt abgerufen am 19.05.2022).

nehmen, mit dem kein direktes Nutzungsverhältnis besteht (*third party tracking*). Ein Beispiel für letzteres ist die Verhaltensbeobachtung unter Verwendung von sog. *social plug-ins*, obwohl der beobachtete Besucher der Webseite mit dem Anbieter des *social plug-ins* in keinem Vertragsverhältnis steht.[133] Bereits am Beispiel des „Gefällt mir"-Button von *Facebook* wird deutlich, dass die Übergänge zwischen *first-* und *third-party-tracking* tatsächlich fließend sind und aus Sicht der Anbieter einen Anreiz zur weiten Anwendung von Art. 6 Abs. 1 lit. f DS-GVO setzen.[134]

Die Werkzeuge, die für ein *tracking* eingesetzt werden können, sind sehr unterschiedlich. Hierzu gehören *Cookies*, also kleine eindeutig bestimmbare Textdateien, die auf einer Endeinrichtung gespeichert werden und dieses Gerät identifizieren, wenn über die Endeinrichtung eine Webseite aufgerufen wird. *Cookies* sind zugleich die Grundlage der *social plug-ins*. Auf dieser Grundlage können von den besuchten Webseiten Informationen über die Besucher der Webseite abgefragt werden, wie beispielsweise die IP-Adresse, der Zeitpunkt des Zugriffs auf die Webseite und die Einstellungen des Browsers. Diese Datenerhebungen werden in der Praxis häufig weiterhin automatisch gestartet, ohne dass der Besucher der Webseite dies aktiv ermöglichen muss (hierzu sogleich).[135]

Ähnlich funktionieren andere Werkzeuge, die an eindeutige Kennungen einer Endeinrichtung anknüpfen (sog. *unique strings*) oder Endeinrichtung über deren spezifische technische Einstellungen identifizieren (sog. *fingerprints*)[136] und die personenbezogene Daten über die besuchten Webseiten oder die Nutzung von Apps speichern und selbstständig an den Anbieter des jeweiligen Werkzeugs übermitteln.[137] Sofern das *offline*-Verhalten ebenfalls beobachtet und ausgewertet werden soll, kommen beispielsweise Schnittstellen über *Bluetooth* und andere Mittel zur Nahfeldkommunikation (NFC), beispielsweise mithilfe elektromagnetischer Wellen (sog. *radio-frequency identification* oder kurz: RFID) in Betracht, die es – nicht nur bei durch den Nutzer aktivierter

---

[133] So übermittelte die Webseite von *Fashion-ID* auf Grundlage der Software hinter dem „Gefällt mir"-Button von *Facebook* auch Daten von Besucher der Webseite, die keine Kunden der Kommunikationsplattform von Facebook sind: *EuGH*, Urt. v. 29.06.2019, C-40/17 = GRUR 2019, 958 (Rn. 27) – *Fashion ID*.

[134] Die Übergänge sind fließend, weil viele Nutzer von Dritt-Webseiten und Dritt-Apps zugleich Kunden der Anbieter der Tracking-Werkzeuge – insbesondere GAFAM und BAT – sind. Hierzu: *Hacker*, Datenprivatrecht, 2020, S. 25 f.; *Mellet/Beauvisage*, Consumption Markets & Culture 2019, 1 (8).

[135] Ohne endgültige Entscheidung darüber, ob eine Einwilligung erforderlich ist oder eine Interessenabwägung genügen kann: *EuGH*, Urt. v. 29.07.2019, C-40/17 = GRUR 2019, 958 (Rn. 88/97) – *Fashion ID*.

[136] Instruktiv: *Hanloser*, ZD 2018, 213 ff.; *Jandt*, ZD 2018, 405 ff.; *Jentzsch*, in: Stiftung Datenschutz (Hrsg.), Dateneigentum und Datenhandel, 2019, S. 177 (184 ff.); *Hacker*, Datenprivatrecht, 2020, S. 25 ff.

[137] *Hanloser*, ZD 2018, 213 (214); *Acar u. a.*, Facebook Tracking Through Social Plug-ins. Technical report prepared for the Belgian Privacy Commission, 2015, S. 14.

Schnittstelle[138] – ermöglichen, das Bewegungsprofil des Nutzers einer Endeinrichtung nachzuvollziehen[139] oder Daten aus der Endeinrichtung auszulesen.[140]

Der bislang wichtigste ökonomische Ansatz für die Verwertung der erstellten Profile sind die personalisierte oder jedenfalls stratifizierte Werbung für eigene und fremde Produkte auf den mehrseitigen Plattformen und in den, das gesamte Internet einbeziehenden, Werbenetzwerken von *GAFAM* und *BAT*. Ob für diese Datenverarbeitung derzeit und in Zukunft eine Einwilligung erforderlich ist, eine Interessenabwägung ausreichen kann oder eine Erwähnung dieses Vorgehens in den Nutzungsbedingungen ausreicht, ist noch nicht abschließend entschieden,[141] aktuell (teilweise) Gegenstand mehrerer Vorlageverfahren zum *EuGH*[142] und sollte aufgrund der nachfolgend ausgeführten Gründe jedoch zugunsten der Einwilligung ausfallen.

b) Restriktive Auslegung von Art. 6 Abs. 1 lit. f für Direktwerbung

Seit Verabschiedung von Art. 13 ePrivacy-RL im Jahr 2002 ist die Direktwerbung als berechtigtes Interesse des Verantwortlichen anerkannt. Auf den ersten Blick liegt es nahe, dass die personalisierte Werbung auf Grundlage von Profiling vom europäischen Gesetzgeber auch in der DS-GVO berücksichtigt und weiterhin als ein mögliches berechtigtes Interesse des Verantwortlichen i. S. d. Art. 6 Abs. 1 lit. f anerkannt ist (1).[143]

Bezieht man jedoch den technologischen Fortschritt und die Vielzahl der Beteiligten im Rahmen der Werbenetzwerke von *GAFAM* und *BAT* mit ein, so liegt es nach hier vertretener Auffassung nahe, den Begriff der Direktwerbung

---

[138] *Yanofsky*, Google can still use Bluetooth to track your Android phone when Bluetooth is turned off, 24.01.2018, Quartz (https://qz.com/1169760/phone- data/, zuletzt abgerufen am 19.05.2022).

[139] *Kwet*, In Stores, Secret Surveillance Tracks Your Every Move, 14.06.2019, New York Times (https://www.nytimes.com/interactive/2019/06/14/opinion/bluetooth-wireless-tracking-privacy.html, zuletzt abgerufen am 19.05.2022).

[140] Hierzu bereits: Entschließung der 72. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 26. bis 27. Oktober 2006. Verbindliche Regelungen für den Einsatz von RFID-Technologien, 27.10.2006 (https://www.bfdi.bund.de/SharedDocs/Publikationen/Entschliessungssammlung/DSBundLaender/72DSK-RFID.html, zuletzt abgerufen am 19.05.2022).

[141] Diese fehlende Rechtssicherheit hat der *EuGH* nicht beseitigt, indem er es dem vorlegenden Gericht überlassen hat, welcher Erlaubnistatbestand heranzuziehen ist: *EuGH*, Urt. v. 29.07.2019, C-40/17 = GRUR 2019, 958 (Rn. 88/97) – *Fashion ID*.

[142] In Beantwortung der Vorlagefragen 2a und 2b des ÖOGH muss sich der EuGH jedenfalls dazu äußern, ob dieser Datenverarbeitung auf Grundlage von Art. 6 Abs. 1 lit. b DS-GVO rechtmäßig erfolgen kann: *ÖOGH*, Vorlagebeschl. v. 22.07.2021, 6 Ob 56/21k – *Schrems* [*III*].

[143] In diese Richtung: *Caspar*, in: Simitis/Hornung/Spiecker gen. Döhmann (Hrsg.), Datenschutzrecht, 2019, Art. 21, Rn. 21; *Tavanti*, RDV 2016, 295 (297/Fn. 18); *Piltz*, K&R 2016, 557 (565); *Ehmann*, in: Simitis/Hornung/Spiecker gen. Döhmann (Hrsg.), Datenschutzrecht, 2019, Anhang 3 zu Artikel 6, Rn. 18.

im Kontext von Art. 6 Abs. 1 lit. f DS-GVO restriktiv auszulegen, so dass die Datenverarbeitung innerhalb von Werbenetzwerken nicht auf Grundlage einer Interessenabwägung möglich ist, sondern eine wirksame Einwilligung der Datensubjekte voraussetzt (2).

aa) Ausgangspunkt: Personalisierte Werbung als anerkanntes Interesse

Ein Umkehrschluss zu Art. 21 Abs. 2 Hs. 2 DS-GVO (Widerspruch gegen Profiling für Direktwerbung) und die ausdrückliche Erwähnung von Direktwerbung in ErwG 47 S. 7 DS-GVO legen auf den ersten Blick nahe, dass die automatisierte personalisierte Werbung auf Grundlage eines Profiling vom europäischen Gesetzgeber in der DS-GVO grundsätzlich als ein mögliches berechtigtes Interesse des Verantwortlichen i. S. d. Art. 6 Abs. 1 lit. f DS-GVO anerkannt wurde. Die DS-GVO scheint die Privilegierung der Direktwerbung aus Art. 13 ePrivacy-RL (2002) bruchlos fortzuführen, wenngleich diese Anerkennung als berechtigtes Interesse noch nicht das Ergebnis der anschließend erforderlichen Interessenabwägung im jeweiligen konkreten Einzelfall determiniert.

Gemäß Art. 21 Abs. 2 Hs. 2 DS-GVO wird der Widerspruch durch das Datensubjekt im Fall der Direktwerbung erleichtert. Der Widerspruch gegen Direktwerbung setzt – im Unterschied zu Art. 21 Abs. 1 S. 1 DS-GVO – keine Gründe voraus, die sich aus der besonderen Situation des Datensubjekts ergeben. Darüber hinaus ist die Direktwerbung kein zwingender Grund im Interesse des Verantwortlichen. Somit können Datensubjekte die personalisierte Direktwerbung vergleichsweise leicht beenden. Kurzum: Der europäische Gesetzgeber siedelt die Direktwerbung auf Grundlage eines Profiling am untersten Rand der gerade noch berechtigten Interessen des Verantwortlichen an, gegenüber dem die Interessen, Grundrechte und Grundfreiheiten des Datensubjekts typischerweise nicht überwiegen.[144]

Nach h. A. in der Literatur kommt es für die Rechtmäßigkeit personalisierter Werbung auf eine Interessenabwägung an, in der insbesondere berücksichtigt werden kann, welche Maßnahmen die (gemeinsam) Verantwortlichen ergreifen, um die Interessen der Datensubjekte zu wahren. In diesem Zusammenhang wird unter Rückgriff auf § 15 Abs. 3 S. 3 TMG und Art. 13 Abs. 4 Nr. 6 TMG – also auf diejenigen Vorschriften – die der Umsetzung der ePrivacy-RL (2002) dienen, die Ansicht vertreten, dass eine solche Verarbeitung auf Grundlage von Art. 6 lit. f DS-GVO grundsätzlich möglich sein kann,[145] im Rahmen der Inter-

[144] In Anbetracht der Tatsache, dass – abgesehen von der Direktwerbung – keine andere Verarbeitungssituation Erwähnung findet, ist es plausibel, ErwG 47 S. 7 DS-GVO und die ausdrückliche Einordnung von Direktwerbung als berechtigtes Interesse in Art. 21 Abs. 2 DS-GVO einer erfolgreichen politischen Interessenvertretung durch den Werbesektor zuzuschreiben.

[145] In Anlehnung an § 13 Abs. 4 Nr. 6 TMG für eine Rechtsmäßigkeit unter der Vorausset-

essenabwägung jedoch regelmäßig die Interessen des Datensubjekts überwiegen.[146] Die hierfür zu berücksichtigenden Kriterien sind vielfältig.

Erstens soll das durch eine übergreifende Datenverarbeitung entstehende „unüberschaubare Risiko für die Datensubjekte"[147] ausschlaggebend sein. Dieses Kriterium ist denkbar unbestimmt. Obwohl für die Interessenabwägung gemäß Art. 6 Abs. 1 lit. f DS-GVO jeweils die Umstände des Einzelfalls zu berücksichtigen sind, können jedenfalls sehr abstrakte Risiken und Gefahren die Interessenabwägung nicht zugunsten der Interessen des Datensubjekts entscheiden. Beispielsweise ist allein die Möglichkeit, dass es potenziell zu einem rechtswidrigen Verhalten Dritter – beispielsweise durch *Hacking* – kommt, nicht ausreichend, um zu einem Überwiegen der Interessen des Datensubjekts zu gelangen.[148]

Zweitens soll es für das Überwiegen der Interessen der Datensubjekte bedeutsam sein, dass Datensubjekte jedenfalls kein übergreifendes *tracking* für das Profiling zu erwarten brauchen.[149] Obwohl die „vernünftigen Erwartungen" der Datensubjekte gemäß ErwG 47 S. 1 zu berücksichtigen sind, spricht gegen dieses Kriterium der „vernünftigen Erwartungen", dass gemäß Art. 13 Abs. 2 ePrivacy-RL (unerbetene Nachrichten) seit zwei Jahrzehnten eine europäische Rechtsgrundlage für Direktwerbung für eigene Produkte in einer bestehenden Kundenbeziehung existiert. Somit müssen Gerichte konsequenterweise auch davon ausgehen, dass dieser gesetzlich privilegierte Zweck der Datenverarbeitung mittlerweile nicht mehr grundsätzlich mit den vernünftigen Erwartungen von Datensubjekten unvereinbar ist.[150] Allerdings würde mit dieser

---

zung von strikter Pseudonymisierung der Daten: *Tavanti*, RDV 2016, 295 (306); *Bunnenberg*, Privates Datenschutzrecht, 2020, S. 300.

[146] *LG Berlin*, Urt. v. 16.01.2018, BeckRS 2018, 1060 (Rn. 45); *Hacker*, Datenprivatrecht, 2020, S. 279 f.; *Schantz*, in: Simitis/Hornung/Spiecker gen. Döhmann (Hrsg.), Datenschutzrecht, 2019, Art. 6, Rn. 106; *Metzger*, GRUR 2019, 129 (134); wohl auch: *Ehmann*, in: Simitis/Hornung/Spiecker gen. Döhmann (Hrsg.), Datenschutzrecht, 2019, Anhang 3 zu Artikel 6, Rn. 29/36/43; *DSK*, Zur Anwendbarkeit des TMG für nicht-öffentliche Stellen ab dem 25. Mai 2018, Positionsbestimmung, 2018, S. 3 Rn. 9; *Langhanke*, Daten als Leistung, 2018, S. 103; *Golland*, MMR 2018, 130 (133); *EDPS*, Opinion 4/2017 on the Proposal for a Directive on certain aspects concerning contracts for the supply of digital content, 2017, S. 26 Fn. 84; *Article 29 Data Protection Working Group*, Opinion 03/2013 on purpose limitation, WP 203, 2013, S. 46; a. A. *Gierschmann*, ZD 2018, 297 (300); *Roßnagel*, DuD 2016, 561 (563); *Arning/Moos*, ZD 2014, 242 (245 f.).

[147] *Bunnenberg*, Privates Datenschutzrecht, 2020, S. 301; *Zuiderveen Borgesius*, 5 International Data Privacy Law 2015, 163 (164); *Schwenke*, Individualisierung und Datenschutz, 2006, S. 165. *Bunnenberg* verweist zudem auf die Gefahr, dass aufgrund umfangreichen trackings wiederum besonders sensible Daten ableitbar werden. Dieses Argument geht fehl, weil in diesem Fall der Anwendungsbereich des Art. 6 Abs. 1 lit. f DS-GVO ohnehin nicht eröffnet wäre.

[148] Sehr weit jedoch: *Bunnenberg*, Privates Datenschutzrecht, 2020, S. 301 f.

[149] *DSK*, Orientierungshilfe für die Aufsichtsbehörden zum TMG, März 2019, S. 16 f; im Anschluss hieran: *Bunnenberg*, Privates Datenschutzrecht, 2020, S. 301.

[150] *Härting*, Internetrecht, 2017, Rn. 235; ebenso *DIVSI*, Daten – Ware und Währung, 2014, S. 16.

Argumentation übersehen, dass das insbesondere durch *Facebook* und *Google* (*Alphabet*) vorgenommene Ausmaß der Datenzusammenführung und -auswertung – trotz zunehmender Berichterstattung über diese Praxis in der Tagespresse – für durchschnittliche Datensubjekte weiterhin überraschend sein dürfte.[151]

In diesem Sinne hat der *VGH München* mit Blick auf das Werbenetzwerk *Facebook Custom Audience* entschieden, dass die Weiterleitung von gehashten E-Mail-Adressen durch einen Vertragspartner des Datensubjekts an *Facebook* über das hinausgeht, was ein Datensubjekt typischerweise erwartet, wenn es einem Vertragspartner im Rahmen eines Bestellvorgangs seine E-Mail-Adresse zu Zwecken der Werbung durch diesen Vertragspartner angibt. *Facebook* nutzt die vom Vertragspartner übermittelten Daten im Rahmen von *Custom Audience* für eine Überschneidungsanalyse mit den Kunden anderer Unternehmen und den Nutzern der eigenen Kommunikationsplattformen, um auf dieser Grundlage seine Profilbildung kontinuierlich zu verfeinern und um – jedenfalls auch – dem ursprünglichen Vertragspartner des Datensubjekts die Möglichkeit zur personalisierten Werbung gegenüber dessen Kunden auf anderen Plattformen und Webseiten anzubieten.[152]

Obwohl die Datenübermittlung des Vertragspartners des Datensubjekts an *Facebook* und die Überschneidungsanalyse durch *Facebook* im Ergebnis – zumindest auch – der personalisierten Direktwerbung in einer bestehenden Kundenbeziehung zwischen dem Datensubjekt und dem Vertragspartner dienen kann, hat der *VGH München* – im Ergebnis überzeugend[153] – zum BDSG a. F. entschieden, dass bei einer Abwägung zwischen den „schutzwürdigen Interessen" des Datensubjekts, einschließlich Art. 8 Abs. 1 GRCh, und dem „Interesse" des Händlers an einer Übermittlung von personenbezogenen Daten an *Facebook* zu Werbezwecken, das Interesse des Datensubjekts überwiegt.[154]

Überdies wird im Beschluss des *Bundeskartellamts* im Verfahren gegen *Facebook*[155] teilweise angenommen, dass es für die Interessenabwägung gemäß Art. 6 Abs. 1 lit. f DS-GVO eine Rolle spielt, ob der Verantwortliche ein marktbeherrschendes Unternehmen ist. Diese Berücksichtigung der Wettbewerbssituation[156] ist zwar im Ergebnis richtig. Allerdings sollte die Argumentation nachgeschärft werden. So ist das *Bundeskartellamt* mit Blick auf einen Datenaustausch zwischen Tochterunternehmen von *Facebook* insbesondere deshalb von einem Überwiegen der Interessen der Nutzer ausgegangen, weil *Facebook* eine

---

[151] Hierzu: *Rothmann/Buchner*, DuD 2018, 342 (345).

[152] *VGH München*, Beschl. v. 26.09.2018 – 5 CS 18.1157 = NVwZ 2019, 171 (Rn. 27).

[153] Zur Kritik an der verkürzten Argumentation: Oben: C.I.1.b.

[154] *VGH München*, Beschl. v. 26.09.2018 – 5 CS 18.1157 = NVwZ 2019, 171 (Rn. 27).

[155] *Bundeskartellamt*, Beschl. v. 06.02.2019, B6–22/16.

[156] Hierzu die unten vorgeschlagene kartellrechtsakzessorische, asymmetrische Auslegung und Anwendung von Art. 7 Abs. 3 S. 1 DS-GVO und Art. 7 Abs. 4 DS-GVO: Unten Kapitel 5 C.III.2.a. bzw. II.1.

marktbeherrschende Stellung innehabe und dies *Facebook* ermögliche, seinen Nutzern einseitige Bedingungen für eine Datenverarbeitung aufzuerlegen.[157]

Tatsächlich verfängt dieses Argument der marktbeherrschenden Stellung jedoch im Rahmen der Interessenabwägung – anders als im Rahmen einer Einwilligung[158] – nur indirekt. Die Entscheidungsfreiheit der Datensubjekte ist im Fall einer Verarbeitung auf Grundlage der *gesetzlich* vorgegebenen Interessenabwägung im Ausgangspunkt ebenso irrelevant wie die vorformulierten und gestellten Vertragskonditionen. Für Art. 6 Abs. 1 lit. f DS-GVO kommt es – anders als bei Art. 6 Abs. 1 lit. a und lit. b DS-GVO – gerade nicht auf eine Entscheidung und Erklärung des Datensubjekts an. Infolgedessen kann das Argument der marktbeherrschenden Stellung allenfalls mittelbar im Rahmen der Interessenabwägung verwertet werden, weil im Rahmen der Interessenabwägung bereits zu berücksichtigen ist, dass ein Datensubjekt aufgrund der Marktmacht eines Verantwortlichen, beispielsweise von *Facebook*, davon absehen wird, sein Widerspruchsrecht aus Art. 21 DS-GVO tatsächlich auszuüben.

bb) Korrektur: Keine Direktwerbung durch Werbenetzwerke

Unabhängig vom vernünftigen Erwartungshorizont der Datensubjekte und der Marktposition der (gemeinsam) Verantwortlichen kommt Art. 6 Abs. 1 lit. f DS-GVO nach hier vertretener Auffassung nicht als Rechtsgrundlage für eine automatisierte personalisierte Werbung auf Grundlage von Werbenetzwerken in Betracht.

Zwar ist es zutreffend, dass die Werbewirtschaft mit Art. 13 Abs. 3 ePrivacy-RL (2002), ErwG 47 S. 7 DS-GVO und der Möglichkeit zum Umkehrschluss aus Art. 21 Abs. 2 Hs. 2 DS-GVO einen politischen Erfolg erzielt hat. Diese Privilegierung kann man weiterhin für richtig halten und in diesem Zusammenhang darauf hinweisen, dass eine Rechtmäßigkeit von automatisierter personalisierter Direktwerbung auf Grundlage von Art. 6 Abs. 1 lit. f DS-GVO auch dazu dient, die Datensubjekte vor einer drohenden Einwilligungsmüdigkeit zu bewahren,[159] weil personalisierte Direktwerbung massenhaft auf Grundlage von Werbenetzwerken stattfindet und viele Verantwortliche daran beteiligt sind.

Allerdings legen die h. A. in der Literatur und der *VGH München* den Begriff der Direktwerbung zu weit und ohne Bezug auf dessen ursprünglichen Kontext im Rahmen von Art. 13 ePrivacy-RL (2002) aus.[160] Der Gesetzgeber der DS-

---

[157] *Bundeskartellamt*, Beschl. v. 06.02.2019, B6–22/16, Rn. 783 ff./858; zustimmend *Hacker*, Datenprivatrecht, 2020, S. 281; *Hoeren*, MMR 2019, 137 (138); *Buchner*, WRP 2019, 1243 (1248).

[158] Hierzu Kapitel 5 C.II.1 und III.2.a.

[159] So: *Engeler/Felber*, ZD 2017, 251 (255).

[160] Auf die Herkunft des Begriffs der Direktwerbung aus der alten e-privacy-RL wird regelmäßig nicht eingegangen: Dies hat zur Folge, dass auch personalisierte Werbung, die auf einem Einsatz von umfassenden Tracking-Werkzeugen beruht, zu unkritisch als Fall der Direktwerbung eingeordnet wird: *Caspar*, in: Simitis/Hornung/Spiecker gen. Döhmann

GVO hat diesen im Unionsrecht aus der ePrivacy-RL (2002) bereits geläufigen Begriff – soweit ersichtlich – übernommen. Diese Übernahme des Begriffs legt nahe, dass Art. 6 Abs. 1 lit. f DS-GVO nur für die Direktwerbung des Verantwortlichen und nicht für eine Werbung für ähnliche oder unähnliche Produkte Dritter anzuwenden ist. Infolge seiner Entstehungsgeschichte ist der Begriff der Direktwerbung somit eng zu verstehen.[161] Eine weite Auslegung des Begriffs, die nur auf den Wortlaut von Art. 21 Abs. 2 Hs. 2 DS-GVO (Widerspruch gegen Profiling für Direktwerbung) und die ausdrückliche Erwähnung von Direktwerbung in ErwG 47 S. 7 DS-GVO abstellt, geht über diese Entstehungsgeschichte des Begriffs im Kontext der ePrivacy-RL (2002) hinweg.

Im Bewusstsein, dass der Begriff der Direktwerbung aus der ePrivacy-RL (2002) übernommen wurde, ist es zweifelhaft, dass Art. 6 Abs. 1 lit. f DS-GVO als Rechtsgrundlage für eine automatisierte personalisierte Werbung in Betracht kommt, die auf einem seit 2002 völlig veränderten Ausmaß und grundlegend anderen technischen Werkzeugen beruht.[162] Technologisch betrachtet entstammt der aus der ePrivacy-RL übernommene Begriff der Direktwerbung einem anderen Zeitalter. Insofern bietet die Verhaltensbeobachtung auf Grundlage aktueller *tracking*-Werkzeuge ein Profiling unter Anwendung von künstlicher Intelligenz, das über die Grenzen von Telemedien und Endeinrichtungen hinausgeht und eine Granularität der personalisierten Werbung ermöglicht, die weit über diejenigen Sachverhalte hinausreicht, die dem Gesetzgeber bei Verabschiedung der ePrivacy-RL mit dem Begriff der Direktwerbung ursprünglich vor Augen standen.

Infolgedessen bietet Art. 6 Abs. 1 lit. f DS-GVO nach hier vertretener Auffassung keine Rechtsgrundlage für eine personalisierte Werbung auf Basis von Profiling, sofern die zugrundeliegenden Datenverarbeitungen, einschließlich der Datenübermittlung, durch mehrere (gemeinsam) Verantwortliche[163] erfolgt. Sobald neben dem Verantwortlichen, mit dem das Datensubjekt in einer Kundenbeziehung steht, Dritte hinzukommen, die nicht lediglich Auftragsverarbeiter des Verantwortlichen sind, ist der Anwendungsbereich der Direktwerbung i. S. d. Art. 6 Abs. 1 lit. f i. V. m. Art. 21 Abs. 2 DS-GVO überschritten. Eine Datenverarbeitung zum Zweck der personalisierten Werbung, die neben dem Ver-

---

(Hrsg.), Datenschutzrecht, 2019, Art. 21, Rn. 21; *Tavanti*, RDV 2016, 295 (297/Fn. 18); *Piltz*, K&R 2016, 557 (565); *Ehmann*, in: Simitis/Hornung/Spiecker gen. Döhmann (Hrsg.), Datenschutzrecht, 2019, Anhang 3 zu Artikel 6, Rn. 18.

[161] *Weidert/Klar*, BB 2017, 1858 (1862); *EDSA*, Leitlinien 05/2020 zur Einwilligung gemäß Verordnung 2016/679 v. 04.05.2020, S. 12/Rn. 33; *VGH München*, Beschl. v. 26.09.2018 – 5 CS 18.1157 = NVwZ 2019, 171 (Rn. 27).

[162] Dies (wohl) annehmend, den Begriff der Direktwerbung aber – in Übereinstimmung mit Art. 13 ePrivacy-RL – konsequent auf das Verhältnis zu Bestandskunden reduzierend: *Weidert/Klar*, BB 2017, 1858 (1862).

[163] Zum Begriff der gemeinsamen Verantwortlichkeit: *EuGH*, Urt. v. 29.06.2019, C-40/17 = GRUR 2019, 958 (Rn. 132 f.) – *Fashion ID*; hierzu auch: *Sattler*, GRUR 2019, 1023 ff.

tragspartner des Datensubjekts weitere (gemeinsam) Verantwortliche miteinbezieht, ist infolgedessen schon kein berechtigtes Interesse i. S. d. Art. 6 Abs. 1 lit. f DS-GVO, so dass es auf eine konkrete Interessenabwägung nicht mehr ankommt.[164]

Dieses Verständnis hat zur Konsequenz, dass die Praktiken der aktuell gängigen Werbenetzwerke – beispielsweise *Facebook Custom Audience* oder mithilfe der jeweiligen *Werbe-ID* von *Apple* und *Google* – nur auf Grundlage einer Einwilligung des jeweiligen Datensubjekts gegenüber den jeweils (gemeinsam) Verantwortlichen rechtmäßig sind.[165] Diese Ansicht findet mehrere zusätzliche Stützen in den aktuellen Gesetzgebungsvorschlägen der *EU-Kommission*.

Erstens soll gemäß ErwG 52 S. 4 des Vorschlags der *EU-Kommission* für eine Verordnung über digitale Dienste (engl. Digital Service Act oder kurz: DSA)[166] die

> „Notwendigkeit [bestehen], vor der Verarbeitung personenbezogener Daten für gezielte Werbung die Einwilligung der betroffenen Person einzuholen."

Dabei sollen insbesondere sehr große Plattformen die wesentlichen Kriterien für eine personalisierte Werbung gegenüber den Datensubjekten – ausdrücklich vor Erteilung der Einwilligung – offenlegen.[167]

Zweitens sollen die sog. *Gatekeeper* im Kontext eines Profiling besondere Transparenzpflichten treffen, die gemäß ErwG 61 S. 4 des Vorschlags der *EU-Kommission* für eine Verordnung über bestreitbare und faire Märkte im digitalen Sektor (Digital Markets Act oder kurz: DMA-Vorschlag)[168] insbesondere dann einzuhalten sind, wenn die Endnutzer „um Einwilligung ersucht werden". Zudem soll eine Zusammenführung von personenbezogenen Daten aus den zentralen Plattformdiensten eines *Gatekeepers* mit personenbezogenen

---

[164] Der EuGH deutet an, dass die Verwendung des social plug-in „Gefällt mir"-Button von *Facebook* – jedenfalls nach den von der Vorinstanz festgestellten Tatsachen – einer Einwilligung bedarf, so dass es auf eine (jeweilige) Abwägung mit den berechtigten Interessen der (gemeinsam) Verantwortlichen nicht mehr ankam: *EuGH*, 29.07.2019, C-40/17 = GRUR 2019, 958 (Rn. 88/97) – *Fashion ID*.

[165] Die Auslegung des Begriffs der Direktwerbung i. S. d. Art. 21 Abs. 2 Hs. 2 DS-GVO dürfte auch Gegenstand der von NOYB mit der in Frankreich eingereichten Klage gegen Google sein: *dpa*, Klage gegen *Google*: Datenschutzaktivist geht gegen Werbe-ID auf Android-Handys vor, FAZ, 07.04.2021 (https://www.faz.net/aktuell/wirtschaft/digitec/datenschutzaktivist-geht-gegen-werbe-id-bei-android-vor-17281471.html, zuletzt abgerufen am 19.05.2022).

[166] *EU-Kommission*, Vorschlag für eine Verordnung über einen Binnenmarkt für digitale Dienste (Gesetz über digitale Dienste), v. 15.12.2020, COM(2020) 825 final.

[167] Der Europäische Datenschutzbeauftragte schlägt vor, zusätzliche, „über die Transparenz hinausgehende Vorschriften [zu erwägen], einschließlich einer allmählichen Abschaffung, die in einem Verbot von gezielter Werbung auf der Grundlage von allgegenwärtiger Nachverfolgung mündet": *EDSB*, Zusammenfassung der Stellungnahme zu dem Vorschlag für ein Gesetz über digitale Dienste, ABl. C 149, v. 27.04.2021, S. 3 (5).

[168] *EU-Kommission*, Vorschlag für eine Verordnung über bestreitbare und faire Märkte im digitalen Sektor (Gesetz über digitale Märkte), v. 15.12.2020, COM(2020) 842 final.

Daten aus anderen von ihm oder von Dritten angebotenen Diensten nach Ansicht der *EU-Kommission* ausschließlich auf Grundlage eine Einwilligung möglich sein, Art. 5 lit. a des DMA-Vorschlags.

Kurzum: Das berechtigte Interesse der Direktwerbung sollte nach hier vertretener Auffassung eng ausgelegt werden, so dass es nur in der jeweiligen bestehenden relativen Kundenbeziehung zwischen Datensubjekt und Verantwortlichem zur Anwendung kommt. Sobald mehrere (gemeinsam) Verantwortliche die Daten bündeln oder austauschen ist dies nicht mehr vom Begriff der Direktwerbung umfasst, selbst wenn alle Verantwortlichen und der Betreiber des Werbenetzwerks, jeweils in einer eigenen Kundenbeziehung zum Datensubjekt stehen. Die von *Google*, *Apple*, *Facebook* und anderen Intermediären betriebenen Plattformen sind nicht mehr mit den Formen der Direktwerbung vergleichbar, die dem Gesetzgeber der ePrivacy-RL (2002) zur Jahrtausendwende vor Augen stand. Infolgedessen können sich die Betreiber von mehrseitigen Plattformen, insbesondere *GAFAM* und *BAT*, nur insoweit auf eine durch Art. 6 Abs. 1 lit. f DS-GVO privilegierte Direktwerbung berufen, soweit sie die personenbezogenen Daten ausschließlich für eine Werbung für eigene ähnliche Produkte verarbeiten und mit dem Datensubjekt in einer aktuellen Kundenbeziehung stehen.[169] Soweit das Profiling zur personalisierten Werbung für ihre Werbekunden genutzt wird, sind die Plattformbetreiber auf eine Einwilligung der Datensubjekte angewiesen.[170]

3. Erweiterung des Anwendungsbereichs der Interessenabwägung

Nach hier vertretener und noch zu begründender Auffassung kommt der Einwilligung des Datensubjekts eine Vorrangstellung zu. Infolgedessen ist eine Einwilligung einzuholen, sofern sie nicht unerreichbar oder mit objektiv unverhältnismäßigem Aufwand verbunden ist.[171] Diese Vorrangstellung nimmt die durch Art. 8 Abs. 2 S. 1 GRCh garantierte Möglichkeit zur Einwilligung ernst, gewährleistet die informationelle Privatautonomie der Datensubjekte und setzt außerdem einen Anreiz für Verantwortliche, datenschutzkonforme Einwilligungsmechanismen zu entwickeln und die Datensubjekte dadurch frühzeitig einzubeziehen.[172]

---

[169] Wettbewerbspolitisch liegt es deshalb nahe, das Privileg für Direktwerbung innerhalb einer bestehenden Kundenbeziehung *de lege ferenda* abzuschaffen, soweit dadurch die Eigenwerbung von ohnehin marktmächtigen Plattformen ermöglicht wird, so dass diese mittels Direktwerbung ihre Marktmacht weiter ausbauen können.

[170] Deren wirksame Einholung ist infolge der unten vorgeschlagenen kartellrechtsakzessorischen, asymmetrischen Anwendung von Art. 7 Abs. 4 DS-GVO für marktmächtige Plattformbetreiber besonders schwierig: Hierzu unten Kapitel 5 C.II.1.

[171] Hierzu unten Kapitel 4 A.I. und Kapitel 5 A. und B.

[172] Hierzu unten Kapitel 6 B. und zuletzt: § 26 des Gesetz zur Regelung des Datenschutzes

Trotz dieses grundsätzlichen Vorrangs der Einwilligung, ist bereits jetzt erkennbar, dass die ubiquitäre Datenverarbeitung im Rahmen des sog. Internet of Things (IoT) und insbesondere die restriktive Möglichkeit zur rechtmäßigen Datenverarbeitung von besonders sensiblen personenbezogenen Daten gemäß Art. 9 Abs. 2 DS-GVO den Einwilligungstatbestand erheblich unter Druck setzt (a).

Es lässt sich absehen, dass der Tatbestand der Interessenabwägung, der derzeit nicht zur Verfügung steht, soweit besonders sensible personenbezogene Daten verarbeitet werden, künftig in Betracht kommen muss. Dies gilt insbesondere für die kurzfristige Verarbeitung von Daten durch IoT-Endgeräte, die durch Spontanäußerungen generiert werden (b) und für das Trainieren im Rahmen des maschinellen Lernens (c). Diese beiden Vorschläge sind auf den ersten Blick eine Schwächung der informationellen Privatautonomie, weil der Verantwortliche dann gerade nicht mehr auf eine Einwilligung des Datensubjekts angewiesen wäre. Tatsächlich führt eine solche Lösung jedoch zur Entlastung der Datensubjekte, indem dadurch volkswirtschaftlich wichtige Entwicklungen ermöglicht werden, solange dadurch für einzelne Datensubjekte gerade keinen besonderen Risiken entstehen.

a) Verarbeitung besonders sensibler personenbezogener Daten

Die Definition der besonderen Kategorien personenbezogener Daten (nachfolgend: besonders sensible personenbezogene Daten) ist potenziell sehr weit geraten und die Abgrenzung zu den lediglich personenbezogenen Daten ist noch ungeklärt. Gemäß Art. 9 Abs. 1 DS-GVO ist eine Verarbeitung von Daten grundsätzlich untersagt,

> „[…] aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie die Verarbeitung von genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person […]".[173]

Sobald Daten als besonders sensible personenbezogene Daten anzusehen sind, verengt sich die Möglichkeit zur rechtmäßigen Datenverarbeitung im Privatrechtsverhältnis grundlegend. Neben der Interessenabwägung scheidet auch eine vertragsakzessorische Datenverarbeitung (Art. 6 Abs. 1 lit. b DS-GVO) aus. Abgesehen von der *ausdrücklichen* Einwilligung (Art. 9 Abs. 2 lit. a DS-GVO) kommen nur noch sehr spezifische Erlaubnistatbestände in Betracht, die

---

und des Schutzes der Privatsphäre in der Telekommunikation und bei Telemedien v. 23.05.2021 (TTDSG), BGBl. I Nr. 35, v. 28.06.2021, S. 1982 ff.

[173] Definiert werden die Kategorien: „genetische Daten" (Art. 4 Nr. 13 DS-GVO), „biometrische Daten" (Art. 4 Nr. 14 DS-GVO) und „Gesundheitsdaten" (Art. 4 Nr. 15 DS-GVO).

zwar auch noch mit einem Privatrechtsverhältnis im Zusammenhang stehen, aber – abgesehen von der Geltendmachung und Durchsetzung von zivilrechtlichen Rechtsansprüchen[174] – bereits stark durch öffentliche Interessen und staatliche Gewährleistungspflichten geprägt sind und an die Gesundheitsvorsorge bzw. -versorgung,[175] das Sozialrecht,[176] ein Arbeitsverhältnis,[177] eine Datenverarbeitung zu öffentlichen Forschungs- und Archivzwecken[178] oder eine Gefährdung der staatlichen oder öffentlichen Sicherheit[179] anknüpfen.

Somit hat die Einordnung von Daten als „besonders sensibel" grundlegende Bedeutung. In seinem Vorlagebeschluss vom 24.03.2021 an den *EuGH* hat das *OLG Düsseldorf* die rechtlichen Konsequenzen eines weiten Begriffs der besonders sensiblen personenbezogenen Daten auf den Punkt gebracht. Mit seiner Vorlagefrage 2a will das *OLG Düsseldorf* vom *EuGH* wissen, ob beim Erfassen eines Webseiten-Besuchs durch ein Datensubjekt

> „sensible Daten im Sinne des Art. 9 Abs. 1 DSGVO verarbeitet werden, wenn es sich um Webseiten oder Apps handelt, die Bezug zu den Kriterien des Abs. 1 haben, wie etwa Flirting-Apps, Homosexuellen-Partnerbörsen, Webseiten politischer Parteien, gesundheitsbezogene Webseiten".[180]

Sofern es sich um besonders sensible personenbezogene Daten handelt, wenn die Besuche von und Eingaben auf solchen Webseiten über *tracking*-Werkzeuge erfasst und mit anderen personenbezogenen Daten durch den Verantwortlichen verknüpft und verwendet werden, bleibt für das Privatrechtsverhältnis derzeit nur die ausdrückliche Einwilligung des Datensubjekts gemäß Art. 9 Abs. 2 lit. a oder Art. 9 Abs. 2 lit. e DS-GVO (offensichtliches Öffentlichmachen) als Grundlage für eine rechtmäßige Datenverarbeitung.

Mit seiner im Anschluss formulierten Vorlagefrage 2b stellt das *OLG Düsseldorf* eine fundamentale Frage, die man intuitiv als rhetorische Frage charakterisieren möchte: Vorausgesetzt die Daten, die beim Besuch von und durch Eingaben auf solchen Webseiten und Apps erfasst werden, sind besonders sensible personenbezogene Daten, so möchte das *OLG Düsseldorf* wissen, ob dieser Besuch und die Eingabe ein offensichtliches Öffentlichmachen der Daten durch das Datensubjekt im Sinne des Art. 9 Abs. 2 lit. e DS-GVO darstellt.

Welche fundamentale Bedeutung diese Vorlagefrage hat, wird aus der nüchternen Wortwahl des *OLG Düsseldorf* (zu) wenig deutlich. Beantwortet der *EuGH* diese Frage positiv, wäre jedes Verhalten eines Datensubjekts im Inter-

---

174 Art. 9 Abs. 2 lit. f DS-GVO i. V. m. § 24 Abs. 1 Nr. 2, Abs. 2 BDSG.
175 Art. 9 Abs. 2 lit. h DS-GVO.
176 Art. 9 Abs. 2 lit. b DS-GVO.
177 Art. 9 Abs. 2 lit. b DS-GVO i. V. m. § 26 BDSG.
178 Art. 9 Abs. 2 lit. j DS-GVO i. V. m. § 27 BDSG.
179 Art. 9 Abs. 2 lit. g DS-GVO i. V. m. § 24 Abs. 1 Nr. 1, Abs. 2 BDSG.
180 Vorlagefrage 2a des *OLG Düsseldorf*, Vorlagebeschl. v. 24.03.2021, Kart 2/19 (V), GRUR-RS 2021, 8370 (Rn. 37).

net, das nicht in einem besonders geschützten virtuellen Raum stattfindet, als offensichtliches Öffentlichmachen i. S. d. Art. 9 Abs. 2 lit. e DS-GVO zu beurteilen. Die seit Jahren anhaltende Diskussion über *tracking-tools* und Profiling wäre schlagartig erledigt. Datensubjekten mit hoher Datenschutzpräferenz bliebe dann nur noch der berühmte Rat von *Eric Schmidt* (damals *Google*):

„If you have something that you don't want anyone to know, maybe you shouldn't be doing it in the first place".[181]

Die Vorlagefragen 2a und 2b des *OLG Düsseldorf* lassen sich somit auch als zweifacher Warnschuss interpretieren.[182] *Erstens* sollte der Begriff der besonders sensiblen personenbezogenen Daten nicht zu weit ausgelegt werden. *Zweitens* sollten die Voraussetzungen für das Tatbestandsmerkmal des offensichtlichen Öffentlichmachens restriktiv ausgelegt werden.[183]

Legt der *EuGH* den Begriff der besonders sensiblen personenbezogenen Daten sehr weit aus, so hat dies zur Konsequenz, dass die Verarbeitung dieser Daten im Privatrechtsverhältnis regelmäßig auf eine ausdrückliche Einwilligung oder eine weite Auslegung des Art. 9 Abs. 2 lit. e DS-GVO angewiesen ist, weil keine Ausweichmöglichkeit, beispielsweise in Form einer (qualifizierten) Interessenabwägung als Auffangtatbestand in Betracht kommt.[184] Das kann man auf den ersten Blick positiv finden, weil dadurch der Vorrang der Einwilligung und damit die informationelle Privatautonomie gestärkt wird. Im Ergebnis kann auch das offensichtliche Öffentlichmachen durch das Datensubjekt – jedenfalls nach deutschem Rechtsverständnis – als eine Einwilligung gegenüber einem unbestimmten Personenkreis, also der Allgemeinheit, gewertet werden.[185]

Weil Art. 9 Abs. 2 lit. a und lit. e DS-GVO jedoch ein binäres System etablieren, das keinen Spielraum für Interessenabwägungen im Einzelfall lässt, besteht die Gefahr, dass Gerichte diese Interessenabwägung unter „falscher Flagge"

---

[181] Im Interview mit *Maria Bartiromo* auf CNBC am 03.12.2009; zitiert von: The Huffington Post, 07.12.2009 (http://www.huffingtonpost.com/2009/12/07/google-ceo-on-privacy-if_n_383105.html, zuletzt abgerufen am 19.05.2022).

[182] Mit einer Vorlagefrage, die auch ein Öffentlichmachen in der „analogen Welt" einbezieht: *ÖOGH*, Vorlagebeschl. v. 22.07.2021, 6 Ob 56/21k – *Schrems* [III] (Vorlagefrage 4 Rn. 25 ff.). Der ÖOGH legt dem EuGH mit diesem Beschluss u. a. die Frage vor, ob die Erwähnung der eigenen sexuellen Orientierung auf einer (öffentlichen) Podiumsdiskussion ausreicht, so dass *Facebook* diese Information anschließend auf Grundlage von Art. 9 Abs. 2 lit. e DS-GVO rechtmäßig für ein Profiling nutzen kann.

[183] Oben A.II.3.c.

[184] Vorlagefrage 2b des *OLG Düsseldorf*, Vorlagebeschl. v. 24.03.2021, Kart 2/19 (V), Rn. 45 ff. (Rn. 46: „weil das [Datensubjekt] dann den spezifischen Schutz des Art. 9 Abs. 1 DSGVO verloren hätte, ohne dass es einer Einwilligung nach Art. 9 Abs. 2 lit. a) DS-GVO bedürfte. Weitere Erlaubnisgründe gemäß Art. 9 Abs. 2 DSGVO kommen wegen des Geschäftsfelds von Facebook praktisch nicht in Betracht […]".

[185] So für das Einstellen einer (Bild-)Datei mit urheberrechtlich geschütztem Inhalt: *Ohly*, Volenti non fit iniuria, 2001, S. 327 ff.; *ders.*, GRUR 2012, 983 (986 f.); *v. Ungern-Sternberg*, GRUR 2009, 369 (370).

entweder bereits in den Begriff der besonders sensiblen personenbezogenen Daten gemäß Art. 9 Abs. 1 DS-GVO oder in einen dieser beiden Erlaubnistatbestände hineinlesen.[186]

Es wurde bereits vorgeschlagen, die objektive Definition der besonders sensiblen Daten gemäß Art. 9 Abs. 1 DS-GVO durch das ungeschriebene und zudem schwer nachweisbare subjektive Tatbestandsmerkmal einer Auswertungs-[187] bzw. Verwendungsabsicht[188] zu reduzieren.[189] Fehlt diese Tatbestandsvoraussetzung, so soll es sich um lediglich personenbezogene Daten handeln und infolgedessen stünde Art. 6 Abs. 1 lit. f DS-GVO als Grundlage für die Datenverarbeitung zur Verfügung. Allerdings würde dann die subjektive Absicht des Verantwortlichen darüber entscheiden, ob die Daten als personenbezogene oder besonders sensible personenbezogene Daten zu behandeln sind.[190] Die praktischen Unzulänglichkeiten, insbesondere die Beweisschwierigkeiten, die mit einem solchen Ansatz verbunden sind, liegen auf der Hand.

Wird die (weite) Definition des Art. 9 Abs. 1 DS-GVO nicht reduziert, so bleibt als Lösungsweg die Ausdehnung eines Erlaubnistatbestands gemäß Art. 9 Abs. 2 DS-GVO. Entweder müssten die Anforderungen an die Einwilligung gemäß Art. 9 Abs. 1 lit. a DS-GVO reduziert werden, so dass im Einzelfall auch eine konkludente Einwilligung ausreicht, um beispielsweise eine kurzzeitige und für das Datensubjekt mit geringen Risiken verbundene Datenverarbeitung zu ermöglichen. Dieser Weg ist jedoch versperrt, weil der Wortlaut von Art. 9 Abs. 1 lit. a DS-GVO eine ausdrückliche Einwilligung fordert und allein diese Ausdrücklichkeit die Einwilligung in die Verarbeitung von besonders sensiblen personenbezogenen Daten von der Einwilligung in die Verarbeitung von (normalen) personenbezogenen Daten unterscheidet (Art. 6 Abs. 1 lit. a DS-GVO).

Daher ist die dritte Möglichkeit die wahrscheinlichste Variante. Sie deutet sich bereits in den Vorlagefragen 2a und 2b des *OLG Düsseldorf* und der Vor-

---

[186] Mit dieser Kritik an *Vorschaubilder II* (*BGH*, GRUR 2012, 602): *Ohly*, GRUR 2012, 983 (991: „die Einwilligung überdehnt, um ein objektiv interessengerechtes Ergebnis zu erzielen").

[187] Hierfür: *Schulz*, in: Gola (Hrsg.), DSGVO, Art. 9, Rn. 11; *Scholz*, in: Simitis/Hornung/Spiecker gen. Döhmann (Hrsg.), Datenschutzrecht, 2019, Anhang 1 zu Art. 6, Rn. 101.

[188] Diese Möglichkeit ausdrücklich als Abgrenzungskriterium erwähnend: *OLG Düsseldorf*, Vorlagebeschl. v. 24.03.2021 – Kart 2/19 (V) = NZKart 2021, 306 (Rn. 45: „Klärungsbedürftig ist auch, ob die Verwendungsabsicht für die Beurteilung von Bedeutung ist").

[189] Für eine teleologische Reduktion von Art. 9 Abs. 1 DS-GVO, sofern der Verantwortliche sich nicht „den spezifisch sensiblen Informationsgehalt der besonderen Datenkategorie zu Nutze macht": *T. Britz/Indenhuck/Langerhans*, ZD 2021, 559 (562 f).

[190] In diese Richtung geht auch die 3. Vorlagefrage *ÖOGH*, Vorlagebeschl. v. 22.07.2021, 6 Ob 56/21k – *Schrems* [*III*]. Der ÖOGH will vom EuGH wissen, ob besonders sensible personenbezogene Daten verarbeitet werden, sofern diese eine gezielte Filterung von besonderen Kategorien personenbezogener Daten wie politische Überzeugung oder sexuelle Orientierung (etwa für Werbung) erlaubt, auch wenn der Verantwortliche zwischen diesen Daten nicht differenziert.

lagefrage 3 des *ÖOGH*[191] an: Der Begriff des Öffentlichmachens i. S. d. Art. 9 Abs. 2 lit. e DS-GVO könnte im Einzelfall – letztlich als Folge einer Interessenabwägung – großzügig ausgelegt werden. Nachteil dieser Variante ist jedoch, dass eine großzügige Auslegung des Art. 9 Abs. 2 lit. e DS-GVO faktisch ebenfalls zu einem Unterlaufen der von Art. 9 Abs. 1 lit. a DS-GVO geforderten Ausdrücklichkeit führt. Je geringer die Anforderungen an das offensichtliche Öffentlichmachen durch das Datensubjekt sind, desto stärker ähneln die Voraussetzung des Art. 9 Abs. 1 lit. e DS-GVO einer konkludenten Einwilligung des Datensubjekts gegenüber der Allgemeinheit.[192]

Jedenfalls in dem ersten der beiden in den nachfolgenden Abschnitten besprochenen Konstellationen liegt dieser dritte Weg über Art. 9 Abs. 1 lit. e DS-GVO nahe (hierzu sogleich).

Eine rechtmäßige Verarbeitung der besonders sensiblen personenbezogenen Daten sollte – nach hier vertretener Ansicht – *de lege ferenda* möglich sein, sofern Spontanäußerungen besonders sensible personenbezogene Daten generieren und diese für eine Verifizierung der Nutzungsberechtigung lediglich kurzzeitig verarbeitet werden. Nach derzeitiger Rechtslage ist eine solche Verarbeitung jedoch regelmäßig rechtswidrig, weil die Einholung einer ausdrücklichen Einwilligung hierfür praktisch nicht in Betracht kommt und eine weite Anwendung von Art. 9 Abs. 2 lit. e DS-GVO in diesen Fällen wegen der gravierenden Folgen[193] für den Gewährleistungsbereich von Art. 8 Abs. 1 und Art. 7 GRCh verhindert werden sollte.

b) Verarbeitung von besonders sensiblen Daten im Kontext des IoT

Eine der beiden aktuell größten Herausforderung für eine Verwirklichung der informationellen Privatautonomie sind die technischen Fortschritte im Bereich des sog. Internet of Things (IoT).[194]

Für die Verarbeitung von personenbezogenen Daten und der Informationen aus den Endgeräten des berechtigten Nutzers – solche Endgeräte sind regelmäßig die technische Grundlage des IoT – ist eine Einwilligung zwar regelmäßig

---

[191] *ÖOGH*, Vorlagebeschl. v. 22.07.2021, 6 Ob 56/21k – *Schrems* [*III*] (Vorlagefrage 4 Rn. 25 ff.).

[192] Diese Gefahr ist in Art. 9 Abs. 1 lit. e DS-GVO grundsätzlich angelegt, soweit die Anforderungen an die Offensichtlichkeit nicht mit Blick auf die Ausdrücklichkeit i. S. d. Art. 9 Abs. 1 lit. a DS-GVO restriktiv ausgelegt wird.

[193] Liegen die Voraussetzungen des Art. 9 Abs. 1 lit. e DS-GVO vor, so sind diese besonders sensiblen personenbezogenen Daten im Grunde „vogelfrei". Insoweit greift – im Gegensatz zu Fällen der Einwilligung – der Grundsatz der Zweckbindung nicht und eine Begrenzung kommt allenfalls noch über den Grundsatz der Verarbeitung nach Treu und Glauben (Art. 5 Abs. 1 lit. a Var. 2 DS-GVO) in Betracht.

[194] Zur Herausforderung des Datenschutzrechts durch eine autonome, KI-basierte Datenverarbeitung sogleich unten c.

verhältnismäßig einfach zu erreichen. Allerdings ist es für das IoT prägend, dass es auf Sensoren und einer Steuerung durch Gesten, Mimik und Sprache beruht. Diese Entwicklung zur intuitiven und effizienten Steuerung verstärkt[195] die ubiquitären Datenverarbeitung im Alltag. Mit dem zunehmenden Ausmaß, in dem IoT-Anwendungen in Wirtschaft und Gesellschaft zum Einsatz kommen, treten – vom Verantwortlichen regelmäßig unbeabsichtigt – vermehrt Sachverhalte auf, in denen Sensoren besonders sensible personenbezogene Daten generieren, beispielsweise indem ein Datensubjekt in Gegenwart von Mikrophonen über Angelegenheiten spricht, die als besonders sensible personenbezogene Daten einem besonderen Schutz gemäß Art. 9 Abs. 1 DS-GVO unterfallen. Infolgedessen nehmen auch die datenschutzrechtlichen Herausforderungen zu.

Ein offensichtliches Beispiel hierfür ist eine Datenverarbeitung „bei Dritten".[196] Sofern eine Steuerung von Endgeräten mittels Gesten, Mimik und Sprachbefehlen im öffentlichen und privaten Bereich nicht grundsätzlich ausgeschlossen werden soll, setzt selbst ein Endgerät, das den Grundsatz der Datensparsamkeit (Art. 5 Abs. 1 lit. c DS-GVO) und die Anforderungen an den Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen (Art. 25 DS-GVO) umsetzt, ein gewisses Maß an Datenverarbeitung voraus, für die eine vorherige Einwilligung aller potenziell betroffenen Datensubjekte nicht oder nur unter objektiv unverhältnismäßigem Aufwand zu erreichen ist.[197]

Auf Grundlage eines tatsächlich vernünftigen Erwartungshorizonts ist es zunehmend realistisch, wenn Datensubjekte davon ausgehen, dass sie sich im Empfangsbereich von (potenziell) sprachgesteuerten Endgeräten aufhalten. Sofern die faktisch fortschreitende Durchdringung von privaten und öffentlichen Räumen durch die Entwicklung des sog. IoT rechtlich lediglich widergespiegelt und nicht rechtlich gesteuert werden soll,[198] könnten Äußerungen, die Datensubjekte spontan tätigen und die besonders sensible personenbezogene Daten generieren, unter Art. 9 Abs. 2 lit. e DS-GVO subsumiert werden: Im Ergebnis würden das bereits angeführte Zitat von *Eric Schmidt* und die ebenso berühmt-berüchtigte Aussage von *Scott McNealy*,[199] dem damaligen Vorstands-

---

[195] Zusätzlich existiert ein Wettlauf um die Erfassung von Daten, um hieraus Wissen zu generieren: *Labudde*, in: Ebers/Steinrötter (Hrsg.), Künstliche Intelligenz und smarte Robotik im IT-Sicherheitsrecht, 2021, S. 25 (35 f.).

[196] Ebenfalls zu diesem Anwendungsfall von Art. 6 Abs. 1 lit. f DS-GVO: *Hacker*, Datenprivatrecht, 2020, S. 283.

[197] Zu den hiermit im Zusammenhang stehenden Herausforderungen durch die Multi-Relationalität von Daten, oben B.II.

[198] Mit dem Vorschlag eines Rechts auf datenerhebungsfreie Produkte: *Becker*, JZ 2017, 170 ff.; sowie *ders.*, ZGE/IPJ 2017, 371 ff. Mit dem Vorschlag für einen datenerhebungsfreien Rückzugsraum: *Raue*, NJW 2019, 2425 (2426 f.).

[199] Zitiert nach: *Sprengers*, Sun on Privacy: ‚Get Over It', 26.01.1999 (https://www.wired.com/1999/01/sun-on-privacy-get-over-it/, zuletzt abgerufen am 19.05.2022).

vorsitzenden von *Sun Microsystems*, als rechtliche Realität anerkannt („*You have zero privacy anyway – Get over it!*").

Eine solche „Reaktion" der Judikative oder Legislative ginge jedoch mit einer evidenten Verletzung ihre Gewährleistungspflichten aus Art. 8 Abs. 1 und Art. 7 GRCh einher. Dies spricht dafür, dass spontane Äußerungen, die *tatsächlich* in der Hör- oder Sichtweite der Sensoren (Mikrophone, Kamera) eines IoT-Geräts erfolgen, *normativ* kein offensichtliches Öffentlichmachen im Sinne des Art. 9 Abs. 2 lit. e DS-GVO sein sollten. Mit anderen Worten: Die Gegenwart von sensorbasierten Endnutzergeräten sowohl im öffentlichen als auch privaten Raum führt nicht zur Öffentlichkeit i. S. d. Art. 9 Abs. 2 lit. e DS-GVO, weil diese Vorschrift auf einem gefährlichen Alles-oder-Nichts-Prinzip beruht und deshalb ungeeignet ist, soweit eine interessengerechte Lösung im Einzelfall ermöglicht werden soll. Der Begriff der Öffentlichkeit ist anthropozentrisch und mit dem Ziel einer Stärkung der informationellen Privatautonomie auszulegen. Er ist unabhängig davon, wie weit die gesellschaftliche Durchdringung mit IoT-Endnutzergeräten tatsächlich voranschreitet und ob die Betreiber der Endnutzergeräte eine tatsächliche Möglichkeit haben, diese Daten öffentlich zu machen.

Für die Prüfung, unter welchen Voraussetzungen die Verarbeitung von besonders sensiblen personenbezogenen Daten im Kontext des IoT rechtmäßig sein kann, liegt es im Ausgangspunkt nahe, an diejenigen Voraussetzungen anzuknüpfen, die für eine rechtmäßige Videoüberwachung im privaten Bereich gefordert werden.[200] Es dürfte weder zu vertretbaren Kosten noch tatsächlich möglich sein, vor Betreten eines bestimmten Bereichs stets auf den generellen Einsatz von Sensoren oder Kameras hinzuweisen und zusätzlich granulare Ausführungen zu den Verarbeitungszwecken zu geben. Deshalb scheidet eine unmissverständliche, informierte, freiwillige und ausdrückliche Einwilligung gemäß Art. 9 Abs. 1 lit. a i. V. m. Art. 4 Nr. 11 DS-GVO praktisch zumeist aus. Der aus Sicht einer Ermöglichung von informationeller Privatautonomie beste Mechanismus erscheint unrealistisch bzw. wäre mit unverhältnismäßigem Aufwand verbunden.

Weil eine spontane Offenbarung besonders sensibler Daten jedoch auch nicht als ausdrückliche Einwilligung in die Datenverarbeitung gewertet werden kann und eine konkludente Einwilligung mit dem Wortlaut des Art. 9 Abs. 2 lit. a DS-GVO nicht vereinbar ist, sind Konstellationen möglich, in denen es künftig auf eine qualifizierte Interessenabwägung ankommen wird, obwohl diese in Art. 9 Abs. 2 DS-GVO bislang nicht vorgesehen ist.

So ist es insbesondere für eine Identifikation des berechtigten Nutzers und zur Schonung anderer Datensubjekte sinnvoll, einen sehr kurzen automatisierten Sprachabgleich, einschließlich technisch erforderlicher Zwischenspeiche-

[200] Hierzu ausführlich: *Scholz*, in: Simitis/Hornung/Spiecker gen. Döhmann (Hrsg.), Datenschutzrecht, 2019, Anhang 1 zu Art. 6, Rn. 73 ff.

rung *auf dem Endgerät*, auf Grundlage einer Interessenabwägung zu ermöglichen. Anderenfalls würde eine Steuerung von IoT-Endgeräten durch Sprache, Gestik oder Mimik vielfach ausscheiden.[201]

Es entzieht sich aber regelmäßig der Sphäre des Verantwortlichen,[202] wenn er einen spontan geäußerten, aber dennoch besonders sensible Daten produzierenden Wortfetzen lediglich kurzzeitig auf dem Endgerät verarbeitet, um die für das Endgerät allein relevanten Befehle des berechtigten Nutzers herauszufiltern und anschließend rechtmäßig zu verarbeiten.[203] Nicht erforderlich wäre dagegen die langfristige Speicherung auf dem Endgerät oder sogar eine Übermittlung und Speicherung auf einem externen Speichermedium (Server), nachdem ein Abgleich mit den Stimmen der berechtigten Nutzer abgeschlossen wurde. Vielmehr sind die Daten unmittelbar nach Abgleich der Stimme gemäß Art. 17 Abs. 1 lit. a DS-GVO zu löschen.

Das Beispiel der Sprachsteuerung macht bereits deutlich, dass das rasant zunehmende Ausmaß und der technische Fortschritt des IoT erhebliche Interessenkonflikte verursacht, für deren Bewältigung es – neben einer verbesserten technischen Unterstützung zum Einwilligungsmanagement[204] – auch auf Interessenabwägungen ankommen wird.[205] Je „smarter" Endgeräte, Fortbewegungsmittel und die technische Ausstattung von Arbeitsstätten und Wohnraum, aber auch von öffentlichen Gebäuden werden, desto höher steigt – trotz des hier vertretenen Vorrangs der Einwilligung – der Druck, für die Erhebung von personenbezogenen, vor allem aber besonders sensiblen personenbezogenen Daten von Dritten (Gast, Mitfahrer, Arbeitnehmer) bzw. von den eigenen Kunden (Gastgeber, unmittelbarer Nutzer eines smarten Endgeräts) einen Interessenausgleich zu finden.[206]

Es ist tatsächlich und rechtlich ausgeschlossen, dass alle Datensubjekte dazu verpflichtet werden, sich mit einem Gerät auszustatten, das über standardisierte Schnittstellen ständig und überall die eigene Datenschutzpräferenz für eine

---

[201] Davon zu trennen ist die Frage, inwieweit eine Transkription der aufgenommenen Äußerungen für andere Zwecke rechtmäßig sein kann. Hierzu: Wissenschaftliche Dienste – Deutscher Bundestag, Zulässigkeit der Transkribierung und Auswertung von Mitschnitten der Sprachsoftware „Alexa" durch Amazon, WD 10 – 3000 – 032/19, Sachstand, 2019, S. 9.

[202] Auf die aus Sicht des Verantwortlichen bestehende Zufälligkeit des sensiblen Charakters von erfassten Videodaten abstellend: *EDSB*, Leitlinien zur Videoüberwachung, 2010, S. 33.

[203] Die Problematik der Multi-Relationalität der Daten bei ubiquitärer Datenverarbeitung gilt für besonders sensible personenbezogene Daten gleichermaßen: hierzu oben B.II.

[204] Hierzu unten Kapitel 6 B.

[205] Ebenso: *Hacker*, Datenprivatrecht, 2020, S. 312 (Nr. 11). Ebenso, jedoch ohne einen Vorrang der Einwilligung: *Leistner/Antoine/Sagstetter*, Big Data, 2021, S. 280.

[206] Weil regelmäßig der Anbieter eines smarten Endgeräts wie Alexa oder Echo und nicht der individuelle Kunde (beispielsweise der private Gastgeber, in dessen Wohnzimmer das Gerät steht), der Verantwortliche für die im Hintergrund ablaufenden Datenverarbeitungen ist, unterliegen diese Datenverarbeitungen nicht der Ausnahme für private und familiäre Datenverarbeitungen gemäß Art. 2 Abs. 2 lit. c DS-GVO

Vielzahl von Zwecken granular kundtut. Deshalb wird die Anwendung von Art. 6 Abs. 1 lit. f DS-GVO bzw. einer Interessenabwägung auch im Fall eines Verarbeitens von besonders sensiblen personenbezogenen Daten auf absehbare Zeit darüber entscheiden, welches *Mindestmaß* an Datenverarbeitungen ein Datensubjekt als Teil einer sozio-technischen Gesellschaft im Grundsatz akzeptieren muss.[207] Diesem Umstand muss Art. 9 Abs. 2 DS-GVO *de lege ferenda* Rechnung tragen, indem auch eine Interessenabwägung als Erlaubnistatbestand aufgenommen wird. Insbesondere ist diese Erweiterung des Art. 9 Abs. 2 DS-GVO transparenter als der alternative (Ausweich-)Vorschlag, wonach bereits der Begriff des besonders sensiblen personenbezogenen Datums in Art. 9 Abs. 1 DS-GVO durch das Hineinlesen einer zusätzlichen subjektiven Komponente, beispielsweise einer Verwendungsabsicht, reduziert werden soll.[208]

Deshalb ist es nach hier vertretener Auffassung unumgänglich, Art. 9 Abs. 2 DS-GVO um eine Ausnahme für die kurzzeitige automatisierte Verarbeitung von besonders sensiblen personenbezogenen Daten zu ergänzen, soweit diese Daten auf Spontanäußerungen des Datensubjekts beruhen. Infolgedessen werden Verantwortliche nicht mit den Risiken einer unrechtmäßigen Datenverarbeitung belastet, die nicht aus ihrer Verantwortungssphäre stammen, sofern der Verantwortliche diese Daten lediglich kurzzeitig verarbeitet, beispielsweise um die Nutzungsberechtigung des Sprechers bzw. des Handelnden (Gestik/Mimik) zu verifizieren.

c) Besonders sensible Daten als Trainingsdaten für ML

Eine zweite wesentliche Herausforderung für die informationelle Privatautonomie ist die bewusste und unbewusste Verarbeitung von besonders sensiblen personenbezogenen Daten im Kontext von sog. Künstlicher Intelligenz (KI). Insbesondere selbst-lernende Systeme als die derzeit vielversprechendste Ausprägung von KI ist auf große Mengen von Trainingsdaten angewiesen (1), darunter regelmäßig auch solche mit einem besonders sensiblen Personenbezug. Während der Einsatz des trainierten Algorithmus zur Verarbeitung von besonders sensiblen personenbezogenen Daten (*Anwendungsdaten*) gemäß Art. 9 Abs. 2 DS-GVO einer ausdrücklichen Einwilligung der Datensubjekte bedarf, weil die Anwendung regelmäßig unmittelbare Konsequenzen für die informationelle Privatautonomie des Datensubjekts hat, sollte die Verarbeitung von besonders sensiblen personenbezogenen Daten auf Grundlage einer Interessenabwägung rechtmäßig sein, soweit sie ausschließlich Trainingszwecken dient (*Trainingsdaten*) (2).

---

[207] Abweichendes gilt außerhalb des privaten und allgemein gesellschaftlichen Bereichs beispielsweise im Arbeitsverhältnis auf Grundlage von Art. 88 Abs. 2 DS-GVO i. V. m. § 87 Abs. 1 Nr. 6 BetrVG.

[208] Hierzu bereits oben a.

aa) Maschinelles Lernen: Trainieren statt Programmieren

Die derzeit aussichtsreichste Grundlage von KI[209] sind selbst-lernende Systeme (engl.: *machine-learning* oder kurz: ML)[210] und künstliche neuronale Netze (engl.: *artificial neuronal networks* oder kurz: „ANN").[211] Aktuell kommen insbesondere für das Profiling und die anschließende Personalisierung der Werbeansprache noch vorrangig automatisierte Datenverarbeitung auf Grundlage herkömmlicher Algorithmen zur Anwendung. Hiervon unterscheidet sich ML dadurch, dass es in der Lage ist, nicht nur die vom Programmierer vorgegebenen Programmregeln und Heuristiken auf bestimmte Datensammlungen anzuwenden. ML ist darüber hinaus fähig, selbst eigene Lösungen zu simulieren, die Wahrscheinlichkeit zu berechnen, mit der ein vorgegebenes Ziel erreicht wird und infolgedessen Datenverarbeitungsprozesse durchzuführen, die für den Programmierer nicht vorhersehbar und – insbesondere, wenn die zugrundeliegende Datenbasis dynamisch ist – nur schwer oder nicht nachvollziehbar sind (sog. black box).[212]

Das Trainieren von ML mündet in eine eigenständige Erkennung von Korrelationen, die keiner linearen Kette von jederzeit reproduzierbaren kausalen Bedingungen („wenn x, dann y") folgen.[213] Somit können lernfähige Systeme die Regeln, nach denen sie Daten analysieren, selbst entwickeln und infolgedessen in großen Datenbeständen Korrelationen und Muster identifizieren, die für eine programmierte Regel aufgrund der vielen potenziellen Zustandsräume zu komplex sind. Vereinfacht ausgedrückt, ist der bereits trainierte Algorithmus das durch ML entwickelte Instrument, um diese Korrelationen in großen Mengen von Anwendungsdaten erneut aufzufinden.

In Anlehnung an *Herbert Zech* kann man den Übergang von der automatisierten zur autonomen Datenverarbeitung prägnant zusammenfassen:[214] Bei

---

[209] *Russell/Norvig*, Artificial Intelligence: A Modern Approach (2nd ed.), 2003, S. 55; aus haftungsrechtlicher Perspektive: *Wagner*, Produkthaftung für autonome Systeme, AcP 217 (2017), 707 ff.; *Zech*, ZfPW 2019, 198 ff.; *ders.*, Gutachten für den 73. Deutschen Juristentag, 2020, A 39 ff.

[210] Zum maschinellen Lernen: *Ertel*, Grundkurs Künstliche Intelligenz, 2016, S. 191 ff.; *Sorge*, in: Hornung (Hrsg.), Rechtsfragen der Industrie 4.0, 2018, S. 139 (140 ff.); *Alpaydin*, Machine Learning, 2016.

[211] Hierzu instruktiv: *Flasiński*, Introduction to Artificial Intelligence, 2016, S. 157 ff.; *Kubat*, An Introduction to Machine Learning, 2017, S. 91 ff.; sowie *Lewis-Kraus*, The Great A.I. Awakening (https://www.nytimes.com/2016/12/14/magazine/the-great-ai-awakening.html, zuletzt abgerufen am 19.05.2022).

[212] Zur Unterscheidung von überwachtem und nicht überwachtem maschinellen Lernen: *Mainzer*, Künstliche Intelligenz – Wann übernehmen die Maschinen?, 2016, S. 115 ff.; *Kelleher/Tierney*, Data Science, 2018, S. 99 f.; *Ng/Soo*, Data Science – Was ist das eigentlich?, 2018, S. 8 ff.; *Sorge*, in: Hornung (Hrsg.), Rechtsfragen der Industrie 4.0, 2018, S. 139 (140 f.); *Yuan*, Lernende Roboter und Fahrlässigkeitsdelikt, RW 2018, 477 (485 ff.).

[213] *Kernow*, in: Calo/Froomkin/Kerr (Hrsg.), Robot Law, 2016, S. 51 (56 f./73); *Kurzweil*, The Age of Spiritual Machines, 1999.

[214] *Zech*, Gutachten für den 73. Deutschen Juristentag, 2020, A 31 ff.

einer autonomen Datenverarbeitung wird die exogene Programmierung durch ein endogenes Trainieren abgelöst.[215] Bislang finden autonome Datenverarbeitungen vorrangig im virtuellen Raum statt. Beispiel hierfür ist die Spracherkennung und ML-basierte Übersetzung in eine andere (Fremd-)Sprache.

Im Kontext von personenbezogenen Daten kommt ein Einsatz von bereits trainierten Algorithmen insbesondere in Betracht, um komplexe Entscheidungen vorzubereiten.[216] Beispielhafte Anwendungsszenarien[217] sind – neben der personalisierten Werbeansprache[218] – die personalisierte Gesundheitsvorsorge und die Erleichterung der Personalauswahl.[219] Aus datenschutzrechtlicher Perspektive geht die ML-basierte Analyse personenbezogener Daten regelmäßig mit einem Profiling gemäß Art. 4 Nr. 4 DS-GVO einher und erleichtert die Auswahl von attraktiven Vertragspartnern oder dient (potenziell) dazu, personalisierte oder zumindest kleinteilig stratifizierte Preise zu kalkulieren, wie sie für Kreditverträge (Laufzeit, Rate, Sollzins) – wenn auch ohne den Einsatz von ML – bereits seit Jahrhunderten praktiziert werden.[220]

Die Ziele des *Trainierens* dienen dazu, einen zweckgerichteten Algorithmus zu generieren. Dieser ist selbst zunächst abstrakt und ermöglicht potenziell das Auffinden von Korrelationen, führt aber erst durch seinen Einsatz zur Analyse von Anwendungsdaten zur gezielten Bewertung von konkreten Datensubjekten mit dem Ziel einer Entscheidungsfindung.[221] Dennoch weisen auch diese

---

[215] Allerdings sind hybride Datenanalysen für die Praxis derzeit besonders vielversprechend: *Zech*, Gutachten für den 73. Deutschen Juristentag, 2020, A 34/A 41.

[216] Ein Umkehrschluss aus Art. 22 Abs. 1 DS-GVO ergibt die Forderung nach einem menschlichen Letztentscheider („human in the loop").

[217] Bislang sind kaum Anwendungsfälle bekannt, in denen ML als Technik der automatisierten Entscheidungsfindung und -umsetzung zur Anwendung kommt. Sie dient bislang vorrangig zur Verbesserung der Entscheidungsgrundlage: *Gausling*, PinG 2019, 61 (70).

[218] *Perlich/Dalessandro/Raeder/Stitelman/Provost*, Mach Learn 95, 2014, 103 ff.

[219] Für weitere Beispiele mit geringem Personenbezug: *EU Kommission*, On Artificial Intelligence – A European approach to excellence and trust, Brüssel, 19. Februar 2020, https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf, zuletzt abgerufen am 19.05.2022; *Herpig*, Securing Artificial Intelligence, Oktober 2019, https://www.stiftung-nv.de/sites/default/files/securing_artificial_intelligence.pdf, zuletzt abgerufen am 19.05.2022.

[220] *BGH*, Urt. v. 28.01.2014 – VI ZR 156/13 = NJW 2014, 1235 (1237) – *Scorewerte*; Der Einsatzbereich von KI durch Unternehmen wie Zest AI (vormals: Zest Finance Inc.) und Lenddo liegt auf der Hand. Diese Unternehmen bewerten die Kreditwürdigkeit von solchen Personen, die mangels Bankkontos oder Vermögenswerten aus dem Raster klassischer Bonitätsprüfungen fallen. Grundlage dieser Bewertung ist angeblich eine Profilbildung anhand derjenigen personenbezogenen Daten, die der potenzielle Kreditnehmer in Kommunikationsnetzwerken wie *Facebook* hinterlassen hat und zu denen der Nutzer dem Unternehmen einen Zugang einräumt.

[221] Allerdings ist zu beachten, dass die Differenzierung zwischen Trainieren und Anwendung durch die technische Funktionsweise von besonders effizienter ML zunehmend aufgelöst wird. ML ist besonders effizient, wenn sie vollständig auf sog. Online-Lernen setzt und somit unmittelbar in ihrer Einsatzumgebung und parallel zur Anwendung fortlaufend (weiter-)trainiert wird (sog. ML-on-the-fly). Hierzu: *Herpig/Heinemeyer*, in: Ebers/Steinrötter

Trainingsdaten häufig einen Personenbezug auf und diese Personenbezüge sind notwendig, um zwischen möglichst vielen unterschiedlichen Personenbezügen Korrelationen herstellen zu können. Jedenfalls für einige gesellschaftlich erstrebenswerte Ziele kann ML gerade dann seine Stärken entfalten, wenn die Trainingsdaten nicht nur strenge Anforderungen an die Datenqualität, die Rückverfolgbarkeit und die Integrität erfüllen, sondern besonders umfangreich und die potenziellen Zustandsräume infolgedessen sehr komplex sind. Infolgedessen ist auch die Erzeugung von sog. synthetischen Daten, die keinen Bezug zu realen Datensubjekten aufweisen, nicht nur aufwendig, sondern geht regelmäßig mit reduzierten Lernerfolgen einher.

Das Risiko eines datenschutzrechtlichen Verstoßes durch ML ist deshalb besonders hoch, weil kaum zu verhindern ist, dass auch personenbezogene Daten schutzbedürftiger natürlicher Personen, insbesondere Daten von Kindern oder besonders sensible personenbezogene Daten verarbeitet werden, weil ML gerade darauf angewiesen ist, extrem große Mengen von Daten („volume") und damit regelmäßig Daten mit (multiplem) Personenbezug zu verarbeiten.[222] Kurzum: Das große technische, ökonomische und gesellschaftliche Potenzial und das große Risiko von ML (auch) für die Rechte und Freiheiten der Datensubjekte gehen Hand in Hand.

bb) Trainieren von ML auf Grundlage einer Interessenabwägung

Trainingsdaten sind eine wesentliche Voraussetzung für ML und werden in mehreren Phasen der Entwicklung verwendet. Sie sind die Basis dafür, dass ein ML-Modell erstmals trainiert werden kann. Zudem dienen sie dazu, den Algorithmus während der Trainingsphase zu validieren. Zuletzt sind sie erforderlich, um die praktische Einsatzbereitschaft des Algorithmus abschließend zu bewerten.[223]

Im Unterschied zu Anwendungsdaten dienen Trainingsdaten lediglich dazu, dasjenige Instrument zu entwickeln und stetig zu verbessern, das später dazu eingesetzt wird, um in den Anwendungsdaten relevante Muster wiederzufinden oder diese Daten nach vorgegebenen Mustern zu ordnen.

Für das Trainieren werden große Mengen von Daten benötigt, um Korrelationen ausfindig zu machen. Natürlich besteht die Möglichkeit, nur solche Daten

---

(Hrsg.), Künstliche Intelligenz und smarte Robotik im IT-Sicherheitsrecht, 2021, S. 65 (72). Sofern eine ausdrückliche Einwilligung nicht in Betracht kommt, würde die Möglichkeit einer Interessenabwägung ausschließlich für das Trainieren aber immerhin einen datenschutzrechtlich determinierten Anreiz zur klaren technischen und organisatorischen Trennung setzen.

[222] Hierzu bereits oben B.II.

[223] Mit der Illustration anhand einer „Lieferkette von ML": *Herpig/Heinemeyer*, in: Ebers/Steinrötter (Hrsg.), Künstliche Intelligenz und smarte Robotik im IT-Sicherheitsrecht, 2021, S. 65 (72 ff.).

zu verwenden, die keine besonders sensiblen Personenbezüge aufweisen. Je nach Zielsetzung der späteren Anwendung kann ein Personenbezug sogar völlig unerheblich sein. Weder die Analyse von Bildaufnahmen von Verkehrsschildern als eine Voraussetzung für autonomes Fahren noch eine Analyse der Bildaufnahmen von Krebs- und Tumorerkrankungen setzen einen Personenbezug dieser Bilder voraus. Die Identifizierbarkeit eines bestimmten Datensubjekts ist für das Training des Systems gerade nicht ausschlaggebend, sondern erst für die konkrete Anwendung des trainierten Systems. Deshalb folgt bereits aus dem Grundsatz der Datenminimierung (Art. 5 Abs. 1 lit. c DS-GVO) die Pflicht, diese Trainingsdaten zuvor zu anonymisieren.[224]

Weil eine solche vollständige vorherige Anonymisierung jedoch sehr aufwendig ist und eine Besonderheit des ML gerade darin besteht, auch dort Korrelationen herzustellen, wo sie für den menschlichen Verstand nicht oder nur sehr schwierig hergestellt werden können, existiert *stets* das Risiko, dass ein Trainieren mit großen Datenmengen eine Re-Identifizierung von konkreten Datensubjekten ermöglicht. Es wird bereits darüber spekuliert, dass die Unterscheidung zwischen anonymen und personenbezogenen Daten im Kontext von ML nicht mehr sinnvoll aufrecht zu erhalten ist.[225] Gleiches gilt dann jedoch auch für die Unterscheidung zwischen anonymen und besonders sensiblen personenbezogenen Daten. Aus praktischer Sicht liegt eine Vorgehensweise nahe, die auch Betreiber von Bio- und Genbanken in ihren Verarbeitungsprozessen zunehmend implementieren. Um die Risiken einer falschen Klassifikation eines Datensatzes als „anonym" zu verhindern, werden alle Daten so behandelt, als ob sie einen besonders sensiblen Personenbezug aufweisen würden.

Diese Fiktion kann auch für eine Datenverarbeitung durch ML sinnvoll sein, sofern eine Datenverarbeitung rechtssicher ausgestaltet werden soll. Allerdings schließt diese Vorgehensweise die Interessenabwägung als Grundlage für eine Verarbeitung *de lege lata* aus und macht aufwendige Verfahren und Maßnahmen erforderlich, um ein hohes Datenschutzniveau zu gewährleisten.[226] Die technischen Schwierigkeiten der Anonymisierung und die Unsicherheit über die tatsächliche Effektivität dieser Maßnahmen bietet – nach hier vertretener Auffassung – einen Grund dafür, zwar generell davon auszugehen, dass die Verarbeitung von besonders sensiblen personenbezogenen Daten gesteigerte Risiken für das Datensubjekt birgt, diese Verarbeitung aber dennoch auf Grundlage einer Interessenabwägung zuzulassen.

---

[224] Zur Frage, ob die Anonymisierung selbst eine Datenverarbeitung ist: *Hornung/Wagner*, ZD 2020, 223 ff.

[225] *Weichert*, ZD 2013, 251 (257); *Boehme-Neßler*, DuD 2016, 419 (422); *Specht,* GRUR Int. 2017, 1040 (1046); *Hornung/Wagner*, CR 2019, 565; *Leistner/Antoine/Sagstetter*, Big Data, 2021, S. 216 ff.

[226] Mit Blick auf die datenschutzrechtlichen Vorgaben für die Sicherheit der Datenverarbeitung: *Sattler*, in: Ebers/Steinrötter (Hrsg.), Künstliche Intelligenz und smarte Robotik im IT-Sicherheitsrecht, 2021, S. 197 (217 ff.).

Vier wesentliche Gründe sprechen dafür, dass auch die Datenverarbeitung von besonders sensiblen personenbezogenen Daten *de lege ferenda* auf Grundlage einer Interessenabwägung möglich sein sollte und als Beschränkung der informationellen Privatautonomie zu rechtfertigen ist,[227] sofern durch technische und organisatorische Maßnahmen sichergestellt ist, dass diese ausschließlich für Trainingszwecke erfolgt.

Erstens verfolgt der europäische Gesetzgeber mit der DS-GVO insgesamt und insbesondere im Kontext des Profiling einen Ansatz, der sich am jeweiligen Risiko der Verarbeitung für das Datensubjekt orientiert.[228] Dies spricht dafür, eine Datenverarbeitung im Trainingsumfeld großzügiger zu beurteilen als die anschließende Anwendung des trainierten Systems als Werkzeug für eine konkrete Entscheidungsfindung. Regelmäßig steigt erst durch den Einsatz des bereits trainierten Algorithmus das Risiko für individuelle Datensubjekte.

Zweitens dienen Trainingsdaten – anders als Anwendungsdaten – lediglich dazu, dasjenige Instrument zu entwickeln und stetig zu verbessern, das später dazu eingesetzt wird, in den Anwendungsdaten relevante Muster wiederzufinden oder diese Daten nach vorgegebenen Mustern zu ordnen und auf dieser Basis Entscheidungen über das Ob und das Wie der Werbeansprache oder über ein konkretes Vertragsangebot zu treffen oder die Analyse oder das Analyseergebnis als Dienstleistung anzubieten („AI as a Service“).

Obwohl die Identifizierbarkeit eines bestimmten Datensubjekts für das Training des Systems häufig nicht ausschlaggebend ist, weil das Ziel lediglich das Auffinden von Korrelationen und nicht die gezielte Vorbereitung einer konkreten Entscheidung gegenüber einem bestimmten Datensubjekt ist, können diese Personenbezüge in Trainingsdaten hilfreich sein, um zwischen möglichst vielen unterschiedlichen Personenbezügen Korrelationen herstellen zu können. Jedenfalls sofern die durch ML möglichen Innovationen über technische Analysen hinausgehen und auch der Analyse gesellschaftlicher Phänomene dienen soll, ist es überzeugend, das Training der ML zu erleichtern und eine solche Verarbeitung auf Grundlage einer Interessenabwägung zu ermöglichen.[229]

Drittens ist die grundsätzlich vorrangig einzuholende ausdrückliche Einwilligung im Zusammenhang mit dem Trainieren von ML wegen der benötigten Datenmenge und der zu Beginn schwer zu definierenden Verarbeitungszwecke regelmäßig unerreichbar oder jedenfalls unverhältnismäßig. Solange kein kon-

---

[227] Abgesehen von kollektiven Rechtschutzmechanismen bleiben dem individuellen Datensubjekt Ansprüche auf Information und die Möglichkeit zum Widerspruch.

[228] Dennoch wird gerade mit Blick auf KI eine grundlegende Neuorientierung des Datenschutzrechts gefordert, die das spezifische Bedrohungspotenzial der jeweiligen Verarbeitungskontexte stärker in den Blick nimmt: *Purtova*, Law, Innovation and Technology 10 (2018), 40 (79 f.); *Veil*, NVwZ 2018, 686 (692 ff.); *Martini/Hohmann*, NJW 2020, 3573 (3578).

[229] Diese Wertung findet sich ebenfalls in der Privilegierung der Verarbeitung von besonders sensiblen personenbezogenen Daten für die öffentliche wissenschaftliche Forschung in Art. 9 Abs. 1 lit. j DS-GVO und § 27 Abs. 1 S. 1 BDSG wieder.

kretes, in ein Verhalten (einschließlich Unterlassen) gegenüber einem Datensubjekt mündendes Profiling stattfindet, ist das Risiko für das individuelle Datensubjekt gering und die Einholung einer Einwilligung von allen betroffenen Datensubjekten ist entweder unerreichbar oder mit Blick auf den Zweck des Trainierens mit einem objektiv unzumutbaren Aufwand verbunden.

Nach hier vertretener Auffassung genügt es für die Annahme einer Unverhältnismäßigkeit, dass eine Kontaktaufnahme zu den Datensubjekten den Personenbezug der Daten erst herstellt oder erweitert und damit die Risiken für die Datensubjekte zusätzlich erhöht. Es ist nicht im Interesse eines risikoorientierten Datenschutzes, wenn personenbezogene Trainingsdaten zusätzlich in einzelne Datensätze unterteilt, kategorisiert und mit einer Möglichkeit zur Kontaktaufnahme zum jeweiligen Datensubjekt versehen werden. Durch ein solches Hinzuspeichern der Kontaktdaten der Datensubjekte als Voraussetzung für die Einholung einer ausdrücklichen Einwilligung erhöht sich das Risiko der Datenverarbeitung für die Datensubjekte unnötig. Diese Wertung lässt sich auch Art. 11 Abs. 1 DS-GVO entnehmen.[230]

Überdies ist die Einholung der Einwilligung regelmäßig unverhältnismäßig, soweit die Verarbeitung der Trainingsdaten gerade nicht darauf abzielt, konkrete Entscheidungen gegenüber individuellen Datensubjekten zu ermöglichen, sondern lediglich der Entwicklung eines Instruments dient, das erst im Anschluss in seine Einsatzumgebung überführt wird.

Viertens spricht auch ein Blick auf die derzeitigen Quellen von personenbezogenen Trainingsdaten[231] dafür, das bloße Trainieren von ML mit besonders sensiblen personenbezogenen Daten auf Grundlage einer Interessenabwägung im Grundsatz zu ermöglichen. Zwar können Verbraucherdaten, beispielsweise *Clickstreams* und der *Browser*-Verlauf, von (Entwickler-)Plattformen, kommerziellen Einrichtungen und Forschungsinstituten bezogen werden.[232] Allerdings ist es für viele Unternehmen kaum möglich oder mit unverhältnismäßigen Kosten verbunden, sofern sie wirksame ausdrückliche Einwilligung der Datensubjekte für die mit ML verfolgten Zwecke kontinuierlich verifizieren müssen. Insofern würde die Forderung nach einer lückenlos überprüfbaren Einwilligung in die Verarbeitung der Daten für ein ML-Training gerade die Position derjenigen Verantwortlichen verschlechtern, die über keinen eigenen stabilen Zugang zu großen Datenmengen verfügen. Im Gegensatz dazu befinden sich

---

[230] Hiernach sind Verantwortliche nicht verpflichtet, *zusätzliche* personenbezogene Daten zu verarbeiten, soweit diese ausschließlich dazu dienen würden, um die Vorgaben der DS-GVO einzuhalten. Die datenschutzrechtlichen Pflichten des Verantwortlichen sollen nicht die Risiken für Datensubjekte erhöhen, indem infolgedessen zusätzliche personenbezogene Daten verarbeitet werden.

[231] Vgl. *Badr*, Top Sources For Machine Learning Datasets, 13. Januar 2019, https://towardsdatascience.com/top-sources-for-machine-learning-datasets-bb6d0dc3378b.

[232] *Herpig/Heinemeyer*, in: Ebers/Steinrötter (Hrsg.), Künstliche Intelligenz und smarte Robotik im IT-Sicherheitsrecht, 2021, S. 65 (73).

diejenigen Unternehmen erneut im Vorteil, die – wie beispielsweise *GAFAM* und *BAT*[233]– selbst über einen direkten und dynamischen technischen Zugang zu den *Clickstreams* und zu dem *Browser*-Verlauf ihrer unzähligen Kunden verfügen (sog. *data pipeline*).[234]

II. Herausforderung: Gefahr eines Unterlaufens der Einwilligung

Neben dem Nachteil, dass Art. 6 Abs. 1 lit. f DS-GVO mit einer erheblichen Rechtsunsicherheit einhergeht und der Anwendungsbereich der Interessenabwägung paradoxerweise sowohl potenziell zu weit (Direktwerbung in Werbenetzwerken) als auch zu eng ist (keine Interessenabwägung für Verarbeitung von besonders sensiblen personenbezogenen Daten), liegt ein wesentlicher Nachteil darin, dass die vagen Voraussetzungen der Interessenabwägung und die Rechtsunsicherheit einen Anreiz dafür setzen, die Voraussetzungen der Einwilligung zu unterlaufen.

Gemäß Art. 4 Nr. 11 i. V. m. Art. 7 DS-GVO erfordert eine Einwilligung eine *informierte*, *unmissverständliche* und – sofern besonders sensible personenbezogene Daten betroffen sind – eine *ausdrückliche* Willensbekundung des Datensubjekts, die zudem *freiwillig* sein muss (Art. 7 Abs. 4 DS-GVO) und im Grundsatz jederzeit und grundlos *widerruflich* ist (Art. 7 Abs. 3 S. 1 DS-GVO).[235] Die vergleichsweise detaillierten Anforderungen an eine Einwilligung haben zur Folge, dass die Einwilligung meist so gestaltet wird, dass sie getrennt von anderen Erklärungen zu erteilen ist, regelmäßig in einem zweistufigen Verfahren (sog. *Double Opt-In*) eingeholt und anschließend gesondert dokumentiert wird.

Zudem fordert Art. 4 Nr. 11 DS-GVO eine eindeutig bestätigende Handlung für eine wirksame Einwilligung. Ein Schweigen von Datensubjekten kann keine einwilligende Wirkung entfalten, vgl. ErwG 32 S. 3 DS-GVO.[236]

---

[233] Beispielsweise *GAFAM* und *BAT* wäre eine Berufung auf diese Interessenabwägung erschwert, soweit sie über einen direkten Kontakt zu Datensubjekten verfügen und es ihnen deshalb relativ leicht möglich wäre, eine ausdrückliche Einwilligung der Datensubjekte in die Verarbeitung besonderes sensibler personenbezogener Daten für das Trainieren von ML einzuholen. Für die Zumutbarkeit der Einholung einer Einwilligung darf es insbesondere keine Rolle spielen, dass an eine Einwilligung gegenüber marktmächtigen Verantwortliche nach hier vertretener Auffassung strengere Anforderungen zu stellen sind: Kapitel 5 C.II.1 und III.2.a.

[234] Das Outsourcing von Speicherkapazitäten als Teil von Cloud-Diensten, ist neben dem sog. Tracking das wichtigste Instrument, um Zugang zu wertvollen Trainings- (und Anwendungsdaten) zu erhalten: *Murgia*, NHS trusts sign first deals with Google. Contracts with five trusts to share patient data are part of transfer of DeepMind, 19.09.2019 (https://www.ft.com/content/641e0d84-da21-11e9-8f9b-77216ebe1f17, zuletzt abgerufen am 19.05.2022).

[235] Zu den einzelnen Voraussetzungen: Kapitel 4 A.II.

[236] Zudem kann dem Schweigen eines Verbrauchers gegenüber einem Unternehmer kein

Die Interessenabwägung ist im Vergleich hierzu ein stiller Erlaubnistatbestand. Im Anwendungsbereich des Art. 6 Abs. 1 lit. f DS-GVO ist der Verantwortliche gerade nicht auf eine Mitwirkung des Datensubjekts angewiesen. Vielmehr handelt es sich bei der Interessenabwägung zunächst um einen internen Vorgang des Verantwortlichen. Er muss lediglich über seine berechtigten Interessen (Art. 13 Abs. 1 lit. d bzw. Art. 14 Abs. 2 lit. b DS-GVO) und das bestehende Widerspruchsrecht informieren (Art. 21 Abs. 4 DS-GVO), die berechtigten Interessen des Datensubjekts berücksichtigen und diese mit seinen eigenen berechtigten Interessen – bis an die Grenze eines *non liquet* – abwägen.

Anders als die in informierter Weise erteilte Einwilligung des Datensubjekts kann die Interessenabwägung gemäß Art. 6 Abs. 1 lit. f DS-GVO – trotz der bestehenden Informationspflichten – vergleichsweise leicht in der Datenschutzerklärung „versteckt" werden, ohne infolgedessen stets am AGB-rechtlichen Transparenzgebot zu scheitern. Zudem dürften an die Pflicht zur Information über das Widerspruchsrecht aus Art. 21 Abs. 4 DS-GVO regelmäßig geringere Anforderungen gestellt werden als an die Pflicht zur Information über das Widerrufsrecht gemäß Art. 13 Abs. 2 lit. c und Art. 7 Abs. 3 S. 3 DS-GVO. Infolgedessen ist den Datensubjekten das Widerspruchsrecht regelmäßig weniger bekannt, als das Recht zum Einwilligungswiderruf, auf das in unmittelbarem Zusammenhang mit der – häufig ausdrücklich[237] – erteilten Einwilligung hinzuweisen ist.

Wenngleich eine allzu optimistische Interessenabwägung durch den Verantwortlichen das Risiko eines hohen Bußgelds birgt, bietet eine Datenverarbeitung auf Grundlage von Art. 6 Abs. 1 lit. f DS-GVO aus Sicht des Verantwortlichen dennoch einige Vorteile gegenüber der viel detaillierter und restriktiver ausgestalteten Einwilligung. Da keinerlei Willensbekundung des Datensubjekts erforderlich ist, unterliegt die Interessenabwägung – jedenfalls im Ausgangspunkt – auch nicht einer Prüfung der Freiwilligkeit, einschließlich des sog. Kopplungsverbots gemäß Art. 7 Abs. 4 DS-GVO.[238]

---

vertraglich bindender Erklärungsgehalt entnommen werden, so dass auch Art. 6 Abs. 1 lit. b DS-GVO (vertragsakzessorische Datenverarbeitung) als Grundlage ausscheidet. Vgl. den Rechtsgedanken aus § 241a BGB. Gegenausnahmen, in denen dem Schweigen die Fiktion einer Vertragsannahme auslöst: § 516 Abs. 2 BGB. Ausnahmsweise eine positive Erklärungsbedeutung zugeschrieben wird: § 416 Abs. 1 S. 2 BGB. Zum Schweigen als Billigung und damit Eintritt einer aufschiebenden Bedingung: § 455 S. 2 BGB. Zum Rechtsverkehr zwischen Kaufleuten: §§ 362 Abs. 1 S. 2, 75h, 91a HGB. Hierzu: *Medicus/Petersen*, Bürgerliches Recht – AT, 11. Aufl. 2016, Rn. 387 ff.

[237] Anders als die bloße Information über eine Verarbeitung gemäß Art. 6 Abs. 1 lit.f DS-GVO im Rahmen von AGB, kann eine Einwilligung nicht lediglich passiv erfolgen ErwG 43 DS-GVO; sowie zu Art. 15 Abs. 3 ePrivacy-RL: *EuGH*, Urt. v. 01.10.2019, C-673/17 = GRUR 2019, 1198 – *Planet 49*; sowie im Anschluss hieran für § 5 Abs. 3 TMG: *BGH*, Urt. v. 28.05.2020 – I ZR 7/16 = GRUR 2020, 891 – *Cookie Einwilligung II*.

[238] Für eine direkte Berücksichtigung von Art. 7 Abs. 4 DS-GVO i. R. v. Art. 6 Abs. 1 lit. f DS-GVO: *Hacker*, Datenprivatrecht, 2020, S. 281; hierzu oben: C.I.2.b.aa.

Nach hier vertretener Auffassung ist zwar der Einwilligungswiderruf gemäß Art. 7 Abs. 3 S. 1 DS-GVO als gleichzeitiger Widerspruch gegen eine Fortsetzung der identischen Datenverarbeitung für den identischen Zweck auszulegen.[239] Dennoch kann diese Synchronisierung der beiden Erlaubnistatbestände nicht verhindern, dass der Verantwortliche, der einen Widerruf der Einwilligung fürchtet, von vornherein umfassend auf Art. 6 Abs. 1 lit. f DS-GVO setzt, um gar nicht erst auf eine widerrufliche Einwilligung zurückgreifen zu müssen.

Weil auch das Recht des Datensubjekts auf Datenportabilität gemäß Art. 20 Abs. 1 lit. a DS-GVO nur dann zur Anwendung kommt, wenn die Datenverarbeitung auf einer Einwilligung beruht (Art. 6 Abs. 1 lit. a DS-GVO) oder vertragsakzessorisch erfolgt (Art. 6 Abs. 1 lit. b DS-GVO), besteht aus Perspektive des Verantwortlichen ein weiterer Anreiz dafür, die für ihn belastenden Folgen der Datenportabilität zu vermeiden, indem er versucht, die Daten auf Grundlage von Art. 6 Abs. 1 lit. f DS-GVO zu verarbeiten.

Kurzum: Die Gefahr, dass über Art. 6 Abs. 1 lit. f DS-GVO die Anforderungen an eine Einwilligung und die Rechtsfolgen des Einwilligungswiderrufs unterlaufen werden können,[240] ist nach hier vertretener Auffassung dadurch zu begrenzen, dass der Einwilligung ein Vorrang einzuräumen ist.[241] Die Nichteinholung der Einwilligung obwohl diese mit Blick auf den Verarbeitungszweck mit einem verhältnismäßigen Aufwand möglich wäre, ist deshalb ein wesentlicher Aspekt, der in die Beurteilung der Interessenabwägung gemäß Art. 6 Abs. 1 lit. f DS-GVO zulasten des Verantwortlichen einfließen sollte.

III. Herausforderung: Geringere faktische Kontrolldichte

Im Vergleich zur Einwilligung (lit. a) und zur vertragsakzessorischen Datenverarbeitung (lit. b) unterliegt die Interessenabwägung gemäß Art. 6 Abs. 1 lit. f DS-GVO faktisch einer geringeren externen Kontrolle.[242] Dies hat mehrere Gründe.

---

[239] Hierzu oben: A.IV.2.; zur Umsetzung in einem Kontroll-Cockpit: Kapitel 6 B.II.2.a.

[240] In seiner Entschließung zum Bewertungsbericht der EU-Kommission spricht das Europäische Parlament lediglich unspezifisch von der Sorge, „dass das ‚berechtigte Interesse' sehr häufig missbräuchlich als Rechtsgrundlage für die Verarbeitung genannt wird", *Entschließung des EU-Parlaments* v. 25.03.2021 zu dem Bewertungsbericht der Kommission über die Durchführung der Datenschutz-Grundverordnung zwei Jahre nach Beginn ihrer Anwendung, 2020/2717(RSP) Nr. 7.

[241] A. A. *Simitis*, NJW 1998, 2472 (2476); *Radlanski*, Das Konzept der Einwilligung in der datenschutzrechtlichen Realität, 2016, S. 205; *Härting*, CR 2016, 735 (739); *Engeler*, ZD 2018, 55 (56); *Peitz/Schweitzer*, NJW 2018, 275 (277); *Veil*, NVwZ 2018, 686 (688); *Leistner/Antoine/Sagstetter*, Big Data, 2021, S. 248 f.

[242] Dies ist deshalb besonders riskant, weil privatwirtschaftlich organisierte Verantwortliche es gerade und im Gegensatz zu Behörden nicht gewohnt sind, ihre eigenen Interessen mit denjenigen des Datensubjekts in einer fast schizophrenen Weise abzuwägen. Auf die Gefahr

Wie gerade ausgeführt, handelt es sich bei der Interessenabwägung im Ausgangspunkt um einen internen Vorgang des Verantwortlichen, über dessen Existenz, Ergebnis und Begründung das Datensubjekt allenfalls nachträglich potenziell etwas erfährt (Art. 13 Abs. 1 lit. d bzw. Art. 14 Abs. 2 lit. b DS-GVO) und dann hiergegen Widerspruch erheben kann (*Opt-Out*). Diese Situation ist mit einer Datenverarbeitung auf Grundlage einer informierten Einwilligung bereits deshalb nicht vergleichbar, weil den Datensubjekten i. R. v. Art. 6 Abs. 1 lit. f DS-GVO gar nicht erst vor Augen geführt wird, dass sie eine Wahlmöglichkeit haben. Im Fall der Einwilligung und des Einwilligungswiderrufs hat das Datensubjekt zumindest eine realistische Chance, die Datenverarbeitung wahrzunehmen und diese kritisch zu hinterfragen. Art. 6 Abs. 1 lit. f DS-GVO ist im Vergleich dazu ein stiller Tatbestand, so dass jedenfalls die Datensubjekte selbst zunächst keine Veranlassung haben dürften, eine Datenverarbeitung auf Grundlage von Art. 6 Abs. 1 lit. f DS-GVO kritisch zu hinterfragen oder sie einer gerichtlichen Überprüfung zuzuführen.

Auch im Vergleich zu Art. 6 Abs. 1 lit. b DS-GVO ist eine Datenverarbeitung auf Grundlage einer Interessenabwägung insoweit weniger transparent, weil Art. 6 Abs. 1 lit. b DS-GVO – nach hier vertretener und noch zu begründender Auffassung – restriktiv auszulegen ist,[243] so dass dieser Erlaubnistatbestand nur für untergeordnete Datenverarbeitungen und nicht für eine Kommerzialisierung von personenbezogenen Daten als vertragliche Haupt- oder Gegenleistung in Betracht kommt. Somit können auf Grundlage von Art. 6 Abs. 1 lit. b DS-GVO nur solche Datenverarbeitungen rechtmäßig sein, die für jedes Datensubjekt eine logische und vernünftigerweise zu erwartende Konsequenz des geschlossenen Vertrags und damit zumindest Gegenstand eines sachgedanklichen Mitbewusstseins des Datensubjekts bei Vertragsschluss sind.[244]

Hinzu kommt, dass Datensubjekte, die Verbraucher sind, selbst bei Zweifeln an der Rechtsmäßigkeit der Datenverarbeitung kaum eine Veranlassung haben, diese gerichtlich überprüfen zu lassen. Eine Kombination aus rationaler Apathie und den für das einzelne Datensubjekt regelmäßig nur sehr geringen materiellen und immateriellen Schäden (sog. Streuschäden) führt dazu, dass eine Kontrolle der Rechtmäßigkeit von Datenverarbeitungen regelmäßig auf die Initiative einer Aufsichtsbehörde oder auf die Klageerhebung eines aktivlegiti-

---

einer strukturellen, eigene Interessen bevorzugenden Neigung (bias) des Verantwortlichen hinweisend: *Hoffmann-Riem*, Innovation und Recht, 2016, S. 726.

[243] Hierzu unten Kapitel 3 D.

[244] Für ein anderes Verständnis, das Art. 6 Abs. 1 lit. b DS-GVO als zentralen oder zumindest neben der Einwilligung gleichberechtigten Erlaubnistatbestand ansieht: *Hacker*, Datenprivatrecht, 2020, S. 397 ff. Folgt man diesem Verständnis ist es konsequent, die wesentlichen Anforderungen an die Einwilligung entweder auf Art. 6 Abs. 1 lit. b DS-GVO analog anzuwenden oder einen vergleichbaren Schutz der Datensubjekte mithilfe vertragsrechtlicher Abstützungen – insbesondere im Rahmen einer AGB-Kontrolle – zu versuchen: *Hacker*, Datenprivatrecht, 2020, S. 541 ff. Zu den Nachteilen dieses Ansatzes: Kapitel 3 C.I.

mierten Verbandes zurückgeht.[245] Aus Sicht des Otto-Normal-Datensubjekts ist es sogar dann rational, sich apathisch zu verhalten, wenn es der Datenverarbeitung widersprochen hat, ein Verantwortlicher die Fortsetzung der Datenverarbeitung aber mit zwingenden Gründen legitimiert. Insoweit besteht durchaus das Risiko, dass es – abgesehen von Prozessen, die durch Datenschutz-Aktivisten oder Verbraucherschutzverbände initiiert werden – nur sehr selten zu einer gerichtlichen Kontrolle der Abwägungsvorgänge gemäß Art. 6 Abs. 1 lit. f und Art. 21 Abs. 1 S. 2 DS-GVO kommen wird. Ein individuelles Vorgehen durch Datensubjekte kommt – bislang[246] – regelmäßig nur in Betracht, sofern ein Datensubjekt entweder das „Hobby Datenschutz" betreibt oder die gerichtliche Auseinandersetzung – wie (wohl) im Fall von *Maximilian Schrems* – zumindest auch als politisches und gesellschaftliches Engagement versteht.

Weil Art. 6 Abs. 1 lit. f DS-GVO *de lege lata* nicht für eine Verarbeitung von besonders sensiblen personenbezogenen Daten herangezogen werden kann[247] und eine Interessenabwägung regelmäßig auch nicht für Geschäftsmodelle in Betracht kommt, die auf einer umfassenden Verwertung personenbezogener Daten beruhen, ist es verständlich, dass sowohl die Aufsichtsbehörden als auch Verbraucherverbände ihr Augenmerk stärker auf solche Datenverarbeitungsprozesse richten, die intensiver in den Schutz personenbezogener Daten und die Privatsphäre eingreifen und die – insbesondere bei besonders sensiblen Daten – grundsätzlich auf eine ausdrückliche Einwilligung des Datensubjekts angewiesen sind.

Infolgedessen ist die Kontrolldichte für Datenverarbeitungen auf Grundlage von Art. 6 Abs. 1 lit. f DS-GVO grundsätzlich geringer, es sei denn, solche Unternehmen berufen sich auf diese Rechtsgrundlage, deren erfolgreiche Geschäftsmodelle maßgeblich auf der Verwertung von personenbezogenen Daten basieren.[248] Infolgedessen besteht das Risiko, dass Datenverarbeitungen, die auf Art. 6 Abs. 1 lit. f DS-GVO gestützt werden, nur selten einer behördlichen oder gerichtlichen Kontrolle unterzogen werden, sofern diese nicht durch Unternehmen erfolgen, die faktisch – wie *GAFAM* – unter ständiger Aufsicht und öffentlicher Beobachtung stehen.

---

[245] Zur teilweisen Abhilfe eines Durchsetzungsdefizits durch die Möglichkeit von Verbandklagen nach DS-GVO und UWG: *Ohly*, GRUR 2019, 686 (688); *Köhler*, WRP 2018, 1269 (1275 f.).

[246] Bislang haben sich deutsche Gerichte mit der Zuerkennung eines immateriellen Schadensersatzes zurückgehalten. Sie setzen insoweit die Leitlinien fort, die bislang für ein Schmerzensgeld bei Verletzung von Persönlichkeitsrechten entwickelt wurden. Ansprüche auf Schadensersatz gemäß Art. 82 DS-GVO scheiterten regelmäßig an einer ungeschriebenen Bagatellschwelle. Hierzu zuletzt: *LG Karlsruhe*, Urt. v. 09.02.2021, Az 4 O 67/20. Das BVerfG hatte diese Rechtsansicht zuvor allerdings dem EuGH vorgelegt: *BVerfG*, Beschl. v. 14.01.2021, 1 BvR 2853/19.

[247] Zur Notwendigkeit einer Erweiterung oben: C.I.3.b. und c.

[248] *EuGH*, Urt. v. 01.10.2019, C-673/17 = GRUR 2019, 1198 – *Planet 49*. Im Anschluss hieran: *BGH*, Urt. v. 28.05.2020, I ZR 7/16 = GRUR 2020, 891 – *Cookie Einwilligung II*.

D. Fazit: Funktion als Schrittmacher

Aus der privatrechtlichen Perspektive einer abgestützten informationellen Privatautonomie sollte Art. 6 Abs. 1 lit. f DS-GVO auf die Funktion als Auffangtatbestand und Schrittmacher beschränkt werden.

Dies entspricht der Tatsache, dass Art. 6 Abs. 1 lit. f DS-GVO als Generalklausel ausgestaltet wurde. Leider ist es dem europäischen Gesetzgeber nicht gelungen, diesen weiten Tatbestand durch Regelbeispiele oder wenigstens Kriterien für seine Anwendung zu konkretisieren. Infolgedessen bleibt diese Aufgabe nun dem *EuGH* überlassen und soweit es diesem nicht gelingt, einer Reform der DS-GVO vorbehalten.

Zunächst steht die Judikative vor der Herausforderung, anhand von Art. 6 Abs. 1 lit. f DS-GVO verlässliche Typisierungen herauszubilden.[249] Nur wenn die nationalen Gerichte dem *EuGH* Auslegungsfragen zu Art. 6 Abs. 1 lit. f DS-GVO im Lichte der maßgeblichen Unionsgrundrechte vorlegen,[250] hat dieser überhaupt eine Möglichkeit, harmonisierend auf die nationale Anwendung dieses Auffangtatbestands einzuwirken.

Selbst für den Fall, dass den *EuGH* solche Vorlageverfahren erreichen[251] und diese den *EuGH* nicht überlasten, ist das Verfahren gemäß Art. 267 AEUV für eine einheitliche und unionsweite Herausbildung von Fallgruppen schlecht geeignet, weil der *EuGH* allenfalls Fragen zur unions(grund)rechtskonformen Auslegung und diese regelmäßig nur abstrakt beantworten kann.[252] Je nach künftiger Auslegung des Art. 6 Abs. 1 lit. f DS-GVO durch die nationalen Gerichte, hat die Interessenabwägung das Potenzial entweder zum Inkubator oder zum Hemmschuh neuer datengetriebener Geschäftsmodelle zu werden.[253]

Im Vergleich zu Art. 6 Abs. 1 lit. f DS-GVO sind die Voraussetzungen der Einwilligung gemäß Art. 6 Abs. 1 lit. aA, Art. 4 Nr. 11, Art. 7 ff. DS-GVO uni-

---

[249] Dies ist besonders ärgerlich, wenn man bedenkt, dass die §§ 28, 28a, 30a BDSG a. F. spezifischere Anforderungen an eine Interessenabwägung kannten als der aktuelle Art. 6 Abs. 1 lit. f DS-GVO. Hierzu: *Buchner/Petri*, in: Kühling/Buchner (Hrsg.), DS-GVO/BDSG, 3. Aufl. 2020, Art. 6, Rn. 145.

[250] Zum lediglich funktionalen Spielraum der nationalen Gerichte bei der Anwendung von Art. 6 Abs. 1 lit. f DS-GVO: *Marsch*, Das Europäische Datenschutzgrundrecht, 2018, S. 352 ff./361 ff.

[251] Aktuell: *OLG Düsseldorf*, Vorlagebeschl. v. 24.03.2021 – Kart 2/19 (V), GRUR-RS 2021 8370 Rn. 54 ff.

[252] Noch zurückhaltend: *EuGH*, Urt. v. 20.05.2003, verb. C-465/00 u. a. (Rn. 84 ff.) – *Österreichischer Rundfunk*; *EuGH*, Urt. v. 06.11.2003, C-101/01 = EuZW 2004, 245 (Rn. 85 ff.) – *Lindqvist*. Dagegen mit abschließender Interessenabwägung: *EuGH*, Rs. C-131/12 = NJW 2014, 2257 – *Google Spain*; hierzu: *Marsch*, Das Europäische Datenschutzgrundrecht, 2018, S. 368 („Es ist jedoch schon aus Gründen knapper Ressourcen davon auszugehen, dass der EuGH nicht zu jeder Konstellation einer Interessenabwägung im Datenschutzrecht Stellung nehmen wird").

[253] *Sattler*, in: Ochs/Friedewald/Hess/Lamla (Hrsg.), Die Zukunft der Datenökonomie, 2019, S. 215 (240).

onsweit detailliert vorgegeben. Auch deshalb sollte eine Interessenabwägung nur subsidiär zur Einwilligung in Betracht kommen, um das Ziel des freien Verkehrs personenbezogener Daten im Binnenmarkt i. S. d. Art. 1 Abs. 3 DS-GVO nicht zu gefährden.

Diese Subsidiarität von Art. 6 Abs. 1 lit. f DS-GVO gegenüber der Einwilligung beruht auf der Grundannahme, dass die unter einem vertretbaren Aufwand zu erreichende Willensbekundung eines Datensubjekts zur Förderung der informationellen Privatautonomie vorzugswürdig ist. Zudem setzt diese Subsidiarität einen Anreiz für Verantwortliche, Datensubjekte frühzeitig – insbesondere in Form von Personal Information Management Systemen (PIMS) und Einwilligungsassistenten – einzubeziehen.[254]

Darüber hinaus legt die Interessenabwägung die Entscheidungshoheit zunächst in die Hände des Verantwortlichen. Trotz der Möglichkeit, die eigene Entscheidungszuständigkeit – in den Grenzen des Art. 21 Abs. 1 S. 2 DS-GVO – durch einen Widerspruch weitgehend herstellen zu können und obwohl der offene Tatbestand des Art. 6 Abs. 1 lit. f DS-GVO es zulässt, die strengeren Anforderungen an eine Einwilligung, insbesondere an die Freiwilligkeit gemäß Art. 7 Abs. 4 DS-GVO auch im Rahmen der Interessenabwägung mittelbar zu berücksichtigen, bleibt die Datenverarbeitung auf Grundlage von Art. 6 Abs. 1 lit. f DS-GVO im Ausgangspunkt eine heteronome Entscheidung, an der das Datensubjekt selbst nicht beteiligt ist.[255]

Dies spricht dafür, Art. 6 Abs. 1 lit. f DS-GVO insbesondere dann restriktiv anzuwenden, wenn eine unmittelbare Kommerzialisierung der personenbezogenen Daten im Zentrum der Datenverarbeitung steht. Deshalb ist das derzeit ubiquitäre *tracking* von Datensubjekten, das anschließende Profiling und das darauf basierende Angebot an Werbekunden, für diese personalisierte Werbung an die Datensubjekte auszuspielen, keine gemäß Art. 6 Abs. 1 lit. f DS-GVO rechtmäßige Datenverarbeitung. Soweit Art. 21 Abs. 2 und ErwG 47 S. 7 DS-GVO die *Direktwerbung* ausdrücklich als berechtigtes Interesse anerkennen, ist dieser Begriff aufgrund der grundlegend veränderten technologischen Möglichkeiten seit der erstmaligen Verwendung des Begriffs in der ePrivacy-RL (2002) restriktiv auszulegen.

Eine personalisierte Direktwerbung auf Grundlage von Profiling sollte nur gemäß Art. 6 Abs. 1 lit. f DS-GVO rechtmäßig sein, soweit diese Datenverarbeitung ausschließlich innerhalb der bestehenden Kundenbeziehung zwischen dem Verantwortlichen und dem Datensubjekt erfolgt und ähnliche Produkte des Verantwortlichen beworben werden. Die Datenverarbeitungen, die insbesondere im Rahmen der Werbenetzwerke von *GAFAM* durchgeführt werden,

---

[254] Unten Kapitel 6 B. sowie zuletzt § 26 TDDSG.

[255] *Sattler*, in: Lohsse/Schulze/Staudenmayer (Hrsg.), Data as Counter-Performance – Contract Law 2.0, 2020, S. 225 (242 f.).

können nicht auf Grundlage von Art. 6 Abs. 1 lit. f DS-GVO erfolgen, selbst wenn das Datensubjekt zu allen am Werbenetzwerk beteiligten Unternehmen jeweils eine Kundenbeziehung unterhält.

Während die Datenverarbeitungen auf Grundlage einer Interessenabwägung – bei (zu) weiter Auslegung des Begriffs der Direktwerbung – potenziell zu umfangreich gerät, ist der Anwendungsbereich der Interessenabwägung andererseits zu eng ausgefallen, soweit besonders sensible personenbezogene Daten verarbeitet werden. Obwohl der Schutz von Datensubjekten in gesteigertem Maße erforderlich ist, sofern Daten i. S. d. Art. 9 Abs. 1 DS-GVO verarbeitet werden, hat der Verantwortliche es selbst nicht immer in der Hand, ob er Daten dieser Kategorie verarbeitet.

Die Entwicklungen des IoT – insbesondere die Steuerung durch Sprache, Gestik und Mimik – und die potenziellen Innovationen auf Grundlage von ML sprechen dafür, dass in Zukunft auch eine Verarbeitung von besonders sensiblen personenbezogenen Daten auf Grundlage einer Interessenabwägung möglich sein sollte. Die Erfahrungen des deutschen Gesetzgebers mit dem BDSG a. F. lehren, dass zusätzliche spezifische Erlaubnistatbestände – beispielweise für eine IoT-Berechtigungs-Verifikation oder ein Trainieren von ML – ebenfalls möglich wären, aber keine technikneutrale Generalklausel ersetzen können.[256]

Mit hier vertretener Auffassung sollte die Interessenabwägung im Privatrechtsverhältnis auf die Funktion eines Schrittmachers reduziert werden. Dies ermöglicht es und dient ausdrücklich dazu, der Einwilligung einen Vorrang einzuräumen.[257] Infolgedessen kommt eine Einwilligung im Privatrechtsverhältnis nur dann nicht in Betracht, wenn eine solche unerreichbar ist oder ihre Einholung mit Blick auf den legitimen Zweck, die Anzahl der lediglich peripher betroffenen Datensubjekte, die Art und den Umfang der Verarbeitung objektiv unverhältnismäßig ist.

Zur Klarstellung: Es liegt kein Fall der Unerreichbarkeit oder Unverhältnismäßigkeit vor, nur weil Datensubjekte die Einwilligung grundsätzlich oder in der Hoffnung auf eine bessere (Gegen-)Leistung des Verantwortlichen verweigern. Vielmehr ist jedenfalls die ausdrückliche Einwilligungsverweigerung zugleich als Widerspruchserklärung gegen eine identische Datenverarbeitung auf Grundlage von Art. 6 Abs. 1 lit. f DS-GVO auszulegen, so dass eine anschließende Datenverarbeitung – neben Art. 6 Abs. 1 lit. c und lit. d DS-GVO – nur

---

[256] Hierzu oben: B.I.

[257] Daraus folgt zudem die Notwendigkeit, die Voraussetzungen dafür zu verbessern, dass die Einwilligung nicht nur formell, sondern auch materiell als Grundlage für eine informationelle Privatautonomie dienen kann, hierzu: unten Kapitel 5 C.II. und C.III. sowie Kapitel 6; a. A. (wohl) *Leistner/Antoine/Sagstetter*, Big Data, 2021, S. 247 („Muss der *speziellste Erlaubnistatbestand* Anwendung finden" [Hervorhebung im Original]). Sie plädieren jedoch an anderer Stelle für eine Stärkung der Einwilligung: „Eine rechtliche und praktische *Ertüchtigung der Einwilligung* in die Datennutzung […] de lege lata und de lege ferenda wäre hier der transparentere, direktere Weg" [Hervorhebung im Original]).

beim Nachweis zwingender Gründe i. S. d. Art. 21 Abs. 1 S. 2 DS-GVO in Betracht kommt.[258]

Nur sofern man den Willen von Menschen entweder geringschätzt oder ihnen keine Erfahrungs- und Lernerfolge zutraut, liegt es nahe, Art. 6 Abs. 1 lit. f DS-GVO einen weiten Anwendungsbereich einzuräumen. Zugespitzt formuliert: Abgesehen von der hier vertretenen Anwendung im Fall der Unerreichbarkeit oder Unverhältnismäßigkeit der Einholung einer Einwilligung ist eine großzügige Anwendung von Art. 6 Abs. 1 lit. f DS-GVO nur dann konsequent, sofern man davon überzeugt ist, dass Datenschutzbehörden und Gerichte die (mutmaßlichen) Präferenzen von Datensubjekten besser kennen, als die Datensubjekte selbst.

[258] Oben: A.IV.2. sowie Kapitel 6 B.II.2.a.

3. Kapitel

Entlastungsfunktion der vertragsakzessorischen Datenverarbeitung

Sofern die voraussetzungsarme Generalklausel der Interessenabwägung eng ausgelegt wird, führt dies zwar zu einem – mit Blick auf die informationelle Privatautonomie erstrebenswerten – Vorrang der Einwilligung. Zugleich erhöht diese Auslegung jedoch das Interesse der Verantwortlichen daran, die Einwilligung zu vermeiden und eine Datenverarbeitung stattdessen auf Grundlage von Art. 6 Abs. 1 lit. b DS-GVO durchführen zu können. Aus Sicht der Verantwortlichen könnten auch auf diesem Weg die strengeren datenschutzrechtlichen Anforderungen an eine wirksame Einwilligung vermieden werden.[1]

Gemäß Art. 6 Abs. 1 lit. b DS-GVO ist die Datenverarbeitung rechtmäßig, soweit sie für die Erfüllung eines Vertrags mit dem Datensubjekt erforderlich ist. Infolgedessen kann Art. 6 Abs. 1 lit. b DS-GVO als gesetzlicher, aber vertragsakzessorischer Erlaubnistatbestand bezeichnet werden. Er knüpft an die Willenserklärung des Datensubjekts an, die zum Abschluss eines Vertrags geführt hat oder zumindest an die vorvertragliche Kontaktaufnahme durch das Datensubjekt.[2]

Bei unreflektierter Lesart liegt es nahe, Art. 6 Abs. 1 lit. b DS-GVO als große Öffnungsklausel der DS-GVO für das nationale Schuldrecht zu verstehen. Zwar ist eine Datenverarbeitung gemäß Art. 6 Abs. 1 lit. b DS-GVO gerade nur rechtmäßig, soweit sie für die Erfüllung eines Vertrags auch erforderlich ist. Allerdings könnte dieser unionsautonome Begriff der Erforderlichkeit von den jeweiligen vertraglichen Leistungsbestimmungen abhängig sein und stünde infolgedessen – in den Grenzen, die das jeweilige nationale Recht einem Vertrag setzt – mittelbar zur Disposition der Vereinbarung zwischen Verantwortlichem und Datensubjekt. Diese Ansicht wird von *Facebook*[3] vertreten und sowohl vom

---

[1] Diese Strategie verfolgt *Facebook*. Der ÖOGH hat die Abgrenzung zwischen Art. 6 Abs. 1 lit. a und lit. b DS-GVO im Fall des Facebook-Nutzungsvertrags nun dem EuGH vorgelegt: *ÖOGH*, Vorlagebeschl. v. 22.07.2021, 6 Ob 56/21k – *Schrems [III]* (Vorlagefrage 1 Rn. 8 ff.).

[2] Nach dem eindeutigen Wortlaut bietet Art. 6 Abs. 1 lit. b DS-GVO keine Rechtsgrundlage für eine nachvertragliche Datenverarbeitung, so dass es hierfür auf eine konkludente Einwilligung (Art. 6 Abs. 1 lit. a DS-GVO) ggfs. durch ergänzende Vertragsauslegung oder eine Interessenabwägung (Art. 6 Abs. 1 lit. f DS-GVO) ankommt.

[3] *BKartA*, BeckRS 2019, 4895 Rn. 635 und 642 – *Facebook*. Kritisch dazu: *Buchner*, WRP 2019, 1243 (1246 f.).

LG Wien als auch vom *OLG Wien*[4] einstweilen – bis zur Entscheidung des *EuGH* über den Vorlagebeschluss des *ÖOGH*[5] – geteilt.[6]

Auf den zweiten Blick ist es jedoch komplizierter. Zwar öffnet Art. 6 Abs. 1 lit. b die DS-GVO im Grundsatz für das gesamte jeweilige nationale Vertragsrecht. Damit ist aber noch nicht entschieden, ob und wie sich die sonstigen Anforderungen und Grundsätze der DS-GVO auf die Auslegung und Anwendung des nationalen Schuldrechts auswirken können und müssen. Darüber hinaus bedarf es keiner großen Vorstellungskraft um vorherzusehen, dass die detaillierten Anforderungen der DS-GVO an eine wirksame Einwilligung leicht auf Grundlage des nationalen Schuldrechts ausgehebelt werden könnten, wenn ein Verantwortlicher stattdessen einen transparenten zweiseitigen Schenkungsvertrag anbietet, in dem der Verantwortliche sich zur Bereitstellung von „kostenlosen" digitalen Produkten und das Datensubjekt zum „kostenlosen" Zugang zu personenbezogenen Daten verpflichtet.[7] Dies verdeutlicht, dass der Anwendungsbereich des Art. 6 Abs. 1 lit. b DS-GVO nur dann sinnvoll bestimmt werden kann, wenn die jeweiligen Konsequenzen für die anderen Erlaubnistatbestände der DS-GVO berücksichtigt werden.

Kurzum: Das Verhältnis zwischen der DS-GVO und dem nationalen, nur teilweise harmonisierten Schuldrecht ist deutlich komplizierter, als es der (zu) schlichte Wortlaut des Art. 6 Abs. 1 lit. b DS-GVO suggeriert (A). Obwohl eine weite Anwendbarkeit von Art. 6 Abs. 1 lit. b DS-GVO eine Datenverarbeitung auf den ersten Blick durchaus erleichtert (B), wird schnell deutlich, dass die Anwendung des Art. 6 Abs. 1 lit. b DS-GVO regelmäßig in einer AGB-Kontrolle mündet, in deren Zentrum jedoch die – durch die Judikative nicht zu be-

---

[4] *OLG Wien*, Urt. v. 07.12.2020 (nicht rechtskräftig), GZ 11 R 153/20f, 11 R 154/20b-99 S. 28: „Insbesondere ist es legitim, dass ein marktwirtschaftlich operierendes Unternehmen, das für bestimmte Dienstleistungen kein Geld verrechnet, im Rahmen der Gesetze auf anders geartete Finanzierungsquellen zurückgreift. […] Denn nur diese Datenverwertung ermöglicht maßgeschneiderte Werbung, die das von der Beklagten *geschuldete ‚personalisierte Erlebnis'* in wesentlichem Maße prägt und der Beklagten zugleich die für den Aufrechterhaltung der Plattform *und die Erzielung eines Gewinns* notwendigen Einkünfte *verschafft*. Diese Datenverarbeitung ist daher für die Vertragserfüllung ‚erforderlich' iSd Art 6 Abs. 1 lit. b DSGVO" [Hervorhebung durch den Verfasser]. Sh. auch die Zusammenfassung der Prozessgeschichte: *ÖOGH*, Vorlagebeschl. v. 22.07.2021, 6 Ob 56/21k – *Schrems* [III] (Rn. 44 ff.).

[5] *ÖOGH*, Vorlagebeschl. v. 22.07.2021, 6 Ob 56/21k – *Schrems* [*III*].

[6] Hierzu ausführlich unten C.III.3.

[7] Es liegt nahe, diese Gestaltung im B2C-Verhältnis als Umgehung des Anwendungsbereichs gemäß Art. 3 Abs. 1 Hs. 2 DID-RL zu werten. Möglicherweise wollte der deutsche Gesetzgeber diese Umgehungsmöglichkeit durch § 516a Abs. 1 BGB verhindern. Hiernach finden die Vorschriften des §§ 327 ff. BGB auch dann Anwendung, wenn ein Unternehmer einem Verbraucher „digitale Produkte schenkt", und der Verbraucher dem Unternehmer personenbezogene Daten bereitstellt oder sich hierzu verpflichtet. Warum in diesem Fall einer Gegenleistung des Verbrauchers überhaupt eine Schenkung des Unternehmers vorliegen soll, bleibt das Geheimnis des Gesetzgebers. Skeptisch auch: *Spindler*, MMR 2021, 528 (533); *Rosenkranz*, ZUM 2021, 195 (204).

wältigende – Beurteilung der Angemessenheit des vertraglichen Synallagmas steht.

Im Ergebnis überwiegen die Nachteile, sofern die Vereinbarung von personenbezogenen Daten als vertragliche Haupt- bzw. Gegenleistung am Maßstab von Art. 6 Abs. 1 lit. b DS-GVO zu messen ist (C). Dies spricht nach hier vertretener Auffassung für eine restriktive Auslegung von Art. 6 Abs. 1 lit. b DS-GVO. Sein Anwendungsbereich wird dadurch so stark eingeschränkt, dass sich seine Funktion darin erschöpft, den Einwilligungstatbestand und damit zugleich die Datensubjekte zu entlasten, so dass letztere ihre kognitiven Ressourcen und intellektuellen Fähigkeiten auf die für den Schutz der personenbezogenen Daten und der Privatsphäre wichtigeren Datenverarbeitungen konzentrieren können, deren Rechtmäßigkeit gerade von einer Einwilligung abhängig ist (D).

A. Komplexes Verhältnis zum nationalen Schuldrecht

Legt man den Erlaubnistatbestand aus Art. 6 Abs. 1 lit. b DS-GVO – beispielsweise mit *Philipp Hacker* – weit aus, dann muss die Rechtmäßigkeit derjenigen Geschäftsmodelle, die – wie beispielsweise die Nutzung des Netzwerks von *Facebook*[8] – auf einer umfangreichen Verarbeitung personenbezogener Daten beruht, anhand des jeweiligen nationalen Schuldrechts erfolgen. Während der Begriff der Erforderlichkeit ein unionsautonom zu bestimmendes Tatbestandsmerkmal des Art. 6 Abs. 1 lit. b DS-GVO ist, definiert das jeweilige rechtsgeschäftliche Schuldverhältnis, welche Leistungspflichten bestehen und infolgedessen erfüllt werden müssen. Hierfür sind im Ausgangspunkt jedoch das nationale Schuldrecht und die darin jeweils vorgesehenen Vertragstypen maßgeblich.

Infolgedessen eröffnet eine weite Auslegung der vertragsakzessorischen Datenverarbeitung gemäß Art. 6 Abs. 1 lit. b DS-GVO eine verflochtene Wechselwirkung im europäischen Mehrebenensystem. Das nationale Schuldrecht ist maßgeblich für die Beurteilung, welche Leistungspflichten vertraglich wirksam vereinbart werden können. Die unionsrechtsautonome Auslegung der Erforderlichkeit i. S. d. Art. 6 Abs. 1 lit. b DS-GVO entscheidet darüber, ob die vereinbarten Leistungen in eine *vertragsakzessorische* rechtmäßige Datenverarbeitung münden. Weil die DS-GVO in ihrem Anwendungsbereich Vorrang genießt, müssten die nationalen Gerichte bei Anwendung des – lediglich teilweise harmonisierten – nationalen Schuldrechts eine extrem komplexe Prüfung vornehmen.[9]

---

[8] So vertritt Facebook die Ansicht, dass ihre Datenverarbeitung weitgehend für die Erfüllung des *Facebook*-Nutzungsvertrags erforderlich ist: dieser Ansicht – als Instanzengericht – folgend: *OLG Wien*, Urt. v. 07.12.2020 (nicht rechtskräftig), GZ 11 R 153/20f, 11 R 154/20b-99 S. 27 f.). Hierzu: *ÖOGH*, Vorlagebeschl. v. 22.07.2021, 6 Ob 56/21k – *Schrems* [III] (Vorlagefrage 1 Rn. 8 ff.).

[9] Für diese Herangehensweise: *Hacker*, Datenprivatrecht, 2020, S. 397 ff.

Diese komplexe Wechselwirkung im europäischen Mehrebenensystem beruht auf dem Vorrang des Unionsrechts, der sich über die Vertragsakzessorietät der Datenverarbeitung gemäß Art. 6 Abs. 1 lit. b DS-GVO auch auf die Anwendung des nationalen Schuldrechts auswirkt. Diese Wechselwirkung setzt nach *Philipp Hacker* die Prüfung voraus,

„ob auf unionsrechtlicher Ebene (Anwendungsvorrang) oder im Rahmen eines speziellen Rechtsgebiets (Sachintegration) ein bestimmtes Risiko eine abschließende Regelung dergestalt erfahren hat, dass alle Eventualitäten berücksichtigt werden sollten. Sofern eine mitgliedsstaatliche Regelung ein eigenständiges Risiko adressiert (Risikospezifizität), und im Rahmen des Anwendungsvorrangs zudem mit den Zielsetzungen des Unionsrechts vereinbar ist (Zielkompatibilität), kann sie neben der DS-GVO Anwendung finden".[10]

Diese (hyper-)komplexe Vorgehensweise, (hypothetisch) angewandt durch hunderte nationale Gerichte und Datenschutzbehörden der EU-Mitgliedstaaten, dürfte die binnenmarktorientierte Anpassung des Datenschutzrechts für den privatrechtlichen Bereich grundlegend gefährden.

Weil die DS-GVO auch dann unmittelbar und direkt anwendbar bleibt, wenn eine Datenverarbeitung auf Grundlage von Art. 6 Abs. 1 lit. b DS-GVO erfolgen soll, steht es den Gerichten und den nationalen Datenschutzbehörden, die über die Rechtmäßigkeit einer vertragsakzessorischen Datenverarbeitung entscheiden bzw. die Aufsicht ausüben, gerade nicht frei, blindlings das nationale Schuldrecht auf einen Vertrag zwischen Datensubjekt und Verantwortlichem anzuwenden.[11] Insbesondere gelten die allgemeinen Grundsätze der rechtmäßigen Datenverarbeitung gemäß Art. 5 Abs. 1 DS-GVO für jede Datenverarbeitung und damit unabhängig davon, welcher Erlaubnistatbestand des Art. 6 Abs. 1 DS-GVO herangezogen wird.

Somit können die Gesetzgeber und Gerichte der Mitgliedstaaten kein autonomes Datenschuldrecht entwickeln und die Datenverarbeitung anschließend mit Hilfe von Art. 6 Abs. 1 lit. b DS-GVO als rechtmäßig beurteilen.[12] Diesen Weg hatten allerdings das *LG Wien* und *OLG Wien* eingeschlagen, ohne das Problem der Wechselwirkung zwischen Art. 6 Abs. 1 lit. b DS-GVO und dem

---

[10] *Hacker*, Datenprivatrecht, 2020, S. 538.

[11] So zur Doppelfunktion des Art. 6 Abs. 1 lit. b DS-GVO: *Wendehorst/v. Westphalen*, NJW 2016, 3745 (3749); *Steinmetz*, Die Kontrollsperre des § 307 Abs. 3 BGB bei Verträgen über immaterielle Gegenstände, demnächst, S. 297.

[12] Dagegen aus einer vertragsrechtlichen Perspektive: *Steinmetz*, Die Kontrollsperre des § 307 Abs. 3 BGB bei Verträgen über immaterielle Gegenstände, demnächst, S. 298 f. („Das Datenschutzrecht ‚spiegelt' mit Art. 6 Abs. 1 lit. b DS-GVO indes nur eine vertragsrechtliche Situation im Rahmen der Zulässigkeit der Datenverarbeitung wider, so dass es nach hier vertretener Auffassung näher läge, das durch das Vertragsrecht geschaffene ‚Problem' der Ausweitung der Leistungspflichten auch im Rahmen des Vertragsrechts selbst zu lösen. Sowohl die datenschutzrechtliche Erforderlichkeit als auch der vertragscharakteristische Hauptgegenstand beurteilen sich maßgeblich anhand des mit der jeweiligen Vereinbarung verfolgten Zwecks. Aus diesem Grund entsteht ein gewisser Gleichlauf der Beurteilungskriterien").

nationalen Schuldrecht anzusprechen.[13] Der *ÖOHG* hat Zweifel an dieser Rechtsansicht der Instanzengerichte zu Art. 6 Abs. 1 lit. b DS-GVO. Er hat das Verfahren (auch) deshalb ausgesetzt und dem *EuGH* u. a. die Frage vorgelegt, ob eine Datenverarbeitung durch *Facebook* auf Grundlage des Nutzungsvertrags i. V. m. Art. 6 Abs. 1 lit. b DS-GVO erfolgen kann, oder ob eine Einwilligung der Datensubjekte gemäß Art. 6 Abs. 1 lit. a DS-GVO erforderlich ist.[14]

Unabhängig davon, dass zunächst die jeweiligen Anwendungsbereiche der einzelnen Erlaubnistatbestände des Art. 6 Abs. 1 DS-GVO klarer voneinander abgegrenzt werden müssen, könnten die nationalen Gerichte das Vorlageverfahren gemäß Art. 267 Abs. 2 bzw. Abs. 3 AEUV auch nutzen, um eine unionsrechtskonforme Auslegung und Anwendung der nationalen privatrechtlichen Regelungen – beispielsweise von § 307 Abs. 2, Abs. 3 BGB oder § 138 BGB[15] zu erreichen.[16] Infolgedessen steht aus methodischer Perspektive und vermittelt über ein mehrstufiges Verfahren, ein Weg durch das komplexe Mehrebenensystem aus europäischem Datenschutz- und (teilharmonisierten) nationalem Schuldrecht zur Verfügung.

Zudem stehen den Gerichten mit dem Grundsatz der Verhältnismäßigkeit und dem Grundsatz einer Datenverarbeitung nach Treu und Glauben zwei flexible Instrumente zur Verfügung. Weil die Voraussetzung der Erforderlichkeit in Art. 6 Abs. 1 lit. b DS-GVO ausdrücklich genannt ist[17] und der Grundsatz einer Verarbeitung nach Treu und Glauben in Art. 5 Abs. 1 lit. a Var. 2 DS-GVO geregelt wurde, sind beide Instrumente zudem vom jeweiligen nationalen Schuldrecht unabhängig und damit unionsautonom.

Auf dieser Grundlage könnte die Beurteilung eines Vertrags über die Verwertung von personenbezogenen Daten als synallagmatischer Leistungsgegenstand auch dann noch korrigiert werden, wenn das nationale Recht hiervon – beispielsweise gemäß § 307 Abs. 3 BGB Abstand nimmt – und einen solchen atypischen Vertrag als wirksam anerkennt. Dennoch begründet ein solcher Lösungsweg über Art. 6 Abs. 1 lit. b DS-GVO neben wenigen Erleichterungen für eine rechtmäßige Datenverarbeitung (B) vor allem gravierende Herausforderungen (C).

---

[13] Indem es nach Ansicht des *OLG Wien* für ein Profiling für personalisierte Werbung durch *Facebook* nicht auf eine Einwilligung, sondern es für deren Rechtmäßigkeit auf ein, in der „österreichischen Rechtsordnung nicht ausdrücklich geregeltes, also atypisches Schuldverhältnis" ankommt, wird die Einheitlichkeit und damit der freie Verkehr personenbezogener Daten im EU-Binnenmarkt gefährdet, *OLG Wien*, Urt. v. 07.12.2020, GZ 11 R 153/20f, 11 R 154/20b-99 S. 27 f.

[14] So die Vorlagefrage 1: *ÖOGH*, Vorlagebeschl. v. 22.07.2021, 6 Ob 56/21k – *Schrems* [*III*].

[15] Hierzu: *Hacker*, Datenprivatrecht, 2020, S. 541 f.

[16] *EDSA*, Leitlinien 2/2019 zur Verarbeitung personenbezogener Daten gemäß Artikel 6 Absatz 1 Buchstabe b DSGVO, Version 2.0, 08.10.2019, Rn. 23. (abrufbar unter: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-22019-processing-personal-data-under-article-61b_de, zuletzt abgerufen am 19.05.2022).

[17] Hierzu: *Hacker*, Datenprivatrecht, 2020, S. 262 ff.

B. Erleichterungen durch eine vertragsakzessorische Datenverarbeitung

Zu den Vorteilen einer Öffnung der DS-GVO für Verträge auf Grundlage des nationalen Schuldrechts zählt insbesondere die Möglichkeit zum Experimentieren. Weil die tatsächlichen Entwicklungen im Bereich der Verwertung von personenbezogenen Daten sehr dynamisch sind, könnten mit Hilfe der unterschiedlichen Beurteilungen durch nationale Gerichte auf Grundlage des jeweils nationalen Schuldrechts – eine systematische Auswertung der mitgliedstaatlichen Rechtsprechung vorausgesetzt – verschiedene Lösungsansätze getestet werden. Art. 6 Abs. 1 lit. b DS-GVO wäre der Ausgangspunkt eines flexiblen und dezentralen gerichtlichen Entdeckungsverfahrens (I).

Zudem bietet eine Datenverarbeitung, deren Rechtmäßigkeit von den zwischen Verantwortlichem und Datensubjekt vereinbarten Vertragsbedingungen abhängt, das Potenzial, einer Differenzierung zum Durchbruch zu verhelfen, die in der DS-GVO fehlt. Die Relevanz des nationalen Schuldrechts würde es ermöglichen, besser danach zu unterscheiden, ob ein Datensubjekt als Unternehmer oder als Otto-Normal-Datensubjekt und damit in der Eigenschaft als Verbraucher handelt (II).

I. Nationales Schuldrecht als Entdeckungsverfahren

Ein wesentlicher Vorteil einer weiten Auslegung von Art. 6 Abs. 1 lit. b DS-GVO ist augenfällig. Die Geschäftsmodelle, die (auch) auf einer Verwertung von personenbezogenen Daten beruhen, sind technologisch getrieben, nehmen derzeit sehr dynamisch zu und weisen im Detail große Unterschiede auf. Je größer die Dynamik der Lebenssachverhalte ist, desto wichtiger ist es aus rechtlicher Perspektive, flexible Reaktionsmöglichkeit vorzuhalten. Infolgedessen kann das Recht seiner Steuerungsfunktion nachkommen, ohne neue Geschäftsmodelle bereits *ex ante* mit prohibitiven Verhaltenskosten zu belegen.

Generalklauseln sind eine bewährte Möglichkeit, um auf eine solche tatsächliche Dynamik zur reagieren. Die Interessenabwägung gemäß Art. 6 Abs. 1 lit. f DS-GVO könnte – wie bereits im vorausgegangenen Kapitel ausgeführt – eine solche Schrittmacherfunktion grundsätzlich ausfüllen. Allerdings wurde im vorherigen Kapitel bereits herausgearbeitet, warum eine Interessenabwägung aus Sicht eines entwicklungsoffenen Experimentierens zwei wesentliche Nachteile hat. Obwohl die nationalen Datenschutzbehörden und Gerichte die Interessenabwägung – im Streitfall – selbst vornehmen, wenden sie dennoch Unionsrecht an und haben bei Zweifeln an der unionsrechtskonformen Anwendung und Auslegung die Möglichkeit (Art. 267 Abs. 1 AEUV) bzw. die Pflicht (Art. 267 Abs. 3 AEUV) entscheidungserhebliche Auslegungsfragen dem *EuGH* vorzu-

legen. Hat der *EuGH* einmal über die unionsrechtlich richtige Auslegung von Art. 6 Abs. 1 lit. f DS-GVO entschieden, so engt diese auch die nationalen Gerichte und Behörden insoweit ein.

Im Unterschied zur Interessenabwägung bietet Art. 6 Abs. 1 lit. b DS-GVO den Gerichten und Behörden der Mitgliedstaaten die Möglichkeit, durch die Anwendung des jeweiligen – allenfalls teilweise harmonisierten – nationalen Schuldrechts zunächst selbst den Spielraum für eine Verarbeitung von personenbezogenen Daten abzustecken. Welche Datenverarbeitung erforderlich ist, um einen Vertrag zu erfüllen, hängt stark davon ab, welche vertragstypologische Einordnung die nationalen Gerichte auf Grundlage des nationalen Schuldrechts vornehmen. Beispielsweise beurteilte das *OLG Wien* die Datenverarbeitung durch *Facebook* (jetzt: *Meta Platforms*) – einschließlich der Datenverarbeitung für ein Profiling für personalisierte Werbung – als erforderlich für die Erfüllung eines in der „österreichischen Rechtsordnung nicht ausdrücklich geregelte[n], also atypische[n], Schuldverhältnis[es]“.[18]

Weil dieser nationale Spielraum im B2C-Bereich insbesondere durch die Klausel-RL,[19] die DID-RL,[20] die Warenkauf-RL[21] und die Verbraucherrechte-RL[22] und sowohl im B2C als auch B2B durch die Voraussetzung der Erforderlichkeit gemäß Art. 6 Abs. 1 lit. b DS-GVO und den Grundsatz der Datenverarbeitung nach Treu und Glauben gemäß Art. 5 Abs. 1 lit. a Var. 2 DS-GVO begrenzt wird, bestehen zudem wichtige unionsrechtliche Planken innerhalb derer sich die nationale Rechtsprechung und Datenschutzaufsicht halten muss.

Zudem hat Art. 6 Abs. 1 lit. b DS-GVO gegenüber der Interessenabwägung den Vorteil, dass das Datensubjekt immerhin Vertragspartei ist und für den

---

[18] Das *OLG Wien* prüfte den Nutzungsvertrag von Facebook anschließend anhand von § 879 Abs. 1 ABGB auf einen Verstoß gegen die guten Sitten und eine AGB-Kontrolle anhand des auf Art. 5 Klausel-RL beruhenden und deshalb europaweit harmonisierten Transparenzgebots gemäß § 864a ABGB (inhaltlich überraschende Klausel und formelle Einhaltung des Transparenzgebots): *OLG Wien*, Urt. v. 07.12.2020, GZ 11 R 153/20f, 11 R 154/20b-99 S. 27 f. (nicht rechtskräftig). Der *ÖOGH* hat Zweifel an der Anwendbarkeit von Art. 6 Abs. 1 lit. b DS-GVO und hat die Abgrenzung zwischen Art. 6 Abs. 1 lit. a und lit. b DS-GVO im Fall eines solchen Nutzungsvertrags nun dem EuGH vorgelegt: *ÖOGH*, Vorlagebeschl. v. 22.07. 2021, 6 Ob 56/21k – *Schrems* [*III*] (Vorlagefrage 1 Rn. 8 ff.).

[19] Richtlinie 93/13/EWG v. 05.04.1993 über missbräuchliche Klauseln in Verbraucherverträgen, ABl. v. 21.04.1993, L 95, S. 29 ff., zuletzt geändert durch Richtlinie 2011/83/EU v. 25.10. 2011, ABl. v. 22.11.2011, L 304, S. 64 ff.

[20] Richtlinie (EU) 2019/770 über bestimmte vertragsrechtliche Aspekte der Bereitstellung digitaler Inhalte und digitaler Dienstleistungen vom 20.05.2019, ABl. v. 22.05.2019, L 136, S. 1 ff.

[21] Richtlinie (EU) 2019/771 über bestimmte vertragsrechtliche Aspekte des Warenkaufs, zur Änderung der Verordnung (EU) 2017/2394 und der Richtlinie 2009/22/EG sowie zur Aufhebung der Richtlinie 1999/44/EG vom 20.05.2019, ABl. v. 22.05.2019, L 136, S. 28 ff.

[22] Richtlinie (EU) 2019/2126 v. 27.11.2019 zur Änderung der Richtlinie 93/13/EWG des Rates und der Richtlinien 98/6/EG, 2005/29/EG und 2011/83/EU des Europäischen Parlaments und des Rates zur besseren Durchsetzung und Modernisierung der Verbraucherschutzvorschriften der Union („Omnibus-RL“), ABl. v. 18.12.2019, L 328, S. 7 ff.

Vertragsabschluss eine eigene Willenserklärung abgegeben hat. Im Gegensatz dazu ist die Interessenabwägung gemäß Art. 6 Abs. 1 lit. f DS-GVO ein interner Prozess des Verantwortlichen und erfolgt ohne Beteiligung des Datensubjekts.

II. Nationales Vertragsrecht als Differenzierungsfeld

Die teilweise Öffnung der strengen Vorgaben der DS-GVO für das nationale Schuldrecht hätte großes Potential, um den Schutz der informationellen Privatautonomie auf Grundlage des nationalen und teilweise harmonisierten Schuldrechts feiner auszudifferenzieren.

Wie bereits in Kapitel 1 ausgeführt, hat der europäische Gesetzgeber mit der DS-GVO einen einheitlichen horizontalen Ansatz gewählt, der mit Blick auf die tatsächlichen Phänomene der Datenverarbeitungen unterkomplex ist. Um dies zu verdeutlichen, genügt es, sich die traditionellen kommerziellen Selbstvermarktungsstrategien von Sportlern oder Schauspielern ins Gedächtnis zu rufen oder sich das vergleichsweise neue Phänomen der sog. Influencer anzusehen. Die DS-GVO unterscheidet jedoch nicht danach, ob ein Datensubjekt als anwaltlich beratener Unternehmer handelt, der unter Verwertung von personenbezogenen Daten jährlich mehrere Millionen Euro Einkommen erzielt oder als Verbraucher, der für die Nutzung der Produkte von *Facebook* einen Zugang zu personenbezogenen Daten eröffnet, um sich über die vom Elternbeirat oder von der Schulleitung initiierte *WhatsApp*-Gruppe des Klassenverbands über den schulischen Alltag seines Kindes auf dem Laufenden zu halten.

Es ist ein grundlegendes und offenkundiges Defizit, dass die Regelungen der DS-GVO ohne eine vorherige, detaillierte Analyse ihrer jeweiligen Konsequenzen für privatrechtliche Leistungsbeziehungen verabschiedet wurden. Mutmaßlich hatte der europäische Gesetzgeber vorrangig Datensubjekte vor Augen, die als Verbraucher handeln und sich mit Verantwortlichen konfrontiert sehen, die aus dem Kreis von *GAFAM* stammen. Es liegt nahe, dass der europäische Gesetzgeber den Einfluss der DS-GVO auf diejenigen jahrzehntealten Märkte schlichtweg übersehen hat, auf denen mehr oder weniger bekannte Persönlichkeiten die vermögenswerten Bestandteile ihre Persönlichkeitsrechte kommerzialisieren. Die hierfür erforderlichen Verwertungshandlungen beruhen stets auf einer Verarbeitung von (besonders sensiblen) personenbezogenen Daten.

Allenfalls sofern im Einzelfall keine rein kommerziellen, sondern zudem äußerungsrechtliche Belange im Vordergrund stehen, besteht mit dem sog. Presseprivileg in Art. 85 Abs. 1 DS-GVO eine potenzielle Öffnungsklausel für die nationalen Vorschriften der Mitgliedstaaten. Sowohl die Vorgängernorm des Art. 9 Datenschutz-RL (1995) als auch Art. 85 DS-GVO enthalten als sog. Presseprivileg keine Öffnung für die kommerzielle Verwertung von Persönlich-

keitsrechten, weil deren weite Auslegung zugunsten der Meinungsfreiheit ausdrücklich mit Blick auf journalistische Tätigkeiten erfolgte.[23]

Die fehlende Sensibilität des europäischen Gesetzgebers für die Auswirkungen der DS-GVO auf privatrechtlich organisierte Rechtsverhältnisse hat zur Konsequenz, dass insbesondere eine unreflektierte gerichtliche oder behördliche Anwendung der Anforderungen an die *Freiwilligkeit* der Einwilligung und deren *Widerruflichkeit* auf unternehmerisch handelnde Datensubjekte gegen den Grundsatz der Verhältnismäßigkeit verstoßen würde.[24]

Deshalb liegt die Option nahe, solche B2B-Verträge, die eine kommerzielle Verwertung der vermögenswerten Bestandteile von Persönlichkeitsrechten zum Gegenstand haben und die auf die Verarbeitung personenbezogener Daten angewiesen sind, durch eine großzügige Auslegung von Art. 6 Abs. 1 lit. b DS-GVO weitgehend[25] aus dem Anwendungsbereich der DS-GVO zu entlassen und den jeweils nationalen Regeln über den Schutz der Persönlichkeit und dem jeweils nationalen Schuldrecht zu überantworten.[26]

In der Folge müsste auch die Voraussetzung der Erforderlichkeit einer Datenverarbeitung für die Erfüllung eines solchen Verwertungsvertrags sehr zurückhaltend ausgelegt und angewendet werden, weil in B2B-Verhältnissen der Vertragsfreiheit der unternehmerisch handelnden Datensubjekten und der Verwerter der Vorrang einzuräumen ist. Infolgedessen wäre es konsequent, dass diese Überantwortung von B2B-Verträgen an das nationale Schuldrecht auch dazu führt, dass die Grundsätze der rechtmäßigen Datenverarbeitung (Art. 5 DS-GVO), der datenschutzfreundlichen Voreinstellungen und Technikgestaltung (At. 25 DS-GVO) und die datenschutzrechtlichen Anforderungen an die Si-

---

[23] Vgl. auch ErwG 153 S. 7 DS-GVO. So bereits für eine Webseite und zu Art. 9 DatenschutzRL: *EuGH*, 16.12.2008, C-73/07 = EuZW 2009, 108 (Rn. 56) – *Satakunnan Markkinapörssi und Satamedia*). Zudem lehnte der EuGH die Anwendbarkeit der Öffnungsklausel des Art. 9 Datenschutz-RL – trotz ihrer Nähe zur Informations- und Meinungsfreiheit – bereits für die Suchmaschine Google von Alphabet ab: *EuGH*, C-131/12 = NJW 2014, 2257 (Rn. 85) – *Google Spain*.

[24] Hierzu unten Kapitel 4 B.I.2. (Freiwilligkeit der Einwilligung) bzw. B.II.2. (freie Widerruflichkeit) sowie Kapitel 5 C.II. und III.

[25] Die allgemeinen Anforderungen an eine rechtmäßige Datenverarbeitung (insbesondere Art. 5 DS-GVO und Art. 25 DS-GVO) und an die Sicherheit der Datenverarbeitung (Art. 32 DS-GVO) bleiben auch im B2B-Verhältnis anwendbar.

[26] In diese Richtung: *Golz/Gössling*, IPRB 2018, 68 (71); sowie *Bunnenberg*, Privates Datenschutzrecht, 2020, S. 265. Obwohl *Bunnenberg* nur den privaten „Verbraucherdatenschutz" behandelt, dient ihm der kurze Exkurs zu „persönlichkeitsrechtlichen Lizenzen", die als „Merchandisingverträge" das B2B-Verhältnis betreffen, als Argument, um alle Datenverarbeitungen, die auf verbindliche Leistungserbringung angewiesen sind, gemäß Art. 6 Abs. 1 lit. b DS-GVO dem nationalen Schuldrecht zu überlassen. An dieser Stelle hätte es jedoch nahegelegen, zu vertiefen, warum „den persönlichkeitsrechtlichen Schutzanforderungen zugunsten von Betroffenen bereits in der zivilrechtlichen Dogmatik hinreichend Rechnung getragen wird" (S. 266). Diese Dogmatik müsste dann konsequenter Weise für jede Verwertung von personenbezogenen Daten – also auch im B2C-Verhältnis – hinreichend sein.

cherheit der Datenverarbeitung (Art. 32 DS-GVO)[27] im B2B-Verhältnis nicht oder allenfalls als mögliche Kriterien im Rahmen von nationalen Generalklauseln berücksichtigt werden.

Diese Option einer datenschutzrechtlichen Deregulierung ausschließlich für das B2B-Verhältnisse könnte jedoch nur der europäische Gesetzgeber durch eine Änderung der DS-GVO oder allenfalls der *EuGH* durch eine teleologische Gesamtreduktion der DS-GVO für unternehmerisch handelnde Datensubjekte erreichen.[28] Voraussetzung dafür wäre die Einsicht, dass Art. 8 GRCh keinen einheitlichen Ansatz von Datenschutzrecht erzwingt. Es wäre also möglich, innerhalb der DS-GVO zu differenzieren und Öffnungsklauseln vorzusehen, soweit Datensubjekte personenbezogene Daten professionell – gemeinsam mit ihren sonstigen Persönlichkeitsrechten – kommerzialisieren.

Allerdings sprechen mehrere Argumente dagegen, Art. 6 Abs. 1 lit. b DS-GVO *de lege ferenda* aufzuspalten oder sogar *de lege lata* unterschiedlich auszulegen, je nachdem, ob ein Datensubjekt einen Vertrag als Verbraucher oder als Unternehmer schließt. Eine gespaltene Auslegung und Anwendung von Art. 6 Abs. 1 lit. b DS-GVO würde die ohnehin bestehenden Herausforderungen bei der Anwendung des Erlaubnistatbestands für vertragsakzessorische Datenverarbeitungen nochmals potenzieren.

C. Herausforderungen der vertragsakzessorischen Datenverarbeitung

Mit der Anwendung von Art. 6 Abs. 1 lit. b DS-GVO sind drei wesentliche und gravierende Herausforderungen verbunden. Art. 6 Abs. 1 lit. b DS-GVO überfordert die nationalen Datenschutzbehörden und Gerichte, soweit sie die Angemessenheit eines vertraglichen Synallagmas überprüfen sollen, das personenbezogene Daten als Leistungsgegenstand vorsieht (I).

Auch die nationalen Datenschutzbehörden und Gerichte sind im Rahmen ihrer Anwendung von Art. 6 Abs. 1 lit. b DS-GVO an die Ziele gemäß Art. 1 DS-GVO und die Grundsätze der rechtmäßigen Datenverarbeitung gemäß Art. 5 Abs. 1 DS-GVO gebunden. Dennoch gefährdet die häufige Anwendung dieses inhaltlich unbestimmten Erlaubnistatbestands die unionsweite Einheitlichkeit des Datenschutzrechts und damit sowohl den Schutz der Datensubjekte als auch den freien Verkehr personenbezogener Daten im Binnenmarkt (II).

---

[27] Unberührt bleiben die hiervon zu trennenden Anforderungen an die IT-Sicherheit: zur Unterscheidung: *Sattler*, in: Ebers/Steinrötter (Hrsg.), Künstliche Intelligenz und smarte Robotik im IT-Sicherheitsrecht, 2021, S. 197 (210 f.).

[28] Aus der umgekehrten Richtung und für eine Reduktion der datenschutzrechtlichen Anforderungen für Verantwortliche, die KMU sind: Evaluationsbericht DS-GVO der EU-Kommission, COM(2020) 264 final, S. 12/19 ff.

Zuletzt hat es der europäische Gesetzgeber versäumt, die Anwendungsbereiche der DS-GVO und der DID-RL miteinander zu synchronisieren. Dies führt zu grundlegenden Abgrenzungsfragen, sofern personalisierte digitale Produkte bereitgestellt werden.[29] Auch aus diesem Grund sollte Art. 6 Abs. 1 lit. b DS-GVO restriktiv ausgelegt und damit der Einwilligung ein Vorrang eingeräumt werden (III).

I. Herausforderung: Überfordernde Angemessenheitskontrolle

Jedenfalls im Kontext der datenschutzrechtlichen Einwilligung ging der europäische Gesetzgeber von einem möglichen Überschneidungsbereich von DS-GVO und der Richtlinie über missbräuchliche Klauseln in Verbraucherverträgen (Klausel-RL)[30] aus. Insoweit gelten die nachfolgenden Ausführungen zwar grundsätzlich gleichermaßen für die Einwilligung, soweit diese – wie regelmäßig – vorformuliert ist. Allerdings besteht die Besonderheit, dass die DS-GVO spezifische und unionsautonome Anforderungen an eine wirksame Einwilligung formuliert, so dass zunächst unmittelbar auf diese Tatbestandsvoraussetzungen (Informiertheit/Freiwilligkeit) und in einem zweiten Schritt unmittelbar auf die Grundsätze der Datenverarbeitung gemäß Art. 5 DS-GVO zurückgegriffen werden kann.[31]

In ErwG 42 S. 3 weist der europäische Gesetzgeber darauf hin, dass eine vom Verantwortlichen vorformulierte Einwilligungserklärung

> „gemäß der Klausel-RL […] in verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache zur Verfügung gestellt werden, und sie keine missbräuchlichen Klauseln beinhalten [sollte]."

Auf den ersten Blick ist dieser Hinweis auf die Anwendbarkeit der Klausel-RL eine Selbstverständlichkeit. Schließlich enthält die DS-GVO keine spezifischen Vorgaben, sofern personenbezogene Daten im Rahmen von AGB als Leistungsgegenstand vereinbart werden.

Allerdings ist dieser Hinweis auf die Klausel-RL im Rahmen der Einwilligung deshalb kurios, weil die Anforderungen an die Informiertheit (Transparenz) und Freiwilligkeit einer datenschutzrechtlichen Einwilligung in der DS-GVO deutlich detaillierter geregelt sind als in der Klausel-RL.[32] Infolgedessen verdeutlicht die weitgehend unqualifizierte Bezugnahme auf die Klausel-RL in

---

[29] Hierzu auch unten C.III.2. sowie Kapitel 5 B.II.2.

[30] Richtlinie 93/13/EWG v. 05.04.1993 über mißbräuchliche Klauseln in Verbraucherverträgen (Klausel-RL), ABl. vom 21.04.1993, L 095, S. 29 ff.

[31] Hierzu unten C.I.3.

[32] So bereits: *BGH*, Urt. v. 11.11.2009, VIII ZR 12/08 = NJW 2010, 864 (Rn. 16) – *Happy Digits*; *BGH*, Urt. v. 16.07.2008, VIII ZR 348/06 = NJW 2008, 3055 (Rn. 15/19) – *Paypal*; a. A. unter der Annahme, eine datenschutzrechtliche Einwilligung und der Vertrag unterlägen ei-

ErwG 43 S. 3 primär, dass der Schutz von Datensubjekten und der Schutz von Verbrauchern in der DS-GVO nicht ausreichend synchronisiert wurde.[33] Der Hinweis steht deshalb in der zweifelhaften gesetzgeberischen Tradition, auf konfliktträchtiges europäisches Sekundärrecht lediglich erratisch und pauschal hinzuweisen, statt die jeweiligen Anforderungen inhaltlich aufeinander abzustimmen.[34]

Werden personenbezogene Daten dagegen als (Haupt-)Leistungsgegenstand vereinbart und soll die Datenverarbeitung deshalb auf Grundlage von Art. 6 Abs. 1 lit. b DS-GVO erfolgen, läuft dies zwangsläufig auf eine AGB-Kontrolle hinaus, so dass die Vorgaben der Klausel-RL regelmäßig zu beachten sind. Allerdings enthält die Klausel-RL nur sehr begrenzte Vorgaben sofern personenbezogene Daten als Bestandteil des vertraglichen Synallagmas vereinbart werden.

Soweit ein Zugang zu personenbezogenen Daten des Datensubjekts in einem synallagmatischen Verhältnis zur (Haupt-)Leistungspflicht des Verantwortlichen steht und die Leistungsvereinbarung auf Grundlage von AGB zustande kommt, wird dieser Vertrag zwar auf seine Transparenz, grundsätzlich jedoch nicht hinsichtlich der Angemessenheit des vertraglichen Synallagmas gerichtlich überprüft. Die Freistellung der Leistungsvereinbarung von einer Angemessenheitskontrolle gemäß § 307 Abs. 3 S. 1 BGB soll den Art. 4 Abs. 2 Klausel-RL umsetzen. Gemäß Art. 4 Abs. 2 Klausel-RL wird der vertragliche *Hauptgegenstand* lediglich einer Transparenzkontrolle, aber keiner Überprüfung auf dessen Angemessenheit unterworfen (1).

Allerdings werden aktuell Zweifel daran geäußert, dass die Begründung für die reduzierte Kontrolle des Hauptgegenstands auch dann gilt, wenn eine Bereitstellung von personenbezogenen Daten ein Bestandteil des vertraglichen Synallagmas ist. Tatsächlich offenbart die Analyse von Art. 4 Abs. 2 Klausel-RL gute Gründe, warum eine gerichtliche Überprüfung der Angemessenheit der synallagmatischen Leistungen sinnvoll sein könnte, sofern personenbezogene Daten als Leitungsgegenstand vereinbart werden (2).

Dennoch bleibt die Schwierigkeit, dass eine praktikable Angemessenheitskontrolle nicht nur die *Kontrollunterworfenheit* der Klausel, sondern auch eine monetäre Bewertung von personenbezogenen Daten als Ausgangspunkt für die *Fähigkeit* zur Kontrolle durch die Gerichte voraussetzt.[35] Diese Bewertung

---

ner Art Trennungs- und Abstraktionsprinzip: *Langhanke*, Daten als Leistung, 2018, S. 223; ebenso: *Hacker*, Datenprivatrecht, 2020, S. 433 f.

[33] Hierzu: *Hacker*, in: Lohsse/Schulze/Staudenmayer (Hrsg.), Data as Counter-Performance – Contract 2.0?, 2020, S. 45 ff.; *Wendehorst/v. Westphalen*, NJW 2016, 3745 ff.

[34] Die pauschalen Hinweise auf die DS-GVO in Art. 3 Abs. 8 DID-RL und auf das nationale Vertragsrecht in Abs. 10 DID-RL sind weitere Beispiele für diese unbefriedigende Vorgehensweise. Hierzu: *Sattler*, CR 2020, 145 (Rn. 24).

[35] Mit überzeugender Begründung, dass die Kontrollunterworfenheit einer Klausel von der Kontrollfähigkeit zumindest in *theoretischer* Sicht unterschieden werden kann: *Steinmetz*, Die Kontrollsperre des § 307 Abs. 3 BGB bei Verträgen über immaterielle Gegenstände,

dürfte die Gerichte jedoch regelmäßig überfordern bzw. in eine Anmaßung von Wissen münden. Infolgedessen lässt sich prognostizieren, dass die Judikative auf andere pragmatische Lösungen ausweichen würde, statt sich freiwillig auf das verminte Terrain einer Angemessenheitskontrolle des Synallagmas zu begeben. Erfahrungsgemäß können und wollen Gerichte nicht über einen *iustum pretium* und die datenbasierte *laesio enormis* entscheiden (3).

1. Eingeschränkte Kontrolle des vertraglichen Synallagmas

Gemäß Art. 3 Abs. 1 Klausel-RL ist eine Vertragsklausel als missbräuchlich anzusehen, wenn sie entgegen des Gebots von Treu und Glauben zum Nachteil des Verbrauchers ein erhebliches und ungerechtfertigtes Missverhältnis der vertraglichen Rechte und Pflichten der Vertragspartner verursacht. Somit eröffnet die Klausel-RL grundsätzlich die Möglichkeit zur Überprüfung der Angemessenheit von AGB.

Allerdings sieht Art. 4 Abs. 2 Klausel-RL eine Ausnahme zu Art. 3 Abs. 1 Klausel-RL vor. Hiernach ist weder der Hauptgegenstand des Vertrages noch die Angemessenheit zwischen dem Preis bzw. dem Entgelt und den im Austausch zugesagten Dienstleistungen bzw. Gütern, Gegenstand einer Missbrauchskontrolle, sofern diese Klauseln klar und verständlich formuliert sind. Damit nimmt Art. 4 Abs. 2 Klausel-RL zwei wesentliche Elemente des Vertrags von einer gerichtlichen Kontrolle aus.[36]

Erstens wird aus Art. 4 Abs. 2 Klausel-RL eine Begrenzung der inhaltlichen Kontrolle abgeleitet. Nach Ansicht des *EuGH* sind unter dem *Hauptgegenstand* des Vertrags i. S. d. Art. 4 Abs. 2 Klausel-RL

> „diejenigen Klauseln zu fassen, die seine Hauptleistungen festlegen und ihn als solche charakterisieren".[37]

Jedoch sind solche Klauseln nicht von diesem Ausschluss erfasst, die einen lediglich „akzessorischen Charakter" gegenüber denjenigen Klauseln haben, die „das Wesen des Vertragsverhältnisses selbst definieren".[38]

Zweitens soll auch das *Verhältnis* zwischen den vertraglichen (Haupt- bzw. Gegen-)Leistungspflichten nicht Gegenstand einer gerichtlichen Kontrolle sein. Das Preis-Leistungs-Verhältnis[39] eines vereinbarten Vertrags wird – jenseits

---

2022, S. 188 ff. (291: „Das Vorhandensein eines Maßstabes hat damit als solches keine Bedeutung für die Kontrollunterworfenheit, wenn es in der Sache doch erneut auf die Frage des Funktionierens von Privatautonomie und Wettbewerb ankommt.").

[36] Zur Begründung dieser Ausnahme und ihrer ungenügenden Umsetzung durch § 307 Abs. 3 BGB: *Steinmetz*, Die Kontrollsperre des § 307 Abs. 3 BGB bei Verträgen über immaterielle Gegenstände, 2022.

[37] *EuGH*, Urt. v. 30.04.2014, C-26/13 = NJW 2014, 2335 (Rn. 49 f.) – *Kásler*.

[38] *EuGH*, Urt. v. 30.04.2014, C-26/13 = NJW 2014, 2335 (Rn. 49 f.) – *Kásler*.

[39] ErwG. 19 Klausel-RL.

von § 138 BGB – nicht allein deshalb strenger kontrolliert, weil der Vertrag auf Grundlage von AGB zustande kam.[40]

Zwei wesentliche Argumente sprechen dafür, die Kontrolldichte für den vertraglichen Hauptgegenstand und das Äquivalenzverhältnis zwischen den Leistungsversprechen zu reduzieren (1). Sofern diese Gründe jedoch im Einzelfall oder sogar typischerweise nicht vorliegen, kann eine teleologische Reduktion von § 307 Abs. 3 S. 1 BGB in Betracht gezogen werden (2).[41]

a) Gründe für die Reduktion der gerichtlichen Kontrolldichte

Die Kontrollfreiheit des vertraglichen Hauptgegenstands beruht vorrangig auf der Annahme, dass die Vertragsparteien dem Hauptgegenstand ihre volle Aufmerksamkeit schenken.[42] Damit unterteilt Art. 4 Abs. 2 Klausel-RL und im Anschluss hieran auch § 307 Abs. 3 S. 1 BGB jeden Vertrag, der auf Grundlage von AGB zustande kommt, in zwei Teile: Den Hauptgegenstand und die sonstigen Abreden in Form der AGB.

Anders als den Hauptgegenstand akzeptieren Verbraucher die AGB regelmäßig, ohne von deren Inhalt Kenntnis zu nehmen. Dies tun sie, obwohl sie davon ausgehen, dass die AGB im Interesse des Verwenders formuliert sind und infolgedessen für sie selbst nachteilige Klauseln enthalten. Diese Zustimmung zu den AGB hat mehrere Gründe. Zunächst besteht typischerweise ein Informations- und ein Motivationsgefälle sowie ein Verhandlungsungleichgewicht: Verbraucher sind sich der Tragweite und Bedeutung einzelner Klauseln häufig nicht bewusst, aber sowohl die Kosten für eine informierte Zustimmung (Lektüre/Recherche/Beratung) als auch die Kosten der Verhandlung sind – jedenfalls bei alltäglichen Massengeschäften – prohibitiv hoch und stehen zum ökonomischen Wert solcher Transaktion regelmäßig außer Verhältnis.

Zudem sind die Chancen eines Verbrauchers gering, eine Individualabrede zu erreichen und solche Abreden sind in alltäglichen Massengeschäften volkswirtschaftlich auch gar nicht wünschenswert. Die vertraglichen Bestimmungen von Massengeschäften sind regelmäßig so umfangreich, dass der Aufwand einer de-

---

[40] *EuGH*, Urt. v. 30.04.2014, C-26/13 = NJW 2014, 2335 (Rn. 58) – *Kásler*; *EuGH*, Urt. v. 26.02.2015, C-143/13 = GRUR Int. 2015, 471 (Rn. 70) – *Matai*. Zum Ganzen: *Lüttringhaus*, Vertragsfreiheit und ihre Materialisierung im Europäischen Binnenmarkt, 2018, S. 591 ff. Mit dem Vorschlag, diesen Schutzgrund des Art. 4 Abs. 2 Klausel-RL *de lege ferenda* eindeutig in § 307 Abs. 3 S. 2 BGB aufzunehmen: *Steinmetz*, Die Kontrollsperre des § 307 Abs. 3 BGB bei Verträgen über immaterielle Gegenstände, 2022, S. 224 f.

[41] Weil die unionsrechtlichen Vorgabe einschließlich Art. 4 Abs. 2 Klausel-RL gemäß Art. 8 Klausel-RL lediglich Mindestanforderungen sind, wird eine strengere Angemessenheitskontrolle im nationalen Recht, insbesondere über § 138 Abs. 1 BGB, nicht durch die Klausel-RL blockiert. Aus diesem Grund für besondere Klauselverbote im Kontext der Einwilligung: *Wendehorst*, JZ 2021, 974 (983 f.); hierzu unten C.I.3.a.

[42] *Stoffels*, JZ 2001, 843 (847).

taillierten Auseinandersetzung mit diesen AGB zu groß wäre. Es ist deshalb rational und effizient, wenn Verbraucher diese nicht lesen.[43] Sofern es zu einem Streit über den Inhalt der AGB kommt, werden diese stattdessen *ex post* gerichtlich überprüft.[44] Es ist also gerade ein Zweck der AGB-Kontrolle, einen effizienten Abschluss von alltäglichen Massengeschäften zu ermöglichen, so dass eine detaillierte individuelle Auseinandersetzung mit diesen Klauseln überflüssig wird.

Diese gerichtliche Kontrolle lässt sich zudem damit begründen, dass AGB selbst kaum Gegenstand von Wettbewerb sind, gerade weil rationale Verbraucher sie nicht mit den AGB von Konkurrenten vergleichen und in vielen Branchen – trotz bestehenden Wettbewerbs – kaum Unterschiede zwischen den AGB auftreten.[45] Zugespitzt: Die Klauselkontrolle ist die effizienzsteigernde rechtliche Antwort auf die Tatsache, dass AGB faktisch nicht gelesen werden (sollen).

Von dieser *ex post*-Kontrolle ist Art. 4 Abs. 2 Klausel-RL eine grundlegende Ausnahme. Er beruht auf dem Gedanken, dass der vertragliche Hauptgegenstand die eigentliche Motivation für den Vertragsschluss der Beteiligten ist. Deshalb liegt Art. 4 Abs. 2 Klausel-RL die Annahme zugrunde, dass beide Parteien sich vor Vertragsschluss vorrangig mit diesem Hauptgegenstand auseinandersetzen. Somit basiert Art. 4 Abs. 2 Klausel-RL auf der Einschätzung des europäischen Gesetzgebers, dass die Verbraucher ihre ganze Aufmerksamkeit auf die Hauptleistung, die Gegenleistung und das Verhältnis beider zueinander richten (sollen), während die sonstigen AGB getrost der nachträglichen gerichtlichen Inhaltskontrolle überantwortet werden können. Diese Annahme lässt sich als Postulat einer gesteigerten Aufmerksamkeit für den vertraglichen Hauptgegenstand bezeichnen.

Mithilfe dieses Postulats lässt sich die Ausnahme gemäß Art. 4 Abs. 2 Klausel-RL rechtfertigen, weil der Hauptgegenstand infolgedessen weiterhin einem besonders intensiven Vergleich und deshalb auch einem starken Wettbewerbsdruck ausgesetzt ist. Solange der Hauptgegenstand klar und eindeutig definiert ist – Art. 4 Abs. 2 Klausel-RL sieht gerade keine Ausnahme vom Transparenzgebot des Art. 5 S. 1 Klausel-RL vor – ist eine markt- und wettbewerbsbasierte Herausbildung der synallagmatischen Leistungspflichten nicht nur möglich,

---

[43] Siehe dazu nur: *Basedow*, in: MüKo, BGB, 6. Aufl. 2012, Vor. § 305, Rn. 4 f.; *Grüneberg*, in: Palandt, BGB, 79. Aufl. 2020, Überbl. v. § 305, Rn. 6 und § 305, Rn. 10; *Franck*, ZWeR 2016, 137 (151 f.); *Thomas*, NZKart 2017, 92 (94 f.); *Eisenberg*, 47 Stan. L. Rev. (1995), 211 (241 ff.); spezifisch zum Datenschutzrecht: *Hermstrüwer*, Contracting Around Privacy, (2017) 8 JIPITEC 9, 17 ff.

[44] Weil unwirksame AGB jedoch eine abschreckende Wirkung haben und Verbraucher vor einer gerichtlichen Geltendmachung von Ansprüchen zurückschrecken, soll diese Wirkung von (unwirksamen) AGB durch die Möglichkeit der Unterlassungsklage durch Verbände teilweise kompensiert werden, § 1 UKlaG.

[45] *Lohse*, NZKart, 2020, 292 (293); *Basedow*, in: MüKo, BGB, 6. Aufl. 2012, Vor § 305, Rn. 5; *Grüneberg*, in: Palandt, BGB, 79. Aufl. 2020, Überbl. v. § 305, Rn. 6.

sondern auch wesentlich effizienter, als eine gerichtliche Angemessenheitskontrolle gemäß Art. 3 Abs. 1 Klausel-RL.[46] Letztere würde notwendigerweise die richterliche Kenntnis und Entscheidung über einen angemessenen und somit richtigen oder sogar gerechten Preis voraussetzen.[47]

b) Marktversagen als Grenze der reduzierten Kontrolldichte

Wie ausgeführt, liegt Art. 4 Abs. 2 Klausel-RL die Annahme zugrunde, dass Verbraucher dem Hauptgegenstand ihre Aufmerksamkeit widmen und ihre Entscheidung zum Vertragsabschluss davon abhängig machen. Im Gegensatz zur Transparenzkontrolle, die explizit in Art. 5 Klausel-RL geregelt ist und von der Art. 4 Abs. 2 Klausel-RL gerade keine Ausnahme macht, ergeben sich die Voraussetzungen der Aufmerksamkeit und des funktionierenden Wettbewerbs jedoch lediglich implizit aus Art. 4 Abs. 2 Klausel-RL.

Dies stellt die Judikative vor eine schwierige Herausforderung. Die Gerichte sollen zwar im Grundsatz weder die synallagmatischen Leistungspflichten überprüfen noch über die Angemessenheit von Preis und Leistung befinden. Bestehen jedoch deutliche Hinweise auf ein Marktversagen und infolgedessen evidente Zweifel daran, dass der Wettbewerbsmechanismus funktioniert und

---

[46] Zur Beurteilung der Kontrollunterworfenheit einer Klausel schlägt *Steinmetz* (Die Kontrollsperre des § 307 Abs. 3 BGB bei Verträgen über immaterielle Gegenstände 2022, S. 223 f.), eine dreistufige Vorgehensweise vor: Zunächst ist der Hauptgegenstand des Vertrags im Sinne einer „materiellen Selbständigkeit" herauszuarbeiten, weil „jeder […] für sich genommen selbständige Regelungskomplex […] über einen eigenen, auf Basis nachfolgender Stufen zu bestimmenden, kontrollfreien Hauptgegenstand [verfügt]". Sodann sind auf zweiter Stufe „die als im engsten Sinne zu verstehenden essentialia negotii der jeweiligen Vereinbarung von der Inhaltskontrolle auszunehmen. Dabei handelt es sich nur um solche Vereinbarungen, welche – hinweggedacht – eine für die Annahme eines wirksamen Vertrages hinreichende Einigung entfallen ließen". Sofern die Frage der Kontrollunterworfenheit der fraglichen Klausel noch immer nicht eindeutig beantwortet ist, ist auf der letzten Stufe entscheidend, „ob insoweit von einer hinreichenden Wirkung der Markt- und Wettbewerbskräfte dahingehend ausgegangen werden kann, dass der Klauselverwender bereits auf Ebene der Vertragsgestaltung diszipliniert wird".

[47] Dieses Argument ordnet *Steinmetz* der von der Kontrollunterworfenheit strikt zu trennenden Kontrollfähigkeit zu. Dies überzeugt zwar in der Theorie. Es ist aber wenig überraschend, dass ein Gericht bereits die Kontrollunterworfenheit verneint, sofern es sich – mangels vorhandener Beurteilungsmaßstäbe – nicht in der Lage sieht, über die Angemessenheit einer Klausel zu entscheiden. Mit der Forderung an die Gerichte, dies offen zu kommunizieren: *Steinmetz*, Die Kontrollsperre des § 307 Abs. 3 BGB bei Verträgen über immaterielle Gegenstände, 2022, Zusammenfassung (These 6): „Die Frage nach der Zulässigkeit des Einstiegs in die Inhaltskontrolle ist streng zu trennen von derjenigen nach ihrer tatsächlichen Kontrollfähigkeit anhand rechtlicher Maßstäbe oder gar ihrer Wirksamkeit. Schließlich liegen beiden Stufen unterschiedliche Überlegungen zu Grunde. Eine Klausel ist weder kontrollunterworfen, weil sie unangemessen ist, noch ist sie unangemessen, weil sie kontrollunterworfen ist. Es ist daher auch möglich, dass es trotz Kontrollunterworfenheit in Ermangelung rechtlicher Maßstäbe an der Kontrollfähigkeit mangelt, ebenso wie Klauseln einer Inhaltskontrolle entzogen sein können, für welche Maßstäbe existent wären."

dadurch die Klauselverwender bereits bei der Gestaltung der Klauseln diszipliniert, so könnten die Gerichte über Art. 4 Abs. 2 Klausel-RL hinweggehen und § 307 Abs. 3 S. 1 BGB teleologisch reduzieren.[48] Dies hätte zur Konsequenz, dass jede Leistungsbeschreibung, die zur Datenverarbeitung führt, von dem Tatbestandsmerkmal der Beschreibung des Hauptgegenstands im Sinne des Art. 4 Abs. 2 Klausel-RL ausgenommen wäre, so dass diese Leistungsbeschreibung stets der Inhaltskontrolle unterworfen wäre.[49]

Für eine solche teleologische Reduktion setzt die Klausel-RL jedoch sehr enge Grenzen. Beispielweise genügt es nicht, dass der Leistungsgegenstand – wie beispielsweise eine Versicherung oder Kapitalanlage – sehr komplex ist und dem Vertragsschluss für den einzelnen Verbraucher zugleich wirtschaftlich eine sehr weitreichende Bedeutung zukommt. Vielmehr erwähnen die ErwG der Klausel-RL ausdrücklich den Versicherungsvertrag als Anwendungsbeispiel für Art. 4 Abs. 2 Klausel-RL. Der Ausschluss einer Kontrolle des Hauptgegenstands und des Preis-Leistungs-Verhältnisses folge insoweit, wie bei den Klauseln in Versicherungsverträgen,

„[…] in denen das versicherte Risiko und die Verpflichtung des Versicherers deutlich festgelegt oder abgegrenzt werden, nicht als mißbräuchlich beurteilt werden, sofern diese Einschränkungen bei der Berechnung der vom Verbraucher gezahlten Prämie *Berücksichtigung finden*“ [Hervorhebung durch den Verfasser].

Diese vage Formulierung anhand des Beispiels eines Versicherungsvertrags spricht dafür, dass allein die Komplexität des Hauptgegenstands noch kein hinreichendes Argument dafür ist, Art. 4 Abs. 2 Klausel-RL nicht anzuwenden. Hält man Versicherungsverträge und Verträge mit personenbezogenen Daten als Leistungsgegenstand – beide sind ökonomisch betrachtet Vertrauensgüter[50] – für vergleichbar komplex und riskant, so spricht dies dafür, dass auch die Angemessenheit beispielsweise zwischen einem Zugang zu digitalen Produkten im Austausch gegen einen Zugang zu personenbezogenen Daten keiner generellen Angemessenheitskontrolle unterliegt.

Für die Möglichkeit, die Angemessenheit von personenbezogenen Daten als (Haupt-)Gegenstand zu überprüfen, sprechen allerdings zwei Gründe:

Erstens ist der Hauptgegenstand in diesen Fällen keine vorgegebene Maßeinheit, sondern wird erst durch den Vertrag – gleichsam als rechtliches Produkt – konstituiert. Diese „Normgeprägtheit“ des Hauptgegenstands kann dafür sprechen, dass dieser komplexe Hauptgegenstand zwar Teil der synallagmatischen Leistungsbeziehung ist, aber – mangels transparenten Wettbewerbs für diese

[48] Für eine Änderung des § 307 Abs. 3 BGB plädierend: *Wendehorst*, Verbraucherrelevante Problemstellungen zu Besitz- und Eigentumsverhältnissen beim Internet der Dinge, 2016, S. 89 f.; *Hacker*, in: Lohsse/Schulze/Staudenmayer (Hrsg.), Data as Counter-Performance – Contract 2.0?, 2020, S. 45 (66).

[49] Hierfür: *v. Westphalen/Wendehorst*, BB 2016, 2179 (2186).

[50] Hierzu sogleich unter 2.b.

Leistungsparameter – dennoch gerichtlich auf ihre inhaltliche Angemessenheit zu überprüfen ist.[51]

Zweitens liegt es nahe, dass eine Vereinbarung über personenbezogene Daten als (Haupt-)Leistungsgegenstand ungewöhnlicher und komplexer ist, als ein (weitgehend) standardisierter Versicherungsvertrag. Somit bietet auch die Entstehungszeit der Klausel-RL einen Ansatzpunkt, um eine strengere Angemessenheitskontrolle des Hauptgegenstands zu ermöglichen. Die Klausel-RL datiert aus dem Jahr 1993 und dürfte deshalb die seither bekannt gewordenen Ergebnisse der verhaltensökonomischen Forschung noch nicht berücksichtigen. Die Erkenntnisse über die rationale Begrenztheit menschlicher Entscheidungen nähren grundlegende Zweifel daran, ob die Aufmerksamkeit des Durchschnittsverbraucher für einen derart komplexen Hauptgegenstand genügt, um den von Art. 4 Abs. 2 Klausel-RL vorausgesetzten Wettbewerb zu ermöglichen und infolgedessen auf eine gerichtliche Angemessenheitskontrolle zu verzichten. Zwar könnte eine besonders kenntnisreiche und aufmerksame Gruppe von Verbrauchern – gleichsam stellvertretend für alle Verbraucher – den Wettbewerb zwischen den Anbietern fördern. Fraglich ist jedoch, für welche Produkte eine solche Gruppe überhaupt existiert[52] und ob deren wettbewerbsfördernder Effekt – abweichend von der Maßgeblichkeit der Durchschnittsverbraucher – überhaupt i. R. d. Klausel-RL berücksichtigt werden kann.

Kurzum: Sofern sich für einen Hauptgegenstand typischerweise ein Marktversagen nachweisen lässt, spricht dies im Grundsatz dafür, den vertraglichen Hauptgegenstand und das Verhältnis zwischen den Leistungspflichten über den Art. 4 Abs. 2 Klausel-RL hinaus und unter teleologischer Reduktion von § 307 Abs. 3 S. 1 BGB für eine gerichtliche Überprüfung zu öffnen. Infolgedessen könnten die Gerichte – unabhängig von § 138 BGB – auch den vertraglichen Hauptgegenstand auf seine Angemessenheit inhaltlich überprüfen.

Weil Gerichten aber regelmäßig sowohl das Wissen über ein angemessenes Preisniveau[53] als auch die Fähigkeit fehlt, einen gerechten Preis zu ermitteln,[54]

---

[51] Dies mit Blick auf immaterielle Gegenstände erwägend: *Steinmetz*, Die Kontrollsperre des § 307 Abs. 3 BGB bei Verträgen über immaterielle Gegenstände, 2022, S. 226 ff. Mit Blick auf die Verarbeitung personenbezogener Daten als Leistungsgegenstand jedoch gegen eine generelle Kontrollunterworfenheit (S. 299: „So wie die Inhaltskontrolle in Fällen eingreift, in denen mangels Sensibilität des Marktes für den Klauselinhalt keine Disziplinierung des Klauselverwenders eintritt, so hat sie vor dem Hintergrund der Vertragsfreiheit auszuscheiden, soweit die Vertragspartner die Parameter der vertragscharakteristischen Leistungspflichten festlegen".

[52] Hierzu unten II.3. Zur Möglichkeit von Anbietern, diese kritischen Datensubjekte herauszufiltern und nur diesen ein angemessenes Preis-Leistungs-Verhältnis anzubieten: *Wagner/Eidenmüller*, 86 University of Chicago Law Review 2019, 581 ff.; *Grigoleit/Bender,* in: Busch/De Franceschi (Hrsg.), Data Economy and Algorithmic Regulation, 2020, S. 115 ff.

[53] *EuGH*, Urt. v. 30.04.2014, C-26/13 = NJW 2014, 2335 (Rn. 55) – *Kásler.*

[54] Diesbezüglich optimistischer, schlägt *Hacker* eine Kombination aus einem Test auf Grundlage der hypothetischen ex-ante Verhandlungssituation und einem Sachverständigengutachten („expert testimony") vor: *Hacker*, in: Lohsse/Schulze/Staudenmayer (Hrsg.), Data

scheitert eine solche Inhaltskontrolle des Hauptgegenstands zwar regelmäßig erst am fehlenden Maßstab für die tatsächliche Angemessenheitsprüfung (*Kontrollfähigkeit*), die Gerichte verkürzen aber ihre Begründung, indem sie bereits die vorgelagerte *Kontrollunterworfenheit* der Klausel gemäß § 307 Abs. 3 S. 1 BGB verneinen.[55]

2. Personenbezogene Daten und Marktversagen

Wie bereits ausgeführt dient die AGB-Kontrolle dazu, den schnellen und effizienten Abschluss alltäglicher Massenverträge zu ermöglichen. Der Gesetzgeber geht davon aus, dass diese AGB nicht gelesen werden, sondern entweder infolge einer Überprüfung durch Verbraucherschutzverbände oder erst im Fall von Konflikten zwischen den Vertragsparteien einer gerichtlichen *ex post* Kontrolle unterzogen werden.

Sofern die Verarbeitung personenbezogener Daten zum Leistungsgegenstand gemacht wird, wirkt sich das rationale Desinteresse der Verbraucher an vertraglichen Klauseln jedoch besonders nachteilig aus (a). Zudem besteht auch ein gesteigertes Risiko für ein Marktversagen. Soweit personenbezogene Daten Gegenstand eines Leistungsaustauschs sind, weist dieser Markt wesentliche Merkmale eines atypischen *Akerlof'schen* Zitronenmarkts auf (b). Darüber hinaus wird die mangelnde Aufmerksamkeit der Durchschnittsverbraucher allenfalls teilweise durch die besondere Marktkenntnis einer aufmerksamen Minderheit kompensiert (c).

Somit greifen wesentliche Argumente für die Kontrollfreiheit des Hauptgegenstands gemäß Art. 4 Abs. 2 Klausel-RL bzw. § 307 Abs. 3 S. 1 BGB im Kontext einer Vereinbarung von personenbezogenen Daten als Leistungsgegenstand nicht und der Weg zu einer Angemessenheitskontrolle durch die nationalen Gerichte wird deshalb durch das europäische Sekundärrecht nicht versperrt (d). Solange allerdings der Marktmechanismus selbst nicht dazu in der Lage ist, einen transparenten Wert für personenbezogene Daten zu ermitteln, werden die Gerichte an dieser Aufgabe erst recht scheitern (e).

a) Mangelnde Aufmerksamkeit für den Hauptgegenstand

Offensichtlich würde es Jahre dauern, sofern Datensubjekte versuchen, die Nutzungsbedingungen von Verträgen zu lesen und hieraus abzuleiten, inwie-

---

as Counter-Performance – Contract 2.0?, 2020, S. 45 (71); dies vertiefend: *Hacker*, Datenprivatrecht, 2020, S. 474.

[55] Zu § 307 Abs. 3 S. 1 BGB: *BGH*, Urt. v. 07.11.2014 – V ZR 305/13 = NJW-RR 2015, 181 (182); sowie mit zahlreichen Nachweisen: *BGH*, Urt. v. 25.09.2013 – VIII ZR 206/12 = NJW 2014, 209 (Rn. 17). Zur Kritik an diesem Vorgehen: *Steinmetz*, Die Kontrollsperre des § 307 Abs. 3 BGB bei Verträgen über immaterielle Gegenstände, 2022, These 6.

weit die vertragliche Leistungspflicht des Anbieters eine Verarbeitung von personenbezogenen Daten des Kunden erforderlich macht. Studien belegen die naheliegende Einschätzung, dass auch die sog. Erklärungen zum Datenschutz und Einwilligungserklärungen von rund 75 % der Verbraucher nicht gelesen werden.[56] Allerdings muss dieses Ergebnis zunächst nicht beunruhigen. Schließlich beruht das System der AGB-Kontrolle gerade auf der Erkenntnis, dass AGB vor Vertragsschluss regelmäßig nicht gelesen werden und deshalb einer nachträglichen – gemäß §§ 1, 3 Abs. 1 S. 1 UKlaG auch durch Verbände herbeizuführenden[57] – gerichtlichen Kontrolle unterworfen werden. Allerdings ist eine Gleichstellung gewöhnlicher AGB[58] mit solchen AGB, die eine Verarbeitung von personenbezogenen Daten als synallagmatischen Leistungsgegenstand definieren, nur teilweise sachgemäß.

Sofern personenbezogene Daten als Leistungsgegenstand vereinbart werden, bestehen gleich mehrere Besonderheiten. Zunächst schnüren die Verantwortlichen für die Verarbeitung von personenbezogenen Daten häufig „Pakete" und rechtfertigen diese anschließend – auch mangels diesbezüglich bestehender Rechtssicherheit – pauschal unter Nennung mehrerer Erlaubnistatbestände (regelmäßig durch Aufzählung von Art. 6 Abs. 1 lit. b, lit. c und lit. f DS-GVO).[59]

Sofern der Klauselverwender und Verantwortliche eine Zustimmung zur Datenschutzerklärung verlangt, verschmelzen zudem die Grenzen zur Einwilligung.[60] Ohne Einführung von eindeutigen Feldern für eine Annahme von Anträgen, beispielsweise durch eine Auswahloption zwischen „Zahlungspflichtigen Vertrag abschließen" und „Datenbasierten Vertrag abschließen",[61] ergeben

---

[56] Beispielsweise die Studie 8201 von Allensbacher im Auftrag von Focus, 2019, S. 5: https://d1epvft2eg9h7o.cloudfront.net/filer_public/d5/02/d5026d49-6fb4-4bc8-a188-0b68c3a23159/focus_allensbach.pdf, zuletzt abgerufen am 19.05.2022; sowie: *Obar/Oeldorf-Hirsch*, (2018) 21 Information, Communication & Society, S. 1.

[57] Hierzu zuletzt: *BGH*, Urt. v. 28.05.2020, I ZR 7/16 = NJW 2020, 2540 ff. – *Cookie-Einwilligung II*.

[58] Nur sofern man – mit der hier vertretenen restriktiven Auslegung von Art. 6 Abs. 1. lit. b DS-GVO – in diesen Datenschutzerklärungen lediglich die gemäß Art. 13 Abs. 1 lit. c DS-GVO zu erfolgende Information sieht, kommt es nicht darauf an, dass Datensubjekte diesen Ausführungen ihre Aufmerksamkeit schenken. Es handelt sich dann regelmäßig um gewöhnliche AGB über vertragliche Nebenbestimmungen.

[59] Mit Beispielen: *Metzger*, GRUR 2019, 129 (133 f.).

[60] *Wendehorst/v. Westphalen* sehen gerade darin eine Gefahr, dass Verantwortliche über eine zunehmende Personalisierung der von ihnen vertraglich geschuldeten (Haupt-)Leistung, gezielt den Anwendungsbereich des Art. 6 Abs. 1 lit. b DS-GVO ausdehnen. Deshalb plädieren sie mit Blick auf die insoweit reduzierte AGB-Kontrolle dafür, diesen Erlaubnistatbestand eng auszulegen: *dies.*, NJW 2016, 3745 (3747/3749). Zudem sollen sämtliche Leistungsbeschreibungen, welche zur Datenverarbeitung führen, von dem Tatbestandsmerkmal der Beschreibung des Hauptgegenstands im Sinne des Art. 4 Abs. 2 Klausel-RL ausgenommen und infolgedessen kontrollunterworfen sein: *v. Westphalen/Wendehorst*, BB 2016, 2179 (2186).

[61] Ähnlich: Bericht der Arbeitsgruppe „Digitaler Neustart" der Konferenz der Justizministerinnen und Justizminister der Länder, 2017, 215 f. Derartige Vorschläge wurden – nach anekdotischen Erklärungen – wohl im Rahmen der Verhandlungen über die DID-RL erwo-

sich zahlreiche Gestaltungsmöglichkeiten. Diese laufen jedoch Gefahr, das AGB-rechtliche (und das datenschutzrechtliche) Transparenzgebot zu verletzen. Sind personenbezogene Daten Bestandteil der gegenseitigen Leistungsvereinbarung, so kommt als Rechtsgrundlage für die Datenverarbeitung vorrangig die Einwilligung i. S. d. Art. 4 Nr. 11, Art. 6 Abs. 1 lit. a, Art. 7 DS-GVO in Betracht.[62] Dass die Einwilligung auf den vertraglichen Hauptgegenstand Einfluss hat, liegt jedenfalls dann nahe, wenn die Einwilligung im Zusammenhang mit einem Vertrag erklärt wird und keine andere Gegenleistung des Verbrauchers vorgesehen ist.[63]

Anders als die Einheiten eines anerkannten Zahlungsmittels sind personenbezogene Daten als Leistungsgegenstand jedoch ein komplexes rechtliches Produkt. Im Gegensatz zum monetären Preis können die Kosten, die mit einer Datenverarbeitung auf Grundlage von Art. 6 Abs. 1 lit. b DS-GVO oder auf Grundlage einer Einwilligung einhergehen, nicht effizient mit alternativen Angeboten – seien sie monetär oder ebenfalls datenbasiert – verglichen werden.[64]

Soweit personenbezogene Daten als Teil der synallagmatischen Leistungsbeziehung vereinbart werden, erhalten sie regelmäßig nicht die von Art. 4 Abs. 2 Klausel-RL für den vertraglichen Hauptgegenstand unterstellte gesteigerte Aufmerksamkeit der Verbraucher, sondern teilen das Schicksal aller anderen Klauseln: Auch der Hauptgegenstand des Vertrags wird von Verbrauchern tendenziell akzeptiert, ohne dass sie zuvor die relevanten Klauseln gelesen, bewertet und zur Grundlage ihrer Entscheidung gemacht haben.

Weil das Postulat der gesteigerten Aufmerksamkeit aber der erste wesentliche Grund dafür ist, den Hauptgegenstand gemäß Art. 4 Abs. 2 Klausel-RL und gemäß § 307 Abs. 3 S. 1 BGB keiner Angemessenheitskontrolle zu unterziehen,[65] spricht dies dafür, diese Ausnahme von der Inhaltskontrolle in § 307 Abs. 3 BGB teleologisch zu reduzieren, soweit personenbezogene Daten als

---

gen, konnten sich aber nicht durchsetzen. Es bestand die Befürchtung, dadurch das umstrittene Konzept bzw. die Realität von personenbezogenen Daten als „Gegenleistung" explizit anzuerkennen.

[62] So auch *Metzger*, JZ 2019, 577 (579).

[63] Für eine Datenverarbeitung, die auf Grundlage von Art. 6 Abs. 1 lit. f DS-GVO und damit infolge einer Interessenabwägung erfolgt, ist ein Einfluss auf die vertragliche Leistungsbeziehung aus privatrechtlicher Perspektive eher überraschend. Dennoch scheint der europäische Gesetzgeber bei Verabschiedung von Art. 3 Abs. 1 S. 2 DID-RL davon ausgegangen zu sein, dass die Bereitstellung und Verarbeitung von personenbezogenen Daten auf Grundlage einer Interessenabwägung ebenfalls Teil des vertraglichen Synallagmas sein kann. So auch: *Lohsse/Schulze/Staudenmayer*, Data as Counter-Performance – Contract 2.0?, 2020, S. 15 ff.; *Görs*, ebda., S. 165 (266); *Mischau*, ZEuP 2020, 335 (343).

[64] Dies könnten *Wendehorst/v.Westphalen* zum Anlass genommen haben, Vereinbarungen über personenbezogene Daten stets einer Inhaltkontrolle unterwerfen zu wollen, es sei denn, diese werden ausdrücklich als Gegenleistung bezeichnet: *dies.*, NJW 2016, 3745 (3748). Nach dem Wortlaut von Art. 4 Abs. 2 Klausel-RL bzw. § 307 Abs. 3 BGB wird der Hauptgegenstand jedoch normativ bestimmt und folgt nicht aus einer „Deklaration als Hauptleistung".

[65] *Nebbia*, Unfair Contract Terms in European Law, 2007, S. 115 (130 f.); *Wurmnest*, MüKo,

Leistung vereinbart werden und der Verantwortliche die Datenverarbeitung deshalb auf Grundlage von Art. 6 Abs. 1 lit. b DS-GVO rechtfertigen könnte.[66]

b) Personenbezogene Daten als Leistung – ein Zitronenmarkt

Der zweite Grund dafür, den Hauptgegenstand eines Vertrags nur einer Transparenz-, aber keiner Angemessenheitskontrolle zu unterziehen, beruht auf der Annahme, dass die Präferenzen der Marktteilnehmer vermittelt über Angebot und Nachfrage besser geeignet sind, den „richtigen" Preis zu ermitteln, als ein Gericht.[67]

Wesentliche Voraussetzung dafür, dass der Markt die ihm zugesprochene Aufgabe der Preisbildung als Ergebnis einer fortlaufenden Koordination von Angebot und Nachfrage erfüllen kann, ist jedoch, dass die Mechanismen des Marktes funktionieren. Dies setzt voraus, dass sich überhaupt ein Preis bilden kann und dieser ein leicht wahrnehmbares Signal aussendet, an dem die Marktteilnehmer ihre Entscheidung ausrichten können.[68]

Es bestehen jedoch erhebliche Zweifel daran, dass der Marktmechanismus – unter den aktuellen Bedingungen – einen transparenten Preis für personenbezogene Daten herausbildet und ein solches Signal aussendet. Weil eine rechtmäßige Verarbeitung von personenbezogenen Daten aus rechtlicher Perspektive kein schlichtes Such- oder Erfahrungsgut, sondern ein komplexes Rechtsprodukt ist, ist die rechtmäßige Datenverarbeitung aus ökonomischer Perspektive ein Vertrauensgut. Weder die ausdrückliche Vereinbarung von personenbezogenen Daten als Leistungsgegenstand mittels einer Einwilligung noch die Definition einer vertraglichen Hauptleistung, die ihrerseits die Verarbeitung von personenbezogenen Daten erfordert, haben einen quantitativ eindeutigen und kognitiv leicht erfassbaren monetären Wert. Deshalb kann die auf Grundlage einer Leistungsvereinbarung erfolgende Datenverarbeitung keine Signalfunktion erfüllen, die mit derjenigen eines monetären Preises vergleichbar wäre. Weil der „Datenpreis", der beispielsweise im Austausch für ein personalisiertes Angebot digitaler Produkte zu erbringen ist, nicht transparent und damit auch nicht leicht zu bewerten ist, fehlt es an einem verlässlichen Signal, an dem Datensubjekte ihr Verhalten ausrichten können.

BGB, 2020, § 307, Rn. 13; *Stoffels*, JZ 2001, 843 (847); *Hacker*, in: Lohsse/Schulze/Staudenmayer (Hrsg.), Data as Counter-Performance – Contract 2.0?, 2020, S. 45 (65).

[66] Im Unterschied dazu, erfolgt die Einwilligung regelmäßig formell getrennt von den allgemeinen Nutzungsbedingungen, so dass ihr tendenziell eine höhere Aufmerksamkeit zu Teil wird. Obwohl diese von Verbrauchern regelmäßig ungelesen erteilt wird, ist sich das Datensubjekt als Vertragspartner zumindest abstrakt darüber im Klaren, dass personenbezogene Daten verarbeitet werden. Für Ansätze zur Verbesserung der Transparenz unten Kapitel 6.

[67] *Wurmnest*, MüKo, BGB, 2020, § 307, Rn. 1.

[68] *Hayek*, (1945) 35 American Economic Review 519 (525 ff.); *Stigler*, The Theory of Price, 1987, S. 11 ff.

Infolgedessen bildet die (Haupt-)Leistung, die ein Verantwortlicher im Austausch gegen den Zugang zu personenbezogenen Daten bereitstellt, regelmäßig das einzige wesentliche Kriterium, an dem Verbraucher ihre Nachfrage ausrichten können. Dieser Fokus auf das Angebot des Verantwortlichen setzt für diesen einen Anreiz, alle Anstrengungen darauf zu konzentrieren, möglichst attraktive Leistungen, beispielsweise in Form von digitalen Produkten, anbieten zu können. Um diese finanzieren zu können, ist es im Gegenzug erforderlich, die im Austausch bereitgestellten personenbezogenen Daten möglichst umfassend und effizient zu verarbeiten und zugunsten von zahlungsbereiten Dritten, insbesondere Werbekunden, zu monetisieren. Solange die Datensubjekte den Bedingungen der Leistungsbeschreibung keine Aufmerksamkeit entgegenbringen und solange diese fehlende Aufmerksamkeit nicht durch transparente, einfach zu verarbeitende standardisierte Information kompensiert – zumindest aber ergänzt – wird,[69] existiert kein vertrauenswürdiges Signal, auf dessen Grundlage das Datensubjekt den Wert personenbezogener Daten und infolgedessen das Preis-Leistungs-Verhältnis des Angebots bewerten und es anschließend mit den Angeboten anderer Verantwortlicher vergleichen kann.[70]

Infolgedessen scheiden jene Anbieter langsam aus dem Markt aus, die vor einer Monetisierung der personenbezogenen Daten entweder zurückschrecken oder diese Daten weniger umfassend und weniger effizient verarbeiten können. Erfolg haben diejenigen Anbieter, die jede weitere Möglichkeit zur Monetisierung von personenbezogenen Daten nutzen, um dadurch ihr Angebot an digitalen Produkten noch attraktiver zu gestalten, ihren Marktanteil zu erhöhen und ihren monetären Gewinn zu steigern.[71]

Somit ist der Markt, auf dem Anbieter ihre Leistungen im Austausch gegen einen (rechtmäßigen) Zugang zu personenbezogenen Daten gewähren, ein atypischer „Zitronenmarkt". Atypisch ist dieser Zitronenmarkt deshalb, weil nicht die Qualität der Hauptleistung infolge einer adversen Selektion (sog. *race to the bottom*) sinkt, sondern der (intransparente) „Datenpreis" steigt. Das tatsächliche Schutzniveau für personenbezogene Daten und die Privatsphäre der Datensubjekte sinkt bei gleichzeitiger „Verbesserung" bzw. Ausweitung des im Gegenzug bereitgestellten Zugangs zu digitalen Produkten.[72]

---

[69] Für den Vorschlag einer Kombination aus farblicher Kennzeichnung und Privacy Score: Kapitel 6 A.

[70] Dies gilt ebenfalls für Gerichte: Unten e).

[71] Hiervon unabhängig profitieren *GAFAM* zusätzlich von direkten und indirekten Netzwerkeffekten.

[72] Insofern ist es nicht verwunderlich, dass Apple sich zuletzt und sehr öffentlichkeitswirksam für ein (angeblich) hohes Niveau von Datenschutz einsetzt. Im Unterschied zu *Facebook*, aber auch *Alphabet*, die ihre Geschäftsmodelle überwiegend durch personalisierte Werbung finanzieren, basiert das Geschäftsmodell von *Apple* zusätzlich darauf, Endprodukte gegen monetäres Entgelt zu verkaufen.

Im Gegensatz zu klassischen Zitronenmärkten – wie beispielsweise der Markt für Gebrauchtfahrzeuge –, die nach *Akerlof* aufgrund fehlender Transparenz über die Produktqualität irgendwann gänzlich zum Erliegen kommen,[73] ist ein Wegfall der Nachfrage für das Geschäftsmodell, das auf einem Zugang zu digitalen Produkten gegen einen Zugang zu personenbezogenen Daten beruht, aus zwei Gründen nicht zu erwarten. Obwohl die Kenntnis über eine abstrakte Werthaltigkeit personenbezogener Daten zunimmt, kann die Illusion vom „kostenlosen" oder sehr günstigen Zugang zu digitalen Produkten aufrechterhalten werden, solange der unmittelbare ökonomische Wert von personenbezogenen Daten nicht transparent(er) wird.[74] Zudem wird die Nachfrage nach digitalen Produkten im Austausch gegen eine Gewährung von Zugang zu personenbezogenen Daten auch deshalb nicht einbrechen, weil die fehlende Rivalität hinsichtlich der Nutzung von personenbezogenen Daten[75] die Nachfrage aufrecht erhält. Als Folge der immateriellen Natur und der nahezu kostenlosen und verlustfreien Reproduzierbarkeit von personenbezogenen Daten werden diese nicht knapp. Aus ökonomischer Perspektive[76] sind dem Geschäftsmodell einer Gewährung von Zugang zu digitalen Produkten im Austausch gegen Zugang zu personenbezogenen Daten deshalb kaum Grenzen gesetzt, solange die monetäre Zahlungsbereitschaft derjenigen Unternehmen steigt, die durch ihre Zahlungsbereitschaft für personalisierte Werbung und andere datenbasierte Dienste den Erfolg von mehrseitigen Plattformen als Anbieter von digitalen Produkten begründen. Die Qualität personenbezogener Daten und ihr Wert mag zwar abhängig von der Kaufkraft und Konsumbereitschaft des Datensubjekts schwanken. Eine knappe Ressource sind personenbezogene Daten aufgrund der fehlenden Abnutzung[77] und der fehlenden Rivalität in der Nutzung jedoch nicht.[78]

c) Geringe Kompensation durch eine aufmerksame Minderheit

Empirische Forschung weist darauf hin, dass die Verteilung der Datenschutzpräferenzen in den USA in einer U-förmigen Kurve verläuft. Danach wird der Schutz von personenbezogenen Daten und der Privatsphäre (privacy) entweder für sehr wichtig gehalten oder ihm wird kein Interesse entgegengebracht.[79] Un-

---

[73] *Akerlof*, 84 The Quarterly Journal of Economics 1970, 488 ff.

[74] Zu der hieraus folgenden Notwendigkeit einer transparenzsteigernden Kennzeichnung, unten Kapitel 6 A.II.4.

[75] Hierzu: *Zech*, in: Pertot (Hrsg.), Rechte an Daten, 2020, S. 91 (99).

[76] Zu den kartellrechtlichen Grenzen gemäß § 19 GWB zuletzt: *BGH*, Beschl. v. 23.06.2020 – KVR 69/19 = GRUR 2020, 1318 ff. – *BKartA/Facebook*. Im Anschluss hieran: *OLG Düsseldorf*, Vorlagebeschl. v. 24.03.2021, Kart 2/19 (V).

[77] Allerdings kann die Relevanz der Information sich reduzieren, sobald diese nicht mehr aktuelle Auskunft über (unbefriedigte) Präferenzen des Datensubjekts gibt.

[78] *Zech*, in: Pertot (Hrsg.), Rechte an Daten, 2020, S. 91 (99).

[79] *Acquisti/John/Loewenstein*, 'What is Privacy Worth?' (2009) Working Paper, 26 http://

abhängig von der genauen Verteilung der Präferenzen, sollen jedenfalls die beiden extremen Positionen am jeweiligen Ende des Spektrums tendenziell besonders stark ausgeprägt sein. Sollte dieser Befund sich als zuverlässig herausstellen, so ergeben sich daraus potenziell gegensätzliche Konsequenzen für die inhaltliche Kontrolle von AGB, die personenbezogene Daten als Leistungsgegenstand definieren.

Einerseits greift das von Art. 4 Abs. 2 Klausel-RL vorausgesetzte Postulat der gesteigerten Aufmerksamkeit für den vertraglichen Hauptgegenstand nicht, soweit Datensubjekten der Schutz von personenbezogenen Daten – unabhängig von den Gründen hierfür – nicht wichtig ist. Diejenigen Verbraucher, die weder die Leistungsbeschreibung lesen noch ein Interesse am Schutz von personenbezogenen Daten und ihrer Privatsphäre haben, werden auch durch zusätzliche Maßnahmen zur Förderung von Transparenz (Informationsmodell) kaum davon zu überzeugen sein, ihr Verhalten künftig zu ändern und der Leistungsbeschreibung und deren Auswirkung auf die Datenverarbeitung eine größere Aufmerksamkeit zu schenken. Dies spricht ebenfalls dafür, eine Angemessenheitskontrolle des vertraglichen Synallagmas zuzulassen, so dass es Gerichten im Grundsatz ermöglicht würde, mit Hilfe von mathematischen Modellen und Sachverständigengutachten zu überprüfen,[80] ob zwischen der bereitgestellten Hauptleistung und den im Gegenzug bereitgestellten oder vertraglich versprochenen personenbezogenen Daten ein angemessenes Verhältnis besteht.

Andererseits lässt sich aus der U-förmigen Verteilung der Präferenzen jedoch auch ein Argument gegen eine gerichtliche Angemessenheitskontrolle des vertraglichen Synallagmas ableiten. Die Gruppe derjenigen Datensubjekte, die eine hohe Präferenz für den Schutz ihrer Privatsphäre und ihrer personenbezogenen Daten haben, könnte den AGB eine repräsentative Aufmerksamkeit schenken.[81] Sofern diese Gruppe der aufmerksamen Skeptiker für die Anbieter eine ausreichende ökonomische Größe hat, werden sie auf deren Präferenz reagieren. In der Folge würden auch Angebote unterbreitet, die in einem geringeren Aus-

---

pages.stern.nyu.edu/~bakos/wise/papers/wise2009-6a1_paper.pdf, zuletzt abgerufen am 19.05. 2022.

[80] *Hacker*, in: Lohsse/Schulze/Staudenmayer (Hrsg.), Data as Counter-Performance – Contract 2.0?, 2020, S. 45 (51 f./71).

[81] Vgl. *Gottschalk*, AcP 206 (2006), 555 (564); *Beimowski*, Zur ökonomischen Analyse Allgemeiner Geschäftsbedingungen, 1989, S. 108 f.; *Wagner/Eidenmüller*, 86 University of Chicago Law Review 2019, 581 (607); *Obar/Oehldorf-Hilsch*, 21 Information, Communication & Society 2018, S. 1; *Bakos/Marotta-Wurgler/Trossen*, 43 The Journal of Legal Studies 2014, S. 1; *Ben-Shahar/Chilton*, 45 Journal of Legal Studies 2016, S. 41. Im Lauterkeitsrecht besteht hierzu ein Unterschied. Existieren gespaltene Auffassung durch unterschiedliche Verkehrskreise und werden diese unterschiedlichen Kreise einheitlich – durch Werbung – angesprochen, so kann sich die lauterkeitsrechtliche Beurteilung nach dem strengeren Maßstab richten. Hierzu: *Sosnitza*, WRP 14, 1136 (1141); *Bornkamm/Feddersen*, in: Köhler/Bornkamm/Feddersen (Hrsg.), § 5 UWG, 39. Aufl. 2021 Rn. 1.64.

maß auf die Verarbeitung von personenbezogenen Daten setzen.[82] Diese Angebote würden entweder eine Reduktion der bereitgestellten (digitalen) Produkte vorsehen oder eine Erhöhung des in Geld zu zahlenden Anteils der Gegenleistung.[83]

Eine zunehmende Anzahl der Webseiten von Zeitungen und Nachrichtenmagazinen zeichnen diese Ausdifferenzierung beispielhaft vor.[84] Wenngleich solche datenschonenden Angebote gegen Zahlung von Geld nur für Datensubjekte in Betracht kommen, die sich eine (teilweise) Zahlung eines monetären Preises leisten können und wollen und die nicht dem sog. *privacy-paradoxon* erliegen, hat diese aus personenbezogenen Daten und Geld gemischte oder rein monetäre Gegenleistung auf einem transparenten Markt immerhin eine Signal-Wirkung.[85] Infolgedessen könnten Datensubjekte mit Präferenz für einen besseren Schutz von personenbezogenen Daten eine signifikante Auswirkung auf den Konditionenwettbewerb haben und so dabei helfen, das Bewusstsein und die Bemessungsgrundlage für den ökonomischen Wert von personenbezogenen Daten zu verbessern. Dennoch kann dieses Signal nicht verhindern, dass Menschen rationalen Begrenztheiten unterliegen und die Mehrheit der Datensubjekte den vermeintlich kostenlosen, aber datenbasierten Zugang der Zahlung eines geringen monetären Preises vorziehen, selbst wenn sie zuvor eine Präferenz für einen starken Schutz von personenbezogenen Daten bzw. ihrer Privatsphäre bekundet haben.[86]

d) Keine abschließende Regelung durch die Klausel-RL

Die Auseinandersetzung mit den Wertungen, die Art. 4 Abs. 2 Klausel-RL zugrunde liegen, hat gezeigt, dass jedenfalls ein wesentliches Argument dafür, den vertraglichen Hauptgegenstand keiner Inhalts-, sondern lediglich einer Trans-

---

[82] Zur Frage, ob und inwieweit eine solche Alternative gemäß Art. 7 Abs. 4 DS-GVO verpflichtend anzubieten ist: Unten A.II.4. sowie Kapitel 5 C.II.1.a.

[83] Die Wahrscheinlichkeit für solche alternativen Angebote hängt jedoch nicht nur von der Größe dieser Gruppe und Kaufkraft ihrer Mitglieder ab, sondern auch davon, ob diese in der Lage sind, ihre Präferenzen aufrecht zu erhalten. Notwendige Voraussetzung dafür ist ein ausreichender Wettbewerb zwischen Anbietern, der solche Angebote begünstigt.

[84] Vorrangiger Grund für dieses zweifache Angebot dürfte derzeit jedoch sein, dass risikoaverse Anbieter den Art. 7 Abs. 4 DS-GVO streng im Sinne eines sog. anbieterbezogenen Kopplungsverbots auslegen und deshalb alternative Angebote machen, um die Freiwilligkeit der Einwilligung zu wahren. Hierzu: Unten Kapitel 4 A.II.4. und Kapitel 5 C.II.1.a.

[85] Diese Signalwirkung bliebe selbst dann bestehen, wenn es Verantwortlichen gelingen würde, unterschiedliche Datensubjekte mit unterschiedlichen Präferenzen personalisierte Angebote zu machen, so dass der Wettbewerb um die skeptischen Datensubjekte keine Auswirkungen auf die Konditionen für andere Datensubjekte hat. Hierzu: *Hacker*, Datenprivatrecht, 2020, S. 588 f.

[86] Zur empirisch nachweisbaren Diskrepanz zwischen bekundeter Präferenz und tatsächlichem Verhalten: *Preibusch/Kübler/Beresford*, 13 Electronic Commerce Research (2013), 423 (441/444 f.).

parenzkontrolle zu unterziehen, nicht überzeugt, soweit personenbezogene Daten als Leistungsgegenstand vereinbart werden. Das Postulat einer gesteigerten Aufmerksamkeit, wonach die Vertragsparteien ihre volle Aufmerksamkeit auf den vertraglichen Hauptgegenstand richten und dieser deshalb einen wesentlichen Wettbewerbsparameter bildet, ist mit Blick auf die Vereinbarungen eines Zugangs zur Verarbeitung von personenbezogenen Daten regelmäßig nicht erfüllt. Dieses Defizit spricht im Ausgangspunkt dafür, die Ausnahme in Art. 4 Abs. 2 Klausel-RL bzw. § 307 Abs. 3 S. 1 BGB nicht anzuwenden, sofern personenbezogene Daten als Leistungsgegenstand vereinbart werden.[87]

Eine solche Kontrolle der Angemessenheit von Haupt- und Gegenleistung durch die mitgliedstaatlichen Gerichte wäre möglich, weil die Klausel-RL gemäß Art. 8 lediglich Mindestvorgaben enthält. Tatsächlich sahen spanische Gerichte eine weitergehende und unionskonforme Inhaltskontrolle des vertraglichen Hauptgegenstands und der Angemessenheit von Preis und Leistung vor.[88] Diese Rechtsprechung ist nach Ansicht des *EuGH* mit der Klausel-RL vereinbar,[89] weil Art. 8 Klausel-RL die Möglichkeit für die Mitgliedstaaten eröffne, ein höheres Schutzniveau vorzusehen, indem auch der Hauptgegenstand des Vertrages sowie die Angemessenheit des Entgelts einer Inhaltskontrolle unterworfen werden.[90] Der *EuGH*-Entscheidung lag eine Klausel zugrunde, welche eine spanische Bank in Kreditverträgen zur Finanzierung eines Wohnungskaufs vorsah. Besonderheit dieser Klausel war, dass diese neben dem variablen Zinssatz eine Regelung enthielt, wonach der im Vertrag vorgesehene variable, periodisch anzupassende Nominalzinssatz ab der ersten Anpassung auf den nächsthöheren Viertelprozentpunkt aufgerundet wurde. Die spanischen Instanzengerichte beurteilten diese Aufrundungsklausel als missbräuchlich.

Der *Tribunal Supremo* begründete zunächst, warum diese Aufrundungsklausel ein Bestandteil des Hauptgegenstands des Vertrags im Sinne des Art. 4 Abs. 2 Klausel-RL ist. Da Spanien jedoch Art. 4 Abs. 2 Klausel-RL nicht ins nationale Recht umgesetzt hatte, stand es den spanischen Gerichten nach nationalem Recht frei, auch den Hauptgegenstand auf seine Angemessenheit zu überprüfen. Nach Aussetzung und Vorlage zum *EuGH* bestätigte letzterer, dass eine solche vollständige Angemessenheitsprüfung mit der Klausel-RL vereinbar ist, weil diese gemäß Art. 8 Klausel-RL lediglich eine Mindestharmonisierung schaffe und es deshalb den Mitgliedstaaten freistehe, die Ausnahme des Hauptgegenstands und des Preis-Leistungs-Verhältnisses gemäß Art. 4 Abs. 2

---

[87] Für eine solche (generelle) Angemessenheitskontrolle: *v. Westphalen/Wendehorst*, BB 2016, 2179 (2186).

[88] Hierzu: *Cámara Lapuente*, in: Terryn, Evelyn u. a. (Hrsg.), FS Stuyck, 2013, S. 581 (596 ff.); *Blendel*, Die Ausnahme des Hauptgegenstands und der Angemessenheit von Preis und Leistung von der Inhaltskontrolle, 2014, S. 142/152 ff.

[89] Zur Unionskonformität der spanischen Rechtsprechung: *EuGH*, Urt. v. 03.06.2010, C-284/08 = NJW 2010, 2265 (Rn. 29 ff.) – *Caja de Ahorros*.

[90] *EuGH*, Urt. v. 03.06.2010, C-284/08 = NJW 2010, 2265 (Rn. 44) – *Caja de Ahorros*.

Klausel-RL – im Interesse eines höheren Verbraucherschutzes – nicht ins nationale Recht umzusetzen.

Somit belässt die Klausel-RL auch deutschen Gerichten die Möglichkeit, B2C-Verträge, die auf Grundlage von AGB zustande gekommen sind, einer allgemeinen Angemessenheitskontrolle gemäß § 138 BGB zu unterziehen.[91] Allerdings würde ein solcher Rückgriff auf das nationale Recht die europäischen Harmonisierungsziele beeinträchtigen und eine große Diskrepanz hinsichtlich der Kontrolltiefe in den EU-Mitgliedstaaten könnte eine Angleichung und damit europäisches Sekundärrecht erforderlich machen.

Zusammengefasst: Es gibt gute Gründe dafür, dass Gerichte weder den vertraglichen Hauptgegenstand noch das Preis-Leistungs-Verhältnis auf ihre Angemessenheit überprüfen. Das europäische Sekundärrecht steht einer solchen Kontrolle durch die Gerichte der Mitgliedstaaten auf Grundlage des nationalen Rechts jedoch nicht im Weg.[92] Im Unionsrecht setzt erst die grundrechtlich gemäß Art. 16 GRCh bzw. Art. 6 Abs. 3 EUV zu gewährleistende Vertragsfreiheit einer unbegrenzten und undifferenzierten Kontrolle der *essentialia negotii* eine Grenze.[93]

e) Fehlender Maßstab für eine gerichtliche Angemessenheitskontrolle

Die fehlende Aufmerksamkeit der Verbraucher für den Hauptgegenstand, die fehlende aufmerksame Minderheit, die den Wettbewerb aufrechterhält, und die Tatsache, dass die Klausel-RL lediglich mindestharmonisierend ist, machen den Weg zu einer gerichtlichen Angemessenheitskontrolle des vertraglichen Synallagmas grundsätzlich frei. Sofern also Zweifel daran bestehen, dass sowohl die Klauseln über die Verarbeitung von personenbezogenen Daten (Art. 6 Abs. 1 lit. b DS-GVO) als auch die Einwilligung (Art. 6 Abs. 1 lit. a DS-GVO) Parameter sind, die dem Wettbewerb unterliegen, können diese Leistungsvereinbarungen als AGB – einschließlich der Einwilligung – einer gerichtlichen Angemessenheitskontrolle unterliegen (sog. *Kontrollunterworfenheit*).

---

[91] Diesen Weg kann man über eine teleologische Reduktion von Art. 4 Abs. 2 Klausel-RL bzw. § 307 Abs. 3 BGB erreichen (so: *Hacker*, in: Lohsse/Schulze/Staudenmayer (Hrsg.), Data as Counter-Performance – Contract 2.0?, 2020, S. 45 (66). Alternativ genügt es, § 138 BGB schlicht anzuwenden, weil die Klausel-RL lediglich mindestharmonisierend ist, Art. 8 Klausel-RL.

[92] *EuGH*, Urt. v. 03.06.2010, C-284/08 = NJW 2010, 2265 (Rn. 50) – *Caja de Ahorros*. Mit einer detaillierten Analyse der *EuGH*-Rechtsprechung zu den Grenzen der Inhaltskontrolle gemäß Art. 4 Abs. 2 Klausel-RL: *Steinmetz*, Die Kontrollsperre des § 307 Abs. 3 BGB bei Verträgen über immaterielle Gegenstände, 2022, S. 134 ff.

[93] Hierzu: *Lüttringhaus*, Vertragsfreiheit und ihre Materialisierung im Europäischen Binnenmarkt, 2018, S. 603 f.; sowie *Steinmetz*, Die Kontrollsperre des § 307 Abs. 3 BGB bei Verträgen über immaterielle Gegenstände, 2022, S. 125: „Im Wege der Rückausnahme nimmt § 307 Abs. 3 S. 1 BGB sodann wieder solche Klauseln von der Inhaltskontrolle aus, bei denen die Vermutung der AGB-rechtlichen Schutzbedürftigkeit widerlegt ist und es damit an einem legitimen Zweck oder jedenfalls an der Erforderlichkeit bzw. Angemessenheit des Eingriffs in die formale Freiheit fehlt".

Allerdings ist die unionsrechtliche Zulässigkeit einer Angemessenheitskontrolle eine notwendige, aber noch keine hinreichende Bedingung für eine effektive gerichtliche Kontrolle. Wesentliche Einwände gegen eine gerichtliche Überprüfung der Angemessenheit des vertraglichen Hauptgegenstands bleiben die fehlende verlässliche Grundlage für die Wertberechnung von personenbezogenen Daten und der fehlende Maßstab für eine anschließende Beurteilung, ob der Zugang zu und die Verarbeitung von personenbezogenen Daten in einem angemessenen Verhältnis zu der im Gegenzug erhaltenen Leistung stehen (sog. *Kontrollfähigkeit*).[94]

Die bisher vorgeschlagenen Ansätze zur Überprüfung der Angemessenheit des Austauschverhältnisses sind wissenschaftlich spannend,[95] aber in der Praxis nicht mit vertretbarem Aufwand umsetzbar. Beispielsweise kann die Bewertung von Datensätzen im Rahmen einer Unternehmenstransaktion am Kapitalmarkt einen Hinweis auf den Wert von durchschnittlichen Datensätzen geben.[96] Für eine konkrete Angemessenheitskontrolle ist dieser Wert jedoch allenfalls als Ausgangpunkt geeignet. Auch die Befragung von Experten oder der Datensubjekte kann allenfalls einen ersten groben Ansatzpunkt für einen solchen (subjektiven) Wert geben.[97]

Unter Berücksichtigung des datenschutzrechtlichen Grundsatzes von Treu und Glauben (Art. 5 Abs. 1 lit. a Var. 2 DS-GVO) und – so ein Vorschlag von *Philipp Hacker* – unter (adaptierter) Anwendung der *EuGH*-Rechtsprechung zu *Aziz*[98] und *Menéndez Álvarez*[99] soll die Angemessenheit der Leistungspflichten zumindest einer Evidenzkontrolle unterzogen werden.[100] Im Ergebnis würden Vereinbarungen von personenbezogenen Daten als Leistungsgegenstand eine unangemessene Benachteiligung bedeuten, soweit

„sie nicht das Ergebnis einer hypothetischen, individuellen Vertragsverhandlung des Verwenders mit einem Referenzakteur sein können. Dieser Referenzakteur ist grundsätzlich ein durchschnittlicher Nutzer mit mittelmäßig ausgeprägten Datenschutzpräferenzen".[101]

Dieses Vorgehen ist ein in der Theorie plausibler Ansatz, liefert allerdings nur einen Durchschnittswert, basiert auf einer immensen Komplexität und ist des-

---

[94] Mit dem überzeugenden Appell, auch in der gerichtlichen Begründung künftig eindeutig zwischen der Kontrollunterworfenheit und der Kontrollfähigkeit zu unterscheiden: *Steinmetz*, Die Kontrollsperre des § 307 Abs. 3 BGB bei Verträgen über immaterielle Gegenstände, 2022, These 6.

[95] *Hacker*, in: Lohsse/Schulze/Staudenmayer (Hrsg.), Data as Counter-Performance – Contract 2.0?, 2020, S. 51 ff.

[96] *OECD*, Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value, 2013, S. 18 ff.

[97] *Acquisti/Taylor/Wagman*, (2016) 54 Journal of Economic Literature, 442 (444/447).

[98] *EuGH*, Urt. v. 14.03.2013, C-415/11 = EuZW 2013, 464 (Rn. 68) – *Aziz*.

[99] *EuGH*, Urt. v. 16.01.2014, C-226/12 = BeckRS 2014, 80035 (Rn. 21 f.) – *Menéndez Álvarez*.

[100] *Hacker*, Datenprivatrecht, 2020, S. 445 ff./473 ff.

[101] *Hacker*, Datenprivatrecht, 2020, S. 474.

halb nicht geeignet, leicht praktikable und belastbare Richtwerte für die Angemessenheit zu liefern.

Letztlich existiert weder „die" stabile Datenschutzpräferenz noch „der" Wert von personenbezogenen Daten.[102] Während die Eigenkapitalrendite eines Unternehmens immerhin einen Hinweis darauf geben kann, welchen Wert ein Unternehmen auf Grundlage einer standardisierten Währungseinheit schöpft, bleibt die „Fremddatenrendite" ein Geschäftsgeheimnis und dürfte, abhängig vom jeweiligen Verantwortlichen und vom jeweiligen Datensatz, sehr stark schwanken. Solange die erfolgreichsten Verantwortlichen ihre Wertschöpfungsprozesse nicht offenlegen (müssen), bleibt die Bewertung von personenbezogenen Daten spekulativ und eine Bezifferung anhand eines durchschnittlichen Referenzakteurs setzt eine selbstbewusste Anmaßung von Wissen voraus. Schätzungen nach § 287 ZPO, allgemeine Vermutungsregeln und eine Beweislastumkehr mögen dabei helfen, einen plausibilisierten Wertkorridor zu ermitteln, bleiben aber sehr grobe Instrumente.

In Kenntnis dieser Schwierigkeit hat der europäische Gesetzgeber sich einstweilen dafür entscheiden, die Gerichte davor zu bewahren, den Wert von personenbezogenen Daten beziffern zu müssen.[103] Gemäß Art. 14 Abs. 4 DID-RL ist kein Minderungsrecht zugunsten von Verbrauchern vorgesehen, sofern diese für den Zugang zu nicht vertragsgemäß bereitgestellten digitalen Produkten keinen Preis in Geld bezahlt haben. Der Ausschluss einer (angemessenen) Minderung der bereitzustellenden personenbezogenen Daten soll stattdessen durch eine erleichterte Möglichkeit zur Vertragsbeendigung kompensiert werden, Art. 14 Abs. 6 DID-RL. Dadurch wurde die Herausforderung einer monetären Bewertung von personenbezogenen Daten einstweilen vermieden.

Soweit personenbezogene Daten als Leistungsgegenstand vereinbart werden, stellt sich das identische Problem erneut, sofern schuldrechtliche Ansprüche auf Schadensersatz beziffert werden müssen. Vor dieser Schwierigkeit hat der deutsche Gesetzgeber die Gerichte mit § 327q Abs. 3 BGB ebenfalls bewahrt. Hiernach sind

> „Ersatzansprüche des Unternehmers gegen den Verbraucher wegen einer durch die Ausübung von Datenschutzrechten oder die Abgabe datenschutzrechtlicher Erklärungen bewirkten Einschränkung der zulässigen Datenverarbeitung […] ausgeschlossen."

Auch der alternative Ansatz, mithilfe von (vermeintlich) evidenten Regelbeispielen eine Annäherung an die Unangemessenheit zu entwickeln, ist sehr beschränkt. So mag auf den ersten Blick eine Vermutung dafür sprechen, dass eine

---

[102] So bereits zutreffend: *Buchner*, Die Informationelle Selbstbestimmung im Privatrecht, 2006, S. 178.

[103] Umgekehrt bietet eine asymmetrische, kartellrechtsakzessorische Anwendung von Art. 7 Abs. 4 DS-GVO i. R. d. Einwilligung eine Möglichkeit, marktmächtige Verantwortliche dazu zu zwingen, ihre Leistungen alternativ gegen einen bezifferten monetären Preis anzubieten. Hierzu unten: Kapitel 5 C.II.1.

App, die – nach Einwilligung des Verbrauchers – ein vollständiges GPS-Bewegungsprofil des Nutzers erstellt und im Gegenzug lediglich eine manuelle Steuerung eines LED-Licht am Smartphone ermöglicht (Taschenlampen-App), offenkundig auf einem unangemessenen Leistungsverhältnis beruht.[104] Berücksichtigt man jedoch, dass die Preisgabe von personenbezogenen Daten und die Zustimmung zu Werbemaßnahmen rechtlich statthaft ist, um im Gegenzug eine marginale Chance auf Zuteilung eines ausgelobten Preises zu erlangen,[105] so wird deutlich, dass die Bestimmung eines angemessenen Daten-Leistungs-Verhältnisses noch sehr viel schwieriger ist, als die Bestimmung eines gerechten monetären Preises.[106]

Infolgedessen ist eine praktische Anwendung der bestehenden Möglichkeiten zur Wertermittlung durch die Gerichte sehr unwahrscheinlich, weil sie Berechnungen mit Hilfe komplexer mathematische Modelle durch Experten voraussetzen, die allenfalls in besonders eklatanten (Ausnahme-)Fällen einer datenbasierten *laesio enormis* dazu führen können, den vertraglichen Hauptgegenstand als evident unangemessen zu bewerten.

Solange Kartellbehörden und hierauf spezialisierte Gerichte erhebliche Zweifel daran haben, dass der Marktmechanismus als Entdeckungsverfahren funktioniert, weil auf makroökonomischer Ebene gravierende wettbewerbliche Defizite bestehen, dürfte es den nationalen Gerichten der Mitgliedstaaten kaum gelingen, zuverlässige Werte für eine mikroökonomische Angemessenheitskontrolle zu ermitteln.

Es besteht noch ein weiterer Grund dafür, dass die Gerichte sich weder über Art. 6 Abs. 1 lit. b DS-GVO noch im Rahmen der datenschutzrechtlichen Einwilligung auf das Terrain mathematischer Modellrechnungen begeben werden. Die DS-GVO stellt ihnen wesentlich leichter anzuwendende Instrumente zur Verfügung, um die Datenverarbeitung eines Verantwortlichen im Einzelfall scheitern zu lassen.

---

[104] Mit diesem und weiteren Beispiel: *Hacker*, in: Lohsse/Schulze/Staudenmayer (Hrsg.), Data as Counter-Performance – Contract 2.0?, 2020, S. 43 (71).

[105] Mit sehr knapper Begründung: *OLG Frankfurt a. M.*, Urt. v. 27.06.2019, 6 U 6/19 = ZD 2019, 507 (Rn. 12).

[106] Obwohl die kartellrechtliche Kontrolle gegen Konditionenmissbrauch es nicht voraussetzt, den Wert von Daten monetär zu bemessen, zeigen die Entscheidungen im Verfahren des *BKartA* gegen *Facebook* bereits die Schwierigkeiten auf, die bei einer ökonomischen Bewertung datenbasierter Dienste entstehen („Nach den Feststellungen des Bundeskartellamts *wünschen* erhebliche Teile der privaten *Facebook*-Nutzer einen geringeren Umfang der Preisgabe persönlicher Daten. Bei funktionierendem Wettbewerb auf dem Markt sozialer Netzwerke *wäre* ein entsprechendes Angebot *zu erwarten*. Hierauf *könnten* Nutzer ausweichen, für die der Umfang der Datenpreisgabe ein wesentliches Entscheidungskriterium *wäre*." [Hervorhebungen durch den Verfasser]: Pressemitteilung des *BGH*, Beschl. v. 23.06.2020, KVR 69/19 – *BKartA/Facebook*.

3. Verdrängung der Klausel-RL durch die DS-GVO

Formal lassen sich die Anwendungsbereiche der Klausel-RL und der DS-GVO stringent abgrenzen. Die Pflicht zur Bereitstellung personenbezogener Daten als Leistungsgegenstand wird regelmäßig in den Vertragsklauseln oder der Einwilligung durch den Verantwortlichen vorformuliert, so dass es sich in beiden Fällen grundsätzlich um AGB handelt (a).[107] Tatsächlich wird die DS-GVO den eigenständigen Anwendungsbereich der Klausel-RL jedoch weitgehend überlagern, soweit eine Klausel datenschutzrechtliche Bezüge aufweist. Die Erlaubnistatbestände (Art. 6 DS-GVO) und Grundsätze der rechtmäßigen Datenverarbeitung (Art. 5 DS-GVO) eröffnen ein außerordentliches Potenzial für Einzelfallerwägungen und sind deshalb für die gerichtliche Praxis attraktiv (b).

a) Verhältnis von Klausel-RL und DS-GVO

Das AGB-rechtliche Transparenzgebot (Art. 5 S. 1 Klausel-RL) und die Angemessenheitskontrolle (Art. 3 Abs. 1 Klausel-RL) gehen davon aus, dass ein B2C-Vertrag auf Grundlage von vorformulierten Bedingungen des Unternehmers zustande kommt. Für die Anforderungen an eine rechtmäßige Datenverarbeitung auf Grundlage von Art. 6 Abs. 1 lit. b DS-GVO kommt es nicht auf den Status als Verbraucher an und es ist irrelevant, ob der Vertrag – so regelmäßig – auf AGB basiert. Infolgedessen lassen sich DS-GVO und Klausel-RL zunächst in personeller Hinsicht abgrenzen. Die DS-GVO regelt die Voraussetzungen für eine rechtmäßige Datenverarbeitung zwischen Verantwortlichem und Datensubjekt. Die Klausel-RL etabliert Mindestanforderungen an eine wirksame Verwendung vorformulierter Vertragsklauseln im Verhältnis zwischen Unternehmer und Verbraucher.

Allerdings sind die Vorgaben der DS-GVO an eine wirksame Vereinbarung im Vergleich zur Klausel-RL zugleich strenger und flexibler. Dies gilt insbesondere für eine wirksame Einwilligung, weil die DS-GVO hierfür umfangreiche Anforderungen formuliert (Art. 4 Nr. 11, Art. 6 Abs. 1 lit. a, Abs. 2, Art. 7 und Art. 9).[108] Jenseits dieser spezifischen Anforderungen an die Einwilligung ermöglichen die abstrakten Grundsätze der rechtmäßigen Datenverarbeitung

[107] *Wendehorst/v.Westphalen* weisen darauf hin, dass das Bewusstsein für die vielfachen Vertragsschlüsse gering ausgebildet ist: „Dabei ist nicht nur zu konstatieren, dass Verträge massenhaft und meist ohne hinreichend qualifiziertes Erklärungsbewusstsein des Nutzers geschlossen werden, sondern auch, dass der Nutzer kaum eine Möglichkeit hat, die zahlreichen Vertragsschlüsse zu vermeiden", *dies*., NJW 2016, 3745 (3746).

[108] Somit ist fraglich, ob die AGB-Kontrolle zusätzliche Kriterien zu bieten vermag, die nicht bereits in den spezifischeren Anforderungen an die Einwilligung und in den Grundsätzen der rechtmäßigen Datenverarbeitung (Art. 5 Abs. 1 DS-GVO) enthalten sind: Unter dem BDSG a. F. für eine Berücksichtigung der „datenschutzrechtlichen Maxime einer freiwilligen, informierten und bestimmten Einwilligung" in der AGB-Kontrolle: *Buchner*, Die informationelle Selbstbestimmung im Privatrecht, 2006, S. 253.

gemäß Art. 5 Abs. 1 DS-GVO den Gerichten eine sehr flexible rechtliche Argumentation. Infolgedessen überzeugt es nicht, wenn aufgrund des lediglich mindestharmonisierenden Charakters der Klausel-RL eigenständige nationale Regelung in §§ 308, 309 BGB über die Wirksamkeit datenschutzrechtlicher Einwilligungen entscheiden sollen,[109] so dass diese neben der DS-GVO eine eigenständige Bedeutung erlangen, soweit personenbezogene Daten als Leistungsgegenstand vereinbart werden. Nationale Gerichte sind nicht daran gehindert, sowohl individuelle als auch vorformulierte Einwilligungserklärungen am Grundsatz der Datenverarbeitung nach Treu und Glauben (Art. 5 Abs. 1 lit. a Var. 2 DS-GVO) scheitern zu lassen, sofern die Einwilligung in den relevanten Konstellationen nicht bereits an den Hürden der Informiertheit und Freiwilligkeit gemäß Art. 4 Nr. 11 i. V. m. Art. 7 Abs. 4 DS-GVO hängengeblieben ist.[110] Haben die nationalen Institutionen Zweifel an diesem Weg, so müssen sie diesen zunächst dem *EuGH* vorlegen. Dadurch bleibt der Vorrang der DS-GVO und ihre unionweit einheitliche Anwendung gewahrt. Es besteht dann eine höhere Chance dafür, dass die Wirksamkeit der Einwilligung unionsweit einheitlichen Maßstäben folgt und damit zum Katalysator des freien Verkehrs personenbezogener Daten im Binnenmarkt wird, statt sich in den Netzen des jeweiligen nationalen AGB-Rechts zu verfangen.[111]

Teilweise wird die Ansicht vertreten, dass jedenfalls eine tatsächliche Verletzung der datenschutzrechtlichen Grundsätze gemäß Art. 5 Abs. 1 DS-GVO[112] die Vermutung begründen könne, dass die vertraglichen Leistungen in einem unangemessenen Verhältnis zueinander stehen.[113] Infolgedessen soll der Schutz

---

[109] Im Ergebnis versucht ErwG 42 S. 3 DS-GVO die potenziellen Abgrenzungsschwierigkeiten pauschal zugunsten einer Kumulation von DS-GVO und Klausel-RL zu lösen. Systematische Gedanken zum Verhältnis von DS-GVO und Klausel-RL hat der europäische Gesetzgeber nicht angestellt. Wohl a. A. *Wendehorst/v. Westphalen*, NJW 2016, 3745 (3749); *Wendehorst*, JZ 2021, 974 (983 f.); *Hacker*, in: Lohsse/Schulze/Staudenmayer (Hrsg.), Data as Counter-Performance – Contract 2.0?, 2020, S. 43 (62: „separate and independent assessment").

[110] Bereits die bislang gemachten Vorschläge für eine solche Klauselkontrolle gemäß §§ 308, 309 ff. BGB dürften umstritten sein. Jedenfalls solange zwischen Anbietern Wettbewerb besteht, sollte weder die Einwilligung in eine Datenverarbeitung zur Personalisierung von Preisen (für deren grundsätzliche Rechtmäßigkeit: *Hofmann*, WRP 2016, 1074 (1080 f.)) noch ein Zugriff auf Nutzerdaten zur Aufklärung von Urheberrechtsverstößen durch den Verbraucher unwirksam sein, solange diese Einwilligung informiert und freiwillig erfolgte. a. A. (wohl) *Wendehorst*, JZ 2021, 974 (983).

[111] Natürlich bleibt es erstrebenswert, wenn auf europäischer Ebene die Rahmenbedingungen für die datenschutzrechtliche Einwilligung detaillierter ausgestaltet werden. Für Vorschläge hierzu: Kapitel 5 und Kapitel 6.

[112] Womöglich soll auch eine mögliche Verletzung eines Datenschutzprinzips bereits zugunsten einer Unangemessenheit i. S. d. Art. 3 Abs. 1 Klausel-RL genügen: *Hacker*, in: Lohsse/Schulze/Staudenmayer (Hrsg.), Data as Counter-Performance – Contract 2.0?, 2020, S. 43 (68).

[113] Unentschieden: *Steinmetz*, Die Kontrollsperre des § 307 Abs. 3 BGB bei Verträgen über immaterielle Gegenstände, 2022. Einerseits (S. 298): „Eine solche Lösung auf Ebene des Datenschutzrechts würde die Bedeutung der Inhaltskontrolle spürbar beschränken. Andernfalls wäre jedoch zu entscheiden, ob die Leistungsbeschreibung des Klauselverwenders selbst bei-

von Datensubjekten, die Verbraucher sind,[114] insbesondere dann durch die AGB-rechtliche Angemessenheitskontrolle verstärkt werden, wenn nach der datenschutzrechtlichen Bewertung lediglich ein Grenzfall vorliegt.[115] Zwar würden die datenschutzrechtliche und die AGB-rechtliche Beurteilung – jedenfalls bei Fällen einer evidenten Unangemessenheit von Leistung und Gegenleistung – regelmäßig zu übereinstimmenden Ergebnissen kommen. Allerdings hätte die Prüfung der Angemessenheit i.R.v. Art. 3 Abs. 1 Klausel-RL bzw. § 307 Abs. 1 S. 1 BGB den Vorteil, dass die Bewertung der Angemessenheit auf Grundlage einer Simulation der hypothetischen *ex ante* Verhandlungssituation anhand eines durchschnittlichen Referenzakteurs erfolgen könne.[116]

Für diesen von *Philipp Hacker* vorgeschlagenen Ansatz spricht die Bemühung um eine transparente Methodik. Zunächst müsste begründet werden, warum der vertragliche Hauptgegenstand – abweichend von Art. 4 Abs. 2 Klausel-RL bzw. § 307 Abs. 3 S. 1 BGB – ausnahmsweise einer gerichtlichen Kontrolle unterliegt.[117] Sodann würde das Gericht sich tatsächlich mit den ökonomischen Parametern zur Bestimmung des Wertes von personenbezogenen Daten befassen (müssen) und den – mit Hilfe von Sachverständigen – ermittelten monetären Wert ins Verhältnis zur vertraglichen Leistung des Unternehmers setzen.

Gegen diesen Ansatz sprechen die aus Sicht der Gerichte verfügbaren Alternativen.[118] Die DS-GVO bietet mehrere Optionen, um einer AGB-rechtlichen

---

spielsweise daraufhin überprüft werden kann, ob sie gegen die Prinzipien des Art. 25 DS-GVO (privacy by design und privacy by default) verstößt und eine etwaige Unwirksamkeit auch auf die datenschutzrechtliche Ebene durchschlägt". Anderseits (S. 298 f.): „Das Datenschutzrecht ‚spiegelt' mit Art. 6 Abs. 1 lit. b DS-GVO indes nur eine vertragsrechtliche Situation im Rahmen der Zulässigkeit der Datenverarbeitung wider, so dass es nach hier vertretener Auffassung näher läge, das durch das Vertragsrecht geschaffene ‚Problem' der Ausweitung der Leistungspflichten auch im Rahmen des Vertragsrechts selbst zu lösen. Sowohl die datenschutzrechtliche Erforderlichkeit als auch der vertragscharakteristische Hauptgegenstand beurteilen sich maßgeblich anhand des mit der jeweiligen Vereinbarung verfolgten Zwecks. Aus diesem Grund entsteht ein gewisser Gleichlauf der Beurteilungskriterien".

[114] Allerdings steht die Klausel-RL einer AGB-Kontrolle der Mitgliedstaaten im B2B-Verhältnis nicht entgegen. Eine solche ebenfalls befürwortend: *Steinmetz*, Die Kontrollsperre des § 307 Abs. 3 BGB bei Verträgen über immaterielle Gegenstände, 2022, C.II.1. S. 127 ff.

[115] *Hacker*, in: Lohsse/Schulze/Staudenmayer (Hrsg.), Data as Counter-Performance – Contract 2.0?, 2020, S. 43 (68).

[116] *Hacker*, in: Lohsse/Schulze/Staudenmayer (Hrsg.), Data as Counter-Performance – Contract 2.0?, 2020, S. 43 (68).

[117] Je nach Umsetzung des Art. 4 Abs. 2 Klausel-RL ins nationale Recht, kann auch ein Hinweis darauf genügen, dass die Klausel-RL gemäß Art. 8 lediglich mindestharmonisierend ist, so dass sie einer Angemessenheitsprüfung des vertraglichen Synallagmas nicht im Wege steht. Es blieb jedoch die Gefahr einer Verletzung des primärrechtlich gewährleisteten Grundsatzes der Vertragsfreiheit. Hierzu: *Lüttringhaus*, Vertragsfreiheit und ihre Materialisierung im Europäischen Binnenmarkt, 2018, S. 616 ff.

[118] *Hacker* nennt zudem selbst drei wesentliche Nachteile seines Vorschlags: Fehlende Präzision, mögliche Vorteile der marktorientierten Findung der Hauptleistungspflichten auf Grundlage von Privatautonomie und die dadurch entstehenden Barrieren für einen Datenzugang für KMU: *ders.*, Datenprivatrecht, 2020, S. 453.

Angemessenheitskontrolle und der damit verbundenen kosten- und zeitintensiven Auseinandersetzung mit Sachverständigengutachten zu entkommen und dennoch – mittelbar – über die Wirksamkeit des vertraglichen Hauptgegenstands zu entscheiden.

Im Zentrum dieser Optionen stehen die umfangreichen Transparenzgebote, die gemäß § 305c S. 1 und § 307 Abs. 3 S. 2 i. V. m. § 307 Abs. 1 S. 2 BGB auch Teil der AGB-Kontrolle sind und zugleich die DS-GVO wie ein roter Faden durchziehen. Hinzu treten weitere flexible Generalklauseln in Form von datenschutzrechtlichen Grundsätzen (Art. 5 Abs. 1 DS-GVO). Die Grundsätze der rechtmäßigen Datenverarbeitung eröffnen den Gerichten Lösungsansätze, die weder zu einer teleologischen Reduktion von § 307 Abs. 3 BGB noch zu einer Auseinandersetzung mit innovativen ökonomischen Theorien zwingen.

Unabhängig davon, ob die Gerichte den Anwendungsbereich des Art. 6 Abs. 1 lit. b DS-GVO weit auslegen oder stattdessen – wie hier vertreten[119] – auf einen Vorrang der Einwilligung setzen, liegt es nahe, dass die mindestharmonisierende Klausel-RL und die AGB-Kontrolle in der gerichtlichen Praxis während einer Übergangszeit weiterhin eine wichtige Rolle spielen werden.[120] Sobald die Gerichte die – aus ihrer Perspektive bestehenden – Vorzüge der DS-GVO jedoch erkannt haben, werden die datenschutzrechtlichen Wertungen dominieren und die AGB-Kontrolle fungiert dann allenfalls noch als Steigbügelhalter, um mithilfe der gesetzlichen Leitbilder (§ 307 Abs. 2 Nr. 2 BGB) in die Prüfung der datenschutzrechtlichen Grundsätze einzusteigen.[121]

b) Höhere Flexibilität der DS-GVO gegenüber der Klausel-RL

Aktuell sind es keine rechtlichen, sondern erkenntnistheoretische Hürden, die gegen eine gerichtliche Angemessenheitskontrolle von personenbezogenen Daten als Bestandteil der *essentialia negotii* sprechen. Weder Art. 4 Abs. 2 Klausel-RL noch § 307 Abs. 3 S. 1 BGB stehen einer Angemessenheitskontrolle von solchen AGB im Weg, die einen Zugang zu personalisierten digitalen Produkten im Austausch gegen eine Bereitstellung von personenbezogenen Daten regeln. Dies gilt sowohl für eine Datenverarbeitung auf Grundlage von Art. 6 Abs. 1 lit. b DS-GVO als auch auf Grundlage von Art. 6 Abs. 1 lit. a DS-GVO. Allerdings führt dieser Weg zu einer Anmaßung von ökonomischem Wissen über Märkte. Hiervor schrecken Gerichte zurecht immer wieder zurück.[122]

---

[119] Unten Kapitel 4 und 5.

[120] Insofern ist die „Errichtung eines zweiten, spezifisch vertragsrechtlichen Schutzwalls" (*v. Westphalen/Wendehorst*, BB 2016, 2179 (2185); ähnlich: *Wendehorst*, JZ 2021, 974 (983 f.)) zwar möglich, letzterer wird aber gegenüber der DS-GVO kontinuierlich an Bedeutung verlieren.

[121] Ebenso für § 15 TMG bereits: *BGH*, Urt. v. 28.05.2020, I ZR 7/16 = GRUR 2020 – *Cookie-Einwilligung II*.

[122] Als Beispiel kann auch die aufwändige Prozeduralisierung gelten, mit deren Hilfe vor-

Sofern – entgegen hier vertretener Ansicht[123] – angenommen wird, dass eine Vereinbarung von personenbezogenen Daten als Gegenleistung zur Rechtmäßigkeit der Datenverarbeitung gemäß Art. 6 Abs. 1 lit. b DS-GVO führen kann, so können die Gerichte diese Datenverarbeitung dennoch am Grundsatz der Verhältnismäßigkeit („zur Erfüllung des Vertrags erforderlich") oder an einem der allgemeinen datenschutzrechtlichen Grundsätze des Art. 5 Abs. 1 DS-GVO scheitern lassen. Zwar liegt es nahe, dass die Erforderlichkeit i. R. v. Art. 6 Abs. 1 lit. b DS-GVO synchron zur Angemessenheit i. S. d. Art. 3 Abs. 1 Klausel-RL ausgelegt werden kann, sofern die diesbezüglichen Vertragsbedingungen zugleich AGB sind. Zwingend ist diese Einheitlichkeit jedoch nicht.

Gemäß Art. 5 Abs. 1 lit. c DS-GVO (Grundsatz der Datenminimierung) müssen die personenbezogenen Daten

„dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung *notwendige Maß beschränkt* sein".[124]

Obwohl der Wortlaut lediglich auf den Umfang der personenbezogenen Daten abstellt und nicht auf den Umfang der Verarbeitung, soll er dennoch für beides gelten.[125] Somit bietet Art. 5 Abs. 1 lit. c DS-GVO potenziell einen sehr einfachen Weg, um im Einzelfall zu einer Unrechtmäßigkeit der Datenverarbeitung zu gelangen. Allerdings beruht der Grundsatz auf einem einseitigen Fokus auf den Schutz personenbezogener Daten. Infolgedessen ist dieser Grundsatz konzeptionell mit synallagmatischen Austauschverhältnissen schwerlich in Einklang zu bringen. Dies spricht dafür, dem Grundsatz der Datenminimierung jedenfalls keine eigenständige Bedeutung beizumessen, sofern die Datenverarbeitung auf einem Vertrag i. S. d. Art. 6 Abs. 1 lit. b DS-GVO (oder einer Einwilligung in Form der schuldrechtlichen Gestattung)[126] beruht. Mit Hilfe einer vertraglichen Leistungsbestimmung haben Verantwortlicher und Datensubjekt es zunächst selbst in der Hand, die Zweck-Mittel-Relation auch abweichend von Art. 5 Abs. 1 lit. c DS-GVO (Grundsatz der Datenminimierung) zu gestalten.[127]

Sofern man es – entgegen hier vertretener Auffassung[128] – für möglich hält, eine Personalisierung der Leistung vertraglich zu vereinbaren und die Daten-

---

rangig die Prozessbeteiligten dazu angeleitet werden (sollen), selbst zu bestimmen, wann eine patentrechtliche Lizenz FRAND (Fair, Reasonable, And Non-Discriminatory) ist.

[123] Unten D.

[124] [Hervorhebung durch den Verfasser].

[125] *Roßnagel*, in: Simitis/Hornung/Spiecker gen. Döhmann (Hrsg.), DS-GVO, 2019, Art. 5, Rn. 125 ff./129 ff.

[126] Unten Kapitel 4 C.II.

[127] A. A. und für „inhaltliche Angemessenheitskontrolle" auf Grundlage von § 307 Abs. 2 Nr. 1 i. V. m. Art. 5 Abs. 1 lit. c DS-GVO: *Bunnenberg*, Privates Datenschutzrecht, 2020, S. 283. Sofern letzterer den Grundsatz der Datenminimierung (Art. 5 Abs. 1 lit. c DS-GVO) und damit einen strengen Verhältnismäßigkeitsgrundsatz heranziehen möchte, ist jede Vereinbarung automatisch rechtwidrig, die personenbezogene Daten als synallagmatischen Leistungsgegenstand vorsieht.

[128] Hierzu unten II.2.

verarbeitung anschließend auf Grundlage von Art. 6 Abs. 1 lit. b DS-GVO zu rechtfertigen, weil diese nach den Vertragsbestimmungen *subjektiv erforderlich* ist,[129] so spricht dies dafür, den Grundsatz der Datenminimierung im Privatrechtsverhältnis lediglich im Rahmen Art. 6 Abs. 1 lit. f DS-GVO anzuwenden.[130] Wäre der Grundsatz der Datenminimierung (Art. 5 Abs. 1 lit. c DS-GVO) auch auf Fälle des Art. 6 Abs. 1 lit. b DS-GVO – oder der Einwilligung – anwendbar, so ließe sich daraus eine Pflicht des Verantwortlichen zum „dauerhaft datenbilligsten Angebot" ableiten. Weil der Grundsatz zugleich ein ständiges Optimierungsgebot enthalten soll,[131] könnten Datensubjekte den geschlossenen Vertrag auf Grundlage von Art. 5 Abs. 1 lit. c DS-GVO jederzeit nachverhandeln.

Unabhängig davon, ob eine Datenverarbeitung vertragsakzessorisch oder auf Grundlage einer Einwilligung erfolgen soll,[132] liegt es aus gerichtlicher Perspektive deshalb nahe, die Vereinbarung von personenbezogenen Daten als Leistungsgegenstand anhand des datenschutzrechtlichen Grundsatzes einer Verarbeitung nach „Treu und Glauben" (Art. 5 Abs. 1 lit. a Var. 2 DS-GVO) zu beurteilen. Im Gegensatz zu Art. 3 Abs. 1 Klausel-RL enthält Art. 5 Abs. 1 lit. a Var. 2 DS-GVO weder eine inhaltliche Ausrichtung auf das Preis-Leistungs-Verhältnis noch ein Bewertungskriterium. Folglich kann ein Verstoß gegen diesen datenschutzrechtlichen Grundsatz im Einzelfall begründet werden, ohne zuvor den Wert der jeweiligen Leistung ökonomisch bewerten und ohne sich im Anschluss daran auf das dünne Eis einer Abgrenzung zwischen dem datenbasierten *iustum pretium* und der *laesio enormis* wagen zu müssen. Dass die Anwendung des datenschutzrechtlichen Grundsatzes von Treu und Glauben (Art. 5 Abs. 1 lit. a Var. 2 DS-GVO) die Rechtssicherheit gefährdet, ist zwar offensichtlich,[133] dürfte den unter Entscheidungsdruck stehenden Mitgliedern eines Gerichtes aber keine schlaflosen Nächte bereiten.

---

[129] *Engeler*, ZD 2018, 55; so wohl auch: *Leistner/Antoine/Sagstetter*, Big Data, 2021, S. 265 f.; a. A. *Bock*, CR 2020, 173 (175 ff.).

[130] Infolgedessen wird der Grundsatz der Datenminimierung auch nicht durch Entwicklungen wie „Big Data" und das „Internet of Things" gefährdet (so aber: *Roßnagel*, in: Simitis/Hornung/Spiecker gen. Döhmann (Hrsg.), DS-GVO, 2019, Art. 5 Rn. 133 ff.) und Art. 5 Abs. 1 lit. c DS-GVO gefährdet seinerseits diese Entwicklung nicht, solange die Datenverarbeitung den sonstigen Anforderungen an eine rechtmäßige Datenverarbeitung genügt.

[131] *Roßnagel*, in: Simitis/Hornung/Spiecker gen. Döhmann (Hrsg.), DS-GVO, 2019, Art. 5, Rn. 21/127 („Vielmehr ist die Minimierung des Personenbezugs eine Aufgabe, die immer noch besser erfüllt werden kann.").

[132] Für die Einwilligung bieten bereits die Tatbestandsvoraussetzungen der Informiertheit und der Freiwilligkeit einen ersten Beurteilungsansatz, um die Einwilligung im Einzelfall scheitern zu lassen.

[133] Es wird vorgeschlagen, die Unbestimmtheit des Grundsatzes einer Verarbeitung nach Treu und Glauben insbesondere durch einen normativen Brückenschlag zur AGB-Kontrolle und zum UWG zu füllen: *Wendehorst/v. Westphalen*, NJW 2016, 3745; *Roßnagel*, in: Simitis/Hornung/Spiecker gen. Döhmann (Hrsg.), DS-GVO, 2019, Art. 5, Rn. 47.

II. Herausforderung: Gefährdung des einheitlichen Datenschutzrechts

Neben den tatsächlichen Schwierigkeiten einer Kontrolle der Angemessenheit eines Austauschverhältnisses mit personenbezogenen Daten als Leistungsgegenstand hat der mit Art. 6 Abs. 1 lit. b DS-GVO assoziierte Vorteil einer flexiblen Entwicklung auf Grundlage des jeweils teilharmonisierten nationalen Schuldrechts weitere wesentliche Nachteile.

Im Ausgangspunkt ist Art. 6 Abs. 1 lit. b DS-GVO der Erlaubnistatbestand mit der geringsten Regelungsdichte (1). Deshalb besteht die Gefahr, dass die vergleichsweise detaillierten unionsrechtlichen Anforderungen an die Einwilligung infolge einer großzügigen Anwendung von Art. 6 Abs. 1 lit. b DS-GVO umgangen würden (2).

Diese Konsequenz muss aus mehreren Gründen verhindert werden. Zunächst bietet eine vertragsakzessorische Datenverarbeitung keine Vorteile gegenüber der Einwilligung. Die vielfach geäußerte Kritik, die Einwilligung sei letztlich nur die Fiktion einer selbstbestimmten Entscheidung,[134] lässt sich vollständig auf diejenige Willenserklärung des Datensubjekts übertragen, die zum Vertragsabschluss führt und anschließend eine rechtmäßige Datenverarbeitung auf Grundlage von Art. 6 Abs. 1 lit. b DS-GVO ermöglicht (3).

Zudem dürfte die Rechtsfindung und die Rechtsanwendung bei einer komplexen gegenseitigen Wechselwirkung zwischen DS-GVO und nationalem Schuldrecht die Gerichte der Mitgliedstaaten und den *EuGH* überfordern und die Rechtssicherheit gefährden (4). Je mehr Gestaltungsspielraum den nationalen Gesetzgebern und Gerichten über Art. 6 Abs. 1 lit. b DS-GVO i. V. m. dem jeweiligen nationalen Schuldrecht verbleibt, desto unwahrscheinlicher ist es, dass ein unionweit einheitlicher Schutz der Datensubjekte und ein freier Verkehr von personenbezogenen Daten im Binnenmarkt erreicht werden können (5).

Infolgedessen würde eine großzügige Auslegung und Anwendung des Art. 6 Abs. 1 lit. b DS-GVO erheblichen und dringenden Bedarf zur Angleichung des mitgliedstaatlichen Schuldrechts auslösen (6).

1. Geringe Regelungsdichte des Art. 6 Abs. 1 lit. b DS-GVO

Für die Auslegung des Art. 6 Abs. 1 lit. b DS-GVO lässt sich weder aus dessen Wortlaut von noch aus den Erwägungsgründen etwas gewinnen. Die Gründe für die stiefmütterliche Behandlung dieses Erlaubnistatbestands sind nicht eindeutig. Zunächst könnte der europäische Gesetzgeber davon ausgegangen sein, dass Art. 6 Abs. 1 lit. b DS-GVO lediglich eine Brücke ins nationale Schuldrecht

[134] *Simitis*, NJW 1998, 2573 (2476); *Rogosch*, Die Einwilligung im Datenschutzrecht, 2013, S. 17 f.; *Radlanski*, Das Konzept der Einwilligung in der datenschutzrechtlichen Realität, 2016, S. 147/212/239; *Buchner/Kühling*, in: Kühling/Buchner (Hrsg.), DS-GVO, 3. Aufl. 2020, Art. 7, Rn. 10; ähnlich: *Veil*, NJW 2018, 3337 (3344).

schlägt, so dass der europäische Gesetzgeber sich in der DS-GVO schon aus kompetenzrechtlichen Gründen mit weiteren Vorgaben zurückhalten musste.

Alternativ könnte der europäische Gesetzgeber in Art. 6 Abs. 1 lit. b DS-GVO auch eine bloße gesetzliche Klarstellung einer Selbstverständlichkeit gesehen haben. In diesem Fall würde Art. 6 Abs. 1 lit. b DS-GVO lediglich deklaratorisch festhalten, dass eine Datenverarbeitung auch auf Grundlage eines Vertrags erlaubt ist. Allerdings stellt sich in diesem Fall die grundlegende Folgefrage, welches Vorverständnis der europäische Gesetzgeber von „der" Einwilligung hat. Denn auch eine Einwilligung kann – wie der europäische Gesetzgeber durch die Anwendbarkeit der Klausel-RL auf die Einwilligung gemäß ErwG 42 S. 3 DS-GVO selbst implizit voraussetzt – Bestandteil des Vertrags sein.[135] Tatsächlich wird bereits in Erwägung gezogen, zwischen vertraglichen Pflichten auf schuldrechtlicher Ebene und der Einwilligung auf dinglicher Ebene zu trennen.[136] Diese Unterscheidung, die auf einem deutschen sachenrechtlichen Sonderweg beruht, scheint jedoch im Kontext des Unionsrechts und in Bezug auf ein immaterielles Regelungsobjekt wenig überzeugend.[137]

Jedenfalls nach deutschem Verständnis dient eine schuldrechtliche Gestattung auch dazu, die vermögenswerten Bestandteile des Persönlichkeitsrechts zu verwerten.[138] Jedenfalls solange kein „Recht am eigenen Datum" existiert, personenbezogene Daten nicht als Immaterialgüterrecht anerkannt werden und personenbezogene Daten gerade nicht als wirtschaftliches Gut anerkannt und handelbar gemacht werden sollen, liegt es zudem fern, zwischen einem schuldrechtlichen Verpflichtungsgeschäft und einer hiervon getrennten (dinglichen) Einwilligung zu unterscheiden. Eine solche Trennung (und die anschließende Abstraktion) dient vorrangig dem Schutz der Verkehrssicherheit, insbesondere sofern Möglichkeiten eines gutgläubigen Erwerbs fehlen und Schutz gegen nachträgliche (Zwischen-)Verfügungen gewährt werden soll.[139] Es ist sehr zweifelhaft, ob das aus dem Sachenrecht stammende Trennungs- und Abstraktionsprinzip als deutscher Sonderweg[140] überhaupt erstrebenswert[141]

---

[135] Unten Kapitel 4 C.II.2.

[136] Für eine solche – allein an deutscher Dogmatik ausgerichtete – Trennung und Abstraktion aber (wohl): *Metzger*, AcP 216 (2016), 817 (831 f.); *Specht*, JZ 2017, 763 (765: „verfügungsähnlich"); *Langhanke*, Daten als Leistung, 2018, S. 150; *Hacker*, Datenprivatrecht, 2020, S. 162 ff.; *Leistner/Antoine/Sagstetter*, Big Data, 2021, S. 255. Hierzu Kapitel 4 sowie unten C.III.1.

[137] Ähnlich für das Urheberrecht: m. w. N. *Ohly*, in: Schricker/Loewenheim (Hrsg.), Urheberrecht, 6. Aufl. 2020, § 31, Rn. 17.

[138] *Helle*, JZ 2014, 444; *Ohly*, Volenti non fit iniuria, 2002, S. 149.

[139] *Wiegand*, AcP 190 (1990), 112 (119 f.).

[140] *Wesel*, Geschichte des Rechts, 2006, S. 459. („Das war eine Erfindung Savignys, gegen das römische Recht, weil er eine Nebenbemerkung des Juristen Gaius mißverstanden hat").

[141] Mit der Warnung davor, die nationale Dogmatik auf die Schnittstellen von Datenschutzrecht und Vertragsrecht zu übertragen: *Lohsse/Schulze/Staudenmayer*, Data as Counter-Performance – Contract 2.0?, 2020, S. 9 (21). Hierzu auch unten: Kapitel 4 C.III.1.

und mit den unionsautonomen Vorgaben für die Einwilligung vereinbar wäre.[142]

Mutmaßlich ist der europäische Gesetzgeber selbst davon ausgegangen, dass die praktische Bedeutung und die Brisanz des Anwendungsbereichs von Art. 6 Abs. 1 lit. b DS-GVO im Vergleich zur Einwilligung und zur Interessenabwägung nur gering ist. Hierfür spricht, dass der europäische Gesetzgeber den Art. 6 Abs. 1 lit. b DS-GVO in der Abgrenzung zum bestehenden und künftigen nationalen Recht der Mitgliedstaaten nicht erwähnt.[143] Jedenfalls sind die Regelungen und Erwägungsgründe für Art. 6 Abs. 1 lit. f DS-GVO – trotz ihrer erheblichen, im vorherigen Kapitel aufgezeigten Defizite – umfangreicher[144] und insbesondere für die Einwilligung[145] sehr viel komplexer und detaillierter ausgefallen. Dies spricht dafür, dass Art. 6 Abs. 1 lit. b DS-GVO – jedenfalls im Verhältnis zur Einwilligung – lediglich subsidiär anzuwenden ist. Anderenfalls besteht die Gefahr, dass die Anforderungen der DS-GVO an eine wirksame Einwilligung über den Umweg des nationalen Schuldrechts der Mitgliedstaaten unterlaufen werden.

2. Gefahr einer Umgehung der Anforderungen an die Einwilligung

Lässt man den unergiebigen Wortlaut von Art. 6 Abs. 1 lit. b DS-GVO und den formalen Kompetenzrahmen hinter sich und nimmt stattdessen die systematischen Zusammenhänge in den Blick, dann sprechen die besseren Argumente ebenfalls für eine sehr restriktive Anwendung von Art. 6 Abs. 1 lit. b DS-GVO.

Es besteht die Gefahr, dass die detaillierten Anforderungen der DS-GVO an eine wirksame Einwilligung durch Art. 6 Abs. 1 lit. b DS-GVO unterlaufen werden könnten.[146] Aus Sicht der Verantwortlichen bietet Art. 6 Abs. 1 lit. b DS-GVO die Möglichkeit zu einer „Flucht aus der Einwilligung".[147] *Einerseits* bliebe für die Einwilligung Art. 6 Abs. 1 lit. a DS-GVO nur noch die schlichte,

---

[142] Ebenfalls für eine schuldrechtliche Einordnung: *Buchner*, Die Informationelle Selbstbestimmung im Privatrecht 2006, 237; *Rogosch*, Die Einwilligung im Datenschutzrecht, 2013, S. 44. Allgemein zur Abgrenzung nach unterschiedlichen Stufen der Einwilligung für das deutsche Privatrecht (ohne Datenschutzrecht) : *Ohly*, Volenti non fit iniuria, 2002, S. 448 ff.

[143] Der ErwG 10 S. 3 und S. 5 f. DS-GVO nennen ausdrücklich nur den Spielraum für nationale Gesetzgebung, der durch die Erlaubnistatbestände aus Art. 6 Abs. 1 lit. c und lit. e DS-GVO und für die Verarbeitung sensibler personenbezogener Daten eröffnet wurde, vgl. Art. 9 Abs. 2 lit. b, g–j DS-GVO.

[144] Vgl. ErwG 46–48 und Art. 21 Abs. 1 DS-GVO, ErwG 69–70 DS-GVO.

[145] Vgl. Art. 7 ff. DS-GVO, ErwG 42–43 DS-GVO.

[146] *Wendehorst/v. Westphalen*, NJW 2016, 3745 (3747); *Engeler*, ZD 2018, 55 (56); *Funke*, Einwilligung im Zivilrecht, 2017, S. 271.

[147] Hierzu: *Sattler*, in: Ochs/Friedewald/Hess/Lamla (Hrsg.), Die Zukunft der Datenökonomie, 2019, S. 215 (225 ff.); so auch: *Frenzel*, in: Paal/Pauly (Hrsg.), DS-GVO, 2021, Art. 7, Rn. 26; ähnlich *Albers/Veit*, in: Brink/Wolff (Hrsg.) BeckOK, DatenschutzR, DS-GVO, Art. 6, Rn. 27; *Bunnenberg*, Privates Datenschutzrecht, 2020, S. 46.

den Verantwortlichen einseitig begünstigende Einwilligung übrig; sobald eine Einwilligung Teil eines Synallagmas wird, wäre sie Teil des Vertrags i. S. d. Art. 6 Abs. 1 lit. b DS-GVO. *Andererseits* käme es weiterhin auf eine ausdrückliche Einwilligung an, soweit besonders sensible personenbezogene Daten verarbeitet werden und das Datensubjekt deshalb besonders schutzwürdig ist, Art. 9 Abs. 2 lit. a DS-GVO.

Gerade aufgrund dieser Gefahr einer Flucht aus der Einwilligung[148] überwiegen nach hier vertretener Auffassung eindeutig die Nachteile, sofern die Rechtmäßigkeit einer Datenverarbeitung über Art. 6 Abs. 1 lit. b DS-GVO maßgeblich vom nationalen Schuldrecht der Mitgliedstaaten abhängt.[149] Obwohl auch das nationale Schuldrecht – insbesondere im B2C-Verhältnis – in wichtigen Bereichen bereits angeglichen wurde, entscheidet regelmäßig die Auslegung von nationalen Generalklauseln über die Rechtmäßigkeit einer Datenverarbeitung gemäß Art. 6 Abs. 1 lit. b DS-GVO.[150] Die detaillierten Anforderungen der DS-GVO an eine wirksame datenschutzrechtliche Einwilligung würden durch Art. 6 Abs. 1 lit. b DS-GVO über das nationale Recht unterlaufen oder müssten über ein sehr komplexes Verfahren – bestenfalls – zweifach rekonstruiert werden. Um einen weitgehenden Gleichlauf mit den Anforderungen an die Einwilligung zu erreichen, möchte *Philipp Hacker* die Erforderlichkeit i. R. v. Art. 6 Abs. 1 lit. b DS-GVO in Übereinstimmung mit der in Art. 7 Abs. 4 DS-GVO vorausgesetzten Freiwilligkeit auslegen.[151]

Gelingt es dem *EuGH* jedoch nicht, diese Rekonstruktion auf Grundlage des Rechts von 27 Mitgliedstaaten zu synchronisieren, so sind sowohl der Schutz der Datensubjekte als auch der freie Verkehr von personenbezogenen Daten auf dem europäischen Binnenmarkt und damit die wesentlichen Ziele und die Rechtfertigung der DS-GVO erneut gefährdet (hierzu unten 5.).[152]

---

[148] Zum Wechsel von einer Einwilligung zu Art. 6 Abs. 1 lit. b DS-GVO durch Facebook infolge der Anwendbarkeit der DS-GVO: *ÖOGH*, Vorlagebeschl. v. 22.07.2021, 6 Ob 56/21k – *Schrems* [*III*] (Rn. 7 f.).

[149] A. A. und damit für eine schuldrechtlich dominierte Lösung: *Schulz*, in: Gola (Hrsg.), DS-GVO, Art. 6, Rn. 27/37; *Engeler*, ZD 2018, 55 (58).

[150] Vorgeschlagen werden eine echte Inhaltskontrolle – unter teleologischer Reduktion von § 307 Abs. 3 BGB (*Wendehorst/v.Westphalen*, NJW 2016, 3745 (3749); *Hacker*, Datenprivatrecht, 2020, S. 67 ff.) sowie eine „inhaltliche Angemessenheitskontrolle" auf Grundlage von § 307 Abs. 2 Nr. 1 i. V. m. Art. 5 Abs. 1 lit. c DS-GVO (*Bunnenberg*, Privates Datenschutzrecht, 2020, S. 283). Sofern letzterer den Grundsatz der Datenminimierung (Art. 5 Abs. 1 lit. c DS-GVO) und damit einen strengen Verhältnismäßigkeitsgrundsatz heranziehen möchte, ist jede Vereinbarung automatisch rechtwidrig, die personenbezogene Daten als synallagmatischen Leistungsgegenstand vorsieht. Überzeugender ist eine Lösung über die Einwilligung, weil diese auf der Ebene des Unionsrecht liegt. Dabei sollte der flexiblere Maßstab von Treu und Glauben (Art. 5 Abs. 1 lit. a DS-GVO) ausschlaggebend sein: Hierzu oben C.I.3.b.

[151] *Hacker*, Datenprivatrecht, 2020, S. 183 ff.; hierzu oben unter A.I.

[152] Dieses grundlegende Problem unterschätzend: *Bunnenberg*, Privates Datenschutzrecht, 2020, S. 59/85.

3. Keine Überwindung der Defizite der Einwilligung

Vielfach wird an der Einwilligung deshalb Kritik geübt, weil sie aufgrund von Informationsasymmetrien und verhaltensökonomischen Defiziten letztlich nur eine „Fiktion von Selbstbestimmung" biete.[153] Diese Kritik lässt sich jedoch nahtlos auf diejenige Willenserklärung eines Datensubjekts übertragen, die zum Zustandekommen eines Vertrags führt, der personenbezogene Daten als Leistungsgegenstand definiert, so dass die Datenverarbeitung anschließend gemäß Art. 6 Abs. 1 lit. b DS-GVO rechtmäßig ist, soweit sie zur Erfüllung des Vertrags erforderlich ist.

Weil der vertraglich vereinbarte Leistungsgegenstand regelmäßig durch die AGB des Verantwortlichen bestimmt wird, die gesetzlichen Anforderungen an AGB jedoch noch geringer sind als die datenschutzrechtlichen Anforderungen an eine wirksame Einwilligung, hat dies zur Folge, dass der Schutz der Datensubjekte im Falle einer vertragsakzessorischen Datenverarbeitungen gemäß Art. 6 Abs. 1 lit. b DS-GVO potenziell geringer ausfällt. Die Vertragsbedingungen, die darüber entscheiden, welche Datenverarbeitungen für die Erfüllung des jeweiligen Vertrags „erforderlich" sind, können trotz Wahrung der AGB-rechtlichen Transparenzgebote[154] in den Leistungsbestimmungen und damit in den allgemeinen Vertragsbedingungen „versteckt" werden. Im Gegensatz dazu wird die datenschutzrechtliche Einwilligung zwar ebenfalls regelmäßig nicht gelesen, aber immerhin getrennt von den sonstigen AGB eingeholt, um die gemäß Art. 7 Abs. 2 S. 1 DS-GVO geforderte Unmissverständlichkeit der Einwilligung nachweisen zu können.

Kurzum: Die Datenverarbeitung auf Grundlage von Art. 6 Abs. 1 lit. b DS-GVO ist für eine unionsweit einheitliche Materialisierung der informationellen Privatautonomie schlechter geeignet als eine gemäß Art. 4 Nr. 11, Art. 6 Abs. 1 lit. a, Art. 7 ff. DS-GVO detailliert geregelte und durch zusätzliche Mechanismen[155] abstützbare Einwilligung.

---

[153] *Simitis*, NJW 1998, 2573 (2476); m. w. N. *Rogosch*, Die Einwilligung im Datenschutzrecht, 2013, S. 17 f.; *Radlanski*, Das Konzept der Einwilligung in der datenschutzrechtlichen Realität, 2016, S. 147/212/239; *Buchner/Kühling*, in: Kühling/Buchner (Hrsg.), DS-GVO, 3. Aufl. 2020, Art. 7, Rn. 10; ähnlich: *Veil*, NJW 2018, 3337 (3344).

[154] Diese fehlende Aufmerksamkeit der Datensubjekte durch die AGB-Kontrolle könnte durch eine strenge Auslegung der Transparenzpflichten in § 305c BGB und § 307 Abs. 1 S. 2 BGB möglichweise kompensiert werden. Zum Vorteil einer Trennung von datenschutzrechtlicher Einwilligung und den restlichen Vertragsbedingungen, weil dies Intermediären – beispielsweise Aufsichtsbehörden oder Verbraucherschutzverbänden – die (automatisierte) Prüfung von Einwilligungserklärungen erleichtert: m. w. N. *Helberger/Zuiderveen/Borgesius/Reyna*, 54 Common Market Law Review 2017, 1427 (1442); *Jarovsky*, 4 European Data Protection Law Review 2018, 447 (452); m. w. N. *Hacker*, Datenprivatrecht, 2020, S. 257 f./579 f.

[155] Hierzu Kapitel 6.

4. Komplexität und Fehleranfälligkeit der Rechtsfindung

Die oben beschriebene komplexe Wechselwirkung zwischen Art. 6 Abs. 1 lit. b DS-GVO und dem jeweils nationalen Schuldrecht der Mitgliedstaaten[156] offenbart, dass der Schutz der Datensubjekte und die Gewährleistung des freien Verkehrs von personenbezogenen Daten im europäischen Binnenmarkt umso stärker gefährdet werden, je umfangreicher Art. 6 Abs. 1 lit. b DS-GVO zur Anwendung kommt.[157] Nur unter zwei Bedingungen ist es möglich, den freien Verkehr im Binnenmarkt nicht zu torpedieren, obwohl massenhaft Daten auf Grundlage von Art. 6 Abs. 1 lit. b DS-GVO verarbeitet werden.

Erstens müssten alle nationalen Gerichte das jeweilige nationale Schuldrecht strikt unter Einbeziehung der in sich bereits konfliktträchtigen Ziele aus Art. 1 DS-GVO auslegen. Das nationale Schuldrecht würde dann auch keinen „zweiten Schutzwall"[158] bilden, sondern müsste vollständig durch die Anforderungen der DS-GVO an die rechtmäßige Datenverarbeitung determiniert sein.

Zweitens müssten die Gerichte bereits bei geringen Zweifeln an der Vereinbarkeit des nationalen Schuldrechts mit dem Unionsrecht ein Vorlageverfahren zum *EuGH* anstreben, damit die Ziele der DS-GVO und der gemäß Art. 8 GRCh und Art. 16 AEUV zu gewährleistende Schutz der Datensubjekte gewahrt bleibt.

Wie *Philipp Hacker* herausgearbeitet hat, kann eine solche unionsrechtskonforme Auslegung und Anwendung des nationalen Privatrechts gelingen, sofern dieses anhand der generalklauselartig formulierten Grundsätze der Rechtsmäßigkeit der Datenverarbeitung (Art. 5 DS-GVO) ausgerichtet wird. Die Komplexität dieses Unterfangens wurde anhand des Verhältnisses zwischen der AGB-Kontrolle und den datenschutzrechtlichen Grundsätzen bereits deutlich. Zunächst müssten Art. 4 Abs. 2 Klausel-RL und § 307 Abs. 3 S. 1 BGB so ausgelegt werden, dass künftig eine gerichtliche Angemessenheitskontrolle der vertraglichen (Haupt-)Leistungspflichten ermöglicht wird.[159] Wie gesehen, lässt sich dieses Vorgehen dadurch rechtfertigen, dass eine Vereinbarung von perso-

---

[156] Oben A.; hierzu ausführlich: *Hacker*, Datenprivatrecht, 2020, S. 540 ff.

[157] Diese Gefahr würde nochmals durch den Vorschlag potenziert, die Abgrenzung zwischen der Einwilligung und vertragsakzessorischen Datenverarbeitung anhand der „Erforderlichkeit" i. S. d. Art. 6 Abs. 1 lit. b DS-GVO vorzunehmen und diese davon abhängig zu machen, ob dem Verantwortlichen eine Widerruflichkeit der Einwilligung zumutbar ist. So aber: *Bunnenberg*, Privates Datenschutzrecht, 2020, S. 58 ff./84.

[158] Für eine solche Stellung des nationalen Schuldrechts: *v. Westphalen/Wendehorst*, BB 2016, 2179 (2185); so auch für eine (zusätzliche) Kontrolle datenschutzrechtlicher Einwilligungen anhand von – *de lege ferenda* einzuführenden – nationalen Klauselverboten: *Wendehorst*, JZ 2021, 974 (983 f.).

[159] So zuvor ebenfalls und deshalb für eine Änderung des § 307 Abs. 3 BGB plädierend: *Wendehorst*, Verbraucherrelevante Problemstellungen zu Besitz- und Eigentumsverhältnissen beim Internet der Dinge, 2016, S. 89 f. Anders: *BGH*, NJW, 1985, 3013 (3014); *BGH*, 16.07.2008, VIII ZR 348/06 – *Payback*; *BGH*, 11.11.2009, VIII ZR 12/08 – *HappyDigits*).

nenbezogenen Daten als vertragliche (Gegen-)Leistung bislang kein Parameter ist, der einem funktionsfähigen Marktmechanismus unterliegt.[160] Der Markt bringt allenfalls geringe Preissignale hervor, die als Grundlage eines Vergleichs der verfügbaren Angebote dienen können.[161] Zudem ist zweifelhaft, inwieweit ein ausreichender Konditionenwettbewerb durch eine informierte und skeptische Minderheit von Datensubjekten initiiert wird und ob von diesem auch andere Datensubjekte zumindest indirekt profitieren können.[162]

Allerdings ist ein solcher Ansatz über Art. 6 Abs. 1 lit. b DS-GVO i. V. m. dem jeweils nationalen Schuldrecht hyperkomplex.[163] Diese Komplexität ist zwar im europäischen Mehrebenensystem angelegt und somit stets eine Herausforderung der Rechtsfindung und -anwendung.[164] Dennoch hängt dieser Ansatz vollständig von der Kooperationsfähigkeit und -willigkeit der jeweiligen nationalen Gerichte und Datenschutzbehörden ab, so dass die Verwirklichung eines freien Verkehrs von personenbezogenen Daten im Binnenmarkt potenziell in weite Ferne rückt.

Jedenfalls das *LG Wien* und das *OLG Wien*[165] haben kürzlich keine Veranlassung für eine solche Vorlage zum *EuGH* gesehen. Stattdessen hielten sie die sehr umfangreiche Datenverarbeitung durch *Facebook*, einschließlich personalisierter Werbung, für erforderlich i. S. d. Art. 6 Abs. 1 lit. b DS-GVO, damit *Facebook* seinen – nach österreichischem AGB-Recht wirksamen – atypischen Nutzungsvertrag erfüllen und das Kommunikationsnetzwerk finanzieren kann.[166]

Besondere Schwierigkeiten entstehen dadurch, dass zusätzlich auch eine analoge Anwendung von Vorschriften der DS-GVO im nationalen Schuldrecht in

---

[160] Ebenso für die Angemessenheitskontrolle, sofern die Einwilligung des Datensubjekts vertragliche (Gegen-)Leistung ist: *Wendehorst/v. Westphalen*, NJW 2016, 3745 (3749). Dies spricht ebenfalls dafür, der Einwilligung einen Vorgang einzuräumen.

[161] *Hacker*, Datenprivatrecht, 2020, S. 67 ff.

[162] Vgl. *Gottschalk*, AcP 206 (2006), 555 (564); *Beimowski*, Zur ökonomischen Analyse Allgemeiner Geschäftsbedingungen, 1989, S. 108 f.; *Wagner/Eidenmüller*, 86 University of Chicago Law Review 2019, 581 (607); *Obar/Oehldorf-Hilsch*, 21 Information, Communication & Society 2018, S. 1; *Bakos/Marotta-Wurgler/Trossen*, 43 The Journal of Legal Studies 2014, S. 1; *Ben-Shahar/Chilton*, 45 Journal of Legal Studies 2016, S. 41. Hierzu oben: C.I.2.c.

[163] Nach *Hacker* (Datenprivatrecht, 2020, S. 538; sowie oben S. 160) setzt dies stets die gerichtliche (Vor-)Prüfung voraus, „ob auf unionsrechtlicher Ebene (Anwendungsvorrang) oder im Rahmen eines speziellen Rechtsgebiets (Sachintegration) ein bestimmtes Risiko eine abschließende Regelung dergestalt erfahren hat, dass alle Eventualitäten berücksichtigt werden sollten. Sofern eine mitgliedsstaatliche Regelung ein eigenständiges Risiko adressiert (Risikospezifizität), und im Rahmen des Anwendungsvorrangs zudem mit den Zielsetzungen des Unionsrechts vereinbar ist (Zielkompatibilität), kann sie neben der DS-GVO Anwendung finden".

[164] Grundlegend zu diesen Herausforderungen: *Metzger*, Extra legem, intra ius, 2009, S. 115 ff.; *Grigoleit*, AcP 201 (2010), 354; *Gsell*, AcP 214 (2014), 99.

[165] *OLG Wien*, Urt. v. 07.12.2020 (nicht rechtskräftig), GZ 11 R 153/20f, 11 R 154/20b-99 S. 28.

[166] Mit Zusammenfassung der Prozessgeschichte: *ÖOGH*, Vorlagebeschl. v. 22.07.2021, 6 Ob 56/21k – *Schrems* [*III*] (Rn. 44 ff.).

Betracht kommt. So ist es insbesondere überzeugend, dass die spezifischen Voraussetzungen, die Art. 7 Abs. 4 DS-GVO an die Freiwilligkeit einer wirksamen Einwilligung stellt, erst recht für die Freiwilligkeit einer Willenserklärung beim Abschluss eines Vertrags gelten sollten.[167] Es ist aber zweifelhaft, dass dieses Vorgehen in 27 Mitgliedstaaten gleichermaßen gelingen wird. Selbst wenn die nationalen Gerichte das jeweilige nationale Schuldrecht im Lichte der DS-GVO auslegen würden, dürfte die Flut an Vorlagefragen – die Voraussetzung für eine langfristig einheitliche Auslegung wäre – den notorisch überlasteten *EuGH* überfordern.[168]

Weil nach hier vertretener Ansicht ein Weg offensteht, der die oben genannten Vorteile des Art. 6 Abs. 1 lit. b DS-GVO zumindest teilweise verwirklicht, ohne diese mit den gravierenden Nachteilen zu erkaufen, die mit einer weiten Anwendung des Art. 6 Abs. 1 lit. b DS-GVO einhergehen, sollte dieser vertragsakzessorische Erlaubnistatbestand – wie auch anderweitig bereits vorgeschlagen[169] – restriktiv ausgelegt werden.

5. Art. 6 Abs. 1 lit. b als Gefährdung der Regelungsziele der DS-GVO

Je umfangreicher Art. 6 Abs. 1 lit. b DS-GVO und infolgedessen nationales Schuldrecht als Grundlage für eine Datenverarbeitung zur Anwendung kommt, desto unwahrscheinlicher ist es, dass die beiden Regelungsziele der DS-GVO verwirklicht werden können. Rechtsgrundlage der DS-GVO ist das in Art. 16 Abs. 2 AEUV enthaltene und in Art. 1 Abs. 1 DS-GVO wiederholte Doppelziel des Schutzes natürlicher Personen bei der Verarbeitung personenbezogener Daten und die Ermöglichung des freien Verkehrs solcher Daten im Binnenmarkt. Gemäß Art. 1 Abs. 3 DS-GVO darf der freie Verkehr personenbezogener Daten in der Union nicht aus Gründen des Schutzes natürlicher Personen bei der Verarbeitung personenbezogener Daten eingeschränkt oder verboten werden. In-

[167] *Bunnenberg*, Privates Datenschutzrecht, 2020, S. 282 f. („die gleichen Wertungsgesichtspunkte wie bei Art. 7 Abs. 4 DS-GVO [mit] im Vergleich zur Einwilligung verschärfte[m] Maßstab"); ähnlich: *Hacker*, Datenprivatrecht, 2020, S. 264 f.

[168] Diese Grenzen des institutionellen Rahmens übersieht *Bunnenberg* weitgehend, wenn er die Judikative im Mehrebenensystem im Rahmen der Anwendung des bereits voraussetzungsarmen Art. 6 Abs. 1 lit. b DS-GVO zusätzlich damit belasten will, im Einzelfall unter Abwägung aller grundrechtlichen Positionen zu überprüfen, ob das Interesse des Verantwortlichen an einem bindenden Vertrag überwiegt, so dass ihm eine (widerrufliche) Einwilligung als Grundlage unzumutbar ist: *ders.*, Privates Datenschutzrecht, 2020, S. 39/282 f. Dagegen wird diese Gefahr im Zusammenhang mit Art. 6 Abs. 1 lit. f (kurz) erwähnt: ebda., S. 78).

[169] *Langhanke/Schmidt-Kessel*, EuCML 2015, 218 (221), wonach die Funktion von Art. 6 Abs. 1 lit. b DS-GVO darin besteht, Datenverarbeitungen von lediglich unterstützendem Charakter zu erlauben („ancillary activities"). Gegen eine Anwendbarkeit von Art. 6 Abs. 1 lit. b DS-GVO für den Fall, dass der Verantwortliche mit der Datenverarbeitung einen – grundsätzlich zu vermutenden – kommerziellen Zweck verfolgt: *v. Westphalen/Wendehorst*, BB 2016, 2179 (2184 f.); *Wendehorst*, in: Lohsse/Schulze/Staudenmayer (Hrsg.), Data as Counter-Performance – Contract Law 2.0?, 2020, S. 193 (201).

soweit geht Art. 1 Abs. 3 DS-GVO über den allgemeinen Grundsatz des *effet utile* des Art. 4 Abs. 3 EUV deutlich hinaus.

Je einflussreicher die Auslegung des nationalen Schuldrechts für die Rechtmäßigkeit einer Datenverarbeitung ist, desto wahrscheinlicher entwickelt sich der durch die DS-GVO gewährleistete und durch das jeweils nationale Recht gewährte Schutz der Datensubjekte auseinander. Infolge der verbleibenden Unterschiede des jeweiligen nationalen Schuldrechts wird zudem das Ziel eines freien Verkehrs von personenbezogenen Daten im Binnenmarkt grundlegend gefährdet.

Dies verdeutlicht bereits die (zu großzügige) Anwendung von Art. 6 Abs. 1 lit. b DS-GVO in dem aktuellen – nicht rechtskräftigen – Urteil des *OLG Wien*.[170] Indem es nach Ansicht des *OLG Wien* für ein rechtmäßiges Profiling für personalisierte Werbung durch *Facebook* nicht auf eine Einwilligung, sondern auf ein in der „österreichischen Rechtsordnung nicht ausdrücklich geregeltes, also atypisches Schuldverhältnis" ankommt, wird die Einheitlichkeit und damit der freie Verkehr personenbezogener Daten im EU-Binnenmarkt grundlegend gefährdet. Das *OLG Wien* prüfte den Vertrag anschließend anhand von § 879 Abs. 1 ABGB auf einen Verstoß gegen die guten Sitten und eine AGB-Kontrolle anhand des immerhin auf Art. 5 Klausel-RL beruhenden und deshalb europaweit harmonisierten Transparenzgebots gemäß § 864a ABGB (inhaltlich überraschende Klausel und formelle Einhaltung des Transparenzgebots).[171]

Hängt die Verarbeitung personenbezogener Daten regelmäßig davon ab, welche atypischen Nutzungsverträge das jeweilige mitgliedstaatliche Schuldrecht ermöglicht und welche Grenzen anschließend der jeweilige Grundsatz von Treu und Glauben setzt, so fragmentiert die Anwendung von Art. 6 Abs. 1 lit. b DS-GVO den freien Verkehr personenbezogener Daten im europäischen Binnenmarkt. Diese Gefahr betrifft nicht nur eine Datenverarbeitung im B2C-Verhältnis, sondern ebenfalls das B2B-Verhältnis. Infolgedessen kann diese Gefahr für das Doppelziel der DS-GVO auch nicht durch den Vorschlag ausgeräumt werden, Art. 6 Abs. 1 lit. b DS-GVO nur im B2B-Verhältnis großzügiger anzuwenden.[172] Ein solches Auseinanderdriften des Schutzniveaus, das maßgeblich vom nationalen Schuldrecht der Mitgliedstaaten abhängt, ist jedoch nicht nur evident inakzeptabel, soweit Datensubjekte zugleich Verbraucher sind. Vielmehr sprechen die gleichen Bedenken auch gegen eine großzügigere Auslegung von Art. 6 Abs. 1 lit. b DS-GVO im B2B-Verhältnis.

---

[170] Urt. v. 07.12.2020, GZ 11 R 153/20f, 11 R 154/20b-99 S. 27 f.

[171] Der ÖOGH hat die Abgrenzung zwischen Art. 6 Abs. 1 lit. a und lit. b DS-GVO im Fall eines Nutzungsvertrags nun dem EuGH als Vorlagefrage 1 vorgelegt: *ÖOGH*, Vorlagebeschl. v. 22.07.2021, 6 Ob 56/21k (Rn. 8 ff.) – *Schrems* [*III*].

[172] In diese Richtung aber: *Golz/Gössling*, IPRB 2018, 68 (71); sowie *Bunnenberg*, Privates Datenschutzrecht, 2020, S. 265.

Erstens bieten weder Art. 8 GRCh, Art. 16 AEUV noch die DS-GVO – abgesehen von Art. 8 Abs. 1 DS-GVO (Einwilligung durch Kinder) – einen rechtlichen Ansatz, mit dem sich eine Aufspaltung des Art. 6 Abs. 1 lit. b DS-GVO entlang verschiedener Kategorien von Datensubjekten legitimieren ließe. Regelungsobjekt der DS-GVO sind jeweils die personenbezogenen Daten natürlicher Personen.[173]

Zweitens kann die binäre Unterscheidung zwischen Unternehmer und Verbraucher im Einzelfall schwierig sein[174] und würde zudem bereits durch die nationalen Gerichte getroffen. Auch im Kontext einer Datenverarbeitung müssen die nationalen Gerichte auf denjenigen Verbraucherbegriff zurückzugreifen, der unionsrechtlich determiniert ist und in § 13 BGB seine Grundlage gefunden hat. Diesen hat der *EuGH* durch zwei Elemente konkretisiert.[175]

Der unionsrechtliche Verbraucherbegriff beruht sowohl auf rollenbezogenen Vorgängen, welche typischerweise eine Schutzbedürftigkeit auslösen als auch auf einem aus dem Binnenmarktrecht begründeten Informationsdefizit.[176] Dieses Verbraucherleitbild dient als Mittel zur Verwirklichung des Zwecks eines integrierten Binnenmarktes[177] und geht deshalb von einem grundsätzlich selbstbewusst auftretenden Verbraucher aus.

Obwohl der *EuGH* den europäischen Verbraucherbegriff seit Jahrzehnten konkretisiert und weiterentwickelt hat, ist dennoch weitgehend offen, welche Konsequenzen die nationalen Gerichte und Datenschutzbehörde aus der Qualifizierung eines Datensubjekts als Verbraucher im Kontext einer Verarbeitung von personenbezogenen Daten ziehen werden. Die Janusköpfigkeit der Regelungsziele aus Art. 1 Abs. 1 DS-GVO ist insoweit ebenfalls unergiebig, weil zwischen dem Schutz der Datensubjekte und dem freien Verkehr personenbezogener Daten ein echter Zielkonflikt besteht. Dieser Konflikt setzt sich in der Abgrenzung zwischen Unternehmer und Verbraucher fort. Abhängig davon, ob die nationalen Gerichte den Schutz des Datensubjekts oder den freien Datenverkehr betonen wollen, könnten sie – beispielsweise für die Bewertung einer Handlung von Influencern – zugunsten einer Eigenschaft als Unternehmer oder als Verbraucher tendieren oder unterschiedliche Anforderungen an einen

---

[173] Auch insoweit bieten die Voraussetzungen der Informiertheit und Freiwilligkeit der Einwilligung eine bessere Möglichkeit zur Berücksichtigung der persönlichen Eigenschaften des Datensubjekts als eine pauschale Unanwendbarkeit von Art. 6 Abs. 1 lit. b im B2C-Verhältnis.

[174] Dies lässt anhand der Abgrenzungsschwierigkeiten zwischen einem privaten und geschäftlichen Handeln i.S.d. § 2 Nr. 1 UWG eines sog. Influencer illustrieren. Hierzu beispielsweise die Leitsätze: KG, Urt. v. 08.01.2019 – 5 U 83/18 – *Vrenifrost*; *Köhler*/Bornkamm/Feddersen, UWG, 2021, § 2, Rn. 23/62 sowie § 5a, Rn. 7.80a ff.

[175] *EuGH*, NJW 2012, 2257 (Rn. 39) – *Banco Español de Crédito*; *EuGH*, NJW 2013, 2253 (Rn. 41) – *RWE Vertrieb*; *EuGH*, NJW 2013, 2579 (Rn. 31) – *Asbeek Brusse und de Man Garabito*.

[176] *EuGH*, Urt. v. 05.12.2013 – C-508/12 = NJW 2014, 841 (Rn. 26) – *Vapenik/Thurner*.

[177] Ähnlich: *Micklitz* in: MüKo, BGB, 8. Aufl. 2018, BGB, § 13, Rn. 3.

wirksamen Vertrag mit einem Verbraucher stellen. Jenseits der DS-GVO existiert bislang kein Ansatz für eine europäische Harmonisierung der vertraglichen Aspekte für eine Bereitstellung von personenbezogenen Daten durch einen Verbraucher.[178]

Die nationalen Datenschutzbehörden und Gerichte entscheiden weitgehend selbstständig darüber,[179] ob und in welchem Ausmaß personenbezogene Daten wirksam als vertraglicher Leistungsgegenstand vereinbart und infolgedessen gemäß Art. 6 Abs. 1 lit. b DS-GVO rechtmäßig verarbeitet werden können.[180] Infolgedessen könnte über Art. 6 Abs. 1 lit. b DS-GVO i. V. m. dem nationalen Schuldrecht das Schutzniveau im Vergleich zu dem mit der DS-GVO angestrebten Schutz verkürzt oder erweitert werden.

Dadurch entsteht *drittens* das Risiko, dass sich neben einem nationalen Schuldrecht für die Bereitstellung personenbezogener Daten durch Verbraucher zusätzlich ein nationales Schuldrecht für die Bereitstellung von personenbezogenen Daten durch unternehmerisch handelnde Datensubjekte entwickelt.[181] Infolgedessen würde nicht nur der Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, sondern insbesondere das zweite in Art. 1 Abs. 1 und Abs. 3 DS-GVO festgeschriebene Ziel eines freien Verkehrs personenbezogener Daten im Binnenmarkt gefährdet. Bestimmt das jeweils nationale und allenfalls teilharmonisierte Schuldrecht gemäß Art. 6 Abs. 1 lit. b DS-GVO über die Rechtmäßigkeit einer Übermittlung der Daten in das Territorium eines anderen EU-Mitgliedstaats, so lässt sich dieses Binnenmarktziel nicht erreichen. Mittelfristig entstünde ein erneuter europäischer Gesetzgebungsbedarf (hierzu sogleich: 6.), um den europäischen Binnenmarkt für personenbezogenen Daten zu integrieren und spätestens zu diesem Zeitpunkt müsste zwischen Datensubjekten differenziert werden, je nachdem, ob sie als Verbraucher oder als Unternehmer handeln.

---

[178] Mit dem (abstrakten) Vorschlag, eigenständige nationale Klauseln in §§ 308, 309 BGB einzuführen, um anhand dieser die Einwilligung zu kontrollieren: *Wendehorst*, JZ 2021, 974 (983 f.). Wenngleich die Klausel-RL nur Mindestanforderungen stellt und einem solchen Vorschlag deshalb nicht entgegensteht, ist jedoch fraglich, ob zusätzliche nationale Klauselkontrollen mit der DS-GVO und infolgedessen mit dem Unionsrecht vereinbar sind.

[179] Als unionsrechtliche Korrekturmöglichkeit bliebe die – durch Disposition der Parteien aber gestaltbare – „Erforderlichkeit der Verarbeitung" (Art. 6 Abs. 1 lit. b DS-GVO) und ggfs. die Anwendung der Grundsätze der rechtmäßigen Datenverarbeitung (Art. 5 Abs. 1 DS-GVO).

[180] Einen Vergleich zwischen der Bereitstellung von Arbeitskraft und der Bereitstellung (bestimmter) personenbezogener Daten herstellend: *E. Posner/Weyl*, Radical Markets, 2019, S. 209 ff.; so bereits *Lanier*, Who Owns the Future?, 2013. Selbst wenn dieser Vergleich plausibel wäre, hätte es für § 310 Abs. 4 BGB (adaptierte AGB-Kontrolle von Arbeitsverträge) keine Bedeutung, weil es insoweit bislang gerade an vergleichbaren Regelungen wie Tarifverträge, Betriebs- und Dienstvereinbarungen fehlt.

[181] Eine gewisse Einheitlichkeit könnte durch die ePrivacy-VO erreicht werden. Weil sie die Vertraulichkeit der Kommunikation schützt, soll sie unabhängig davon Anwendung finden, ob der Endnutzer ein Verbraucher oder ein Unternehmer ist.

Viertens wäre eine solche Differenzierung mit der Konsequenz verbunden, dass die spezifischen Abstützungen der informationellen Privatautonomie, die der europäische Gesetzgeber für die Einwilligung in Art. 4 Nr. 11, Art. 6 Abs. 1 lit. a und Art. 7 ff. DS-GVO detailliert ausgearbeitet hat, infolge der weiten Anwendung von Art. 6 Abs. 1 lit. b DS-GVO kaum zur Anwendung kommen (hierzu bereits oben: 2.). Dies ist auch deshalb misslich, weil diese Anforderungen an die Einwilligung – zumindest im Einzelfall – auch für solche Datensubjekte sinnvoll sind, die unternehmerisch handeln.[182] Zudem ist die Auslegung und Anwendung der unionsautonomen Anforderungen an die Einwilligung besser geeignet, um eine einheitliche Rechtslage zu gewährleisten und die Ziele aus Art. 1 DS-GVO zu verwirklichen.

Selbst wenn unionsweit Einigkeit darüber bestehen sollte, dass eine Angemessenheitskontrolle des vertraglichen Synallagmas abweichend von Art. 4 Abs. 2 Klausel-RL sinnvoll ist, sofern personenbezogene Daten als Leistungsgegenstand vereinbart werden, folgt daraus noch lange nicht, dass die Gerichte einheitliche Kriterien für die Bewertung der Angemessenheit finden werden.[183] Weder das Ziel der Gleichwertigkeit des Schutzniveaus durch die Gewährleistung eines gleichmäßigen und hohen Datenschutzniveaus für natürliche Personen (Art. 1 Abs. 2 DS-GVO) noch die Beseitigung der Hemmnisse für den Verkehr personenbezogener Daten in der Union (Art. 1 Abs. 3 DS-GVO)[184] lässt sich auf diesem Weg erreichen.

Als Fazit lässt sich festhalten: Je großzügiger Art. 6 Abs. 1 lit. b DS-GVO ausgelegt und angewendet wird, desto größer ist die Gefahr, dass das jeweilige mitgliedstaatliche Schuldrecht die rechtsangleichende Wirkung der DS-GVO im Privatrechtsverhältnis aushebelt.

6. Notwendigkeit umfassender Angleichung des Datenschuldrechts

Je umfangreicher Verantwortliche Art. 6 Abs. 1 lit. b DS-GVO als Grundlage für eine rechtmäßige Datenverarbeitung heranziehen können und je maßgeblicher deshalb das jeweilige nationale Schuldrecht wird (atypische Schuldverhältnisse/nationaler Grundsatz von Treu und Glauben/Angemessenheitskontrolle, einschließlich Wucherverbot), desto wichtiger wird es aus europäischer Perspektive, das Doppelziel des Art. 1 Abs. 1 DS-GVO durch eine künftige unionsrechtliche Begrenzung der vertraglichen Gestaltungsfreiheiten zu verwirklichen.

---

[182] Dies gilt insbesondere mit Blick auf die Beurteilung der Freiwilligkeit einer Einwilligung gegenüber marktmächtigen Verantwortlichen. Unten Kapitel 5 C.II.1.

[183] Konsequenterweise müsste i. R. d. Angemessenheit die jeweilige monetäre Kaufkraft im jeweiligen Mitgliedstaat ebenfalls berücksichtigt werden. Dadurch würde jedoch das Ziel eines freien Verkehrs personenbezogener Daten im einheitlichen Binnenmarkt ebenfalls beeinträchtigt.

[184] ErwG 10 S. 1 DS-GVO.

Ein Versuch, den Vorteil der Flexibilität des nationalen Rechts mit einem freien Verkehr personenbezogener Daten und dem (hohen) Schutz der Datensubjekte zu vereinen, könnte sich schnell als Quadratur des Kreises herausstellen. Im Vorgriff auf dieses Spannungsverhältnis zwischen den Zielen der DS-GVO und dem nationalen Schuldrecht wird bereits eine Änderung von § 307 Abs. 3 BGB[185] und eine Reform der Klausel-RL vorgeschlagen. Beides soll dazu dienen, spezifische Kriterien für eine Angemessenheitskontrolle zu etablieren, sofern personenbezogene Daten Teil der vertraglichen Leistung sind.[186]

Dieser Ansatz liegt deshalb auf der Hand, weil die weit überwiegende Anzahl derjenigen Verträge, die personenbezogenen Daten als Leistungsgegenstand vorsehen, auf Grundlage von AGB vereinbart werden. Allerdings besteht die Schwierigkeit gerade darin, praktikable Kriterien für eine inhaltliche Angemessenheitskontrolle aufzustellen, die über die für die Einwilligung geforderte Informiertheit (Transparenz) und Freiwilligkeit der Entscheidung hinausgehen.[187] Infolgedessen ist es überzeugender, dem Einwilligungstatbestand einen Vorrang einzuräumen und diesen anhand der gesetzlichen Voraussetzungen zu einer Stufenleiter fortzuentwickeln (Kapitel 4). Soweit bereits vorgeschlagen wird, auch die Einwilligung durch nationale Regelungen im Rahmen der Klauselkontrolle – für Deutschland in §§ 308, 309 BGB – zu ergänzen, hat dieser Vorschlag, unabhängig davon, ob er mit Unionsrecht (Art. 4 Nr. 11, Art. 6 Abs. 1 lit. a und Art. 7 ff. DS-GVO) vereinbar wäre – dieselben Nachteile für den europäischen Binnenmarkt, wie eine weite Auslegung des Art. 6 Abs. 1 lit. b DS-GVO. Auch insoweit sollten deshalb nationale Alleingänge verhindert werden.

---

[185] *Wendehorst*, Verbraucherrelevante Problemstellungen zu Besitz- und Eigentumsverhältnissen beim Internet der Dinge, 2016, S. 89 f. Damit soll die Rechtsprechung des BGH (*BGH*, 16.07.2008, VIII ZR 348/06 – *Payback*; *BGH*, 11.11.2009, VIII ZR 12/08 – *Happy-Digits*) korrigiert werden, weil dieser sich nicht in der Lage gesehen hatte, Datenschutzerklärungen einer Missbrauchskontrolle zu unterziehen.

[186] *Wendehorst*, Verbraucherrelevante Problemstellungen zu Besitz- und Eigentumsverhältnissen beim Internet der Dinge, 2016, S. 85 ff.; *dies.*, in: Lohsse/Schulze/Staudenmayer (Hrsg.), Data as Counter-Performance – Contract Law 2.0?, 2020, S. 193 (207); *Hacker*, ebda., S. 47 (66 ff.).

[187] Insofern ist mit einer Reform der Klausel-RL gegenüber dem von *Hacker* (Datenprivatrecht, 2020, S. 474) vorgeschlagenen modifizierten „Aziz-Test" wenig gewonnen. Sehr vage bleiben die von *Bunnenberg* vorgeschlagenen Alternativen. Hiernach soll sowohl für die „datenschutzrechtliche Lösung" (für die Einwilligung i. R. v. Art. 7 Abs. 4 DS-GVO und für Art. 6 Abs. 1 lit. b DS-GVO i. R. v. der „Erforderlichkeit") als auch für die „schuldrechtliche Lösung" (jeweils: § 307 Abs. 2 Nr. 1 i. V. m. Art. 5 Abs. 1 lit. c DS-GVO (Grundsatz der Datenminimierung)) stets eine inhaltliche Angemessenheitsüberprüfung anhand der „konkreten Autonomie- und Teilhaberisiken" (S. 273/283) als „Bestandteil eines grundrechtssensiblen Privatrechts" (S. 320) erfolgen. *Ders.*, Privates Datenschutzrecht, 2020, S. 279 f. (Einwilligung) und S. 282 f. (vertragsakzessorische Datenverarbeitung).

III. Herausforderung: Keine Synchronisierung von DS-GVO und DID-RL

Die Komplexität, die eine gerichtliche Überprüfung der Rechtmäßigkeit einer Datenverarbeitung gemäß Art. 6 Abs. 1 lit. b DS-GVO i. V. m. mit dem nationalen Schuldrecht auslöst, lässt sich am Verhältnis zwischen DS-GVO, DID-RL und dem nationalen Schuldrecht illustrieren.

Der europäische Gesetzgeber hat die DS-GVO und die DID-RL nicht synchronisiert (1). Auch die Stellungnahme des *Europäischen Datenschutzausschuss* (EDSA) ist mehrdeutig, enthält keine klare Aussage zum Verhältnis zwischen Art. 6 Abs. 1 lit. b DS-GVO und der DID-RL und wirft deshalb mehr Fragen auf, als sie beantwortet (2). Warum Art. 6 Abs. 1 lit. b DS-GVO gerade mit Blick auf die DID-RL restriktiv ausgelegt werden sollte, wird abschließend anhand eines aktuellen Vorlageverfahrens zum *EuGH* offenkundig (3).

1. Keine Synchronisierung durch den europäischen Gesetzgeber

Auf den ersten Blick scheint Art. 3 Abs. 10 DID-RL einen gewissen Spielraum für eine Anwendung von Art. 6 Abs. 1 lit. b DS-GVO i. V. m. mit dem nationalen Schuldrecht zu eröffnen. Immerhin soll die Freiheit der Mitgliedstaaten zur Regelung von Aspekten des allgemeinen Vertragsrechts, insbesondere die Wirksamkeit, die Nichtigkeit oder die Wirkungen eines Vertrags gemäß Art. 3 Abs. 10 DID-RL „unberührt" bleiben, soweit diese Aspekte nicht in der DID-RL geregelt werden.[188] Somit könnten Art. 3 Abs. 10 DID-RL und Art. 6 Abs. 1 lit. b DS-GVO sich gut ergänzen, indem beide den Weg in das nationale Schuldrecht ebnen.

Dieser erste Eindruck täuscht: Der europäische Gesetzgeber hat mehrfach deutlich gemacht, dass er Art. 6 Abs. 1 lit. b DS-GVO lediglich geringe Bedeutung beimisst, sofern eine Transaktion auf einem Zugang zu digitalen Produkten gegen einen Zugang zu personenbezogenen Daten beruht. Zwar eröffnet Art. 3 Abs. 1 S. 2 DID-RL den Anwendungsbereich der DID-RL zunächst ausdrücklich für solche Transaktionen. Allerdings soll die in diesem Zusammenhang erfolgende Datenverarbeitung nach dem Willen des europäischen Gesetzgebers wohl gerade nicht gemäß Art. 6 Abs. 1 lit. b DS-GVO i. V. m. dem Vertrag über digitale Produkte erfolgen. Vielmehr stellt Art. 3 Abs. 1 S. 2 DID-RL im zweiten Halbsatz klar, dass der Anwendungsbereich der DID-RL nicht eröffnet ist, wenn

„die vom Verbraucher bereitgestellten personenbezogenen Daten durch den Unternehmer *ausschließlich zur Bereitstellung* digitaler Inhalte oder digitaler Dienstleistungen im

[188] Jedenfalls offenbart die Aussage, die DID-RL lasse die DS-GVO „unberührt" (Art. 3 Abs. 8 S. 2 DID-RL) ein Wunschdenken, das durch eine rechtliche Analyse schnell von der Realität eingeholt wird: *Sattler*, NJW 2020, 3623 (3627 ff.).

Einklang mit dieser Richtlinie oder zur Erfüllung von vom Unternehmer einzuhaltenden rechtlichen Anforderungen verarbeitet werden *und* der Unternehmer diese Daten *zu keinen anderen Zwecken verarbeitet*." [Hervorhebung durch den Verfasser]

Diese etwas umständliche Formulierung legt folgende Interpretation nahe: Nach dem impliziten Verständnis des europäischen Gesetzgebers scheidet Art. 6 Abs. 1 lit. b DS-GVO als Rechtsgrundlage für eine Datenverarbeitung aus, sofern der Verbraucher dem Unternehmer den Zugang zu personenbezogenen Daten im Austausch gegen einen Zugang zu digitalen Produkten vertraglich zusagt. Zwar ist eine Verarbeitung von personenbezogenen Daten gerade ausschließlich zur Bereitstellung digitaler Produkte und damit i. S. d. Art. 6 Abs. 1 lit. b DS-GVO möglich, es liegt dann aber kein Fall des Art. 3 Abs. 1 S. 2 DID-RL vor und die DID-RL ist nicht anwendbar.

In diesem Fall dienen die personenbezogenen Daten ausschließlich der Erbringung der geschuldeten (Haupt-)Leistung durch den Anbieter und sind gerade nicht die synallagmatische (Gegen-)Leistung, die an die Stelle eines monetären Entgelts tritt. Kurzum: Allein die Tatsache, dass personenbezogene Daten im Kontext eines Vertrages verarbeitet werden, führt gerade noch nicht zur Eröffnung des Anwendungsbereichs der DID-RL bzw. der §§ 327 ff. BGB.[189]

Immerhin lässt sich aus einem Umkehrschluss zu Art. 3 Abs. 1 S. 2 DID-RL ableiten, dass die europäischen Vorgaben für Verträge über die Bereitstellung digitaler Produkte keine Anwendung finden, sofern ein Unternehmer gegenüber Verbrauchern personalisierte digitale Produkte anbietet *und* der Verbraucher hierfür weder einen monetären Preis zahlt noch personenbezogene Daten für andere Zwecke bereitstellt als eben diese Personalisierung der digitalen Produkte. Diese „atypische Schenkung" von personalisierten digitalen Produkten kommt in zwei Fällen in Betracht.

Entweder dient sie als begrenztes Lockangebot des Unternehmers, um den Verbraucher erst noch vom Abschluss eines Vertrags zu überzeugen, in dessen Rahmen der Verbraucher im Austausch gegen die personalisierten digitalen Produkte entweder einen Geldbetrag zahlt oder darin einwilligt, dass personenbezogene Daten auch für andere Zwecke als die Personalisierung der digitalen Produkte verarbeitet werden.

Alternativ kommen Geschäftsmodelle in Betracht, im Rahmen derer ein Unternehmer personalisierte digitale Produkte bereitstellt und diese vollständig durch die Anzeige von generischer, also nicht-personalisierter Werbung finanzieren kann. Auch in diesem Fall würden die Daten ausschließlich für die Personalisierung der digitalen Produkte verarbeitet und nicht für andere Zwecke.

---

[189] Natürlich kann die DID-RL gemäß Art. 3 Abs. 2 S. 1 DID-RL anwendbar sein, wenn die Verarbeitung zur Bereitstellung der digitalen Produkte i. S. d. Art. 6 Abs. 1 lit. b DS-GVO erforderlich ist *und* der Verbraucher sich im Austausch für den Zugang zu digitalen Produkten *zudem* zur Zahlung eines monetären Entgelts oder zur Bereitstellung zusätzlicher personenbezogener Daten als Gegenleistung verpflichtet.

Aus den verfügbaren Materialien zur DID-RL lässt sich nicht entnehmen, ob der Gesetzgeber diese durch generische Werbung finanzierten personalisierten digitalen Produkte übersehen hat oder – als Unterfall einer unentgeltlichen Bereitstellung von digitalen Produkten – ausdrücklich nicht in den Anwendungsbereich der DID-RL bringen wollte.[190]

Im Ergebnis liegen beide Varianten der „atypischen Schenkung" außerhalb des in Art. 3 Abs. 1 S. 2 geregelten Anwendungsbereichs der DID-RL.[191] Allerdings dürften diese Varianten der Bereitstellung von personalisierten digitalen Produkten ohne jegliche Gegenleistung in der Praxis allenfalls eine ganz untergeordnete Rolle spielen. Diese Unklarheit des Unionsrechts hat den deutschen Gesetzgeber nicht davon abgehalten, die Anwendung der Regelungen der DID-RL gemäß § 516a Abs. 1 BGB auch auf solche Verträge zu erweitern.[192]

Gerade weil der europäische Gesetzgeber sich mit Beispielsfällen für Art. 6 Abs. 1 lit. b DS-GVO auffällig zurückhält, wäre es auch möglich, dass eine Personalisierung von digitalen Produkten stets eine Einwilligung des Datensubjekts voraussetzt. Zwar legt die Formulierung von ErwG 38 S. 3 DID-RL nahe, dass sich ein Anbieter von digitalen Produkten für die Datenverarbeitung auch auf andere Rechtsgrundlagen als die Einwilligung stützen kann. Allerdings erwähnt die DID-RL nur die Einwilligung ausdrücklich und bemüht sich ausschließlich darum, das Verhältnis zwischen der DID-RL und der datenschutzrechtlichen Einwilligung zu erläutern. So stellt ErwG 39 S. 1 DID-RL klar, dass das Widerrufsrecht des Datensubjekts gemäß Art. 7 Abs. 3 S. 1 DS-GVO auch im Zusammenhang mit den durch die DID-RL erfassten Verträgen uneingeschränkt gelten soll. Zudem bleibt es gemäß ErwG 40 S. 2 DID-RL ausdrücklich dem jeweiligen mitgliedsstaatlichen Vertragsrecht überlassen, welche Folgen ein Einwilligungswiderruf für den Vertrag über digitale Produkte hat.[193]

Zusammengefasst: Obwohl dies nicht eindeutig ist, legt eine Zusammenschau von Art. 3 Abs. 1 S. 2 und ErwG 38–40 DID-RL ein Verständnis nahe,[194] wo-

[190] Hierzu Kapitel 5 B.II.2.

[191] Sie erinnern an das Angebot kostenloser (analoger) Zeitungen, die durch generische Werbung finanziert werden und damit an ein Geschäftsmodell, das infolge der Möglichkeiten des *tracking* und der personalisierten Werbung immer weniger vorhanden ist.

[192] Insoweit ist es auch fraglich, ob die DID-RL auf Verträge Anwendung findet, in denen sich ein Unternehmer zur Schenkung von digitalen Produkten verpflichtet und der Verbraucher personenbezogene Daten bereitstellt oder zusagt. Während diese Erweiterung gegenüber Art. 3 Abs. 1 DS-GVO durch einen Unternehmer gemäß Art. 22 Abs. 2 DID-RL freiwillig möglich ist, verstößt eine solche gesetzliche Erstreckung der DID-RL auf unentgeltliche Verträge gegen Art. 4 a. E. DID-RL: Somit dient § 516a Abs. 1 S. 1 Nr. 1 BGB zwar dazu, eine Umgehung von §§ 327 ff. BGB durch die Vereinbarung von zwei „gegenseitigen" Schenkungen zu vermeiden. Die Vorschrift läuft jedoch Gefahr, unionsrechtswidrig zu sein.

[193] Der deutsche Abgrenzungsversuch findet sich in § 327q BGB. Hierzu kritisch: *Sattler*, NJW 2020, 3623 (3628).

[194] Hinzu kommt, dass im ErwG 14 S. 1 des Vorschlags der EU-Kommission vom 09.12.2015, COM(2015) 634 final) noch ein Bezug auf einen Vertrag enthalten war („[…] auf der Grundlage eines *Vertrags*, der Zugang zu Fotos des Verbrauchers gestattet" [Hervorhe-

nach der Anwendungsbereich der DID-RL entweder eine monetäre Gegenleistung oder eine datenschutzrechtliche Einwilligung oder eine gemischte Gegenleistung des Datensubjekts voraussetzt. Offen ist jedoch, ob eine Verarbeitung von personenbezogenen Daten ausschließlich zu dem Zweck, eine vertraglich geschuldete Personalisierung von digitalen Produkten vorzunehmen, gemäß Art. 6 Abs. 1 lit. b DS-GVO rechtmäßig ist,[195] ob in diesem Fall die DID-RL überhaupt anwendbar ist und falls dies zu bejahen ist, welche Folgen es für die durch die DID-RL harmonisierten Rechte des Verbrauchers hat, wenn der Verbraucher für die Personalisierung der digitalen Inhalte mangelhafte oder falsche personenbezogene Daten bereitstellt.[196]

2. Mehrdeutige Stellungnahme des EDSA

Auch der *Europäische Datenschutzausschuss* (EDSA) hat sich in seinen Leitlinien 2/2019 zur Verarbeitung personenbezogener Daten gemäß Art. 6 Abs. 1 lit. b DS-GVO nicht eindeutig positioniert.[197] *Einerseits* geht der *EDSA* davon aus, dass jedenfalls verhaltensbasierte Online-Werbung auf Grundlage von Profiling häufig zur Finanzierung von „Online-Diensten" verwendet wird. Auch wenn die Erbringung solcher Online-Dienste indirekt durch eine personalisierte Werbung finanziert wird, reiche

„dies allein nicht aus, um zu begründen, dass sie für die Erfüllung des betreffenden Vertrags [über Online-Dienste] erforderlich ist".[198]

Infolgedessen könne die Erstellung von Nutzerprofilen zu dem Zweck, auf dieser Grundlage gezielte Werbung zu ermöglichen, nicht gemäß Art. 6 Abs. 1 lit. b DS-GVO erfolgen.[199] Somit wäre die DID-RL also nur anwendbar, wenn der Zugang zu personenbezogenen Daten über das hinausgeht, was bereits gemäß

---

bung durch den Verfasser]), der im verabschiedeten ErwG 25 S. 9 DID-RL eindeutig abgeändert wurde („wenn der Verbraucher seine *Einwilligung* erteilt, dass Material, das als personenbezogene Daten zu betrachten ist, wie z. B. Fotos […] die der Verbraucher ins Internet hochlädt". [Hervorhebung durch den Verfasser].

[195] Mit der noch weitergehenden Frage, ob auch die Datenverarbeitung für personalisierte Werbung als Finanzierungsmodell durch *Facebook* von Art. 6 Abs. 1 lit. b DS-GVO abgedeckt ist: *ÖOGH*, Vorlagebeschl. v. 22.07.2021, 6 Ob 56/21k (Rn. 8 ff.) – *Schrems [III]*). Hierzu oben II.5 und unten 3.

[196] Der europäische Gesetzgeber hat sich nicht zu der Variante geäußert, dass ein Unternehmer personalisierte digitale Produkte anbietet, hierfür personenbezogene Daten verarbeitet und der Verbraucher im Gegenzug ein monetäres Entgelt zahlt. In diesem Fall wäre der Anwendungsbereich der DID-RL – aufgrund des monetären Entgelts – eröffnet.

[197] *EDSA*, Leitlinien 2/2019 für die Verarbeitung personenbezogener Daten gemäß Artikel 6 Absatz 1 Buchstabe b DSGVO im Zusammenhang mit der Erbringung von Online-Diensten für betroffene Personen, Version 2.0, v. 08.10.2019.

[198] *EDSA*, Leitlinien 02/2019, Nr. 53.

[199] *EDSA*, Leitlinien 02/2019, Nr. 56.

Art. 6 Abs. 1 lit. b DS-GVO rechtmäßig ist, weil es zur Vertragserfüllung erforderlich ist. Dieses Verständnis ist mit Art. 3 Abs. 1 S. 2 DID-RL vereinbar.

Andererseits räumt der *EDSA* jedoch ein, dass die Personalisierung ein wesentliches Element bestimmter digitaler Online-Dienste darstellen kann und daher in einigen Fällen – insbesondere aus Sicht der Datensubjekte – als für die Erfüllung eines Vertrags über *personalisierte* Online-Dienste erforderlich angesehen werden könne.[200]

Mit seiner Wortwahl der *Online-Dienste* wahrt der *EDSA* begrifflich einen Abstand zum Gegenstand der DID-RL, welche die Bereitstellung *digitaler Inhalte und digitaler Dienste* (insgesamt: digitale Produkte) regelt. Zudem erwähnt der *EDSA* die bekannten Kommunikationsplattformen von *Facebook (Instagram)*, *XING*, *LinkedIn oder Twitter* nicht, obwohl die Anwendbarkeit der DID-RL auf diese Plattformern für die Verbraucher offensichtlich von herausragender Relevanz wäre. Infolge dieser kuriosen Wortwahl bleibt offen, ob nach Ansicht des *EDSA* zumindest Teile der von diesen Plattformen durchgeführten Datenverarbeitungen gemäß Art. 6 Abs. 1 lit. b DS-GVO i. V. m. mit dem jeweiligen Nutzungsvertrag rechtmäßig sind, weil die Nutzer eine Personalisierung in Form der Verknüpfung mit bestimmten Personen erwarten und vom Datensubjekt eingestellte Information (beispielsweise sog. *posts*) gerade den relevanten „Freunden" und „Verbindungen" angezeigt werden sollen.[201]

Würden diese Daten „ausschließlich für die Bereitstellung" von *personalisierten* digitalen Produkten verarbeitet[202] – diese Ansicht vertritt *Facebook*[203] – so hätte dies zur Konsequenz, dass der Anwendungsbereich der DID-RL nicht eröffnet wäre, *soweit* die Datenverarbeitung – beispielsweise durch *GAFAM* – für die vertraglich vereinbarte Personalisierung des Angebots erforderlich ist.

Sobald die personenbezogenen Daten darüber hinaus für andere Zwecke als die Personalisierung der digitalen Produkte verarbeitet werden, würde Art. 6

---

200 *EDSA*, Leitlinien 02/2019, Nr. 57.

201 *EDSA*, Leitlinien 2/2019 zur Verarbeitung personenbezogener Daten gemäß Artikel 6 Absatz 1 Buchstabe b DSGVO, Version 2.0, 08.10.2019, Rn. 57 f. (abrufbar unter: https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines-art_6-1-b-adopted_after_public_consultation_de_0.pdf, zuletzt abgerufen am 19.05.2022).

202 Mit dem Versuch, eine Trennung zwischen solchen personenbezogenen Daten einzuziehen, ohne die ein auf Kommunikation ausgerichtetes soziales Netzwerk nicht funktionieren kann (insoweit: Art. 6 Abs. 1 lit. b DS-GVO) und solchen Daten, die Werbezwecken dienen (insoweit: Art. 6 Abs. 1 lit. a DS-GVO): *Mackenrodt/Wiedemann*, ZUM 2021, 89 (98). Allerdings ist schon zweifelhaft, ob die Verarbeitung des „Profilfotos, des Geburtsdatums, der Heimatstadt etc." notwendig ist, um ein Nutzerprofil anzulegen. Zudem kann das Profilfoto bereits ein besonders sensibles Datum sein, so dass dessen Verarbeitung auf Grundlage von Art. 6 Abs. 1 lit. b DS-GVO ausscheidet. Ebenfalls großzügiger für eine Anwendung von Art. 6 Abs. 1 lit. b DS-GVO: *Heinzke/Engel*, ZD 2020, 189 (191); *Leistner/Antoine/Sagstetter*, Big Data, 2021, S. 266.

203 *BKartA,* BeckRS 2019, 4895 Rn. 635 und 642 – *Facebook*. Kritisch dazu: *Buchner,* WRP 2019, 1243 (1246 f.). Hierzu sogleich unten: 3.

Abs. 1 lit. b DS-GVO als Verarbeitungsgrundlage ausscheiden.[204] Infolgedessen würde die Datenverarbeitung zu anderen Zwecken als der Erfüllung der vertraglich geschuldeten (Haupt-)Leistung, einer anderen Rechtsgrundlage bedürfen und der Anwendungsbereich der DID-RL wäre deshalb wiederum insgesamt eröffnet, also auch für die personalisierten digitalen Produkte.

Diese vom *EDSA* vertretene Auslegung von Art. 6 Abs. 1 lit. b DS-GVO ist bereits deshalb problematisch, weil auf dieser Grundlage keine klare Abgrenzung des Anwendungsbereichs der DID-RL möglich ist.[205] Während die Datenverarbeitung zur Personalisierung von ansonsten kostenlosen digitalen Produkten außerhalb der DID-RL stünde, sind die DID-RL bzw. die nationalen Gesetze zu deren Umsetzung (für Deutschland: §§ 327 ff. BGB) anwendbar, sobald die Datenverarbeitung auch anderen Zwecken dient oder das Datensubjekt ein monetäres Entgelt zahlt. Typisch für viele neue Geschäftsmodelle, beispielsweise diejenigen von *GAFAM* und *BAT*, sind jedoch digitale Produkte, bei deren Nutzung personenbezogene Daten für ein Profiling verarbeitet werden, dass sowohl dazu dient, die digitalen Produkte zu personalisieren als auch personalisierte Werbung auszuspielen. Das spricht dafür, bereits die Personalisierung von digitalen Produkten bzw. sog. „Online-Diensten" von einer Einwilligung abhängig zu machen. Dann unterliegen diese Geschäftsmodelle eindeutig dem Anwendungsbereich der DID-RL.

3. Art. 6 Abs. 1 lit. b als potenzieller Fluchtweg aus der DID-RL

Eine weite Auslegung und Anwendung von Art. 6 Abs. 1 lit. b DS-GVO birgt nicht nur die Gefahr einer Flucht aus den unionsweit einheitlichen und vergleichsweise detailliert geregelten Anforderungen an eine Einwilligung.[206] Viel-

---

[204] A. A. *Facebook* sowie das *OLG Wien*, Urt. v. 07.12.2020 (nicht rechtskräftig), GZ 11 R 153/20f, 11 R 154/20b-99, S. 28: „Insbesondere ist es legitim, dass ein marktwirtschaftlich operierendes Unternehmen, das für bestimmte Dienstleistungen kein Geld verrechnet, im Rahmen der Gesetze auf anders geartete Finanzierungsquellen zurückgreift. […] Denn nur diese Datenverwertung ermöglicht maßgeschneiderte Werbung, die das von der Beklagten geschuldete ‚personalisierte Erlebnis' in wesentlichem Maße prägt und der Beklagten zugleich die für die Aufrechterhaltung der Plattform *und die Erzielung eines Gewinns* notwendigen Einkünfte *verschafft*. Diese Datenverarbeitung ist daher für die Vertragserfüllung ‚erforderlich' iSd Art 6 Abs. 1 lit. b DSGVO" [Hervorhebung durch den Verfasser].

[205] Dies verdeutlicht das (nicht rechtskräftige) Urteil des *OLG Wien* (Urt. v. 07.12.2020, GZ 11 R 153/20f, 11 R 154/20b-99 S. 27 f.). Hiernach soll auch die für eine personalisierte Werbung erfolgende eigene Datenverarbeitung durch *Facebook* gemäß Art. 6 Abs. 1 lit. b DS-GVO nicht nur für eine Personalisierung der Kommunikation über das Nutzerkonto erforderlich sein, sondern auch um Gewinn zu erzielen. Bestätigt der *EuGH* diese Rechtsauffassung (*ÖOGH*, Vorlagebeschl. v. 22.07.2021, 6 Ob 56/21k (Rn. 8 ff.) – *Schrems [III]*), so würde der Nutzungsvertrag von *Facebook* jedenfalls nach dem Wortlaut von Art. 3 Abs. 1 Hs. 2 DID-RL nicht in den Anwendungsbereich der DID-RL und damit – aus deutscher Perspektive – nicht in den Anwendungsbereich der §§ 327 ff. BGB fallen.

[206] Hierzu oben: C.II.2.

mehr besteht zusätzlich die Gefahr, dass die Bereitstellung von digitalen Produkten dem Anwendungsbereich des Art. 3 Abs. 1 S. 2 DID-RL und damit der §§ 327 ff. BGB entkommt, soweit die Verarbeitung der personenbezogenen Daten gemäß Art. 6 Abs. 1 lit. b DS-GVO zur Vertragserfüllung erforderlich ist *und* der Zugang zu personenbezogenen Daten des Verbrauchers infolgedessen keine „Gegenleistung" i. S. d. Art. 3 Abs. 1 S. 2 DID-RL ist.[207] Jedenfalls bei Erstellung des Referentenentwurfs zur Umsetzung der DID-RL ging der federführende Referent des *BMJV* davon aus, dass die DID-RL und infolgedessen die §§ 327 ff. BGB nicht anwendbar sein würden, sofern die Datenverarbeitung auf Grundlage von Art. 6 Abs. 1 lit. b DS-GVO erfolgt.[208]

Dieser – bislang nicht abschließend geklärte (hierzu sogleich) – Zusammenhang zwischen Art. 6 Abs. 1 lit. b DS-GVO und Art. 3 Abs. 1 S. 2 DID-RL erklärt (zusätzlich), warum es für *Facebook* ein großer Vorteil wäre, sofern der *EuGH* der Ansicht folgt, dass die Verarbeitung von personenbezogenen Daten[209] durch *Facebook* – einschließlich zur Finanzierung mittels personalisierter Werbung – erforderlich ist, um den *Facebook*-Nutzungsvertrag zu erfüllen. Diese Ansicht wird von *Facebook*[210] vertreten und sowohl vom *LG Wien* als auch vom *OLG Wien* einstweilen geteilt. Nach Ansicht des *OLG Wien* handelt es sich bei dem Vertrag um ein in der österreichischen Rechtsordnung nicht ausdrücklich geregeltes, also atypisches Schuldverhältnis. Das *Facebook*-Geschäftsmodell werde in einer Weise

„erläutert, die für jeden auch nur durchschnittlich aufmerksamen Leser leicht verständlich ist. Dieses Modell ist auch weder sittenwidrig iSd § 879 Abs. 1 ABGB noch ungewöhnlich iSd § 864a ABGB. Insbesondere ist es legitim, dass ein marktwirtschaftlich

---

[207] Womöglich hat der deutsche Gesetzgeber versucht, die inhaltlichen Regelungen der DID-RL gemäß § 516a Abs. 1 BGB auch auf diesen Fall zu erstrecken. Dann würden die verbraucherschützenden Vorschriften der §§ 327 ff. BGB unabhängig davon anwendbar sein, ob der Verbraucher irgendeine Gegenleistung erbringt. Einzige Anwendungsvoraussetzung ist die Erbringung personalisierter digitaler Produkte durch einen Unternehmer an einen Verbraucher. Hierzu unten Kapitel 5 B.II.2. Diese Erweiterung wäre jedoch nicht mit Art. 3 Abs. 1 DS-GVO i. V. m. Art. 4 a. E. DID-RL vereinbar und deshalb unionsrechtswidrig. Eine höheres Verbraucherschutzniveau ist gemäß Art. 22 Abs. 2 DID-RL nur möglich, soweit Unternehmer dies freiwillig anbieten.

[208] *Görs*, in: Lohsse/Schulze/Staudenmayer (Hrsg.), Data as Counter-Performance – Contract 2.0?, 2020, S. 265 (266: „[…] the EU lawmakers seem to have found a reasonable and practicable solution: the Digital Content Directive will be applicable where the trader processes personal data provided by the consumer, *except* in cases *where* the processing is *based on article 6(1)(b),* (c) or (e) of the General Data Protection Regulation" [Hervorhebung durch den Verfasser]); ebenso: *Klink-Straub*, NJW 2021, 3217 (3219).

[209] Ausgenommen sind besonders sensible personenbezogene Daten gemäß Art. 9 Abs. 1 DS-GVO. Hierzu deshalb die Vorlagefrage 3 (Auslegung von Art. 9 Abs. 1 DS-GVO) und Vorlagefrage 4 (Auslegung und Reichweite des Art. 9 Abs. 2 lit. e DS-GVO): des *ÖOGH*, Vorlagebeschl. v. 22.07.2021, 6 Ob 56/21k (Rn. 24 ff.) – *Schrems* [*III*].

[210] Diese Ansicht vertritt *Facebook*: *BKartA*, BeckRS 2019, 4895 Rn. 635 und 642 – *Facebook*. Kritisch dazu: *Buchner*, WRP 2019, 1243 (1246 f.).

operierendes Unternehmen, das für bestimmte Dienstleistungen kein Geld verrechnet, im Rahmen der Gesetze auf anders geartete Finanzierungsquellen zurückgreift".[211]

Die Verarbeitung der personenbezogenen Nutzerdaten sei eine tragende Säule des zwischen den Parteien geschlossenen Vertrags:

„Denn nur diese Datenverwertung ermöglicht maßgeschneiderte Werbung, die das von der Beklagten geschuldete „personalisierte Erlebnis" in wesentlichem Maße prägt und der Beklagten zugleich die für die Aufrechterhaltung der Plattform und die Erzielung eines Gewinns notwendigen Einkünfte verschafft. Diese Datenverarbeitung ist daher für die Vertragserfüllung „erforderlich" iSd Art 6 Abs. 1 lit. b DSGVO."[212]

Mit Vorlagebeschluss vom 22.07.2021 hat der *ÖOGH* dem *EuGH* diese fundamentale Frage zur Abgrenzung zwischen einer vertragsakzessorischen Datenverarbeitung und der Einwilligung vorgelegt.[213] Zwar geht es in diesem Prozess zwischen *Maximilian Schrems* und *Facebook* weder um vertragliche Aspekte der Bereitstellung digitaler Produkte noch ist die DID-RL bzw. deren Umsetzung ins österreichische Recht entscheidungserheblich; die DID-RL war zum Zeitpunkt des Vorlagebeschlusses zwar umzusetzen, aber gemäß Art. 24 Abs. 1 S. 2 DID-RL noch nicht anwendbar. Dennoch ist es wichtig, dass dem *EuGH* vor seiner Entscheidung bewusst wird, dass er nicht nur über die grundlegende Abgrenzung zwischen Art. 6 Abs. 1 lit. a und Art. 6 Abs. 1 lit. b DS-GVO entscheidet, sondern diese Entscheidung – zumindest mittelbar – Auswirkungen für den Anwendungsbereich der DID-RL bzw. der jeweiligen nationalen Umsetzungsgesetze haben kann.

Folgt der *EuGH* – ebenso wie das *LG Wien* und das *OLG Wien* – der Ansicht von *Facebook*, so würde das wesentliche Geschäftsmodell von *Facebook* auf Grundlage von Art. 6 Abs. 1 lit. b DS-GVO[214] den detaillierten datenschutzrechtlichen Anforderungen an die Einwilligung entgehen und es bestünde zudem die Gefahr, dass das Geschäftsmodell zusätzlich den vollharmonisierten verbraucherschützenden Vorschriften der DID-RL bzw. der §§ 327 ff. BGB entkommt.

Sofern der *EuGH* – ebenso wie das *LG Wien* und das *OLG Wien* – die Datenverarbeitung durch *Facebook*, einschließlich personalisierter Werbung zur

---

[211] *OLG Wien*, Urt. v. 07.12.2020, GZ 11 R 153/20f, 11 R 154/20b-99, S. 28.

[212] *OLG Wien*, Urt. v. 07.12.2020, GZ 11 R 153/20f, 11 R 154/20b-99, S. 28, sowie die Zusammenfassung der Prozessgeschichte: *ÖOGH*, Vorlagebeschl. v. 22.07.2021, 6 Ob 56/21k – *Schrems* [*III*] (Rn. 44 ff.).

[213] *ÖOGH*, Vorlagebeschl. v. 22.07.2021, 6 Ob 56/21k – *Schrems* [*III*] (Vorlagefrage 1 Rn. 8 ff.).

[214] Zu den Nachteilen der verbleibenden AGB-Kontrolle und den (begrenzten) Möglichkeiten zur unionsweiten Harmonisierung anhand der Grundsätze der rechtmäßigen Datenverarbeitung (Art. 5 Abs. 1 DS-GVO): oben C.II.5. und D.

Finanzierung und Gewinnerzielung, als für die Vertragserfüllung erforderliche Datenverarbeitung im Sinne des Art. 6 Abs. 1 lit. b DS-GVO beurteilt, schließt das nicht aus, diese vertragsakzessorische Datenverarbeitung dennoch als einen anderen Zweck im Sinne des Art. 3 Abs. 1 S. 2 DID-RL zu beurteilen. Dann wären die DID-RL und die §§ 327 ff. BGB anwendbar.[215]

Bei diesem Verständnis wäre die Datenverarbeitung für die personalisierte Bereitstellung digitaler Produkte und für eine personalisierte Werbung aus *datenschutzrechtlicher* Perspektive für die Erfüllung des *Facebook*-Nutzungsvertrags erforderlich und damit datenschutzrechtlich rechtmäßig, diese Daten würde jedoch gerade nicht ausschließlich zur Bereitstellung von personalisierten digitalen Produkten im Sinne des Art. 3 Abs. 1 S. 2 DID-RL verarbeitet. Im Ergebnis wäre die Erforderlichkeit der Datenverarbeitung zur Erfüllung des Vertrags im Rahmen von Art. 6 Abs. 1 lit. b DS-GVO weiter zu verstehen, als die Beurteilung, ob Daten ausschließlich zur Bereitstellung von personalisierten digitaler Produkte verarbeitet werden (Art. 3 Abs. 1 S. 2 DID-RL).

Dass es dem *EuGH* gelingt, derart feingliedrig zwischen der vertragsakzessorischen Datenverarbeitung im Sinne der DS-GVO und der Datenverarbeitung, die ausschließlich der Bereitstellung personalisierter digitaler Produkte dient (DID-RL), zu differenzieren, ist zwar nicht ausgeschlossen, es könnte aber Jahre dauern, bis insoweit Klarheit besteht. Jedenfalls zwingt das Vorlageverfahren des *ÖOGH* den *EuGH* nicht dazu, seine Entscheidung über die Abgrenzung der datenschutzrechtlichen Erlaubnistatbestände in Art. 6 Abs. 1 lit. a und lit. b DS-GVO mit Blick auf die potenziellen Folgen für den Anwendungsbereich der DID-RL zu reflektieren.

Es ist deshalb nicht auszuschließen, dass der *EuGH* sich – ebenso wie der europäische Gesetzgeber und der deutsche Gesetzgeber[216] – im Labyrinth aus DS-GVO, DID-RL und Klausel-RL verläuft.[217] Bereits diese Gefahr spricht dafür, Art. 6 Abs. 1 lit. b DS-GVO restriktiv auszulegen und der Einwilligung den Vorrang einzuräumen, sofern digitale Produkte für ein Datensubjekt personalisiert werden. Dadurch würde die unionsweite Synchronisierung von DS-GVO und DID-RL vereinfacht.

---

[215] A. A. *Görs*, in: Lohsse/Schulze/Staudenmayer (Hrsg.), Data as Counter-Performance – Contract 2.0?, 2020, S. 265 (266); *Klink-Straub*, NJW 2021, 3217 (3219).

[216] Insbesondere mit Blick auf § 516a Abs. 1 BGB. Skeptisch zu dieser Vorschrift auch: *Spindler*, MMR 2021, 528 (533); *Rosenkranz*, ZUM 2021, 195 (204).

[217] Indem der deutsche Gesetzgeber in § 327q Abs. 1 und Abs. 3 BGB jeweils an die „Abgabe datenschutzrechtlicher Erklärungen" durch das Datensubjekt anknüpft, scheint auch der deutsche Gesetzgeber davon auszugehen, dass die Beurteilung von personenbezogenen Daten als Gegenleistung entweder auf eine Einwilligung*serklärung* (und Widerrufs*erklärung*) oder eine Interessenabwägung, einschließlich der Möglichkeit zur Widerspruch*erklärung*, angewiesen ist. Jedenfalls kommt es im Rahmen einer vertragsakzessorischen Datenverarbeitung gemäß Art. 6 Abs. 1 lit. b DS-GVO zu keiner solchen Abgabe einer datenschutzrechtlichen Erklärung.

D. Fazit: Entlastungsfunktion von Art. 6 Abs. 1 lit. b DS-GVO

Die geringe Regelungsdichte von Art. 6 Abs. 1 lit. b DS-GVO, die im systematischen Vergleich sehr detaillierten Anforderungen an die wirksame Einwilligung sowie weitere aktuelle europäische Rechtsakte und Gesetzgebungsvorhaben sprechen dafür, dass der europäische Gesetzgeber der vertragsakzessorischen Datenverarbeitung allenfalls eine sehr untergeordnete Bedeutung zugedacht hat.

Dies gilt sowohl für Art. 3 Abs. 1 S. 2 DID-RL als auch für die Verordnung über europäische Daten Governance (englisch: Data Governance Act oder DGA).[218] Letzterer sieht sowohl für die Weitergabe personenbezogener Daten durch öffentliche Stellen (Art. 5 Abs. 6 DG-VO) als auch für das Konzept des sog. Datenaltruismus (Art. 2 Nr. 16 und Art. 25 DG-VO) eine Einwilligung als Grundlage für die Datenverarbeitung vor. Die DG-VO geht mit keinem Wort auf eine vertragsakzessorische Datenverarbeitung ein, obwohl jedenfalls mit Blick auf das Konzept des sog. Datenaltruismus die Nähe zur Schenkung auf der Hand liegt.

Wie bereits erwähnt, spricht für einen Vorrang der Einwilligung zudem, dass die Einwände, die gegen die Einwilligung vorgebracht werden, bruchlos auf die Willenserklärung von Datensubjekten und damit auf denjenigen Vertrag übertragen werden können, den eine Anwendung von Art. 6 Abs. 1 lit. b DS-GVO voraussetzt. Infolgedessen ist es überzeugend, den Anwendungsbereich von Art. 6 Abs. 1 lit. b DS-GVO möglichst zu reduzieren und auf dieser Grundlage nur solche Datenverarbeitungen zuzulassen, die eine untergeordnete Hilfsfunktion haben.[219] Hiernach ist beispielsweise die Verarbeitung der Postadresse und der Bankverbindung im Rahmen eines Fernabsatzvertrags über Waren gemäß Art. 6 Abs. 1 lit. b DS-GVO rechtmäßig.

Obwohl Art. 6 Abs. 1 lit. b DS-GVO – im Unterschied zu Art. 6 Abs. 1 lit. f DS-GVO – immerhin mittelbar auf einer Willenserklärung des Datensubjekts beruht,[220] soll die vertragsakzessorische Datenverarbeitung nach hier vertretener Ansicht lediglich verhindern, dass Datensubjekte sich über alltägliche, lediglich periphere Datenverarbeitungen Gedanken machen müssen.[221] Dagegen greift Art. 6 Abs. 1 lit. b DS-GVO nicht für Datenverarbeitungen, die zwar nach dem Wunsch und den vertraglichen Bestimmungen eines Verantwortlichen –

---

[218] Verordnung (EU) 2022/868 vom 30.5.2022 über europäische Daten-Governance und zur Änderung der Verordnung (EU) 2018/1724 (Daten-Governance-Rechtsakt), ABl. v. 3.6. 2022, L 152, S. 1 ff.

[219] *v. Westphalen/Wendehorst*, BB 2016, 2179 (2184 f.); *Langhanke/Schmidt-Kessel*, EuCML 2015, 218 (221).

[220] *Sattler*, in: Lohsse/Schulze/Staudenmayer (Hrsg.), Data as Counter-Performance – Contract 2.0?, 2020, S. 225 (241).

[221] Ähnlich: *Albers/Veit*, in: Brink/Wolff (Hrsg.), BeckOK, DatenschutzR, DS-GVO, Art. 6, Rn. 29.

wie *Facebook* – erforderlich sein sollen, die aber einem eigenständigen kommerziellen Zweck dienen.[222]

Sofern Art. 6 Abs. 1 lit. b DS-GVO lediglich eine periphere, unterstützende Datenverarbeitung ermöglicht,[223] kann eine Datenverarbeitung – jedenfalls im B2C-Verhältnis[224] – nicht gemäß lit. b DS-GVO rechtmäßig sein, nur weil der Verantwortliche den Zugang zu personenbezogenen Daten im Vertrag ausdrücklich als Teil des vertraglichen Synallagmas definiert.[225] Infolgedessen kann eine Datenverarbeitung durch den Anbieter eines Kommunikationsnetzwerks, beispielsweise *Facebook*[226] oder *LinkedIn*, nicht mit einer vertragsakzessorischen Datenverarbeitung begründet werden, selbst wenn die soziale Verknüpfung auf Grundlage personenbezogener Daten Gegenstand der im Nutzungsvertrag vereinbarten synallagmatischen Leistungsbeziehung ist.[227]

In der Folge sind alle Geschäftsmodelle, die personenbezogene Daten als vertraglichen Leistungsgegenstand und nicht als lediglich notwendige Voraussetzung für die Erbringung einer anderen (Haupt)Leistung vorsehen, auf eine wirksame Einwilligung des Datensubjekts angewiesen.[228] Um Abgrenzungsschwierigkeiten und infolgedessen entstehende Lücken im Verbraucher(schutz)recht zu vermeiden, sollte dies selbst für Personalisierungen von digitalen Produkten gelten. Nach diesem Verständnis unterstützt Art. 6 Abs. 1 lit. b

---

[222] Ebenso und mit der Vermutung eines solchen eigenständigen kommerziellen Zwecks zulasten des Verantwortlichen: *v. Westphalen/Wendehorst*, BB 2016, 2179 (2184 f.); *Langhanke/Schmidt-Kessel*, EuCML 2015, 218 (221).

[223] Zur Bedeutung der Einbeziehung von Verrichtungs- und Erfüllungsgehilfen beispielsweise zur Zahlungsabwicklung oder Auslieferung: Unten Kapitel 5 B.III.

[224] Die DS-GVO unterscheidet nicht zwischen Datenverarbeitungen im B2C- und B2B-Verhältnis. Um die Kommerzialisierung personenbezogener Daten im Rahmen von Werbe- und Sponsoring-Verträgen mit Prominenten abzubilden, könnte Art. 6 Abs. 1 lit. b DS-GVO im B2B-Verhältnis zwar eine großzügigere Anwendung finden: *Sattler*, NJW 2020, 3623 (3627); hiergegen jedoch oben: B.II.2.

[225] A. A. *Hacker*, Datenprivatrecht, 2020, S. 260 ff. Allerdings dürfte eine Verarbeitung auf Grundlage von lit. b DS-GVO infolge der komplexen Wechselwirkung zwischen europäischem Datenschutzrecht und nationalem Privatrecht, insbesondere gemäß § 307 Abs. 2, Abs. 3, § 138, § 242 BGB, im Ergebnis einer nahezu identischen Kontrolle unterliegen, wie eine Verarbeitung auf Grundlage einer datenschutzrechtlichen Einwilligung: *Hacker*, Datenprivatrecht, 2020, S. 264/540 ff.

[226] *Facebook* scheint davon auszugehen, die Nutzerdaten weitgehend auf Grundlage von Art. 6 Abs. 1 lit. b DS-GVO verarbeiten zu können: *BKartA*, BeckRS 2019, 4895, Rn. 635 und 642 – *Facebook*. Hierzu ebenfalls kritisch: *Buchner,* WRP 2019, 1243 (1246 f.).

[227] A. A. *OLG Wien*, Urt. v. 07.12.2020, GZ 11 R 153/20f, 11 R 154/20b-99 S. 28; sowie die Zusammenfassung der Prozessgeschichte: *ÖOGH*, Vorlagebeschl. v. 22.07.2021, 6 Ob 56/21k – *Schrems* [*III*] (Rn. 44 ff.).

[228] A. A. *Bunnenberg*, der – ohne ein Beispiel zu nennen – gerade dann Datenverarbeitungen auf Grundlage von Art. 6 Abs. 1 lit. b DS-GVO zulassen möchte, wenn dem Verantwortlichen eine unverbindliche, weil widerrufliche Einwilligung nicht zugemutet werden kann bzw. soll: *ders*., Privates Datenschutzrecht, 2020, S. 39/282 f. Diese Bedenken lassen sich jedoch besser durch Anerkennung einer Möglichkeit zur befristeten Disposition über die freie Widerruflichkeit der Einwilligung lösen. Hierzu unten: Kapitel 4 C.II.2. sowie Kapitel 5 C.III.

DS-GVO die informationelle Privatautonomie der Datensubjekte indem er die Notwendigkeit einer Einwilligung nur entfallen lässt, soweit diese bloße Förmelei wäre und die Aufforderung zur Einwilligung deshalb allenfalls die unerwünschte Einwilligungsmüdigkeit der Datensubjekte verstärkt.[229] Indem Art. 6 Abs. 1 lit. b DS-GVO den Einwilligungstatbestand in solchen alltäglichen und banalen Konstellationen entlastet, bleibt das Erfordernis einer Einwilligung den aus datenschutzrechtlicher Perspektive gravierenderen Vertragsabschlüssen vorbehalten. Dadurch wird die Aufmerksamkeit der Datensubjekte geschont und fokussiert.[230] Infolgedessen können Datensubjekte sich auf diejenigen – weiterhin stark zunehmenden – Transaktionen konzentrieren, in denen die Verarbeitung personenbezogener Daten als vertraglicher Leistungsgegenstand vereinbart wird, beispielweise im Austausch gegen einen Zugang zu (personalisierten) digitalen Produkten.

Anders als es der Wortlaut des Art. 6 Abs. 1 lit. b DS-GVO auf den ersten Blick nahelegt, erfolgt eine solche Datenverarbeitung, die an die Stelle eines monetären Entgelts tritt, jedoch nicht vertragsakzessorisch, sondern auf Grundlage einer Einwilligung, in Form einer rechtsgeschäftlichen zweiseitigen schuldrechtlichen Gestattung.[231]

---

[229] Damit ist die Gefahr der automatischen Zustimmung zur Einwilligungsaufforderung gemeint. Allgemein zum Abnutzungseffekt von Information im datenschutzrechtlichen Kontext: *Calo*, 87 Notre Dame Law Review 2012, 1027 (1030 f.); *Efroni* u. a. 5 European Data Protection Law Review 2019, 352 (359); sowie generell zu diesem Effekt: *Hacker*, Verhaltensökonomik und Normativität, 2017, S. 612 f.

[230] Ähnlich *Buchner*, Die informationelle Selbstbestimmung im Privatrecht, 2006, S. 258.

[231] Hierzu unten Kapitel 4 C.II.2.

4. Kapitel

Die Einwilligung als Nukleus des europäischen Datenschuldrechts

Sofern personenbezogene Daten als synallagmatischer Leistungsgegenstand erfasst werden sollen, haben sich die Erlaubnistatbestände einer vertragsakzessorischen Datenverarbeitung (Art. 6 Abs. 1 lit. b DS-GVO) und einer Datenverarbeitung auf Grundlage einer Interessenabwägung (Art. 6 Abs. 1 lit. f DS-GVO) aus mehreren Gründen als ungeeignet herausgestellt. Zu diesen Gründen zählt insbesondere die Gefahr, dass die spezifischeren Anforderungen an eine wirksame Einwilligung unterlaufen werden, je weiter der Anwendungsbereich der beiden anderen Erlaubnistatbestände ausgedehnt wird. Insofern ist es konsequent und überzeugend, dass der europäische Gesetzgeber und die *EU-Kommission* seit Verabschiedung der DS-GVO verstärkt auf die Einwilligung setzen, wenn es darum geht, personenbezogene Daten als Leistungsgegenstand rechtlich anzuerkennen.[1] Damit rückt die Einwilligung ins Zentrum der informationellen Privatautonomie.

Nachfolgend werden die Anforderungen der DS-GVO an die datenschutzrechtliche Einwilligung analysiert. In diesem Zusammenhang wird deutlich, warum der Einwilligungstatbestand dafür geeignet ist, die Vereinbarung von personenbezogenen Daten als Leistungsgegenstand zu erfassen (A).

Allerdings wird auch offenkundig, dass der Tatbestand der Einwilligung sein Potenzial im Kontext eines europäischen Datenschuldrechts nur dann voll entfalten kann, wenn das sog. Kopplungsverbot (Art. 7 Abs. 4 DS-GVO) und die sog. freie Widerruflichkeit (Art. 7 Abs. 3 S. 1 DS-GVO) mit Blick auf den Verhältnismäßigkeitsgrundsatz und anhand des in Art. 1 DS-GVO vorgegebenen datenschutzrechtlichen Doppelziels privatrechtssensibel auslegt und angewendet werden (B).

Unter dieser Voraussetzung ist es möglich und sinnvoll, den unionsautonomen Begriff der Einwilligung stärker auszudifferenzieren, so dass zwei Stufen der Einwilligung möglich werden (C). Diese Unterscheidung bildet zudem die Basis für die in Kapitel 5 vorgeschlagene Stufenleiter der datenschutzrechtlichen Erlaubnistatbestände zur Gewährleistung der abgestützten informationellen Privatautonomie.

---

[1] Vgl. Art. 3 Abs. 1 S. 2 DID-RL (hierzu oben Kapitel 3 C.III.) bzw. Art. 2 Nr. 16, Art. 9 Abs. 2 lit. b und Art. 25 des DG-VO.

A. Vorrang der Einwilligung

Wie bereits in den vorausgegangenen Kapiteln deutlich geworden ist, sprechen mehrere Gründe dafür, dass der Einwilligung im Kontext privatrechtlicher Datenverarbeitungen ein Vorrang zukommt (I). Hieran anschließend werden die wesentlichen Voraussetzungen einer wirksamen datenschutzrechtlichen Einwilligung analysiert (II). In diesem Zusammenhang wird bereits deutlich, dass die Anforderungen der DS-GVO an die Einwilligung in hohem Maße auslegungsbedürftig sind.

I. Gründe für einen Vorrang der Einwilligung

Der Vorrang der Einwilligung gegenüber einer vertragsakzessorischen Datenverarbeitung und einer Datenverarbeitung auf Grundlage einer Interessenabwägung hat mehrere Gründe. Zunächst kommt die Einwilligung einem individualrechtlich ausgerichteten Datenschutz am nächsten (1). Zudem folgt dieser Vorrang der Einwilligung aus der Systematik der Erlaubnistatbestände (2). Darüber hinaus begünstigt die vergleichsweise hohe Regelungsdichte der Einwilligung ein hohes Maß an Einheitlichkeit der Rechtsanwendung (3) und ihre unionsautonom zu bestimmenden Voraussetzungen ermöglichen es, den freien Verkehr von personenbezogenen Daten im europäischen Binnenmarkt zu verwirklichen (4).

1. Datenschutz als Individualschutz

Die generellen Verarbeitungsverbote aus Art. 6 Abs. 1 und Art. 9 Abs. 1 DS-GVO eröffnen den Datensubjekten eine Entscheidungszuständigkeit, ohne dass der Gesetzgeber an personenbezogenen Daten ein subjektives oder sogar ein absolutes Recht zugewiesen hat.[2] Dennoch statuiert diese Entscheidungszuständigkeit ein rechtliches Können, indem sie der „Handlungsfähigkeit des Individuums etwas hinzufügt, was es von Natur aus nicht besitzt".[3]

---

[2] Obwohl die überzeugenderen Argumente für die Anerkennung eines subjektiven Rechts am personenbezogenen Datum sprechen und insbesondere mit den Ansprüchen auf Schadensersatz, Löschung und Portabilität bereits wesentliche Voraussetzungen hierfür bestehen, ist die Diskussion noch offen und nicht Gegenstand dieser Untersuchung. Auch an dieser Stelle wirkt es sich aus, dass der europäische Gesetzgeber es ausdrücklich ablehnt, personenbezogene Daten als immaterielles (Handels-)Gut anzuerkennen, obwohl subjektive Rechte an Persönlichkeitsaspekten längst anerkannt sind. Hierzu m. w. N.: *Sattler,* in: Bakhoum u. a. (Hrsg.), Personal Data in Competition, Consumer Protection and Intellectual Property Law – Towards a Holistic Approach? 2018, S. 27 (41 ff.).

[3] *Alexy*, Theorie der Grundrechte, 2011, S. 213; ebenso in Anlehnung hieran: *Bunnenberg*, Privates Datenschutzrecht, 2020, S. 31.

Diese Entscheidungszuständigkeit hat der europäische Gesetzgeber bislang jedoch primär negativ ausgestaltet. Sie beruht auf dem Verarbeitungsverbot und der unionsgrundrechtlich garantierten Möglichkeit zur Einwilligung, die gemäß Art. 8 Abs. 2 S. 1 GRCh gewährleistet ist.[4] Während Art. 8 Abs. 2 S. 1 GRCh diese Zuständigkeit des Individuums konstituiert, gestalten Art. 6 Abs. 1 lit. a i. V. m. Art. 4 Nr. 11, Art. 7 ff. DS-GVO die Zuständigkeit im Sinne einer Kompetenznorm[5] aus, also einer Norm, die privatautonomes Handeln in Form von ein- und mehrseitigen Rechtsgeschäften ermöglicht.[6] Zwar beruht auch die vertragsakzessorische Datenverarbeitung (Art. 6 Abs. 1 lit. b DS-GVO) immerhin noch auf dem sachgedanklichen Mitbewusstsein des Datensubjekts bei Abgabe derjenigen Willenserklärung, die zum Vertragsschluss geführt hat. Dennoch ist die gemäß Art. 7 Abs. 2 S. 1 DS-GVO regelmäßig getrennt erfolgende Einwilligungserklärung – trotz der bestehenden Kritik am Einwilligungsmodell[7] – die eindeutigere datenschutzrechtliche Willensbekundung des Datensubjekts.

Die DS-GVO beschränkt sich nicht auf ein Verarbeitungsverbot. Mit dem sog. Recht auf Vergessenwerden (Art. 17 DS-GVO), dem Recht auf Datenportabilität (Art. 20 DS-GVO), dem Anspruch auf Schadensersatz, einschließlich immaterieller Schäden (Art. 82 Abs. 1 DS-GVO), und der Möglichkeit zur Einwilligung erfüllt der individualrechtliche Schutz der Datensubjekte vor einer Verarbeitung personenbezogener Daten die beiden Anforderungen, die mit der Abwehr- und Dispositionsbefugnis an ein subjektiven Recht gestellt werden.[8] Damit sind personenbezogene Daten ein immaterielles Gut, aber kein Immaterialgüterrecht, weil hierfür – aus persönlichkeitsrechtlichen Gründen – das wesentliche Charakteristika der Verfügbarkeit durch Übertragung bzw. Einräumung gegenständlicher Rechte fehlt.[9]

Obwohl durch die Eröffnung von Entscheidungszuständigkeit auf Grundlage der datenschutzrechtlichen Einwilligung gerade noch keine Zuweisung eines absoluten subjektiven „Rechts am eigenen Datum" erfolgt[10] und jede rechts-

---

[4] Hierzu oben Kapitel 1 B.II.3.b.bb sowie: *Klement*, in: Simitis/Hornung/Spiecker gen. Döhmann (Hrsg.), Datenschutzrecht, 2019, Art. 7, Rn. 25.

[5] *Alexy*, Theorie der Grundrechte, 2011, S. 213/300 ff.

[6] *Flume*, Allgemeiner Teil des Bürgerlichen Rechts, Teil 2, 1992, S. 7.

[7] Hierzu: *Simitis*, NJW 1998, 2573 (2476); jeweils m. w. N.: *Rogosch*, Die Einwilligung im Datenschutzrecht, 2013, S. 17 f.; *Radlanski*, Das Konzept der Einwilligung in der datenschutzrechtlichen Realität, 2016, S. 147/212/239; *Buchner/Kühling*, in: Kühling/Buchner (Hrsg.), DS-GVO, 3. Aufl. 2020, Art. 7, Rn. 10; ähnlich: *Veil*, NJW 2018, 3337 (3344).

[8] Zur Diskussion: *Ohly*, Volenti non fit iniuria, 2002, S. 181 f.

[9] Grundlegend zur Unterscheidung zwischen Persönlichkeits- und Immaterialgüterrechten anhand des Grads der Verkehrsfähigkeit und damit der Übertragbarkeit des Rechts: *Kohler*, Autorrecht, 1880, S. 74.

[10] M.w.N. *Sattler*, in: Bakhoum u. a. (Hrsg.), Personal Data in Competition, Consumer Protection and Intellectual Property Law – Towards a Holistic Approach? 2018, S. 27 (41 ff.); a. A. *Buchner*, Die informationelle Selbstbestimmung im Privatrecht, 2006, S. 313.

geschäftliche Einräumung von Befugnissen zur Datenverarbeitung nur relativ wirkt,[11] ermöglicht die Einwilligung dem Datensubjekt dennoch die mehrfache wirtschaftliche Verwertung dieser Entscheidungszuständigkeit. Die datenschutzrechtliche Einwilligung ist damit eine Erlaubnis, die ein abstrakt-generelles Verbot (Art. 6 Abs. 1 DS-GVO bzw. Art. 9 Abs. 1 DS-GVO) durch eine konkret-individuelle Eingriffsbefugnis zugunsten des Verantwortlichen modifiziert.[12]

Dies hat zur Folge, dass die privatautonome Kommerzialisierung von personenbezogenen Daten durch das Datensubjekt – jedenfalls im Ausgangspunkt[13] – umso umfangreicher möglich ist, je restriktiver die gesetzlichen Erlaubnistatbestände der DS-GVO ausgelegt werden. Konkret: Je strenger das Tatbestandsmerkmal der Erforderlichkeit in Art. 6 Abs. 1 lit. b und lit. f DS-GVO ausgelegt wird, desto stärker sind Verantwortliche darauf angewiesen, eine wirksame Einwilligung einzuholen, weil das Verarbeitungsverbot im Privatrechtsverhältnis regelmäßig nur noch durch die Legitimationswirkung[14] einer Einwilligung aufgehoben werden kann.[15]

2. Systematik der DS-GVO

Wie bereits im Zusammenhang mit Art. 6 Abs. 1 lit. f und lit. b DS-GVO ausgeführt, lassen sich der DS-GVO und dem ihr zugrundeliegenden Art. 8 GRCh mehrere systematische Argumente für einen Vorrang der Einwilligung im Privatrechtsverhältnis entnehmen.

---

[11] Gemäß Art. 20 Abs. 2 DS-GVO hat das Datensubjekt zwar „das Recht, zu erwirken, dass die personenbezogenen Daten direkt von einem Verantwortlichen einem anderen Verantwortlichen übermittelt werden". Hieraus folgt jedoch allenfalls eine treuhänderisch gebundene Geltendmachung des Anspruchs des Datensubjekts durch den neuen Verantwortlichen. Zu den Möglichkeiten und Grenzen der Datentreuhand: *Wendehorst/Schwamberger/Grinzinger*, in: Pertot (Hrsg.), Rechte an Daten, 2020, S. 103 ff.; *Kühling*, ZfDR 2021, 1 ff.

[12] So bereits zur Einwilligung im deutschen Privatrecht: *Ohly*, Volenti non fit iniuria, 2002, S. 173 f.

[13] Regelmäßig hängt der Wert von personenbezogenen Daten vom Kontext der Verarbeitung ab. Soweit sie personalisierter Werbeansprache dient, ist der ökonomische Wert der Daten insbesondere von der Kaufkraft und produktspezifischen Konsumbereitschaft des Datensubjekts abhängig.

[14] So der zutreffende Ausdruck von *Bunnenberg*, Privates Datenschutzrecht, 2020, S. 35.

[15] Unterstellt man – entgegen der Realität – einen funktionierenden, transparenten Markt, so steigt der „Preis" für eine Einwilligung je restriktiver Art. 6 Abs. 1 lit. b und lit. f DS-GVO ausgelegt werden. Hieraus ergibt sich im Umkehrschluss die wichtige Frage, welche gemeinwohlorientierten Zwecke, insbesondere im Bereich der Forschung, durch eigene Erlaubnistatbestände gefördert werden sollen, ohne auf eine Einwilligung des Datensubjekts angewiesen zu sein. Hierzu Art. 89 DS-GVO, ErwG 159 DS-GVO und insbesondere § 27 Abs. 1 BDSG, der – abweichend von Art. 9 Abs. 2 DS-GVO – eine Verarbeitung von besonders sensibler personenbezogener Daten zu Zwecken der Forschung ermöglichen soll, ohne dass hierfür die Einwilligung erforderlich sein soll.

Zunächst wird nur die Einwilligung – im Gegensatz zu den anderen Erlaubnistatbeständen – *ausdrücklich* in Art. 8 Abs. 2 S. 1 GRCh genannt.[16] Sie schließt bereits den Eingriff in den Schutzbereich von Art. 8 Abs. 1 GRCh aus, statt einen Eingriff lediglich zu rechtfertigen.

Zudem sieht die DS-GVO gerade dann eine Einwilligung vor, wenn die Risiken für die Datensubjekte typischerweise besonders hoch sind. So kann die Verarbeitung besonders sensibler personenbezogener Daten weder vertragsakzessorisch noch auf Grundlage einer Interessenabwägung erfolgen, vgl. Art. 9 Abs. 2 DS-GVO.[17] Hierdurch bringt der europäische Gesetzgeber seine Überzeugung zum Ausdruck, dass der Einwilligung – gerade dann, wenn die Risiken für das Datensubjekt besonders hoch sind – im Vergleich zu den beiden anderen Erlaubnistatbeständen eine höhere Legitimationskraft beizumessen ist.[18]

Diese Wertung findet sich ebenfalls in Art. 22 Abs. 2 lit. c DS-GVO, Art. 20 Abs. 1 lit. a DS-GVO und Art. 49 Abs. 1 S. 1 lit. a DS-GVO, wonach eine Einwilligung, nicht aber Art. 6 Abs. 1 lit. f DS-GVO als Grundlage für eine automatische Entscheidungsfindung in Betracht kommt, einen Anspruch auf Datenportabilität auslöst oder als Grundlage für eine rechtmäßige Übermittlung personenbezogener Daten in einen Drittstaat dient. Indem diese drei Vorschriften auch eine vertragsakzessorische Datenverarbeitung als Grundlage vorsehen,[19] wird erneut deutlich, dass der Interessenabwägung gemäß Art. 6 Abs. 1 lit. f DS-GVO im Privatrechtsverhältnis lediglich die Funktion eines Schrittmachers und Auffangtatbestands zugedacht ist.[20]

Darüber hinaus sind sowohl die Voraussetzungen an eine wirksame Einwilligung als auch die im Zusammenhang mit der Einwilligung bestehenden Rechte des Datensubjekts deutlich umfassender. Während die Tatbestände des Art. 6 Abs. 1 lit. b und lit. f DS-GVO nur durch einen Rückgriff auf die Grundsätze der rechtmäßigen Datenverarbeitung in Art. 5 Abs. 1 DS-GVO[21] bzw. zusätz-

---

[16] Die anderen Erlaubnistatbestände folgen aus dem Ausgestaltungsauftrag an den Gesetzgeber gemäß Art. 8 Abs. 2 S. 1 Hs. 2 Var. 2 GRCh („sonstigen gesetzlich geregelten legitimen Grundlagen").

[17] Zu den erforderlichen Erweiterungen für Spontanäußerungen und das Trainieren von ML: oben Kapitel 2 C.I.3.b. und c.

[18] Ebenso: *Bunnenberg*, Privates Datenschutzrecht, 2020, S. 77; a. A. und damit für einen Vorrang der Fremdbestimmung durch – hoffentlich wohlmeinende – Behörden und Gerichte: *Veil*, NJW 2018, 3337 (3344: „Trotz der berechtigten Kritik am Rechtsinstitut der Einwilligung hält sich hartnäckig die Vorstellung, die Einwilligung habe Vorrang vor allen anderen Erlaubnistatbeständen („Primat der Einwilligung"). Das ist nur mit der Mythologie zu erklären, die sich um die Idee der informationellen Selbstbestimmung rankt").

[19] Art. 22 Abs. 2 lit. a DS-GVO, Art. 20 Abs. 1 lit. a DS-GVO und Art. 49 Abs. 1 lit. c DS-GVO.

[20] Dies spricht aus systematischer Perspektive zudem dafür, dass Art. 6 Abs. 1 lit. b DS-GVO seinerseits ein Vorrang zu Art. 6 Abs. 1 lit. f DS-GVO zukommt. Hierzu: unten Kapitel 5 A.

[21] Oben Kapitel 3 A. und C.II.4–6.

liche Leitlinien und Selbstregulierung bestimmbar werden,[22] sind die Voraussetzungen und Folgen der Einwilligung zwar ihrerseits noch unterkomplex (hierzu Kapitel 5), aber dennoch vergleichsweise detailliert in der DS-GVO geregelt. Art. 4 Nr. 11, Art. 6 Abs. 1 lit. a, Abs. 4 und Art. 7 ff. DS-GVO enthalten vielfach spezifische Konkretisierungen zu den allgemeinen Grundsätzen in Art. 5 Abs. 1 DS-GVO.[23]

Infolgedessen ist die Einwilligung gegenüber der vertragsakzessorischen Datenverarbeitung und der Interessenabwägung aufgrund ihrer spezifischeren Anforderungen aus systematischer Perspektive als *vorrangig* anzusehen. Diese detaillierten Tatbestandsvoraussetzungen würden leerlaufen, sofern eine identische Datenverarbeitung über Art. 6 Abs. 1 lit. b oder lit. f DS-GVO unter Wahrung geringerer tatbestandlicher Anforderungen zu erreichen wäre.[24]

Zuletzt lässt sich auch dem § 26 TDDSG, dem Art. 2 Nr. 16 und Art. 25 DG-VO-Vorschlag und der anhaltenden Diskussion über die ePrivacy-VO entnehmen, dass die Bedeutung der Einwilligung für digitale Geschäftsmodelle zwar umstritten ist, aber eher an Bedeutung zunehmen wird, vgl. ErwG 20–21 ePrivacy-VO-Vorschlag.[25]

3. Einheitlichkeit der Rechtsanwendung

Die höhere Regelungsdichte des Einwilligungstatbestands und das gem. Art. 25 DG-VO geplante, aber bislang nicht publizierte modulare europäische Einwilligungsformular haben ganz erhebliche Vorteile für eine unionsweit einheitliche Auslegung und Anwendung der DS-GVO. Damit dient die Einwilligung der Verwirklichung eines hohen, unionsweit einheitlichen Datenschutzniveaus und eines freien Verkehrs personenbezogener Daten im Binnenmarkt, Art. 1 DS-GVO.

Im Gegensatz hierzu bietet der Tatbestand des Art. 6 Abs. 1 lit. b DS-GVO – abgesehen von der Erforderlichkeit der Datenverarbeitung für die Vertragserfüllung – keinerlei unionweit einheitliche tatbestandliche Voraussetzungen. Damit kommt es auf das jeweilige Schuldrecht der 27 Mitgliedstaaten und dessen Auslegung durch die nationalen Aufsichtsbehörden und Gerichte an.

---

[22] Oben Kapitel 2 C.I.1.b. und c.

[23] Beispielsweise die „Informiertheit" (Art. 4 Nr. 11 DS-GVO) als Konkretisierung des Grundsatzes der Transparenz, die „Freiwilligkeit" (Art. 4 Nr. 11 und Art. 7 Abs. 4 DS-GVO als Konkretisierung des Grundsatzes einer Datenverarbeitung nach Treu und Glauben und die „Zweckbindung" bzw. „Zweckkompatibilität" (Art. 4 Nr. 11 bzw. Art. 6 Abs. 4 DS-GVO) als Konkretisierung des Grundsatzes der Zweckbindung.

[24] Ebenso *Wendehorst/v. Westphalen*, NJW 2016, 3745 (3747); *Engeler*, ZD 2018, 55 (56); *Bunnenberg*, Privates Datenschutzrecht, 2020, S. 51 f./76 f.

[25] Vorschlag der EU-Kommission vom 10.01.2017 für eine Verordnung über die Achtung des Privatlebens und den Schutz personenbezogener Daten in der elektronischen Kommunikation und zur Aufhebung der Richtlinie 2002/58/EG, COM(2017) 10 final.

Wie bereits ausgeführt[26] besteht zwar die theoretische Möglichkeit, dass die Ziele der DS-GVO auch auf Grundlage von Art. 6 Abs. 1 lit. b DS-GVO langfristig erreicht werden können. Insbesondere die von *Philipp Hacker* erwogene und bereits mehrfach zitierte zweifache Rekonstruktion im Mehrebenensystem,[27] die im Ergebnis regelmäßig zu einer mit der DS-GVO konformen Auslegung des nationalen Schuldrechts anhand der datenschutzrechtlichen Grundsätze (Art. 5 DS-GVO) führen dürfte, *kann* im Idealfall langfristig auf Grundlage der Rechtsprechung des *EuGH* und damit unter enormen Transaktionskosten zu einer starken Annäherung der nationalen schuldrechtlichen Vorgaben führen.[28]

Dies setzt aber voraus, dass die Gerichte der Mitgliedstaaten sich – über Art. 4 Abs. 2 Klausel-RL (bzw. § 307 Abs. 3 S. 1 BGB) hinaus[29] – dazu in der Lage sehen, eine einheitliche Angemessenheitsprüfung auf Grundlage von Art. 5 Abs. 1 lit. a DS-GVO (Grundsatz von Treu und Glauben) vorzunehmen[30] oder dass die Klausel-RL mit Blick auf die Vereinbarung von personenbezogenen Daten einer grundlegenden Reform unterzogen wird.[31] Kurzum: Ohne einen tiefgreifenden Eingriff in die Klausel-RL und ohne spezifischere Vorgaben für schwarze und graue Klauseln, gefährdet die über Art. 6 Abs. 1 lit. b DS-GVO eröffnete Anwendung des jeweils nationalen Schuldrechts durch die Gerichte der 27 Mitgliedstaaten die Erreichung des Doppelziels der DS-GVO aus Art. 1 DS-GVO.

Auch Art. 6 Abs. 1 lit. f DS-GVO ist aus Perspektive der Einheitlichkeit eine offene Flanke. Weil es insoweit auf eine Interessenabwägung unter Wahrung des Verhältnismäßigkeitsgrundsatzes ankommt, dient die Interessenabwägung als flexibler Lösungsmechanismus im konkreten Einzelfall. Nachdem weder die ursprünglich geplante Konkretisierung durch die *EU-Kommission* noch eine anderweitige Konkretisierung im Gesetzgebungsverfahren durchsetzbar waren, sollte die Interessenabwägung im Interesse einer einheitlichen Rechtsanwen-

---

[26] Oben Kapitel 3 A. und C.II.6.

[27] Danach setzt jede Anwendung des nationalen Privatrechts i. V. m. Art. 6 Abs. 1 lit. b DS-GVO die Prüfung voraus, „ob auf unionsrechtlicher Ebene (Anwendungsvorrang) oder im Rahmen eines speziellen Rechtsgebiets (Sachintegration) ein bestimmtes Risiko eine abschließende Regelung dergestalt erfahren hat, dass alle Eventualitäten berücksichtigt werden sollten. Sofern eine mitgliedsstaatliche Regelung ein eigenständiges Risiko adressiert (Risikospezifizität), und im Rahmen des Anwendungsvorrangs zudem mit den Zielsetzungen des Unionsrechts vereinbar ist (Zielkompatibilität), kann sie neben der DS-GVO Anwendung finden". *Hacker*, Datenprivatrecht, 2020, S. 538.

[28] So *Hacker*, Datenprivatrecht, 2020, S. 540 ff.; sowie die „schuldrechtliche Lösung" bei *Bunnenberg*, Privates Datenschutzrecht, 2020, S. 53 f. Letzterer bevorzugt deshalb – mit der wohl herrschenden Ansicht eine „datenschutzrechtliche Lösung", die letztlich jedoch in einer strengen Prüfung der Erforderlichkeit als dem einzigen datenschutzrechtlichen Tatbestandmerkmal erschöpft, ebda. S. 54 ff.

[29] Oben Kapitel 3 C.I.2.

[30] Hierfür fehlen jedoch praxistaugliche Kriterien: Oben Kapitel 3 C.I.2.e. und C.I.3.

[31] *Wendehorst*, Verbraucherrelevante Problemstellungen zu Besitz- und Eigentumsverhältnissen beim Internet der Dinge, 2016, S. 89 f.

dung möglichst selten zur Anwendung kommen. Zudem hat Art. 6 Abs. 1 lit. f DS-GVO bei (falscher) Vorlagefreudigkeit der nationalen Gerichte das Potenzial, den notorisch überlasteten *EuGH* regelmäßig zur Auslegung dieser Generalklausel anhand der Unionsgrundrechte zu zwingen.[32] Legen die nationalen Gerichte aber nicht vor und wenden sie Art. 6 Abs. 1 lit. f DS-GVO häufig an, so hat dieser das Potenzial die „loose cannon" an Deck des europäischen Datenschutzrechts zu werden. Immerhin würde die häufige und großzügige Anwendung der Interessenabwägung erheblichen Druck auf den europäischen Gesetzgeber ausüben, diesen Tatbestand bei nächster Gelegenheit durch Fallgruppen zu konkretisieren,[33] weil anderenfalls die Ziele aus Art. 1 DS-GVO gefährdet würden.

Kurz zusammengefasst: Sollen die Ziele eines einheitlichen hohen Schutzniveaus für Datensubjekte und eines freien Verkehrs personenbezogener Daten im Binnenmarkt verwirklicht werden, so spricht dies für einen Vorrang der Einwilligung. In Art. 4 Nr. 11, Art. 6 Abs. 1 lit. a und Art. 7 ff. DS-GVO sind bereits detaillierte europäische Vorgaben enthalten, die der *EuGH* im Rahmen von Vorlageverfahren vergleichsweise leicht durch eine unionsgrundrechtskonforme Auslegung präzisieren kann.

4. Unionsautonomie

Mit den Vorzügen einer einheitlichen Rechtsanwendung ist der Vorteil der Unionsautonomie unmittelbar verbunden. Anders als Art. 6 Abs. 1 lit. b DS-GVO, der den Weg in das nationale Schuldrecht öffnet, ist der Einwilligungstatbestand – anders als wohl vom *BGH* vertreten[34] – weitgehend unabhängig vom nationalen Schuldrecht. Infolgedessen fehlt im Zusammenhang mit der datenschutzrechtlichen Einwilligung auch ein Ansatzpunkt für eine „schuldrechtliche Lösung", die allein auf das nationale Recht abstellt.[35]

---

[32] Hier könnte das dem *EuGH* vom *BVerfG* (Urt. v. 06.11.2019 – 1 BvR 276/17 = GRUR 2020, 88 – *Recht auf Vergessen II*) angetragene Kooperationsverhältnis zwar etwas Abhilfe leisten, birgt jedoch zugleich die Gefahr einer Kakophonie durch 27 Verfassungsgerichte.

[33] In seiner Entschließung zum Bewertungsbericht der EU-Kommission spricht das Europäische Parlament von der Sorge, „dass das ‚berechtigte Interesse' sehr häufig missbräuchlich als Rechtsgrundlage für die Verarbeitung genannt wird", *Entschließung des EU-Parlaments* v. 25.03.2021 zu dem Bewertungsbericht der Kommission über die Durchführung der Datenschutz-Grundverordnung zwei Jahre nach Beginn ihrer Anwendung, 2020/2717(RSP) Nr. 7.

[34] Anders als vom *BGH* behauptet, belässt der Einwilligungstatbestand den Mitgliedstaaten keine Gestaltungsspielräume. Vielmehr legt die DS-GVO die Voraussetzungen einer datenschutzrechtlichen Einwilligung *direkt* fest. Möglicherweise bestehende Lücken sind auf Grundlage der zu beachtenden Grundsätze der rechtmäßigen Datenverarbeitung (Art. 5 Abs. 1 DS-GVO) zu schließen. Jedenfalls hätte dieser Versuch des BGH, das nationale Vertragsrecht gegenüber der DS-GVO – nachträglich – zu immunisieren gemäß Art. 267 Abs. 3 AEUV eine Vorlage zum EuGH erfordert. *BGH*, Beschl. v. 23.06.2020, KVR 69/19 = NZKart 2020, 863 (Rn. 109) – *Facebook*. Diesen Fehler des BGH korrigierend: Vorlagefrage 3 des *OLG Düsseldorf*, Beschl. v. 24.03.2021, Kart 2/19 (V), Rn. 50 ff.

[35] A. A. *Bunnenberg*, Privates Datenschutzrecht, 2020, S. 260.

Im Unterschied zu Art. 6 Abs. 1 lit. b DS-GVO verweist die Interessenabwägung in Art. 6 Abs. 1 lit. f DS-GVO zwar nicht auf das nationale Recht der Mitgliedstaaten. Infolgedessen muss die Auslegung dieses Erlaubnistatbestands vorrangig unionsautonom und anhand der Vorgaben der DS-GVO und subsidiär anhand des europäischen Primärrechts erfolgen. Allerdings besteht im Rahmen der Interessenabwägung gemäß Art. 6 Abs. 1 lit. f DS-GVO gerade eine Pflicht der Gerichte, die jeweiligen Umstände des Einzelfalls umfassend zu berücksichtigen. Infolgedessen sind die Tatbestandsvoraussetzungen des Art. 6 Abs. 1 lit. f DS-GVO zwar unionsautonom auszulegen, die Verpflichtung zur Einzelfallgerechtigkeit dürfte jedoch verhindern, dass in wenigen Jahren durch Richterrecht eine stringente, unionsweit einheitliche Rechtslage i. S. einer typisierten Fallgruppenbildung entsteht.

Somit hat die Einwilligung aus europäischer Perspektive und mit Blick auf die Ziele der DS-GVO einen wesentlichen Vorteil. Die Definition der Einwilligung in Art. 4 Nr. 11 DS-GVO und ihre Konkretisierungen in Art. 6 Abs. 1 lit. a und Abs. 4, Art. 7, Art. 8 und 9 Abs. 1 lit. a DS-GVO enthalten unionsautonome, einheitliche Mindestvoraussetzungen. Sofern sich im Einzelfall Regelungslücken oder Auslegungszweifel ergeben, können diese mithilfe der Grundsätze für eine rechtmäßige Datenverarbeitung, insbesondere durch den unionsrechtlichen Grundsatz von Treu und Glauben (Art. 5 Abs. 1 lit. a Var. 2 DS-GVO) durch den *EuGH* geschlossen bzw. behoben werden.[36]

Soweit der Wortlaut des Art. 7 Abs. 4 und Abs. 3 S. 1 DS-GVO unbestimmt bzw. zu weit ausgefallen ist, lässt er sich – ebenfalls unter Berücksichtigung der unionsgrundrechtlichen Gewährleistungspflichten– eng auslegen[37] bzw. teleologisch reduzieren,[38] wobei gerade die teleologische Reduktion von Unionsrecht nicht nur den Zweck der konkreten Norm, sondern zudem „systemprägend" mit Blick auf die Binnenmarktfinalität des Sekundärrechts erfolgt[39] und dadurch dabei hilft, die Harmonisierungsziele zu verwirklichen. Sofern das in Art. 16 AEUV konstituierte und in Art. 1 DS-GVO verankerte Doppelziel der DS-GVO, also die Gewährleistung des Rechts auf Schutz personenbezogener

---

[36] *Hacker* geht im Kontext der Einwilligung ebenfalls von einem Vorrang des Unionsrechts aus. Dieses bedürfe lediglich in zwei Fällen der analogen Ergänzung durch die deutschen Regelungen der Rechtsgeschäftslehre: Erstens müssten für die Anfechtung der § 119 Abs. 1 und Abs. 2 BGB analog angewendet werden, sofern der Verantwortliche die Anfechtbarkeit der Einwilligung kannte oder kennen musste, § 142 Abs. 2 BGB. Zweitens sollen die §§ 163 ff. BGB analog angewendet werden, sofern die Einwilligung im Rahmen einer Stellvertretung erfolgt. *ders.*, Datenprivatrecht, 2020, S. 539 (Nr. 4). Allerdings lassen sich auch diese beiden Lücken mithilfe des Grundsatzes von Treu und Glauben gemäß Art. 5 Abs. 1 lit. a DS-GVO und damit unionsautonom und ohne Rückgriff auf die nationale Rechtsgeschäftslehre lösen.

[37] Für Art. 7 Abs. 4 DS-GVO (Freiwilligkeit der Einwilligung): Kapitel 5 C.II.

[38] Für Art. 7 Abs. 3 S. 1 DS-GVO (freie Widerruflichkeit der Einwilligung): Kapitel 5 C.III.1.

[39] *Schmidt-Kessel*, in: Riesenhuber (Hrsg.), Europäische Methodenlehre, 3. Aufl. 2015, S. 379 („Akzentverschiebung hin zu einem Verständnis […] als Steuerungsinstrument und weniger als Instrument des klassischen Interessenausgleichs").

Daten und der freie Verkehr personenbezogener Daten im Binnenmarkt effektiv verwirklicht werden sollen, bietet die unionsautonome datenschutzrechtliche Einwilligung dafür die am besten geeignete Grundlage.

Dieses Potenzial der Einwilligung muss jedoch genutzt werden. Das setzt voraus, dass der *EuGH* sich der zentralen Bedeutung der Einwilligung bewusst ist und die gesetzlichen Anforderungen im Lichte dieses Doppelziels behutsam und folgenorientiert weiterentwickelt. Verkennt der *EuGH* diese Chance und legt die Einwilligung sehr streng aus, beispielweise weil er den Datenschutz vorschnell mit einem Schutz von Verbrauchern assoziiert und damit verkürzt, so steigt der Druck auf die wenig geeigneten Erlaubnistatbestände in Art. 6 Abs. 1 lit. b und lit. f DS-GVO. Auf deren Auslegung und Anwendung durch die Aufsichtsbehörden und Gerichte der Mitgliedstaaten hat der *EuGH* jedoch nur einen vergleichsweise geringen Einfluss.

II. Voraussetzungen der Einwilligung

Somit lohnt es sich, einen Blick auf die unionsautonomen Voraussetzungen der datenschutzrechtlichen Einwilligung zu werfen. Ausgangspunkt ist die Definition in Art. 4 Nr. 11 DS-GVO. Danach ist eine Einwilligung

> „jede freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist".

Diese allgemeine Definition wird durch Art. 6, Art. 7 und Art. 8 DS-GVO zusätzlich präzisiert.[40] So enthält Art. 8 Abs. 1 S. 1 DS-GVO eine Konkretisierung der Freiwilligkeit in Form der Einwilligungsfähigkeit von Kindern (1) und Art. 6 Abs. 4 DS-GVO ergänzt die Zweckbestimmung (2). Die Informiertheit der Einwilligung wird durch datenschutzrechtliche Informationspflichten ergänzt (3). Mit Blick auf die Freiwilligkeit wird zwischen der Einwilligungserteilung (4) und der Fortdauer der Freiwilligkeit einer bereits erteilten Einwilligung (5) unterschieden.

1. Einwilligungsfähigkeit als Spezifikation der Freiwilligkeit

Obwohl die geistige Reife gleichermaßen Einfluss auf die Chance eines Datensubjekts hat, den Inhalt einer Einwilligung richtig zu verstehen und somit die Informiertheit der Einwilligung betreffen kann, werden die besonderen Anfor-

[40] Soweit besonders sensible personenbezogene Daten verarbeitet werden sollen, muss die Einwilligung gemäß Art. 9 Abs. 2 lit. a DS-GVO zudem *ausdrücklich* erfolgen.

derungen an die Einwilligungsfähigkeit eines Kindes als Präzisierung der Freiwilligkeit der Einwilligung gewertet.[41]

Wird das Angebot von Diensten der Informationsgesellschaft im Sinne von § 4 Nr. 25 DS-GVO[42] direkt an ein Kind gerichtet, so ist die Einwilligung des Kindes in die Datenverarbeitung rechtmäßig, wenn das Kind das sechzehnte Lebensjahr vollendet hat, Art. 8 Abs. 1 S. 1 DS-GVO. Ausweislich ErwG 38 DS-GVO soll dadurch der typischerweise geringeren geschäftlichen Erfahrung von Kindern Rechnung getragen werden.

Überraschend ist, dass die durch Art. 8 Abs. 1 S. 1 DS-GVO vorgenommene Präzisierung der Freiwilligkeit lediglich mit Blick auf Dienste der Informationsgesellschaft erfolgt. Dadurch erleichtert es Art. 8 Abs. 1 S. 1 DS-GVO den Anbietern von Diensten der Informationsgesellschaft auf schlichte, ihnen zumutbare Altersabfragen zu setzen und bei Angabe eines Alters ab 16 Jahren von der Einwilligungsfähigkeit ausgehen zu können. Im Ergebnis eröffnet Art. 8 Abs. 1 S. 1 DS-GVO den Anbietern von Diensten der Informationsgesellschaft eine größere Rechtssicherheit[43] als den Anbietern anderer Dienste, obwohl ihr komplexes Geschäftsmodell auch für Kinder – trotz der üblichen Bezeichnung als *digital natives* – regelmäßig nicht leichter zu durchschauen ist.

Soweit es sich nicht um Dienste der Informationsgesellschaft handelt und somit keine klaren Altersgrenzen gelten, bleibt es bei einer unionsautonomen Bestimmung der Einwilligungsfähigkeit als Voraussetzung der Freiwilligkeit im Sinne des Art. 4 Nr. 11 DS-GVO. Die Freiwilligkeit der Einwilligung ist deshalb im Einzelfall zu beurteilen und richtet sich nach der tatsächlichen Einwilligungsfähigkeit. Danach ist einwilligungsfähig, wer in der Lage ist, die Bedeutung seiner Erklärung unter Berücksichtigung der Art, des Umfanges, des Anlasses und des Zwecks der jeweiligen Datenverarbeitung zu erfassen.[44] Jedenfalls bis zur Etablierung von Fallgruppen durch die Judikative, bleibt die Einwilligungsfähigkeit jenseits der Einwilligung im Rahmen eines Angebots von Diensten der Informationsgesellschaft vage.[45]

---

[41] M.w.N. *Klement*, in: Simitis/Hornung/Spiecker gen. Döhmann (Hrsg.), Datenschutzrecht, 2019, Art. 8, Rn. 2.

[42] Dieser verweist auf die Definition in Art. 1 Abs. 1 lit. b der Richtlinie (EU) 2015/1535 vom 09.09.2015 über ein Informationsverfahren auf dem Gebiet der technischen Vorschriften und der Vorschriften für die Dienste der Informationsgesellschaft, ABl. v. 17.09.2015 L 241, S. 1 ff.

[43] Weil das Internet die Anonymität begünstigt und nur eingeschränkte Möglichkeiten lässt, die tatsächliche geistige Verfassung zu überprüfen, ist eine solche feste Altersgrenze essentiell für eine rechtssichere Datenverarbeitung: Hierzu: *Rogosch*, Die Einwilligung im Datenschutzrecht, 2013, S. 50 ff.

[44] *Klement*, in: Simitis/Hornung/Spiecker gen. Döhmann (Hrsg.), Datenschutzrecht, 2019, Art. 8, Rn. 10.

[45] Gegen feste Altersgrenzen: *Buchner*, Die Informationelle Selbstbestimmung im Privatrecht, 2006, S. 249 f; *Radlanski*, Das Konzept der Einwilligung in der datenschutzrechtlichen Realität, 2016, S. 102 f.

Vollends unschlüssig erscheint dieser punktuelle Regelungsansatz einer Einwilligungsfähigkeit, soweit Art. 8 Abs. 1 S. 1 DS-GVO zwar eine Sonderregelung für Angebote von Diensten der Informationsgesellschaft enthält, aber beispielsweise keine Vorgaben für die Einwilligungsfähigkeit macht, sofern besonders sensible personenbezogene Daten verarbeitet werden. Erklären lässt sich diese Diskrepanz damit, dass Art. 8 DS-GVO von der *EU-Kommission* ursprünglich als klare Absenkung des Alters für Einwilligungen im Online-Bereich konzipiert war – geplant war ursprünglich eine Altersgrenze von lediglich 13 Jahren – und diese angedachte Erleichterung der Einwilligung erst im Gesetzgebungsverlauf und durch die Anhebung der Altersgrenze auf 16 Jahre einen anderen Zweck erhalten hat.

Aufgrund von ErwG 38 DS-GVO wird der Eindruck verstärkt, dass es sich bei dem verabschiedeten Art. 8 Abs. 1 S. 1 DS-GVO nach dem Willen des Gesetzgebers um eine Vorschrift zum Schutz von Kindern handeln soll.[46] Gemäß Art. 8 Abs. 1 S. 3 DS-GVO haben die Mitgliedstaaten zudem die Möglichkeit, die Altersgrenze für eine Einwilligung „zu diesen Zwecken" – also für Angebote von Diensten der Informationsgesellschaft – auf bis zu 13 Jahre abzusenken. Von dieser Öffnungsklausel hat Deutschland keinen Gebrauch gemacht.

Die in Art. 8 Abs. 3 DS-GVO enthaltene Klarstellung, dass die Altersgrenze für eine Einwilligung das allgemeine Vertragsrecht der Mitgliedstaaten unberührt lässt, ist im Grunde eine Selbstverständlichkeit, die sich bereits aus dem Anwendungsbereich der DS-GVO ergibt. Umgekehrt lässt sich hieraus aber auch nicht ableiten, dass die nationalen Regelungen zur Geschäftsfähigkeit – §§ 2, 104 ff. BGB – Einfluss auf die unionsautonom zu bestimmende Einwilligungsfähigkeit haben.[47]

2. Bestimmtheit und Zweckbindung

Gemäß Art. 4 Nr. 11 DS-GVO muss die Einwilligung „für den bestimmten Fall" erfolgen. Im Unterschied zu dieser deutschen Sprachfassung wird aus der englischen und französischen Sprachfassung deutlich, dass diese Bestimmtheit letztlich den äußeren Tatbestand umschreibt, der vorausgesetzt wird, um anschließend überhaupt bestimmen zu können, ob Datensubjekte die geplante Art

---

[46] *Klement*, in: Simitis/Hornung/Spiecker gen. Döhmann (Hrsg.), Datenschutzrecht, 2019, Art. 8, Rn. 5.

[47] Ebenso *Klement*, in: Simitis/Hornung/Spiecker gen. Döhmann (Hrsg.), Datenschutzrecht, 2019, Art. 8, Rn. 33. Umgekehrt geht *Klement* davon aus, dass die Diskrepanz zwischen der Einwilligungsfähigkeit gemäß Art. 8 Abs. 1 S. 1 und der jeweils durch das nationale Recht determinierten Geschäftsfähigkeit in der Lage ist, den Druck für eine europäische Harmonisierung der Rechtsgeschäftslehre zu erhöhen. Für die Entstehung eines solchen Drucks auf das nationale Recht spricht zudem, dass der Einwilligung von Minderjährigen für die deutsche Diskussion über die Rechtsnatur der Einwilligung und die Anwendung der Regeln der Rechtsgeschäftslehre große Bedeutung zukommt: *Ohly*, Volenti non fit iniuria, 2002, S. 201 ff.

der Datenverarbeitung wahrgenommen, verstanden und in ihren Willen aufgenommen haben.[48]

Somit ist die Bestimmbarkeit eine wesentliche Voraussetzung dafür, dass das Datensubjekt seine informationelle Privatautonomie überhaupt ausüben kann. Die objektive Reichweite der Legitimationswirkung der Einwilligung umfasst nur solche Datenverarbeitungen, die für das Datensubjekt im Zeitpunkt der Einwilligung nach objektivem Empfängerhorizont vorhersehbar waren und deshalb typischerweise in die der Einwilligung vorausgehende Bewertung der Risiken und Chancen durch das Datensubjekt Eingang gefunden haben. Zum Mindestmaß der Bestimmtheit zählen die Festlegung der Kategorien der personenbezogenen Daten,[49] die Identität der Verantwortlichen,[50] die Arten der Datenverarbeitung,[51] die Identität möglicher Datenempfänger[52] und der Zweck der Datenverarbeitung.

Der Zweck der Datenverarbeitung ist nach Ansicht des europäischen Gesetzgebers von herausragender Bedeutung. Dies lässt sich daran ablesen, dass dieser Zweck zunächst Teil der Bestimmtheit einer Einwilligung ist (Art. 4 Nr. 11 DS-GVO), die „Zweckbindung" zudem als eigenständiger Grundsatz jeder rechtmäßigen Datenverarbeitung formuliert ist (Art. 5 Abs. 1 lit. b DS-GVO) und in Art. 6 Abs. 4 DS-GVO zumindest die Kompatibilität des ursprünglichen mit dem aktuellen Verarbeitungszweck ausdrücklich geregelt wird. Die Bestimmtheit des Zwecks ist für das Datensubjekt deshalb von besonderer Bedeutung, weil der Zweck die Chancen und Risiken einer Datenverarbeitung maßgeblich beeinflusst und eine klare Zweckbestimmung am besten geeignet ist, die Konsequenzen einer künftigen Datenverarbeitung vorhersehbar zu machen.

Probleme bereitet die Zweckbestimmung im Rahmen von Geschäftsmodellen, die auf der Verarbeitung von personenbezogenen Daten basiert, um – beispielweise unter Einsatz von ML – neue Erkenntnisse zu generieren[53] und Datensubjekten möglichst personalisierte digitale Produkte anbieten zu können. Weil der Zweck in diesen Fällen nicht von vornherein eindeutig definiert werden kann, haben Verantwortliche ein Interesse daran, den Zweck möglichst breit zu fassen, damit eine leichte Abweichung vom ursprünglichen Zweck möglich bleibt, ohne hierfür eine neue Einwilligung einholen zu müssen.

---

[48] Vgl. die englische Sprachfassung: „specific […] indication of the data subject's wishes"; In der französischen Sprachfassung: „manifestation de volonté […] spécifique". Hierzu *Klement*, in: Simitis/Hornung/Spiecker gen. Döhmann (Hrsg.), Datenschutzrecht, 2019, Art. 7, Rn. 69.

[49] Art. 4 Nr. 1, 13–15/Art. 9 Abs. 1 DS-GVO.

[50] Art. 4 Nr. 7 DS-GVO.

[51] Art. 4 Nr. 2 DS-GVO.

[52] Art. 4 Nr. 9 DS-GVO.

[53] Für die Möglichkeit einer Verarbeitung auf Grundlage einer Interessenabwägung, insbesondere soweit besonders sensible personenbezogene Daten ausschließlich dem Trainieren von ML dienen: oben Kapitel 2 C.I.3.c.

Gleichzeitig muss jedoch sichergestellt werden, dass die Entscheidungszuständigkeit über ein verändertes Risiko der Datenverarbeitung beim Datensubjekt verbleibt.

Infolgedessen besteht ein Spannungsverhältnis zwischen dem Grundsatz der Zweckbindung und der in Art. 6 Abs. 4 DS-GVO für den Fall der Einwilligung etwas großzügiger formulierten Zweckkompatibilität. Es ist das mit Art. 6 Abs. 4 DS-GVO verbundene Regelungsziel, einen Ausgleich zwischen der zu gewährleistenden Kontrolle des Datensubjekts und einem Mindestmaß an Flexibilität für den Verantwortlichen zu schaffen. Dies soll dadurch erreicht werden, dass der Verantwortliche zunächst selbst anhand des vorgegebenen Kriterienkatalogs beurteilt, ob der verfolgte Verarbeitungszweck mit demjenigen Zweck vereinbar ist, zu dem die personenbezogenen Daten ursprünglich erhoben wurden.

Diese Funktion des Art. 6 Abs. 4 DS-GVO wird durch das Beurteilungskriterium in Art. 6 Abs. 4 lit. d DS-GVO am besten zum Ausdruck gebracht. Obwohl die Berücksichtigung der „möglichen Folgen der beabsichtigten Weiterverarbeitung" für das Datensubjekt auf den ersten Blick denkbar unspezifisch ist, wird hieran deutlich, dass der Verantwortliche sich für die Beurteilung der Zweckkompatibilität in die Lage des Datensubjekts versetzen muss, um die Chancen und Risiken der Zweckänderung zu bewerten. Ist der neue Zweck mit Blick auf die Risiken nicht mehr mit dem ursprünglichen Verarbeitungszweck vergleichbar, so war die ursprüngliche Einwilligung des Datensubjekts mit Blick auf diesen neuen Zweck nicht bestimmt, hat insoweit keine Legitimationswirkung und der Verantwortliche muss infolgedessen eine erneute oder zusätzliche Einwilligung einholen.

Der bestehende Konflikt zwischen den rechtlichen Anforderungen an die Bestimmtheit und der tatsächlichen Dynamik der Datenverarbeitung ist mit Blick auf die Verarbeitung von besonders sensiblen Gesundheitsdaten zu Forschungszwecken besonders gravierend. Diese Daten haben einerseits ein immenses Potenzial für die Forschung – einschließlich der Anwendungen von maschinellem Lernen – andererseits ist das Risiko für Datensubjekte extrem hoch, sofern diese Daten beispielsweise Versicherungsunternehmen oder potenziellen Arbeitgebern (unbeabsichtigt) zugänglich werden, bevor eine Versicherungspolice oder ein Arbeitsvertrag abgeschlossen wird. Mit Blick auf die Bestimmtheit der Einwilligung besteht die Herausforderung darin, dass Forschung – bereits definitionsgemäß – zukunftsoffen und sehr dynamisch ist.[54]

Dies führt zu der Debatte, ob eine Einwilligung auch dann noch bestimmt ist, wenn dieser Zukunftsoffenheit von Forschung Rechnung getragen wird. Mitt-

[54] Deshalb für eine weite Rahmeneinwilligung zuletzt: *Leistner/Antoine/Sagstetter*, Big Data, 2021, S. 252 („eine Art nutzungsbezogener Rahmeneinwilligung") sowie S. 261 („höheren nutzungsbezogenen Abstraktionsebene").

lerweile zeigt sich die *Datenschutzkonferenz* (DSK) davon überzeugt, dass eine erweiterte Einwilligung (sog. broad consent) ermöglicht werde sollte,[55] sofern diese durch (besonders) strenge technische und organisatorische Schutzmaßnahmen und durch eine besonders enge behördliche Aufsicht flankiert werden.[56]

3. Informiertheit

Gemäß Art. 5 Abs. 1 lit. a Var. 1 DS-GVO ist eine Datenverarbeitung grundsätzlich nur rechtmäßig, wenn sie in transparenter Weise erfolgt. Dieser Grundsatz wird gemäß Art. 4 Nr. 11 DS-GVO dahingehend konkretisiert, dass die Einwilligung in informierter Weise erfolgen muss. Die Informiertheit des Datensubjekts ist ein Ziel der DS-GVO und eine an den Verantwortlichen gerichtete Forderung, dem Datensubjekt vor dessen Einwilligungserteilung Information bereitzustellen.

Dagegen beschreibt die Informiertheit nicht den tatsächlichen geistigen Zustand des Datensubjekts im Zeitpunkt der Einwilligung. Infolgedessen ist ein Datensubjekt bereits dann informiert, wenn es über zumutbare Möglichkeiten verfügt, sich vor Einwilligungserteilung über die wesentlichen Merkmale der Datenverarbeitung Klarheit zu verschaffen und deren Bedeutung intellektuell zu erfassen.[57] Somit meint Informiertheit im Sinne des Art. 4 Nr. 11 DS-GVO lediglich die *potenzielle Informiertheit* und damit einen fiktiven, aber tatsächlich unter zumutbarem Aufwand erreichbaren Zustand des Datensubjekts.

Im Ergebnis richtet sich die Informiertheit der Einwilligung nicht an das Datensubjekt, sondern löst Pflichten des Verantwortlichen aus, der Daten auf Grundlage der Einwilligung verarbeiten möchte. Erfüllt der Verantwortliche diese Informationspflichten, so kann er sich diesbezüglich auf die Wirksamkeit der Einwilligung verlassen. Das Desinteresse des Datensubjekts an der gut zugänglichen und sachlich richtigen Information geht zulasten des einwilligenden

---

[55] Als Alternative bliebe nur eine Erweiterung des Anwendungsbereichs für eine Interessenabwägung. Oben Kapitel 2 C.I.3.

[56] Einerseits skeptisch: *DSK*, Beschluss der 97. Konferenz zur Auslegung des Begriffs „bestimmte Bereiche wissenschaftlicher Forschung" im Erwägungsgrund 33 der DS-GVO, 03.04.2019, S. 2 (https://www.datenschutzkonferenz-online.de/media/dskb/20190405_auslegung_bestimmte_bereiche_wiss_forschung.pdf, zuletzt abgerufen am 19.05.2022); Andererseits mit einem positiven Beschluss der *DSK* zu den Einwilligungsdokumenten der Medizininformatik-Initiative des Bundesministeriums für Bildung und Forschung v. 15.04.2020 (https://www.datenschutzkonferenz-online.de/media/dskb/20200427_Beschluss_MII.pdf, zuletzt abgerufen am 19.05.2022). Zur Umsetzung dieses sog. broad consent im Rahmen eines Kontroll-Cockpit: Kapitel 6 B.II.1.a.bb.

[57] Je nach Komplexität, kann es im Ausnahmefall sein, dass ein Datensubjekt auch die Obliegenheit trifft, sich sachkundige Beratung einzuholen. Dies ist jedoch nur bei für das Datensubjekt besonders schwerwiegenden Einwilligungen und nicht als allgemeine Standardmaßnahme vertretbar: a. A. wohl *Klement*, in: Simitis/Hornung/Spiecker gen. Döhmann (Hrsg.), Datenschutzrecht, 2019, Art. 7, Rn. 72.

Datensubjekts, weil der Verantwortliche nicht die Erklärungsfahrlässigkeit von Datensubjekten trägt. Während das Datensubjekt grundsätzlich selbst das Risiko zu verantworten hat, ob es die bei vertretbarem Aufwand zugängliche Information auch tatsächlich zur Kenntnis nimmt, trägt der Verantwortliche das Risiko, dass die wesentliche Information richtig, transparent und inhaltlich vollständig aufbereitet ist und so zur Verfügung steht, dass die um die Einwilligung typischerweise ersuchten Datensubjekte[58] diese potenziell zur Kenntnis nehmen können, sofern sie dies wollen.[59]

Um dem Verantwortlichen eine gewisse Rechtssicherheit zu ermöglichen, werden die wichtigsten Informationspflichten durch die DS-GVO konkretisiert, ohne dass diese jedoch abschließend sind. Hierzu zählt die Information über die Identität des Verantwortlichen, die Zwecke der Datenverarbeitung (ErwG 42), die Kategorie der verarbeiteten Daten (Art. 9 Abs. 1 DS-GVO) und die Arten der Verarbeitung, einschließlich deren Verwendung für eine automatische Entscheidungsfindung gemäß Art. 22 Abs. 2 lit. c DS-GVO oder deren Übermittlung in Drittländer (Art. 49 Abs. 1 S. 1 lit. a DS-GVO). Gemäß Art. 7 Abs. 3 S. 3 i. V. m. Art. 13 Abs. 2 lit. c DS-GVO muss der Verantwortliche die Datensubjekte zudem über das – regelmäßig bestehende – Widerrufsrecht informieren.

Weil die DS-GVO einen risikoorientierten Ansatz verfolgt,[60] hängen die Anforderungen an die Informationsbereitstellung vom Risiko der Datenverarbeitung für die Rechte des Datensubjekts ab. Dies ist wichtig, weil es für die Wirkung von Information – wie für Medizin – maßgeblich auf die Dosis ankommt (Gefahr eines *information overload*). Infolgedessen besteht ein gewisser Zielkonflikt zwischen der Verständlichkeit und der Vollständigkeit von Information.[61]

Eine Lösung für dieses Dilemma bieten mehrstufige und modular aufgebaute Einwilligungsformulare.[62] Während die erste Stufe ein leichtes Verständnis der für das Datensubjekt wesentlichen Risiken ermöglicht, ist auf den leicht zugänglichen höheren Stufen die Granularität und Komplexität der Information

[58] Diese potenzielle Informiertheit und die Pflicht des Verantwortlichen kann nach hier vertretener Ansicht jedoch variieren, soweit für den Verantwortlichen erkennbar, eine bestimmte Gruppe von Datensubjekten angesprochen wird und in die Datenverarbeitung einwilligen soll: Hierzu unten Kapitel 5 C.II.2.

[59] Insofern liegt es nahe, Art. 7 Abs. 2 S. 1 DS-GVO als eine Klarstellung und nicht als eine Beschränkung auf Fälle der „schriftlichen Erklärung, die noch andere Sachverhalte betrifft" auszulegen. Jedenfalls hindert diese Vorschrift nicht daran, die Anforderungen an die Verständlichkeit der Information auf Grundlage des Grundsatzes der Transparenz (Art. 5 Abs. 1 lit. a Var. 1 DS-GVO) anzupassen.

[60] So offenkundig: Art. 35 DS-GVO. Zu diesem Ansatz und den daraus folgenden Konsequenzen: *Veil*, ZD 2015, 347 ff.

[61] Hierzu: *Buchner*, Die Informationelle Selbstbestimmung im Privatrecht, 2006, S. 258 ff.; *Hermstrüwer*, Informationelle Selbstgefährdung, 2016, S. 82.

[62] Dieser Ansatz soll durch das geplante europäische Einwilligungsformular für einen Datenaltruismus ebenfalls verfolgt werden: Art. 22 Abs. 2 des Vorschlags für eine Daten-Governance-VO (COM(2020) 767 final). Zum Spannungsverhältnis zwischen Transparenz und Vollständigkeit unten: Kapitel 6 A.I. und B.I.3.

gesteigert. Ein solches gestuftes Modell gewährleistet die Informiertheit derjenigen Datensubjekte, die eine hohe Datenschutzpräferenz haben und bereit sind, sich auch mit komplexer Information auseinanderzusetzen und ihre Entscheidung danach auszurichten. Zudem dienen die höherstufigen Informationsebenen dazu, die Einhaltung der Anforderungen gegenüber Datenaufsichtsbehörden und den klagebefugten Verbänden[63] zu dokumentieren.

Hierin liegt auch die Bedeutung von (standardisierten) Bildsymbolen im Sinne von Art. 12 Abs. 7 DS-GVO.[64] Aus Sicht des Verantwortlichen bedeutet dies, dass eine selbstständige Einführung von solchen Symbolen – idealerweise branchenspezifisch oder sogar branchenübergreifend – auch im eigenen Interesse ist. Zudem folgt aus Art. 8 Abs. 1 GRCh und Art. 16 AEUV eine unionsgrundrechtliche Gewährleistungspflicht des europäischen Gesetzgebers. Er muss sicherstellen, dass die gemäß Art. 8 Abs. 2 S. 1 GRCh garantierte Möglichkeit zur Einwilligung nicht nur formell besteht, sondern auch materieller Ausdruck der informationellen Privatautonomie ist. Solange die europäischen Institutionen ihrer Gewährleistungspflicht selbst nicht nachkommen und insbesondere die *EU-Kommission* von Art. 12 Abs. 8 i. V. m. Art. 92 DS-GVO keinen Gebrauch macht,[65] sollte die Einführung von eigenen, plausiblen Bildsymbolen – jedenfalls sofern diese nicht evident auf eine Verharmlosung der Risiken der Datenverarbeitung angelegt sind – ausschließlich zugunsten der Verantwortlichen berücksichtigt werden.[66] Sie sind zumindest als Indiz für die Informiertheit der Einwilligung des Datensubjekts zu werten.[67]

4. Freiwilligkeit der Einwilligungserteilung

Gemäß Art. 4 Nr. 11 DS-GVO setzt eine wirksame Einwilligung voraus, dass das Datensubjekt durch eine freiwillige Willensbekundung zu verstehen gibt, mit der Datenverarbeitung einverstanden zu sein.[68] Dass eine Einwilligung

[63] Zur Frage inwieweit die DS-GVO hinsichtlich der Rechtsdurchsetzung – insbesondere gegenüber dem UWG – abschließend ist: Vorlagebeschl. des *BGH*, v. 28.05.2020, I ZR 186/17 = GRUR 2020, 896 (Rn. 33 ff.) – *App-Zentrum*. Zur Beschränkung einer möglichen Klagebefugnis auf Verbraucherschutzverbände „als Datenschützer": *Köhler*, WRP 2018, 1269 (1269); gegen eine lauterkeitsrechtliche Klagebefugnis von Mitbewerbern: *LG Bochum*, K&R 2018, 737; *LG Wiesbaden*, K&R 2019, 281; *LG Magdeburg*, K&R 2019, 210; *LG Stuttgart*, WRP 2019, 1089 (Rn. 13 ff.); *Köhler*, ZD 2018, 337; *ders.*, WRP 2019, 1279; *Ohly*, GRUR 2019, 686; *Spittka*, GRUR-Prax 2019, 4. Für eine Klagebefugnis von Mitwerbern: *OLG Hamburg*, WRP 2018, 1510 (Rn. 25); *OLG Naumburg*, GRUR 2020, 210; *Uebele*, GRUR 2019, 694 ff.

[64] Hierzu: ErwG 60 S. 5 f. DS-GVO. Frühzeitig zu „privacy nutrition labels": *Ciocheti*, John Marshall Journal of Computer and Information Law, 2008, No.1, 1 ff.

[65] Hierzu unten Kapitel 6 A.II.1.

[66] Zur Einführung solcher Bildsymbole durch *Apple*: *Chen*, What We Learned From Apple's New Privacy Labels, New York Times, 27.01.2021 (https://www.nytimes.com/2021/01/27/technology/personaltech/apple-privacy-labels.html, zuletzt abgerufen am 19.05.2022).

[67] Hierzu unten: Kapitel 6 A.II.3.b.

[68] Anders ist dies im bürgerlichen Recht. Dort ist die Entscheidungsfreiheit kein Kriteri-

schon begrifflich nicht auf einer Drohung oder auf physischem Zwang beruhen kann, ist eigentlich selbstverständlich.[69] Die Freiwilligkeit der Willensbekundung unterscheidet die Einwilligung von der Nötigung.

Allerdings existieren andere, weniger eindeutige Konstellationen. Dann liegt zwar vordergründig und formell betrachtet eine Entscheidung des Datensubjekts vor, jedoch bestehen in materieller Hinsicht Zweifel an der Freiwilligkeit dieser Einwilligung. Um diese Sachverhalte erfassen zu können, bestimmt Art. 7 Abs. 4 DS-GVO, dass

„bei der Beurteilung, ob die Einwilligung freiwillig erteilt wurde, […] dem Umstand in größtmöglichem Umfang Rechnung getragen werden [muss], ob unter anderem die Erfüllung eines Vertrags, einschließlich der Erbringung einer Dienstleistung, von der Einwilligung zu einer Verarbeitung von personenbezogenen Daten abhängig ist, die für die Erfüllung des Vertrags nicht erforderlich sind."

Dieser Wortlaut von Art. 7 Abs. 4 DS-GVO ist auf den ersten Blick unsinnig und auf den zweiten Blick zumindest sehr ungeschickt gewählt. Abgesehen von dem Fall, dass besonders sensible personenbezogene Daten verarbeitet werden, ist eine Einwilligung schlichtweg überflüssig, sofern die Datenverarbeitung zur Erfüllung eines Vertrags erforderlich ist. In diesem Fall greift bereits der Erlaubnistatbestand aus Art. 6 Abs. 1 lit. b DS-GVO. Eine Einwilligung wäre in diesem Fall also objektiv überflüssig, aber *deswegen* nicht unfreiwillig. Nur weil bereits der gesetzliche, aber vertragsakzessorische Erlaubnistatbestand des Art. 6 Abs. 1 lit. b DS-GVO greift, führt dies nicht zu einer Unfreiwilligkeit einer womöglich zusätzlich, aus Gründen der Absicherung eingeholten Einwilligung.[70]

Allenfalls in Extremfällen, in denen die Einholung einer zusätzlichen Einwilligung für den rechtskundigen Verantwortlichen eindeutig und evident überflüssig ist, könnte ein Datensubjekt durch die dennoch erfolgende Aufforderung zur Einwilligung über deren Erforderlichkeit getäuscht werden. Dieser theoretische Sachverhalt betrifft dann jedoch vorrangig die Informiertheit und allenfalls mittelbar die Freiwilligkeit der Einwilligung.

Mit anderen Worten: Die wesentliche Verarbeitungssituation, in der die Einwilligung zur Anwendung kommt, ist gerade diejenige, in der einem Verantwortlichen gerade keine Möglichkeit zur vertragsakzessorischen Datenverarbeitung zur Verfügung steht. Grund dafür kann sein, dass diese Verarbeitung über das hinausgeht, was für die Vertragserfüllung erforderlich ist, oder dass

---

um für die Wirksamkeit einer Willenserklärung, sondern lediglich ein Anfechtungsgrund: *Lorenz*, Der Schutz vor dem unerwünschten Vertrag, 1997, S. 227 ff.

[69] *Stemmer*, in: Brink/Wolff (Hrsg.), BeckOK DatenschutzR, Art. 7, Rn. 39; *Klement*, in: Simitis/Hornung/Spiecker gen. Döhmann (Hrsg.), Datenschutzrecht, 2019, Art. 7, Rn. 48.

[70] A. A. und mit der Vorstellung, dass Art. 6 Abs. 1 lit. a und lit. b DS-GVO klar voneinander abgrenzbar sind, so dass es keine Graubereiche gibt: *EDSA*, Leitlinien 05/2020 zur Einwilligung gemäß Verordnung 2016/679, Version 1.1, v. 04.05.2020, Nr. 26 a. E. und Nr. 31.

Art. 6 Abs. 1 lit. b DS-GVO trotz eines bestehenden Vertragsverhältnisses dennoch nicht als Grundlage in Betracht kommt.

Die erste Konstellation liegt regelmäßig dann vor, wenn eine über die Vertragserfüllung hinausgehende Verwertung von personenbezogenen Daten, beispielsweise für personalisierte Werbung stattfindet. Die zweite Konstellation kommt insbesondere in Betracht, soweit auch besonders sensible personenbezogene Daten verarbeitet werden, so dass der Verantwortliche *insoweit* regelmäßig zusätzlich zum Vertrag auf eine (ausdrückliche) Einwilligung angewiesen ist, Art. 9 Abs. 2 lit. a DS-GVO. Kurzum: Anders als es der Wortlaut von Art. 7 Abs. 4 DS-GVO suggeriert, kommt die Einwilligung gerade dann in Betracht, wenn eine Datenverarbeitung über das hinausgeht, was für die Erfüllung eines Vertrags erforderlich ist.

Auch ein Blick in ErwG 43 DS-GVO ist nur teilweise erhellend.[71] Immerhin lässt sich ErwG 43 S. 1 DS-GVO entnehmen, dass das Gebot der Freiwilligkeit insbesondere dann beeinträchtigt sein kann,

> „wenn zwischen der betroffenen Person und dem Verantwortlichen ein klares Ungleichgewicht besteht, insbesondere wenn es sich bei dem Verantwortlichen um eine Behörde handelt, und es deshalb in Anbetracht aller Umstände in dem speziellen Fall unwahrscheinlich ist, dass die Einwilligung freiwillig gegeben wurde."

Damit erfasst ErwG 43 S. 1 DS-GVO generalklauselartig solche Konstellationen, in denen das Datensubjekt dem Verantwortlichen – im Einzelfall – *strukturell* („Ungleichgewicht") oder *situativ* („aller Umstände") typischerweise derart unterlegen ist, dass eine Willensbekundung rechtlich nicht mehr als Ausdruck von Privatautonomie gewertet werden darf.[72] Ergänzend stellt ErwG 43 S. 2 DS-GVO klar, dass eine Einwilligung nicht als freiwillig erteilt *gilt*,

> „wenn zu verschiedenen Verarbeitungsvorgängen von personenbezogenen Daten nicht gesondert eine Einwilligung erteilt werden kann, obwohl dies im Einzelfall angebracht ist."

Infolge dieser Fiktion in ErwG 43 S. 2 DS-GVO wird Art. 7 Abs. 4 DS-GVO häufig als *Kopplungsverbot* bezeichnet.[73] Passender ist die Bezeichnung als *Trennungsgebot*, weil hiernach Datenverarbeitungen – soweit angebracht – getrennt werden sollen, die inhaltlich nicht voneinander abhängig sind. Unzusammenhängendes soll nicht künstlich gebündelt und einer ausschließlich *in toto* abzugebenden Einwilligung unterworfen werden.

---

[71] Zu den wiederholten Widersprüchen zwischen den Erwägungsgründen und den Normen siehe *Gola*, K&R 2017, 145 (147).

[72] In diese Richtung auch *BVerfG*, Urt. v. 23.10.2006, 1 BvR 2027/02 = JZ 2007, 576 (577). Hiernach kann es an der Freiwilligkeit fehlen, wenn eine Leistung des Verantwortlichen für die Sicherung der persönlichen Lebensverhältnisse des Datensubjekts von solcher Bedeutung ist, dass die „denkbare Alternative, zur Vermeidung einer zu weitgehenden Preisgabe von persönlicher Informationen von einem Vertragsschluss ganz abzusehen, für ihn unzumutbar ist".

[73] Hierzu ausführlich unten B.I.1. und Kapitel 5 C.II.1.a–c.

Abschließend wiederholt ErwG 43 S. 2 DS-GVO fast wortwörtlich zu Art. 7 Abs. 4 DS-GVO – und damit in überflüssiger Weise –, dass eine Einwilligung als unfreiwillig gilt, wenn die Erfüllung eines Vertrags von ihr abhängig ist, obwohl diese Einwilligung für die Erfüllung nicht erforderlich ist.

Kurios ist, dass in ErwG 43 S. 1 DS-GVO nur eine Behörde als Beispiel für eine strukturelle Unterlegenheit genannt wird, aber kein Äquivalent für eine Datenverarbeitung durch Privatrechtssubjekte. Dies schließt die Übertragung dieses Erwägungsgrunds auf Verantwortliche, die Privatrechtsubjekte sind, zwar nicht aus, liefert aber ein offenkundiges Indiz dafür, dass dem europäischen Gesetzgeber bei Verabschiedung der DS-GVO das Bewusstsein für deren Auswirkungen auf das Privatrecht fehlte. Dennoch begründet die Tatsache, dass in ErwG 43 S. 1 DS-GVO lediglich die Einwilligung gegenüber einer Behörde erwähnt wird, bislang keine grundlegenden Zweifel daran, dass Art. 7 Abs. 4 DS-GVO auch im privatrechtlichen Horizontalverhältnis gilt. Verblüffend ist allerdings, dass in ErwG 43 DS-GVO keinerlei Bezugnahme und Abgrenzung zum kartellrechtlichen Verbot des Missbrauchs einer marktbeherrschenden Stellung (Art. 102 AEUV) vorgenommen wurde.

Aufgrund seines missglückten Wortlauts und seiner ökonomischen Konsequenzen gehört Art. 7 Abs. 4 DS-GVO zu den eindeutig misslungenen und infolgedessen heftig umstrittenen Regelungen der DS-GVO. Entweder lässt sich aus Art. 7 Abs. 4 DS-GVO eine Pflicht des Verantwortlichen zur alternativen Kontrahierung gegen monetäres Entgelt ableiten[74] (sog. strenges Kopplungsverbot) oder er etabliert lediglich eine Pflicht der Aufsichtsbehörden und Gerichte, die Freiwilligkeit der Einwilligung unter Berücksichtigung aller wesentlichen Umstände des Einzelfalls zu beurteilen.[75]

Während die aus Art. 7 Abs. 4 DS-GVO konkret abzuleitenden Pflichten umstritten sind,[76] dient die Vorschrift jedenfalls dazu, die formelle Selbstbestimmung des Datensubjekts im Einzelfall zu materialisieren. Somit konstituiert Art. 7 Abs. 4 DS-GVO eine zentrale Abstützung der informationellen Privatautonomie von Datensubjekten.

5. Widerruflichkeit der Einwilligung

Gemäß Art. 7 Abs. 3 S. 1 DS-GVO hat das Datensubjekt das Recht, seine Einwilligung jederzeit zu widerrufen. Zudem muss der Widerruf – woran es in der

---

[74] So *ÖOGH*, Urt. v. 31.08.2018, 6 Ob 140/18h = ZD 2019, 72 (Rn. 46). Hierzu: *Schwamberger*, GPR 2019, 57.

[75] So ausdrücklich zur Vorgängernorm der Datenschutz-RL: *Corte di Cassazione*, Urt. v. 02.07.2018 – Nr. 17278, unter 2.5. Hierzu kritisch: *Pertot*, GPR 2019, 54 (55 ff.). Zur Verletzung der jeweiligen Vorlagepflicht durch den ÖOGH und den Corte di Cassazione: *Sattler*, GRUR 2019, 1023 (1025).

[76] Hierzu unten Kapitel 5 C.III.

Praxis regelmäßig fehlt[77] – ebenso einfach möglich sein, wie die ursprüngliche Erteilung der Einwilligung. Damit die Datensubjekte ihr Widerrufsrecht kennen, ist der Verantwortliche gemäß Art. 7 Abs. 3 S. 3 i. V. m. Art. 13 Abs. 2 lit. c bzw. Art. 14 Abs. 2 lit. d DS-GVO verpflichtet, die Datensubjekte darüber zu informieren. Weil der Widerruf lediglich *ex nunc* wirkt, bleibt zwar die Rechtmäßigkeit der bisherigen, auf der ursprünglichen Einwilligung basierenden Verarbeitung durch den Widerruf unberührt.[78] Allerdings benötigt der Verantwortliche ab diesem Zeitpunkt nicht nur eine andere Grundlage für die künftige Datenverarbeitung; anderenfalls gilt wieder das Verarbeitungsverbot aus Art. 6 Abs. 1 bzw. Art. 9 Abs. 1 DS-GVO. Vielmehr ist der Verantwortliche darüber hinaus gemäß Art. 17 Abs. 1 lit. b DS-GVO auch zur Löschung der Daten verpflichtet, sofern keine der Ausnahmen gemäß Art. 17 Abs. 3 DS-GVO greift.[79]

Zweifellos ist die Möglichkeit, eine datenschutzrechtliche Einwilligung jederzeit und ohne Angabe von Gründen generell und sogar konkludent zu widerrufen, eine für das Privatrecht überraschend großzügige Einräumung von Autonomie zugunsten der Datensubjekte. Zudem ist es eine – im Vergleich zum deutschen Recht – bestehende Besonderheit dieses Rechts zum Widerruf, dass der Einwilligungswiderruf nach h. A. auch dann möglich sein soll, wenn der Einwilligungsempfänger bereits mit der durch die Einwilligung erlaubten Handlung begonnen hat und selbst seine im Austausch versprochene Leistung gegenüber dem Datensubjekt (teilweise) erbracht hat.[80]

---

[77] Obwohl dies bereits gemäß Art. 7 Abs. 3 DS-GVO rechtlich vorgegeben ist, wird ausgerechnet diese wesentliche Anforderung bislang von den Aufsichtsbehörden nur defizitär mit Bußgeldern bedacht. Zum Vorschlag von standarisierten Erklärungen zur Beendigung der Datenverarbeitung („Kontroll-Cockpit"), unten: Kapitel 6 B.III.

[78] Die Wirkung der Einwilligung entfällt allerdings von Anfang an (*ex tunc*), sofern diese Einwilligung nicht in informierter Weise oder nur unfreiwillig erklärt wurde, § 4 Nr. 11 DS-GVO. Für eine ergänzende Anwendung von § 119 Abs. 1 und Abs. 2 BGB i. V. m. § 142 Abs. 2 BGB sofern der Einwilligungsempfänger – oder sein Vertreter, § 166 Abs. 1 BGB – die Anfechtbarkeit kannten oder fahrlässig nicht kannten: *Hacker*, Datenprivatrecht, 2020, S. 369. Das gleiche Ergebnis lässt sich jedoch auch auf Grundlage des unionsautonomen Grundsatzes einer Datenverarbeitung nach Treu und Glauben (Art. 5 Abs. 1 lit. a Var. 2 DS-GVO) erzielen, so dass es auf einen solchen Rückgriff auf das nationale Recht der Mitgliedstaaten nicht ankommt. Mit grundlegenden Zweifeln an der praktischen Bedeutung einer Anfechtung der Einwilligung mit *ex tunc*-Wirkung: *Neuner*, JuS 2021, 617 (623 f.). Differenzierend für schuldrechtliche Gestattungen (anfechtbar) und für höchstpersönliche, einseitige Einwilligungen (teleologische Reduktion von §§ 142, 143 BGB): *Ohly*, Volenti non fit iniuria, 2002, S. 370 ff.

[79] Zudem dürfte der Widerruf der Einwilligung häufig auch als Widerspruchserklärung gegen eine Verarbeitung auf Grundlage einer Interessenabwägung (Art. 6 Abs. 1 lit. f DS-GVO) auszulegen sein, wenngleich der Widerspruch – anders als der Widerruf der Einwilligung – regelmäßig einen Grund voraussetzt, der sich aus der besonderen Situation des Datensubjekts ergibt, Art. 21 Abs. 1 S. 1 DS-GVO. Nur im Fall eines Widerspruchs gegen Direktwerbung ist keine Begründung erforderlich, Art. 21 Abs. 2 DS-GVO.

[80] Für einen Ausschluss der sog. freien Widerruflichkeit nach Beginn der Leistungserbringung durch den Verantwortlichen: Noch zur Datenschutz-RL von 1995 bzw. zum BDSG a. F.: *Kilian*, Gedächtnisschrift für Steinmüller, 2014, S. 195 (212); *ders.*, CRi 2002, 169 ff.; so für die DS-GVO: *Klement*, in: Simitis/Hornung/Spiecker gen. Döhmann (Hrsg.), Datenschutz-

Zudem folgt aus Art. 7 Abs. 3 S. 1 DS-GVO die Frage, ob die Möglichkeit zum freien Widerruf bereits dann beeinträchtigt ist, wenn der Verantwortliche das Datensubjekt nicht nur gemäß Art. 13 Abs. 2 lit. c i. V. m. Art. 7 Abs. 3 S. 3 DS-GVO über das Widerrufsrecht und dessen Folgen informiert, sondern diese Information mit dem Hinweis verbindet, dass der Verantwortliche sich vorbehält, mit einem Datensubjekt nach einem Einwilligungswiderruf künftig keine Leistungsbeziehung mehr einzugehen. Sollte bereits eine solche Ankündigung von künftigen Konsequenzen mit dem Recht zum jederzeitigen sog. freien Widerruf gemäß Art. 7 Abs. 3 S. 1 DS-GVO unvereinbar sein, so würde das Widerrufsrecht zugunsten des Datensubjekts und zulasten des Verantwortlichen sogar in die künftige Vertragsbeziehung der Beteiligten ausstrahlen. Soweit ersichtlich, wird ein solcher Ansatz noch nicht vertreten. Er wäre jedoch konsequent, wenn man ErwG 42 S. 5 DS-GVO wörtlich nimmt,[81] wie es Aufsichtsbehörden teilweise vertreten.[82]

Ein derart scharfes Schwert, das jede vertragliche Bindungswirkung generell durchschlägt, lässt sich mit Art. 8 Abs. 1 GRCh zwar begründen, aber nicht rechtfertigen. Die Befürworter einer strikten Auslegung scheuen das Pathos nicht, sich hierbei auf die Menschenwürde zu berufen.[83] Sie sollten dabei aber beachten, dass die Menschenwürde – jedenfalls nach deutscher Grundrechtsdogmatik zu Art. 1 Abs. 1 GG – für das Recht auf informationelle Selbstbestimmung nur als Auslegungsunterstützung herangezogen wurde.[84] Zudem diente die grundrechtliche Ergänzung des Art. 2 Abs. 1 GG durch Art. 1 Abs. 1 GG ursprünglich lediglich als Klarstellung, dass der Schutz von Persönlichkeitsrechten auf Menschen beschränkt ist. Juristischen Personen, die sich auf einen Schutz gemäß Art. 2 Abs. 1 GG berufen können, sollten keine Persönlichkeitsrechte gewährt werden.[85]

---

recht, 2019, Art. 7, Rn. 92; für einen Ausschluss bei einem „Widerruf zur Unzeit": *Langhanke/Schmidt-Kessel*, EuCML 2015, 218 (221).

[81] „Es sollte nur dann davon ausgegangen werden, dass [ein Datensubjekt] die Einwilligung freiwillig gegeben hat, wenn [es] eine echte oder freie Wahl hat und somit in der Lage ist, die Einwilligung zu verweigern oder zurückzuziehen, *ohne Nachteile* zu erleiden." [Hervorhebung durch den Verfasser]. Die Verwendung des Begriffs „zurückziehen" statt „widerrufen" dürfte ein Fehler der deutschen Sprachfassung sein. Die englische und die französische Sprachfassung von ErwG 42 S. 5 DS-GVO sind insoweit eindeutig („withdraw consent" und „de retirer son consentement").

[82] In diese Richtung: *EDSA*, Leitlinien 05/2020 zur Einwilligung gemäß Verordnung 2016/679, Version 1.1, v. 04.05.2020, Nr. 38.

[83] Rede von *Giovanni Buttarelli* (EU-Datenschutz-Beauftragter), verfügbar unter https://edps.europa.eu/sites/edp/files/publication/17-01-12_digital_content_directive_sd_en.pdf, zuletzt abgerufen am 19.05.2022.

[84] So bereits: *Steinmüller u. a.*, Grundfragen des Datenschutzes, Gutachten im Auftrag des Bundesministeriums des Innern, 1971, BT Drs. VI/3826, S. 88 („Dazu ist zu sagen, daß die Verfasser der Auslegung von Artikel 2 Abs. 1 durch Artikel 1 nur Unterstützungswert zugestehen; sie ist nach unserer Auffassung nicht in der Lage, eine neue Theorie zu Artikel 2 Abs. 1 zu tragen.").

[85] M.w.N. *Jarass*, NJW 1989, 857 (860); *Roßnagel* (NJW 2019, 1) geht darüber hinweg, dass

Nach derzeit vorherrschendem Verständnis[86] können Datensubjekte, die ihre Einwilligung bereuen, ihre bisherige Entscheidung jederzeit und voraussetzungslos für die Zukunft beseitigen.[87] Privatrechtlich betrachtet ist diese jederzeitige, grundlose und generelle Widerruflichkeit der Einwilligung ein voraussetzungsloses Reue-Recht für die Zukunft.[88] Ansprüche des Verantwortlichen auf Schadens-, Wert- oder Aufwandsersatz sollen – insoweit konsequent – ausgeschlossen sein, § 327q Abs. 3 BGB.[89]

Eine derart weitgehende freie Widerruflichkeit ist unproblematisch, soweit ein Datensubjekt seine schlichte, einseitige Einwilligung widerruft. Diese einseitige Einwilligung begünstigt ausschließlich den Einwilligungsempfänger.[90] Solange der Einwilligungsempfänger gegenüber dem Datensubjekt keine eigene Leistung erbringt, hat er kein schutzwürdiges Interesse an einem zeitlich absehbaren Fortbestand der Einwilligung.

Ist die Einwilligung dagegen Bestandteil eines vertraglichen Synallagmas,[91] so gerät die sog. freie Widerruflichkeit in einen Konflikt zum schuldrechtlichen Grundsatz der Gegenseitigkeit einer Leistungsbeziehung (*quid pro quo – do ut des)*. Sofern eine sog. freie Widerruflichkeit jegliche Bindungswirkung *jeder* datenschutzrechtlichen Einwilligungen verhindern würde[92] und infolgedessen

---

das BVerfG das Recht auf informationelle Selbstbestimmung nicht aus Art. 2 Abs. 1 GG *und* Art. 1 Abs. 1 GG entwickelt hat, sondern aus Art. 2 Abs. 1 GG *in Verbindung mit* Art. 1 Abs. 1 GG, wobei die Hinzuziehung von Art. 1 Abs. 1 GG dazu diente, den personellen Anwendungsbereich dieses Rechts auf natürliche Personen zu beschränken; für eine künftige Erweiterung der DS-GVO auf juristische Personen des Privatrechts: *Marsch*, Das Europäische Datenschutzgrundrecht, 2018, S. 276.

[86] *Langhanke/Schmidt-Kessel*, EuCML 2015, 218(221); *Metzger*, AcP 216 (2016), 817 (825); *Specht*, JZ 2017, 763 (765); *Langhanke*, Daten als Leistung, 2018, S. 118; *Bunnenberg*, Privates Datenschutzrecht, 2020, S. 37 ff.; *Schur*, Die Lizensierung von Daten, 2020, S. 165 ff.; *M. Wagner*, Datenökonomie und Selbstdatenschutz, 2020, S. 345 („Denn die Reversibilität bildet einen der wesentlichen Bausteine des informationellen Schutzes der Menschenwürdegarantie").

[87] Weil der Widerruf der Einwilligung regelmäßig auch einen Widerspruch i. S. d. Art. 21 Abs. 1 S. 1 DS-GVO enthalten dürfte, kommt eine anschließende Verarbeitung auf Grundlage von Art. 6 Abs. 1 lit. f DS-GVO nur in Betracht, soweit zwingend schutzwürdige Gründe i. S. d. Art. 21 Abs. 1 S. 2 DS-GVO überwiegen. Somit begrenzt Art. 21 Abs. 1 S. 2 DS-GVO die Rechtfolge eines Widerrufs ausnahmsweise.

[88] *Lobinger*, AcP 195 (1995), 274 ff. (zum Anfechtungsrecht); zur Gefahr der Begründung eines „Reuerechts" durch das Widerrufsrecht: *Glossner*, MAH IT-Recht, 3. Aufl. 2013, Teil 2 Rn. 209; speziell zu § 312g BGB: *Wendehorst*, in: MüKo, BGB, 7. Aufl. 2016, § 312g, Rn. 39; sowie zuletzt: *BGH*, NJW 2016, 1951 – *Tiefpreisgarantie* (mit Anm. *Wendehorst*).

[89] Allenfalls soweit man annimmt, dass ein Datensubjekt – befristet – über das Widerrufsrecht disponieren kann, kommen vertragliche Ansprüche bei Schlecht- oder Nichtleistung im Zeitraum des Ausschlusses der Widerruflichkeit in Betracht. Eine solche Lösung wäre mit § 327q Abs. 3 BGB vereinbar, weil insoweit keine Abgabe einer datenschutzrechtlichen Erklärung vorliegt, hierzu unten: Kapitel 5 C.III.

[90] Unten C.II.1.

[91] So als Folge von Art. 3 Abs. 1 S. 2 DID-RL: *Metzger*, AcP 216 (2016), 817; *Langhanke/Schmidt-Kessel*, EuCML 2015, 218.

[92] A. A. und (wohl) unter der Annahme, das sachenrechtliche – ausschließlich deutsche –

auch kein rechtlich durchsetzbarer Anspruch auf Zugang zu (korrekten) personenbezogenen Daten und deren Verarbeitung begründet werden könnte,[93] läuft der Grundsatz des *pacta sunt servanda* gemäß Art. 7 Abs. 3 S. 1 DS-GVO ins Leere.[94]

Auf den ersten Blick scheinen die Rechtsfolgen einer Widerruflichkeit aus Perspektive der Datensubjekte ausschließlich vorteilhaft zu sein. Sie können ihre eigene Entscheidungszuständigkeit über die Verarbeitung der personenbezogenen Daten jederzeit und voraussetzungslos wiederherstellen. Aus Sicht des Verantwortlichen hat die freie Widerruflichkeit zur Folge, dass die Datenverarbeitung auf Grundlage einer Einwilligung keine Planbarkeit und Kalkulationsgrundlage schafft.[95]

Die personenbezogenen Daten müssen auf Grundlage der Einwilligung verwertet werden, bevor der Widerruf zugeht. Dass die Widerruflichkeit diesen Anreiz für Verantwortliche setzt, offenbart bereits, dass eine zwingende, jederzeitige Widerruflichkeit auch aus Sicht der Datensubjekte Nachteile haben kann und nach hier vertretener Auffassung zudem Gefahr läuft, das Übermaßverbot zu verletzen, damit gegen den Grundsatz der Verhältnismäßigkeit zu verstoßen[96] und zudem eine Marktzutrittsbarriere zu etablieren.[97]

Trennungs- und Abstraktionsprinzips auch in Bezug auf einen verpflichtenden Vertrag und eine davon zu trennende („dingliche") Einwilligung übertragen zu können: *Metzger*, AcP 216 (2016), 817 (831 f.); *ders.*, in: Lohsse/Schulze/Staudenmayer (Hrsg.), Data as Counter-Performance: Contract Law 2.0?, 2020, S. 25 (34 f.); *M. Wagner*, Datenökonomie und Selbstdatenschutz, 2020, S. 424/639. In diese Richtung auch: *Langhanke*, Daten als Leistung, 2018, S. 163 ff.; *Hacker*, Datenprivatrecht, 2020, S. 162; *Leistner/Antoine/Sagstetter*, Big Data, 2021, S. 255, jedoch zurückhaltender: S. 272 f. und S. 373.

[93] *A. A. Bunnenberg*, der die Anwendungsbereiche von Art. 6 Abs. 1 lit. a und lit. b DS-GVO gerade danach abgrenzen möchte, ob im Einzelfall das Interesse des Verantwortlichen an einer vertraglichen Bindung (dann Art. 6 Abs. 1 lit. b DS-GVO) oder das Interesse des Datensubjekts an der Widerruflichkeit (dann Art. 6 Abs. 1 lit. a i. V. m. Art. 7 Abs. 3 DS-GVO) überwiegt: *ders.*, Privates Datenschutzrecht, 2020, S. 39/264 ff.

[94] Trotz der Anwendbarkeit der DS-GVO auf die „Bildnisbearbeitung" (Rn. 40) und obwohl „es sich bei Personenbildnissen um personenbezogene Daten handelt" (Rn. 43a a. E.), geht *Götting* für § 22 KUG weiterhin davon aus, dass die erteilte Einwilligung mit Blick auf die Kommerzialisierung des Rechts am eigenen Bild grundsätzlich unwiderruflich ist. Nur ausnahmsweise und bei Vorliegen eines wichtigen Grundes entsprechend § 42 UrhG soll sie widerruflich sein, dann aber einen Anspruch auf Ersatz des Vertrauensschadens analog § 122 BGB auslösen: *Götting*, in: Loewenheim/Schricker, Urheberrecht, 6. Aufl. 2020, § 22 KUG, Rn. 40 f.

[95] A. A. *Leistner/Antoine/Sagstetter*, Big Data, 2021, S. 249 („aus Sicht des Datenverarbeiters, der rechtssicherste und belastbarste Erlaubnistatbestand"). Dies gilt aber allenfalls für marktmächtige Unternehmen, die einen Einwilligungswiderruf faktisch kaum zu befürchten brauchen.

[96] Hierzu unten B.II.2.; Kapitel 5 C.III.

[97] Zu dieser Tendenz des Datenschutzrechts allgemein: *Gal/Aviv*, Journal of Competition Law and Economics 2020, 349 (351 f./386 ff.).

Schuldrechtlich lässt sich die sog. freie Widerruflichkeit der Einwilligung als auflösende Bedingung der Leistung des Verantwortlichen abbilden.[98] Diese Einordnung korrespondiert mit der Tendenz, vertragliche Austauschbeziehungen auf der Grundlage von Software so zu automatisieren, dass die jeweiligen Leistungsansprüche technisch implementiert sind („*Code is Law*").[99] Technisch gelingt dies, indem bei Eintritt vorgegebener und im Software-Code programmierter Bedingungen („Parameter") eine informationstechnische Reaktion ausgelöst wird, die auf technischem Weg eine virtuelle oder physische Transaktion bewirkt. Abhängig von der Anzahl der codierten Parameter, deren Erfüllung digital mit Hilfe von Datenbanken überprüfbar ist, können komplexe Transaktionen durch Software technisch abgebildet und abgewickelt werden. In beiden Fällen ist die softwarebasierte Analyse von Datenbanken auschlaggebend. Solange die Leistungsbestimmung und die zeitliche Abfolge der Leistungshandlungen vom Eintritt digital überprüfbarer Bedingungen abhängen (falls X + Y, wird Z ausgeführt) sind solchen Leistungsbeziehungen in Form sog. „smart contracts" technisch keine Grenzen gesetzt.[100] Der Code eines Computerprogramms kann die rechtliche Durchsetzung von bestehenden Ansprüchen – jedenfalls aus Sicht desjenigen, der das Programm kontrolliert – teilweise substituieren. Infolge dieser technischen Form von „Kodifizierung" entstehen lange Ketten von Mikro-Transaktionen, wobei die Verteilung der jeweiligen technischen Fähigkeiten und der jeweiligen Verhandlungsmacht darüber entscheiden, wer in Vorleistung geht.

Weil die sog. freie Widerruflichkeit den Leistungsaustausch jederzeit beenden kann und weil die Anbieter digitaler Produkte regelmäßig die technische Grundlage dieses Austauschs kontrollieren, führt ein Verständnis des Art. 7 Abs. 3 S. 1 DS-GVO, wonach die sog. freie Widerruflichkeit generell und zwingend zu beachten ist, zu einer Dominanz solcher Leistungsbeziehungen, in denen die Datensubjekte – auch technisch durch Software (Code) – dazu gezwungen sind, mit den personenbezogenen Daten in Vorleistung zu gehen.[101]

---

[98] Das EU-Parlament erwähnt ein solches Verständnis, wonach der Zugang zu personenbezogenen Daten als Bedingung ausgestaltet werden kann. Allerdings wird dieser Ansatz nicht vertieft: Bericht des EU-Parlaments, 27.11.2017, S. 8, ("The report deletes the term 'counter-performance', criticized by the EDPS, and replaces it with the term 'condition'"), http://www.europarl.europa.eu/RegData/etudes/BRIE/2018/614707/EPRS_BRI%282018%29614707_EN.pdf, zuletzt abgerufen am 19.05.2022). Ebenso: *EDSA*, Leitlinien 05/2020 zur Einwilligung gemäß Verordnung 2016/679, Version 1.1, v. 04.05.2020, Nr. 37; *Hacker*, ZfPW 2019, 148 (172 ff.); *ders.*, Datenprivatrecht, 2020, S. 228 f.; ähnlich: *Riehm*, in: Pertot (Hrsg.), Rechte an Daten, 2020, S. 194 f.

[99] Grundlegend: *Lessig*, Code and other laws of cyberspace, 1999.

[100] Hierzu m.w.M. *Sattler*, BB 2018, 2243 (2249).

[101] So im Rahmen von sog. Telematik-Tarifen mit nachträglicher teilweiser Prämienerstattung in Abhängigkeit vom vergangenen Fahrverhalten: *Sattler*, JZ 2017, 1036 (1041).

B. Die Einwilligung zwischen Unter- und Übermaßverbot

Art. 8 Abs. 2 S. 1 GRCh bringt zum Ausdruck, dass die Möglichkeit in eine Verarbeitung von personenbezogenen Daten einzuwilligen, Teil der individuellen Persönlichkeitsentfaltung und deshalb unionsgrundrechtlich zu gewährleisten ist.[102] Erst durch die Eröffnung der Möglichkeit, in die Datenverarbeitung gemäß Art. 6 Abs. 1 lit. a DS-GVO einzuwilligen, entgeht der Unionsgesetzgeber einem Verstoß gegen das Untermaßverbot zur Gewährleistung der Selbstbestimmung der Datensubjekte. Danach ist die Einwilligungsmöglichkeit zur Wahrung des Untermaßverbots zwingend vorzusehen, weil die beiden weiteren privatrechtlich relevanten Erlaubnistatbestände in Art. 6 Abs. 1 lit. b und lit. f DS-GVO – in unterschiedlichem Ausmaß – durch Elemente der Fremdbestimmung geprägt sind.[103]

Der europäische Gesetzgeber hat die infolge der Einwilligungsmöglichkeit im Privatrechtsverhältnis bestehende formelle informationelle Privatautonomie mehrfach durch Abstützungen materialisiert. Insbesondere das ausdrückliche Erfordernis der Freiwilligkeit (Art. 7 Abs. 4 DS-GVO) und die sog. freie Widerruflichkeit (Art. 7 Abs. 3 S. 1 DS-GVO) sollen dazu dienen, den gemäß Art. 8 Abs. 1 und Abs. 2 S. 1 GRCh zu gewährleistenden Schutz personenbezogener Daten zu bieten und so das Untermaßverbot einzuhalten. Weil die Freiwilligkeit und die Widerruflichkeit der Einwilligung jedoch – je nach Auslegung – ihrerseits stark in die Privatautonomie der Verantwortlichen und der (unterschiedlichen) Datensubjekte eingreifen, laufen sie Gefahr, die unternehmerische Freiheit und die Vertragsfreiheit (Art. 16 GRCh bzw. Art. 6 Abs. 3 EUV) und die informationelle Privatautonomie (Art. 8 Abs. 2 S. 1 GRCh) unverhältnismäßig zu beeinträchtigen und somit ihrerseits gegen das Übermaßverbot zu verstoßen.[104] Die Grenzen der Einwilligung, die zugunsten des Einwilligenden gedacht sind, beschränken nicht nur die zu gewährleistenden Grundrechtspositionen der Verantwortlichen, sondern auch die Entscheidungsfreiheit der Datensubjekte. Auch insoweit bedürfen sie einer Rechtfertigung.[105]

Aus Perspektive einer Ermöglichung von informationeller Privatautonomie entscheidet eine privatrechtssensible Auslegung von Art. 7 Abs. 4 DS-GVO (I)

---

[102] Das Europäische Verfassungskonvent hatte zunächst eine Formulierung des Art. 8 GRCh präferiert, wonach „jede Person das Recht hat, über die Weitergabe und Nutzung der sie betreffenden Daten selbst zu entscheiden." Hierzu: *Wolff*, in: Pechstein/Nowak/Häde (Hrsg.), Frankfurter Kommentar, 1. Aufl. 2017, Art. 8, Rn. 6; *Knecht*, in: Schwarze (Hrsg.), EU-Kommentar, Art. 8, Rn. 2.

[103] Hierzu bereits oben: Kapitel 2 und Kapitel 3.

[104] Zu den hieraus zu ziehenden Konsequenzen für eine unionsgrundrechtkonforme Anwendung von Art. 7 Abs. 4 und Auslegung von Art. 7 Abs. 3 S. 1 S-GVO, unten Kapitel 5 C.II. bzw. III.

[105] Ebenso bereits für das deutsche (Verfassungs-)Recht: *Ohly*, Volenti non fit iniuria, 2002, S. 18; *Neuner*, JuS, 2021, 617 (618).

und von Art. 7 Abs. 3 S. 1 DS-GVO (II) darüber, ob die Einwilligung die Funktion erfüllen kann, die ihr nach der Systematik der DS-GVO und durch die unionsgrundrechtliche Garantie der Einwilligung in Art. 8 Abs. 2 S. 1 GRCh zugedacht ist.

I. Grenzen des Übermaßverbots für Art. 7 Abs. 4 DS-GVO

Aus privatrechtlicher Perspektive ruft bereits der oberflächliche Blick auf Art. 7 Abs. 4 DS-GVO ein Störgefühl hervor, an dass sich die unmittelbare Frage anknüpft, ob jedenfalls eine Auslegung von Art. 7 Abs. 4 DS-GVO im Sinne eines strengen Kopplungsverbots[106] mit den Unionsgrundrechten vereinbar ist oder gegen das Übermaßverbot verstößt und damit Gefahr läuft, den Grundsatz der Verhältnismäßigkeit aus Art. 52 Abs. 1 S. 2 GRCh zu verletzen.[107]

Folgt man dem strengen Verständnis von Art. 7 Abs. 4 DS-GVO,[108] unterliegen alle Verantwortlichen einer Pflicht zur alternativen Kontrahierung gegen monetäres Entgelt oder zur schenkungsweisen – also *de facto* durch nicht-personalisierte Werbung finanzierten – Leistungserbringung. Danach ist eine Einwilligung in eine Datenverarbeitung, die über das hinausgeht, was zur Erfüllung eines Vertrags erforderlich ist, nur dann freiwillig, wenn das Datensubjekt frei wählen kann, ob es eine Leistung dieses Verantwortlichen gegen Geld (bzw. schenkungsweise) oder im Austausch gegen eine Einwilligung in die Datenverarbeitung bezieht.

Zwar ist ein Verbot der Kopplung einer Leistung an die Einwilligung bereits aus § 95 Abs. 5 S. 1 TKG und § 28 Abs. 3 lit. b BDSG a. F.[109] bekannt.[110] Im Gegensatz zu Art. 7 Abs. 4 DS-GVO bringen beide Vorschriften jedoch zum Ausdruck, dass es für die Freiwilligkeit einer Einwilligung genügt, wenn andere Diensteanbieter gleichwertige Leistungen gegen monetäres Entgelt anbieten. Inwieweit solche alternativen Angebote auch unter Art. 7 Abs. 4 DS-GVO aus-

---

[106] *Buchner*, DuD 2016, 155 (158); *Kühling/Martini*, EuZW 2016, 448 (451). Hierzu: Kapitel 5 C.II.1.a.

[107] So im Ergebnis: *Klement*, in: Simitis/Hornung/Spiecker gen. Döhmann (Hrsg.), Datenschutzrecht, 2019, Art. 7, Rn. 65.

[108] So: *Albrecht/Jotzo*, Das neue Datenschutzrecht der EU, 2016, S. 70; *Krohm/Müller-Peltze*, ZD 2017, 551 (553); *Golland*, MMR 2018, 130 (134 f.). Zu dieser Möglichkeit auch: *Metzger*, AcP 216 (2016), 817 (823); *Dix*, ZEuP 2017, 1 (7 f.). Frühzeitig dagegen: *Bräutigam*, MMR 2012, 635 (626).

[109] § 28 Abs. 3 lit. b BDSG a. F. lautete: „Die verantwortliche Stelle darf den Abschluss eines Vertrags nicht von einer Einwilligung des Betroffenen nach Absatz 3 Satz 1 abhängig machen, wenn dem Betroffenen ein anderer Zugang zu gleichwertigen vertraglichen Leistungen ohne die Einwilligung nicht oder nicht in zumutbarer Weise möglich ist".

[110] Für ein strenges Kopplungsverbot iRv. § 28 Abs. 3 lit. b BDSG: *Faust*, Digitale Wirtschaft – Analoges Recht: Braucht das BGB ein Update?, DJT-Gutachten 2016, S. 59 (These 3).

reichend sind, ist derzeit umstritten.[111] Jedenfalls jenseits von Beschäftigungs-,[112] Kapitalanlage- und Wohnraummietverträgen,[113] für die mittlerweile regelmäßig von einer strukturellen Unterlegenheit von Arbeitnehmern, Verbrauchern bzw. Mietern ausgegangen wird, ist fraglich, ob stets eine derart eindeutige strukturelle Unterlegenheit von Datensubjekten vorliegt, so dass es gerechtfertigt wäre, eine Einwilligung an der Freiwilligkeit i.S.d. Art. 7 Abs. 4 DS-GVO scheitern zu lassen.

Mit der italienischen *Corte di Cassazione* und dem *ÖOGH* kamen zwei oberste nationale Gerichte auf Grundlage der (alten) italienischen Vorschrift zur Umsetzung der Datenschutz-RL bzw. auf Grundlage von Art. 7 Abs. 4 DS-GVO zu diametralen Ergebnissen. Während die *Corte di Cassazione*[114] das Kriterium der Freiwilligkeit einer datenschutzrechtlichen Einwilligung großzügig und im Sinne einer Pflicht zur Berücksichtigung aller Umstände des Einzelfalls auslegte, vertrat der *ÖOGH*[115] für Art. 7 Abs. 4 DS-GSG ein strenges Kopplungsverbot, so dass bereits die Verknüpfung eines Angebots zum Vertragsabschluss mit einer für die Vertragserfüllung nicht erforderlichen Einwilligung zur Unfreiwilligkeit der Einwilligung führte.

Während die *Corte di Cassazione* Art. 7 Abs. 4 DS-GVO lediglich im Rahmen der Auslegung der entscheidungserheblichen italienischen Vorschrift berücksichtigte, wendete der *ÖOGH* den Art. 7 Abs. 4 DS-GVO ausdrücklich an, wies auf den insoweit bestehenden Streit in der Literatur hin und kam zu der Ansicht, dass im Fall einer

> „Koppelung der Einwilligung zu einer Verarbeitung vertragsunabhängiger personenbezogener Daten mit einem Vertragsschluss […] grundsätzlich davon auszugehen [ist], dass die Erteilung der Einwilligung nicht freiwillig erfolgt".[116]

Anschließend lehnte der *ÖOGH* eine Vorlage des Art. 7 Abs. 4 DS-GVO zum *EuGH* deshalb ab, weil sich diese Unfreiwilligkeit der Einwilligung aufgrund einer Kopplung

---

[111] M.w.N. *Golland*, MMR 2018, 130 (134 f.); *Engeler*, ZD 2018, 55 (57). Im Detail unten: C.II.2.b.

[112] Besonderheiten gelten für datenschutzrechtliche Einwilligungen, die im Zusammenhang mit der Begründung oder Durchführung von Beschäftigungsverhältnis stehen: Für die Zulässigkeit: *Schulz*, in: Gola (Hrsg.), DS-GVO, Art. 7, Rn. 46; *Spelge*, DuD 2016, 775 (780); für eine Unzulässigkeit aufgrund von Ungleichgewichtslage: *Stelljes*, DuD 2016, 787 (788); Art. 29 Gruppe, WP 259, S. 7. m. w. N. *Klement*, in: Simitis/Hornung/Spiecker gen. Döhmann (Hrsg.), Datenschutzrecht, 2019, Art. 7, Rn. 64 ff.

[113] *Kamp/Rost*, DD 2012, 80 (81).

[114] *Corte di Cassazione*, Urt. v. 02.07.2018 – Nr. 17278; Anmerkung hierzu: *Pertot*, GPR 2019, 54 ff.

[115] *ÖOGH*, Urt. v. 31.08.2018, 6 OB 140/18 H; Anmerkung hierzu: *Schwamberger*, GPR 2019, 57 ff.

[116] *ÖOGH*, Urt. v. 31.08.2018, 6 OB 140/18 H, unter Ziffer 4.4.4.

„bereits aus dem Wortlaut der DSGVO und dem zitierten Erwägungsgrund [43] ergibt. Auf konkrete Umstände, aus denen sich im Einzelfall ausnahmsweise eine Zulässigkeit der Koppelung ergeben könnte, hat sich die Beklagte nicht berufen, sodass im vorliegenden Fall auch kein Raum für die Klärung der Frage besteht, in welchen Fällen *ausnahmsweise trotz des grundsätzlichen Verbots* eine derartige Koppelung zulässig sein kann".[117]

Mit dieser Begründung verletzte der *ÖOGH* seine Vorlagepflicht gemäß Art. 267 Abs. 3 AEUV, weil er die Auslegung des Art. 7 Abs. 4 DS-GVO gerade nicht als entscheidungsunerheblich dahinstehen ließ, sondern sich in der Sache für ein Verständnis als strenges Kopplungsverbot entschied.

Mit dem *EDSA* vertritt eine wichtige, wenngleich nicht entscheidende, europäische Institution eine ähnlich strenge Ansicht zu Art. 7 Abs. 4 DS-GVO. Der *EDSA* deutet das Erfordernis, den jeweiligen Umständen „in größtmöglichem Umfang Rechnung" zu tragen, als Hinweis darauf,[118] dass es ausnahmsweise

„einen sehr begrenzten Raum für Fälle geben [kann], in denen die Konditionalität die Einwilligung nicht ungültig machen würde".[119]

Somit schließt der *EDSA* aus einer Kopplung von Vertrag und Einwilligung zwar nicht automatisch auf die Unfreiwilligkeit der Einwilligung. Dennoch interpretiert der *EDSA* den Art. 7 Abs. 4 DS-GVO als eine Vorschrift, mit deren Hilfe die DS-GVO sicherstellen soll, dass die Verarbeitung personenbezogener Daten durch eine Einwilligung weder direkt noch indirekt zur Gegenleistung für einen Vertrag werden kann.[120]

Nach Ansicht des *EDSA* ist Art. 7 Abs. 4 DS-GVO streng auszulegen, so dass es für die Freiwilligkeit einer Einwilligung nicht genügt, wenn ein anderer Marktteilnehmer eine gleichwertige Leistung gegen monetäres Entgelt anbietet. Zwar stünde den Datensubjekten mit Blick auf den Gesamtmarkt dann eine Alternative zur Einwilligung zur Verfügung. Nach Ansicht des *EDSA* soll die durch Art. 7 Abs. 4 DS-GVO beabsichtigte „Wahlmöglichkeit" jedoch gerade nicht vom Verhalten anderer Markteilnehmer und davon abhängig sein, ob diese Alternative tatsächlich gleichwertig ist.[121]

---

[117] *ÖOGH*, Urt. v. 31.08.2018, 6 OB 140/18 H, unter Ziffer 4.4.5 [Hervorhebung durch den Verfasser].

[118] *EDSA*, Leitlinien 05/2020 zur Einwilligung gemäß Verordnung 2016/679, Version 1.1, v. 04.05.2020, Nr. 34.

[119] *EDSA*, Leitlinien 05/2020 zur Einwilligung gemäß Verordnung 2016/679, Version 1.1, v. 04.05.2020, Nr. 35.

[120] *EDSA*, Leitlinien 05/2020 zur Einwilligung gemäß Verordnung 2016/679, Version 1.1, v. 04.05.2020, Nr. 26.

[121] Nicht überzeugen kann das Argument des *EDSA*, dass der Verantwortliche die Entwicklungen des Marktes verfolgen müsste, um eine fortgesetzte Gültigkeit der Einwilligung in die Datenverarbeitungstätigkeiten sicherzustellen, da ein Wettbewerber seine Dienstleistungen zu einem späteren Zeitpunkt ändern könnte (*EDSA*, Leitlinien 05/2020 zur Einwilligung gemäß Verordnung 2016/679, Version 1.1, v. 04.05.2020, Nr. 38). Dieses Risiko kann dem Verantwortlichen überlassen bleiben, der sich i. R. v. Art. 7 Abs. 4 DS-GVO auf dieses alternative Angebot des Gesamtmarkts beruft.

Nachdem sich die vom *EU-Parlament* bevorzugte klarere Formulierung eines Kopplungsverbot gerade nicht durchsetzen ließ,[122] geht die Interpretation des *ÖOGH* und des *EDSA* über das hinaus, was sich dem verabschiedeten Wortlaut entnehmen lässt. Weil die Möglichkeit, personenbezogene Daten zu einem vertraglichen Leistungsgegenstand zu machen, von der DS-GVO nicht ausdrücklich adressiert wurde, muss das Plädoyer des *EDSA* gegen die Möglichkeit von „Daten als Gegenleistung" primär durch rechtspolitisches Wunschdenken motiviert sein.[123] Wäre diese strenge Auffassung einer *generellen* Pflicht des jeweiligen künftigen Verantwortlichen zur alternativen Kontrahierung richtig,[124] so würde Art. 7 Abs. 4 DS-GVO nach hier vertretener Auffassung gegen das Übermaßverbot verstoßen, weil jedenfalls mit einem marktbezogenen Verständnis, bei dem auch Angebote Dritter einbezogen werden, ein milderes, ebenso geeignetes Mittel zur Verfügung stehen würde. Die Vorschrift würde infolgedessen unverhältnismäßig in Art. 16 GRCh und Art. 6 Abs. 3 EUV eingreifen und wäre damit unionsgrundrechtswidrig.[125]

Kurzum: Der jeweilige Wortlaut von Art. 7 Abs. 4 DS-GVO und von ErwG 43 DS-GVO ist nicht nur misslungen. Vielmehr muss die Vorschrift unionsgrundrechtskonform ausgelegt werden, weil jedenfalls ein strenges und generelles Kopplungsverbot anderenfalls die unternehmerische Freiheit der Verantwortlichen unverhältnismäßig beschränkt. Die hieraus folgenden Konsequenzen sprechen für eine *kartellrechtsakzessorische, asymmetrische* Auslegung von Art. 7 Abs. 4 DS-GVO, die ausführlich in Kapitel 5 ausgearbeitet wird.[126]

Hier genügt es zunächst zu verdeutlichen, dass eine Auslegung im Sinne eines strengen Kopplungsverbots – wie sie vom *EDSA* und vom *ÖOGH* vertreten wird – solche Verantwortlichen unverhältnismäßig beeinträchtigt, die keine marktbeherrschende Stellung haben (1) und die lediglich solche personenbezogenen Daten verarbeiten, in deren Verarbeitung unternehmerisch handelnde Datensubjekten eingewilligt haben (2).[127]

---

[122] Hierzu: *Kampert*, Datenschutz in sozialen Netzwerken, 2016, S. 244; *Frenzel*, in: Paal/Pauly (Hrsg.), DS-GVO, 2021, Art. 7, Rn. 1.

[123] Die Ablehnung von personenbezogenen Daten als Leistungsgegenstand wird in Nr. 26 und Nr. 27 vorweggenommen. Erst anschließend geht der *EDSA* auf den Wortlaut von Art. 7 Abs. 4 und den ErwG 43 DS-GVO ein: *EDSA*, Leitlinien 05/2020 zur Einwilligung gemäß Verordnung 2016/679, Version 1.1, v. 04.05.2020, S. 11 f.

[124] So ausdrücklich zu ErwG. 43, aber ohne Vorlage zum EuGH: *ÖOGH*, Urt. v. 31.08.2018, 6 Ob 140/18h = ZD 2019, 72 (Rn. 46); a. A. zur Vorgängernorm der Datenschutz-RL: Kopplung nur bei unverzichtbarer und unersetzbarer Leistung („infungibile, […] irrinunciabile") und ebenfalls ohne Vorlage zum EuGH: *Corte di Cassazione*, Urt. v. 02.07.2018 – Nr. 17278, unter 2.5. Hierzu kritisch: *Pertot*, GPR 2019, 54 (55 ff.). Zur Verletzung der jeweiligen Vorlagepflicht: *Sattler*, GRUR 2019, 1023 (1025).

[125] Hierzu unten Kapitel 5 C.III.4.

[126] Kapitel 5 C.II.1.c.cc.

[127] Zu weiteren Differenzierungskriterien unten: Kapitel 5 C.II.2 und 3.

1. Strenges Kopplungsverbot als Marktzutrittsbarriere

Sofern aus Art. 7 Abs. 4 DS-GVO ein sog. strenges anbieterbezogenes Kopplungsverbot folgen würde, so dass die Freiwilligkeit einer Einwilligung immer dann scheitert, wenn ein Verantwortlicher kein alternatives Angebot gegen monetäres Entgelt anbietet, hätte Art. 7 Abs. 4 DS-GVO das Potential, sich zu einer prohibitiv hohen Marktzutrittsbarriere zu entwickeln.

Viele der Geschäftsmodelle, deren Nutzerzahl derzeit besonders schnell wächst, basieren auf mehrseitigen Plattformen und den dadurch generierten direkten und indirekten Netzwerkeffekten.[128] Beispielsweise sind einige Geschäftsbereiche von *GAFAM* und *BAT* gerade deshalb sehr schnell gewachsen und haben zu dominanten Marktpositionen geführt, weil die gegenüber Datensubjekten angebotenen digitalen Produkte keine Bezahlung eines monetären Preises voraussetzen, sondern auf der Verarbeitung von personenbezogenen Daten für unterschiedliche Zwecke beruhen. Ein zentraler Zweck der Datenverarbeitung ist die dadurch ermöglichte Personalisierung von Werbung. Im Ergebnis finanzieren die Werbekunden auf der einen Seite dieser Plattform das Angebot digitaler Produkte gegenüber den beworbenen Datensubjekten. Aufgrund der hierdurch – und durch andere Vereinbarungen[129] – entstehenden Netzwerkeffekte ist das Angebot von digitalen Produkten im Austausch gegen einen rechtmäßigen Zugang zu personenbezogenen Daten auch für neue Geschäftsmodelle zum Ausgangspunkt geworden. Die Gewöhnung der Verbraucher an vermeintlich kostenlose Angebote, zwingt auch neue Wettbewerber vielfach dazu, dieses durch personalisierte Werbung finanzierte Geschäftsmodell zu wählen, um sich überhaupt am Markt behaupten zu können. Zugespitzt könnte man von einem *data processing by default* sprechen.

Sofern Art. 7 Abs. 4 DS-GVO als *generelle* Pflicht zum alternativen Angebot gegen monetäres Entgelt ausgelegt wird, wird es solchen Unternehmen, die neu auf einen Markt streben, verwehrt, die mit dem Betrieb einer mehrseitigen Plattform einhergehen Netzwerkeffekte ebenfalls stringent zu nutzen. Sie müssten ihr Geschäftsmodell gegenüber Datensubjekten von Anfang an in mindestens zwei Varianten, sowohl im Austausch gegen personenbezogene Daten als auch gegen ein monetäres Entgelt anbieten und hätten bereits infolgedessen

---

[128] *Kerber*, GRUR Int. 2016, 639 (642 f.); *Schweitzer/Fetzer/Peitz*, Digitale Plattformen: Bausteine für einen künftigen Ordnungsrahmen, ZEW Discussion Paper No. 16–042, S. 4 ff.; *Drexl*, NZKart 2017, 415 ff.

[129] Die *Mehrseitigkeit* der Plattformen beruht darauf, dass ständig weitere Möglichkeiten der Verwertung der generierten Daten getestet werden. Beispielsweise werden *Facebook* und *Google* (Alphabet) gerade aufgrund der riesigen verfügbaren Mengen an (personenbezogenen) Daten besonders gute Entwicklungschancen im Bereich von machine learning zugetraut. Es ist jedenfalls auch plausibel, dass zusätzliche Verwertungshandlungen für solche Zwecke attraktiv sind, für die eine Zahlungsbereitschaft von Kunden besteht und solange diese Verarbeitungszwecke nicht das Kerngeschäft durch einen Vertrauensverlust gefährden.

eine schlechtere (Fix-)Kostenstruktur als die auf diesen Märkten derzeit dominanten Plattformbetreiber.

Während es aus wettbewerbspolitischen Gründen sinnvoll und wettbewerbsrechtlich zulässig sein kann, gegenüber *Alphabet* für das Angebot der Suchmaschine *Google* und gegenüber *Meta Platforms* für das Angebot seines Kommunikationsnetzwerks *Facebook*[130] aus Art. 7 Abs. 4 DS-GVO eine solche Pflicht zur alternativen Kontrahierung gegen monetäres Entgelt *spezifisch* abzuleiten,[131] würde eine solche *generelle* Pflicht, die auch jedes KMU auf einem durch Wettbewerb geprägten Markt trifft, deren unternehmerische Freiheit unverhältnismäßig beeinträchtigen,[132] ohne dass aus wettbewerbsrechtlichen oder datenschutzrechtlichen Gründen die Notwendigkeit besteht, *per se* an der Freiwilligkeit der Einwilligung des Datensubjekts zu zweifeln, nur weil diese Bestandteil eines Vertrags ist und dazu dient, eine kommerzielle Verwertung der personenbezogenen Daten durch personalisierte Werbung zu ermöglichen.

2. Kommerzialisierung durch Datensubjekte als Unternehmer

Auf den ersten Blick scheint eine aus Art. 7 Abs. 4 DS-GVO abgeleitete *generelle* Pflicht zur alternativen Kontrahierung gegen monetäres Entgelt keinen Einfluss auf die Verwertung von personenbezogenen Daten durch unternehmerisch handelnde Datensubjekte – beispielsweise Leistungssportler, Schauspieler oder sog. Influencer – zu haben. Diese professionellen Selbstvermarkter willigen in eine Datenverarbeitung regelmäßig gerade deshalb ein, weil sie von (gemeinsam) Verantwortlichen im Gegenzug ein monetäres Entgelt dafür erhalten.[133] Die personenbezogenen Daten und vermögenswerten Bestandteile des Persönlichkeitsrechts stehen als vertragliche (Haupt-)Leistung in einem Synallagma zum monetären Honorar oder anderen Vorteilen, die dem Datensubjekt als (Gegen-)Leistung gezahlt bzw. gewährt werden.

---

[130] Sowie für die Einwilligung zur Weiterverarbeitung von über WhatsApp erhobene personenbezogenen Daten durch *Facebook*: Anordnung des *HmbBfDI* gegen Facebook: Verbot der Weiterverarbeitung von WhatsApp-Nutzerdaten durch Facebook, Pressemitteilung v. 11.05.2021: „Ferner erfolgt die Zustimmung nicht aus freien Stücken, da WhatsApp die Einwilligung in die neuen Bestimmungen als Bedingung für die Weiternutzung der Funktionalitäten des Dienstes einfordert", (https://datenschutz-hamburg.de/pressemitteilungen/2021/05/2021-05-11-facebook-anordnung, zuletzt abgerufen am 19.05.2022).

[131] Kritisch: *Körber*, NZKart 2016, 348 (351 ff.); *Franck*, ZWeR 2016, 137.

[132] Die schwach entwickelten sekundären Datenmärkte und deren Effekt als Marktzutritt sind somit nicht ausschließlich Ausdruck einer Fehlfunktion von Märkten, sondern der politischen Wertentscheidungen im Datenschutzrecht: *Schweitzer/Peitz*, Discussion Paper No. 17-043, Datenmärkte in der digitalisierten Wirtschaft: Funktionsdefizite und Regelungsbedarf?, 2017, S. 40; *Schweitzer/Fetzer/Peitz*, Digitale Plattformen: Bausteine für einen künftigen Ordnungsrahmen, ZEW Discussion Paper No. 16–042, 2016, S. 23.

[133] Zu den Möglichkeiten und Grenzen einer solchen Datenverarbeitung auf Grundlage von Art. 6 Abs. 1 lit. b DS-GVO, oben: Kapitel 3 B.II.

Wie bereits ausgeführt, enthält Art. 7 Abs. 4 DS-GVO keine eindeutigen Hinweise für seine korrekte Auslegung. Im Gegenteil: Dass in ErwG 43 DS-GVO nur eine Behörde als Beispiel genannt wird und keinerlei Bezugnahme und Abgrenzung zum kartellrechtlichen Verbot des Missbrauch einer marktbeherrschenden Stellung (Art. 102 AEUV) vorhanden ist, sind – wie bereits ausgeführt – deutliche Indizien dafür, dass dem europäischen Gesetzgeber die notwendige Sensibilität für die Auswirkungen von Art. 7 Abs. 4 DS-GVO auf das Privatrecht fehlte. Diese Sensibilisierung muss deshalb nachträglich durch eine unionsgrundrechtskonforme Auslegung des Art. 7 Abs. 4 DS-GVO erreicht werden. Dies spricht dafür, Art. 7 Abs. 4 DS-GVO jedenfalls dann nicht im Sinne eines strengen Kopplungsverbots auszulegen, sofern der Verantwortliche kein marktmächtiges Unternehmen ist und das Datensubjekt selbst unternehmerisch handelt.

Deshalb folgt aus Art. 7 Abs. 4 DS-GVO nach hier vertretener Auffassung kein generelles strenges Kopplungsverbot, sondern lediglich ein *Gebot zur Berücksichtigung* derjenigen Faktoren, die Zweifel an der Freiwilligkeit einer Einwilligung wecken können. Zu diesen Faktoren zählen insbesondere die Marktmacht des Verantwortlichen, die Eigenschaft des Datensubjekts und die konkreten situativen Umstände der Einwilligung.[134]

II. Grenzen des Übermaßverbots für die sog. freie Widerruflichkeit

Die zweite Stellschraube für eine unionsgrundrechtskonforme Auslegung zur Ermöglichung einer abgestützten informationellen Privatautonomie ist die sog. freie Widerruflichkeit der Einwilligung. Weil sich Art. 8 Abs. 2 S. 1 GRCh kein unionsgrundrechtliches Erfordernis für eine jederzeitige und voraussetzungslose Widerruflichkeit der Einwilligung entnehmen lässt, ist Art. 7 Abs. 3 S. 1 DS-GVO somit eine originär sekundärrechtliche Ausgestaltung der unionsgrundrechtlichen Garantie der Einwilligung aus Art. 8 Abs. 2 S. 1 GRCh.

Anders als Art. 7 Abs. 4 DS-GVO, dessen Wortlaut unbestimmt und infolgedessen einer Auslegung leicht zugänglich ist, wirkt der Wortlaut des Art. 7 Abs. 3 S. 1 DS-GVO auf den ersten Blick eindeutig. Sofern eine Datenverarbeitung ausschließlich auf der Grundlage einer Einwilligung beruht, kann diese Rechtsgrundlage dem Verantwortlichen jederzeit einseitig, voraussetzungs- und für das Datensubjekt grundsätzlich folgenlos entzogen werden.[135] Wie

---

[134] Hierzu detailliert: Kapitel 5 C.II.1–3.

[135] Im Fall des Einwilligungswiderrufs soll der Unternehmer (und Verantwortliche einen Vertrag mit einem Verbraucher (und Datensubjekt) über die Bereitstellung digitaler Produkte gemäß Art. 327q Abs. 2 BGB außerordentlich kündigen können, „wenn ihm unter Berücksichtigung des weiterhin zulässigen Umfangs der Datenverarbeitung und unter Abwägung der beiderseitigen Interessen die Fortsetzung des Vertragsverhältnisses bis zum vereinbarten

scharf das Schwert des Einwilligungswiderrufs potenziell sein könnte, wird aus dem bereits erwähnten ErwG 42 S. 5 DS-GVO deutlich. Hiernach soll von einer Freiwilligkeit der Erteilung der Einwilligung nur dann ausgegangen werden, wenn das Datensubjekt

„eine echte oder freie Wahl hat und somit in der Lage ist, die Einwilligung […] zurückzuziehen, ohne Nachteile zu erleiden".[136]

Dieser Satz dient regelmäßig als ausschlaggebendes rechtliches Argument um zu begründen, dass die Widerruflichkeit der Einwilligung nicht zur Disposition des Datensubjekts stehen dürfe.[137]

Allerdings beruht dieser Satz auf einer gesetzgeberischen Utopie, ist bereits deshalb misslungen und seine argumentative Kraft sollte kritisch hinterfragt werden: Tatsächlich existieren keine menschlichen Entscheidungen, die „ohne Nachteile" sind.[138] Jede Entscheidung trägt zumindest die Opportunitätskosten in sich, die durch die damit verbundene Abwahl von alternativen Möglichkeiten entstehen. Deshalb steht der utopische ErwG 42 S. 5 DS-GVO einer unionsgrundrechtskonformen Auslegung nicht im Wege,[139] die sich darum bemüht, Art. 7 Abs. 3 S. 1 DS-GVO mit dem Grundsatz der Verhältnismäßigkeit gemäß Art. 52 Abs. 1 S. 2 GRCh in Einklang zu bringen.

Ebenso wie ein sog. strenges Kopplungsverbot würde auch die *generelle*, jederzeitige und grundlose Widerruflichkeit der Einwilligung die unternehmerische Freiheit von denjenigen Verantwortlichen unverhältnismäßig beschränken, die neu auf einen Markt treten und gerade keine starke Marktposition haben (1). Zudem muss es zumindest unternehmerisch handelnden Datensubjekten möglich sein, über die Widerruflichkeit der Einwilligung zu disponieren, so dass der zu weit geratene Wortlaut von Art. 7 Abs. 3 S. 1 DS-GVO im B2C-Verhältnis zumindest im Einzelfall und im B2B-Verhältnis regelmäßig durch unionsgrundrechtskonforme Auslegung teleologisch zu reduzieren ist (2).

Vertragsende oder bis zum Ablauf einer gesetzlichen oder vertraglichen Kündigungsfrist nicht zugemutet werden kann", hierzu: *Sattler*, NJW 2020, 3623 (3629 ff.).

[136] Anhand der französischen und der englischen Sprachfassung wird deutlich, dass die deutsche Wortwahl („zurückziehen") missglückt ist, weil damit „widerrufen" gemeint ist.

[137] *Metzger*, in: Lohsse/Schulze/Staudenmayer (Hrsg.), Data as Counter-Performance: Contract Law 2.0?, 2020, S. 25 (35); *Hacker*, Datenprivatrecht, 2020, S. 209.

[138] Deshalb stellt § 107 BGB nicht auf das Fehlen jeglicher Nachteile ab, sondern gerade nur darauf, dass ein Minderjährige durch eine Willenserklärung „nicht lediglich einen *rechtlichen Vorteil erlangt*".

[139] So auch: *Klement*, in: Simitis/Hornung/Spiecker gen. Döhmann (Hrsg.), Datenschutzrecht, 2019, Art. 7, Rn. 92.

1. Die freie Widerruflichkeit als Marktzutrittsbarriere

Die sog. freie Widerruflichkeit lässt sich als Kehrseite der Freiwilligkeit der ursprünglichen Einwilligung gemäß Art. 7 Abs. 4 DS-GVO verstehen.[140] Ein jederzeitiges, voraussetzungslosen Widerrufsrecht wirft deshalb auch ein ähnliches wettbewerbspolitisches Problem auf.

In Märkten mit wenigen oder nur einem dominanten Verantwortlichen ist eine freie Widerruflichkeit eine sinnvolle Abstützung der informationellen Privatautonomie. In diesem Fall verhindert sie, dass Datensubjekte sich nur deshalb (zu) langfristig an einen marktmächtigen Anbieter binden, weil keine datenschutzfreundlicheren Alternativen als Substitute zur Verfügung stehen. So wichtig in diesen Fällen eine leichte Loslösung und ein leichter Wechsel zu einem anderen Verantwortlichen ist (Art. 20 DS-GVO), gerade in diesen Fällen wird die Ausübung des freien Widerrufs – aufgrund der dominanten Marktposition des Einwilligungsempfängers – faktisch regelmäßig ausscheiden. Jedenfalls solange aus Sicht der Datensubjekte kaum gleichwertige alternative Kommunikationsnetzwerke oder Suchmaschinen am Markt verfügbar sind, werden Datensubjekte ihre Einwilligungen gegenüber *Meta Platforms* (*Facebook*) bzw. *Alphabet* (*Google*) nur selten widerrufen.

Wie bereits ausgeführt[141] fällt es softwarebasierten Unternehmen leichter, Einwilligungen technisch zu protokollieren, programmierte Applikationen für deren Widerruf vorzusehen und den erfolgten Widerruf anschließend automatisiert umzusetzen. Infolgedessen ist es plausibel, dass insbesondere diejenigen Verantwortlichen mit einer sog. freien Widerruflichkeit besonders gut zurechtkommen, die vorrangig Datenderivate in Form von personalisierter oder stratifizierter Werbung anbieten, deren Geschäftsmodell nahezu vollständig auf Software basiert und deren Leistungen aus Sicht der Datensubjekte kaum ersetzbar sind. Es ist deshalb wahrscheinlich, dass die freie Widerruflichkeit (ebenso wie andere strikte Anforderungen der DS-GVO) Anbietern – wie *GAFAM* und *BAT* – in dem von ihnen jeweils dominierten Marktsegmenten eher einen Wettbewerbsvorteil verschafft.[142]

Jedenfalls sofern Art. 7 Abs. 3 S. 1 DS-GVO generell und unterschiedslos gilt, besteht die Gefahr, dass er den Marktzutritt für solche Unternehmen erschwert, die zwar ebenfalls digitale Produkte im Austausch gegen personenbezogene Daten bereitstellen wollen, die dabei aber nicht auf vergleichbare Skalen- und Netzwerkeffekte setzen können und deshalb gerade zu Beginn ihrer Tätigkeit auf eine höherer Stabilität der Leistungsbeziehungen zu ihren Kunden angewiesen sind, um über eine gewisse Planungssicherheit zu verfügen.

---

[140] Dies wird auch durch die gemeinsame Behandlung in ErwG 42 S. 5 DS-GVO deutlich.

[141] Oben: A.II.5.

[142] Dies scheint auch die *EU-Kommisson* als wesentlichen Nachteil der DS-GVO identifiziert zu haben, indem sie Erleichterungen für KMU in Betracht zieht: Evaluierungsbericht DS-GVO, COM (2020)264 final, S. 12 (19 ff.).

Kurzum: Soweit es *generell* unzulässig ist, wenn Datensubjekte für einen gewissen Zeitraum über die jederzeitige Widerruflichkeit disponieren, etabliert Art. 7 Abs. 3 S. 1 DS-GVO eine Marktzutrittsbarriere für diejenigen Verantwortlichen, die weniger effektiv in der Verwertung von personenbezogenen Daten sind als die marktdominanten Anbieter. Ohne die Möglichkeit, die jederzeitige Widerruflichkeit der Einwilligung zumindest kurzfristig ausschließen zu können, wird es Unternehmen zusätzlich erschwert,[143] solche Geschäftsmodelle auf dem Markt zu etablieren, die zwar bewusst ein höheres Datenschutzniveau haben, dafür aber auf eine maximale Verwertung der personenbezogenen Daten verzichten, ohne dass dieses datenschonende Modell durch eine zumindest vorübergehende Bindungswirkung der Einwilligung ausgeglichen werden kann. Datenschonende Modelle werden aufgerieben, solange die Forderung eines monetären Entgelts mit der Verbrauchererwartung der durch *GAFAM* und *BAT* geprägten sog. „Kostenlos-Kultur" kollidiert.

Weil infolgedessen auch solche Verantwortliche, die ein – relativ betrachtet – höheres Datenschutzniveau anbieten wollen, einstweilen auf eine Verwertung von personenbezogenen Daten angewiesen bleiben, lässt sich dieses höhere Datenschutzniveau nur dann betriebswirtschaftlich umsetzen, wenn die geringere Datenverwertung durch einen verlässlicheren und längerfristigen Zugang zu personenbezogenen Daten kompensiert wird und es gelingt, dieses höhere Schutzniveau am Markt sichtbar zu machen.[144]

Sofern Art. 7 Abs. 3 S. 1 DS-GVO *generell* und *unterschiedslos* für alle Verantwortlichen gilt, also unabhängig von den jeweils konkreten Marktstrukturen und der Position des jeweiligen Verantwortlichen auf diesem Markt, etabliert er eine Hürde für neue Marktteilnehmer. Diese Hürde wird durch das Recht auf Datenportabilität gem. Art. 20 DS-GVO nochmals verstärkt.[145] Zwar soll dieser Anspruch gerade Lock-In-Effekte reduzieren und den leichten Wechsel zu einem anderen Anbieter – in Kombination mit einem Einwilligungswiderruf – ermöglichen. Allerdings löst dieser Anspruch aus Sicht des Verantwortlichen zunächst Kosten aus, die erwirtschaftet werden müssen.[146]

---

[143] Zu den fehlenden ökonomischen Anreizen für „Privacy by Design": *Grossklags/Acquisti*, Proceedings of the Sixth Workshop on Economics of Information Security, 2007, 1 (12 ff.); *Rubinstein*, Berkeley Technology Law Journal, 26 (3) 2011, 1409 ff.

[144] Die Schwierigkeit, ein hohes Datenschutzniveau als Wettbewerbsvorteil herauszustellen, liegt daran, dass der Marktmechanismus für die Bereitstellung von digitalen Produkten ein „atypischer Zitronenmarkt" teilweise versagt, hierzu oben: Kapitel 3 C.I.2.c. Zu den Möglichkeiten einer Reaktion auf das Marktversagen durch Verbesserung der Markttransparenz (*Signalling*), unten: Kapitel 6 A.II.

[145] *Polanski*, EuCML 2018, 141 (142); *Peitz/Schweitzer*, NJW 2018, 275 (280); *Crémer/de Montjoye/Schweitzer*, Competition policy for the digital era, 2019, S. 82; *Gal/Aviv*, Journal of Competition Law and Economics 2020, 349 (351 f./386 ff.).

[146] Mit dem Hinweis, dass die durch Art. 20 verursachten Kosten das Interesse an einem längerfristigen Vertragsverhältnis begründen: *Schweitzer/Peitz*, Datenmärkte in der digitali-

Sofern Art. 7 Abs. 3 S. 1 DS-GVO allen Verantwortlichen generell die Möglichkeit nimmt, mit Datensubjekten solche Austauschverträge zu schließen, die zumindest eine gewisse zeitliche Bindung ermöglichen, wird ihre unternehmerische Freiheit begrenzt. Auch dem europäischen Gesetzgeber dürften diese Nachteile einer generellen freien Widerruflichkeit bald bewusst werden. Sofern die in der DG-VO geregelte Möglichkeit von beaufsichtigten Datenvermittlern für eine gemeinsame Datennutzung[147] Realität werden und diese – auf Grundlage einer Einwilligung[148] – auch die Verwertung von personenbezogenen Daten treuhänderisch wahrnehmen,[149] wird die vertragliche Disposition über die Widerruflichkeit der Einwilligung ins Zentrum rücken, weil auch die Gründung und Aufrechterhaltung von solchen Datenvermittlern eine gewisse Stabilität der Leistungs- und Rechtsbeziehungen voraussetzt.

Zusammengefasst: Die in Art. 7 Abs. 3 S. 1 DS-GVO angelegte sog. freie Widerruflichkeit setzt – vom Gesetzgeber mutmaßlich unbeabsichtigt – einen Anreiz für solche Geschäftsmodelle, die sich mittels einer möglichst umfassenden Einwilligung einen rechtmäßigen Zugang zu personenbezogenen Daten verschaffen und diesen anschließend möglichst schnell und möglichst umfassend verwerten, bevor die Datensubjekte ihre Einwilligung widerrufen. Dieser Anreiz macht deutlich, dass Art. 7 Abs. 3 S. 1 DS-GVO ins Zentrum einer Auslegung und Anwendung der DS-GVO rückt, sofern die fehlende „vertragliche Unterfütterung" der DS-GVO[150] korrigiert werden soll und nach hier vertretener Auffassung korrigiert werden muss.[151]

2. Kommerzialisierung durch Datensubjekte als Unternehmer

Ebenso wie Art. 7 Abs. 4 DS-GVO offenbart auch Art. 7 Abs. 3 S. 1 DS-GVO ein mangelhaftes Verständnis des europäischen Gesetzgebers für diejenigen Märkte, auf denen unternehmerisch handelnde Datensubjekte seit vielen Jahrzehnten die vermögenswerten Bestandteile ihrer Persönlichkeitsrechte und in diesem Zusammenhang auch personenbezogene Daten kommerzialisieren.

---

sierten Wirtschaft: Funktionsdefizite und Regelungsbedarf? ZEW Discussion Paper No. 17-043 2016, S. 50.

147 Art. 10 Abs. 1 lit. b DG-VO.

148 Art. 12 lit. n DG-VO sieht als Grundlage für eine rechtmäßige Verwertung von personenbezogenen Daten unter Einsatz von Datenvermittlern ausdrücklich nur die Einwilligung vor. Auch der Ansatz eines Datenaltruismus beruht ausdrücklich nur auf einer Einwilligung für die gemäß Art. 25 DG-VO ein europäisches Einwilligungsformular entwickelt und verbindlich vorgegeben werden soll.

149 Art. 12 lit. n DG-VO.

150 *Staudenmayer*, ZEuP 2019, 663 (676).

151 Hierzu unten Kapitel 5 C.III.

Dass Datensubjekte, die als Unternehmer handeln, eine erteilte Einwilligung weder jederzeit noch folgenlos widerrufen können, dürfte bis zur Anwendbarkeit der DS-GVO in den meisten EU-Mitgliedstaaten unbestritten gewesen sein. Beispielsweise verweigerte das *LG München* den Widerruf einer Einwilligung in die Herstellung und Veröffentlichung von Fotografien einer nackten Person, obwohl die abgebildete Person diesen Widerruf mit ihrer mittlerweile gewandelten Lebensführung begründen konnte.[152]

Sogar im Verhältnis zwischen Arbeitgeber und Arbeitnehmer und damit in einer Konstellation, die regelmäßig durch eine ökonomische Abhängigkeit geprägt wird, verweigerte das *BAG* einem Arbeitnehmer ein jederzeitiges, voraussetzungslosen Widerrufsrecht. Im zugrundeliegenden Sachverhalt hatte der Arbeitnehmer eingewilligt, dass er identifizierbar in einem Werbefilm auf der Webseite des Arbeitgebers erscheint. Wenige Monate nach Beendigung des Arbeitsverhältnisses widerrief der Arbeitnehmer seine Einwilligung und verklagte den Arbeitgeber auf Unterlassen, Schadensersatz und Beseitigung, nachdem dieser die Bilder des Arbeitnehmers nicht aus dem öffentlich zugänglichen Werbefilm entfernte. Unter Abwägung der beiderseitigen Interessen entschied das *BAG* gegen einen wirksamen Widerruf und entkoppelte damit den ursprünglichen Arbeitsvertrag von der Einwilligung in die Verarbeitung der personenbezogenen Daten, einschließlich einer öffentliche Wiedergabe.[153] Die Bilder des ehemaligen Arbeitnehmers verblieben auf der Webseite des Arbeitgebers.

Beide Entscheidungen sind nicht zur DS-GVO ergangen, dürften aber dennoch und trotz der sog. freien Widerruflichkeit und des sog. Recht auf Vergessenwerden (Art. 17 DS-GVO) auch seit Anwendbarkeit der DS-GVO Bestand haben. Jedenfalls während eines bestehenden Arbeitsverhältnisses unterliegt eine Datenverarbeitung weiterhin gemäß Art. 88 DS-GVO i. V. m. § 26 BDSG dem nationalen Recht. Auch die Herstellung und Verbreitung von Nacktfotografien in einer Zeitschrift könnte – bei sehr weiter Auslegung – noch unter die Öffnungsklausel der Meinungs-, Presse- und Informationsfreiheit gemäß Art. 85 Abs. 1 DS-GVO fallen. Sobald jedoch die kommerziellen Interessen des Datensubjekts und des Verantwortlichen überwiegen, spricht dies für eine Anwendung der DS-GVO.

Sowohl die Vorgängernorm des Art. 9 Datenschutz-RL (1995) als auch Art. 85 DS-GVO enthalten als sog. Presseprivileg keine klare Öffnung für die kommerzielle Verwertung von Persönlichkeitsrechten. Ihre weite Auslegung zugunsten der Meinungsfreiheit erfolgt(e) vielmehr ausdrücklich mit Blick auf

---

[152] *LG München*, Urt. v. 17.03.1989, 21 U 4729/88 = NJW-RR 1990, 999; anderer Kontext und deshalb Widerruf rechtmäßig*: OLG Koblenz*, Urt. v. 20.05.2014, 3 U 1288/13 = ZUM 2015, 58 – *Widerruf der Einwilligung in Anfertigung intimer Lichtbilder vor Beendigung einer Beziehung*; sowie in der Revision: *BGH*, Urt. v. 13.10.2015, VI ZR 271/14 = GRUR 2016, 315 ff. – *Intime Fotos*.

[153] *BAG*, Urt. v. 11.12.2014, 8 AZR 1010/13 = ZD 2015, 330.

journalistische Tätigkeiten.[154] Infolgedessen dürften die Datenverarbeitung im Rahmen von Verträge zur Verwertung der vermögenswerten Bestandteile von Persönlichkeitsrechten seit Mai 2018 in den Anwendungsbereich der DS-GVO fallen.[155] Die Bedeutung des allgemeinen Persönlichkeitsrechts (§ 823 Abs. 1 i. V. m. Art. 2 Abs. 1, Art. 1 Abs. 1 GG) und des Rechts am eigenen Bild (§ 22 KUG) dürfte seither auf einen Kontext reduziert sein, in dem die Presse-, Wissenschafts- und Kunstfreiheit maßgeblich berührt ist.[156]

Obwohl somit beide Sachverhalte potenziell weiterhin in den Anwendungsbereich des deutschen Rechts fallen, illustrieren die Entscheidungen sehr deutlich, dass die jederzeitige und voraussetzungslose Widerruflichkeit der Einwilligung im Einzelfall unangemessen sein kann. Statt die (anschließende) Verarbeitung auf Grundlage von Art. 6 Abs. 1 lit. f i. V. m. Art. 21 Abs. 1 DS-GVO mit zwingenden Gründen[157] oder mit lit. b DS-GVO[158] zu rechtfertigen – Möglichkeiten, die bei besonders sensiblen Daten ausscheiden – sollte es stattdessen grundsätzlich möglich sein, den sog. freien Widerruf der Einwilligung für einen begrenzten und von Anfang an bestimmten Zeitraum auszuschließen.[159]

Es ist ein eklatanter Konstruktionsfehler der DS-GVO, dass der europäische Gesetzgeber die seit Jahrzehnten praktizierte Kommerzialisierung von personenbezogenen Daten durch bekannte Persönlichkeiten – jenseits der äußerungsrechtlichen Ausnahme für (Boulevard-)Medien (Art. 85 Abs. 1 DS-GVO)[160] –

---

[154] *EuGH*, 16.12.2008, C-73/07 = EuZW 2009, 108 (Rn. 56) – *Satakunnan Markkinapörssi und Satamedia*.

[155] Dies offenlassend, weil die Abwägung gem. §§ 22, 23 KUG auf Grundlage des deutschen Grundgesetzes oder nach Art. 6 Abs. 1 lit. f DS-GVO auf Grundlage der Unionsgrundrechte zum gleichen Ergebnis führen würde: *BGH*, Urt. v. 21.01.2021 – I ZR 207/19, NJW 2021, 1311 (Rn. 51) – *Urlaubslotto*. Mit Kritik hieran, weil sich die Rechtfolgen hinsichtlich eines datenschutzrechtlichen Ersatzes einschließlich immaterieller Schäden (Art. 82 DS-GVO) und eines persönlichkeitsrechtlichen Entschädigungsanspruchs unterscheiden: *Ettig*, NJW 2021, 1274 (Rn. 12).

[156] So auch: *Stender-Vorwachs*, in: Brink/Wolff (Hrsg.), BeckOK Datenschutzrecht, 37. Ed., Stand: 01.02.2021, Art. 85, Rn. 19 („Jedenfalls muss bei jeder Zwecksetzung die meinungsbildende Wirkung im Vordergrund stehen. Gerade im Zeitalter des Internets der Dinge darf nicht jede beliebige Zwecksetzung zur Datenprivilegierung führen können. Es ist also notwendig, dass der einzelstaatliche Gesetzgeber eine Absicherung der Zwecksetzungen vornimmt, die ein Medien- und Wissenschaftsprivileg für wahllos ins Internet gestellte Daten ausschließt". Zu den verbleibenden Abgrenzungsschwierigkeiten zwischen KUG und DS-GVO selbst dann, wenn die Datenverarbeitung eindeutig zu journalistischen Zwecken erfolgt: *Lauber-Rönsberg*, ZUM-RD 2018, 550 (551); *Benedikt/Kranig*, ZD 2019, 4; *Jangl*, ZUM 2021, 103 (105 ff.). Ohne auf die Abgrenzung zwischen KUG und DS-GVO einzugehen und die Voraussetzungen (wohl) kumulierend: *OLG Düsseldorf*, Beschl. v. 20.07.2021, 1 UF 74/21 = ZD 2021, 650 (Rn. 12/13).

[157] So für den Fall eines „opportunistischen" Widerrufs der Einwilligung: *Buchner*, Die informationelle Selbstbestimmung im Privatrecht 2006, 270 f.; *Langhanke/Schmidt-Kessel*, EuCML 2015, 218 (221); *Hacker*, Datenprivatrecht, 2020, S. 278.

[158] So: *Bunnenberg*, Privates Datenschutzrecht, 2020, S. 265 f.

[159] Zu den konkreten Gestaltungsmöglichkeiten unten: Kapitel 5 C.III.

[160] ErwG. 153 S. 7 DS-GVO.

bei Verabschiedung der DS-GVO übersehen hat.[161] Nicht nur bekannte Schauspieler, Leistungssportler und Politiker lizensieren seit Jahrzehnten die vermögenswerten Bestandteile ihrer Persönlichkeitsrechte, insbesondere ihres Namensrechts (§ 12 BGB) und ihres Rechts am eigenen Bild (§§ 22 f. KUG).[162] Gerade jenseits eines äußerungsrechtlichen Zusammenhangs werden die Popularität und ein damit verbundenes Image wirtschaftlich verwertet, indem die Nutzung von Abbildungen, des Namens und sonstiger Merkmale der Persönlichkeit Dritten für deren Produktwerbung gegen Zahlung eines Honorars oder Gewährung eines anderen (geldwerten) Vorteils gestattet wird (sog. Merchandising-Verträge).

Wie der *BGH* für Prominente zutreffend festgestellt hat, führt eine unerlaubte Verwertung von Persönlichkeitsmerkmalen für Werbezwecke weniger zur Beeinträchtigung von ideellen, sondern primär zur Verletzung von kommerziellen Interessen.[163] Im Zentrum stehen nicht Ehre, Ansehen und Menschenwürde, sondern das Interesse daran, ein Image aufzubauen und durch dessen Verwertung (zusätzliches) Einkommen zu erzielen.[164] Geschützt ist die freie Entscheidung darüber, ob und unter welchen Voraussetzungen solche Persönlichkeitsmerkmale von Verantwortlichen genutzt werden können, um unternehmerische Interessen zu verfolgen.[165]

Allerdings können nicht nur bereits berühmte Personen, sondern auch bislang unbekannte Personen ihre Persönlichkeit kurzzeitig oder dauerhaft als Stimme und Gesicht für Produkte oder Unternehmen zur Verfügung stellen und womöglich erst dadurch eine gewisse – auch anderweitig – verwertbare Bekanntheit erlangen.

Ob und inwieweit die bisherigen Einwilligungen (§ 22 Abs. 1 KUG, § 823 Abs. 1 BGB i. V. m. Art. 2 Abs. 1, Art. 1 Abs. 1 GG) und Befugnisse (§ 12 BGB) zur Verwertung von vermögenswerten Bestandteilen des Persönlichkeitsrechts seit Anwendbarkeit der DS-GVO noch Bestand haben und welche Ergänzung sie jedenfalls deshalb benötigen, weil mit den Verwertungshandlungen jeweils datenschutzrechtlich relevante Verarbeitungen einhergehen, ist noch weitgehend offen. Die Antwort hierauf ist weder trivial noch von lediglich theoretischem Interesse. Allerdings machen diese Beispiele nochmals deutlich, dass nur eine Lösung in Betracht kommt, die im Ausgangspunkt auf eine dezentrale Ent-

---

[161] Dies ebenfalls übersehend: *Marsch*, Das Europäische Datenschutzgrundrecht, 2018, S. 364 ff.

[162] Im US-Recht hilft in diesen Fällen, das neben dem „right to privacy" ebenfalls gewährleistete „right to publicity". Hierzu mit einem Vergleich zum europäischen Modell: *Whitman*, (2004) 113 Yale Law Journal, 1151 (http://www.yalelawjournal.org/article/the-two-western-cultures-of-privacy-dignity-versus-liberty, zuletzt abgerufen am 19.05.2022).

[163] *BGH*, Urt. v. 01.12.1999, I ZR 49/97 = GRUR 2010, 709 (712) – *Marlene Dietrich*.

[164] Grundlegend: *Götting*, Persönlichkeitsrechte als Vermögensrechte, 1995, S. 266.

[165] *BGH*, Urt. 08.05.1956, I ZR 62/54 = GRUR 1956, 427 – *Paul Dahlke*; BGHZ 81, 75, 80 = NJW 1981, 2402 – *Carrera*.

scheidung der Datensubjekte setzt. Die alternativen Lösungsvorschläge, die auf eine komplexe Interessenabwägung in jedem Einzelfall und eine anschließende Anwendung von Art. 6 Abs. 1 lit. b DS-GVO (*Jan Niklas Bunnenberg*)[166] oder von Art. 6 Abs. 1 lit. f DS-GVO (*Benedikt Buchner* und *Philipp Hacker*) setzen,[167] verursachen enorme Transaktionskosten und münden dennoch in großer Rechtsunsicherheit.

Deshalb ist es nach hier vertretener Auffassung überzeugend und mit Blick auf die Wahrung der unternehmerischen Freiheit (Art. 16 GRCh) und Vertragsfreiheit (Art. 6 Abs. 3 EUV) auch notwendig, die *generelle* Widerruflichkeit der Einwilligung teleologisch zu reduzieren,[168] so dass der Widerruf zumindest vorübergehend ausgeschlossen werden kann.[169]

III. Fazit

Eine konsequente Einbeziehung üblicher Datenverarbeitungen offenbart ein Spannungsverhältnis zwischen dem Schutz von Datensubjekten vor der Verarbeitung von personenbezogenen Daten (Art. 8 Abs. 1 GRCh) und dem Schutz der Privatsphäre (Art. 7 GRCh) einerseits und der Gewährleistung der unternehmerischen Freiheit und der Vertragsfreiheit der Verantwortlichen und des Datensubjekts andererseits (Art. 16 GRCh bzw. Art. 6 Abs. 3 EUV). Der tatsächlichen und rechtlichen Komplexität dieses Spannungsverhältnisses hat der europäische Gesetzgeber bei Verabschiedung der DS-GVO nicht ausreichend Rechnung getragen. Infolgedessen wurden unionsgrundrechtlich zu gewährleistende Positionen nur unzureichend berücksichtigt.

Symptomatisch für die fehlende privatrechtliche Sensibilität der DS-GVO ist die Formulierung der Ziele in Art. 1 DS-GVO. Diese Definition macht dabei zugleich das ganze Dilemma einer solchen, auf die Regelungsziele ausgerichteten Auslegung von Art. 7 Abs. 4 bzw. der teleologischen Reduktion von Art. 7 Abs. 3 S. 1 DS-GVO deutlich:

---

[166] Für eine abstrakte Vorab-Abwägung zwischen Verbindlichkeitsinteresse des Verantwortlichen (dann Art. 6 Abs. 1 lit. b DS-GVO) und Widerrufsinteresse des Datensubjekts (dann Art. 6 Abs. 1 lit. a DS-GVO und freie Widerruflichkeit): *Bunnenberg*, Privates Datenschutzrecht, 2020, S. 265 f./285.

[167] Für eine Anwendung von Art. 6 Abs. 1 lit. f DS-GVO zugunsten des Verantwortlichen bei „opportunistischem" Widerruf der Einwilligung: *Buchner*, Die informationelle Selbstbestimmung im Privatrecht, 2006, S. 272 ff.; sowie: *Hacker*, Datenprivatrecht, 2020, S. 278. Wobei diese Möglichkeit sehr begrenzt wäre, weil sie für besonders sensible Daten (Art. 9 Abs. 1 DS-GVO) nicht in Betracht kommt.

[168] Zu dieser Möglichkeit und den Voraussetzungen einer teleologischen Reduktion von Art. 7 Abs. 3 DS-GVO bereits: *Sattler*, JZ 2017, 1036 (1043 ff.).

[169] Hierzu unten Kapitel 5 C.III.3.

Während Art. 1 Abs. 1 DS-GVO den Schutz personenbezogener Daten betont, hebt Abs. 2 die binnenmarktintegrale Zwecksetzung hervor. Die DS-GVO ist mit Blick auf ihre Ziele indifferent, sofern man keine Vorrangregelung allein aus der Chronologie ableitet, in der diese Ziele in der Verordnung genannt werden. Auch der Blick in die Erwägungsgründe mit ihrer begrenzten Bedeutung für die (teleologische) Auslegung,[170] neigt die Waage zu keiner Seite. Während ErwG 1 DS-GVO den Schutz natürlicher Personen herauszustellen scheint, fügt ErwG 2 DS-GVO die Grundfreiheiten und die Binnenmarktintegration ein. Sofern die Gewährleistung des freien Verkehrs personenbezogener Daten zwischen den Mitgliedstaaten (ErwG 2 DS-GVO) nicht nur als Feigenblatt zur Begründung der Gesetzgebungskompetenz dienen soll, muss die DS-GVO in einer Weise ausgelegt werden, die einen innereuropäischen Datenverkehr ermöglicht, um so zum

„wirtschaftlichen und sozialen Fortschritt, zur Stärkung und zum Zusammenwachsen der Volkswirtschaften innerhalb des Binnenmarkts sowie zu Wohlergehen natürlicher Personen beizutragen".[171]

Dass dabei ein hohes Schutzniveau[172] erreicht werden soll, darf jedoch nicht dazu führen, das Ziel des wirtschaftlichen Fortschritts auszublenden. Der Schutz natürlicher Personen und die Binnenmarktintegration werden in der DS-GVO regelmäßig zusammen – gleichsam als siamesischer Zwilling des europäischen Datenschutzrechts – angeführt.[173]

Als Ausgangspunkt für eine unionsgrundrechtskonforme Auslegung kann – neben ErwG 1 und 2 DS-GVO und dem janusköpfigen Art. 1 DS-GVO – insbesondere ErwG 4 S. 2 DS-GVO dienen. Hiernach wird der Schutz der Datensubjekte vor einer Verarbeitung von personenbezogenen Daten nicht uneingeschränkt gewährt. Vielmehr muss er

„im Hinblick auf seine gesellschaftliche Funktion gesehen und unter Wahrung des Verhältnismäßigkeitsprinzips gegen andere Grundrechte abgewogen werden."

Zu diesen Grundrechten zählt ErwG 4 S. 3 DS-GVO insbesondere die Informationsfreiheit (Art. 11 Abs. 1 S. 2 Var. 2 GRCh) und die unternehmerische Freiheit (Art. 16 GRCh). Im Ergebnis ist die Einwilligung diejenige Option, die dem Datensubjekt die Entscheidungszuständigkeit über die Verarbeitung von personenbezogenen Daten *ex ante* eindeutig zuweist und damit der vorrangige Anknüpfungspunkt um diesen Ausgleich herzustellen.

---

[170] *Riesenhuber*, in: *ders.* (Hrsg.), Europäische Methodenlehre, 4. Aufl. 2021, S. 306, Rn. 38; *Köndgen/Mörsdorf*, ebda., S. 170 f., Rn. 75–78.

[171] ErwG 2 DS-GVO.

[172] ErwG 6 DS-GVO.

[173] Vgl. ErwG 3, 4, 5, 166 und 170 („Gewährleistung eines gleichwertige Datenschutzniveaus für natürliche Personen und des freien Verkehrs personenbezogener Daten").

Eine weite Anwendung von Art. 6 Abs. 1 lit. b DS-GVO führt zu einer Flucht aus den unionsweit einheitlichen und strengeren Anforderungen an die datenschutzrechtliche Einwilligung.[174] Deshalb ist es vorzugswürdig, der Einwilligung einen Vorrang einzuräumen, so dass sie die Funktion als zentrales Instrument zur unionsweit einheitlichen Gewährleistung von informationeller Privatautonomie verwirklichen kann.

C. Stufenleiter der Einwilligung

Überraschenderweise hat selbst die privatrechtliche Literatur Schwierigkeiten damit, die Einwilligung als Bestandteil einer schuldrechtlichen Vereinbarung einzuordnen. Aufgrund der sog. freien Widerruflichkeit in Art. 7 Abs. 3 S. 1 DS-GVO wird die datenschutzrechtliche Einwilligung regelmäßig mit der schlichten, einseitigen Einwilligung gleichgesetzt (I).

Im Anschluss an die von *Ansgar Ohly* für das deutsche Privatrecht herausgearbeitete Stufenleiter der Gestattungen reicht der Begriff der Einwilligung jedoch von der schlichten, jederzeit widerruflichen Einwilligung im engeren Sinn bis hin zur translativen Übertragung. Nach deutschem Vorverständnis stehen für den – hiervon zu trennenden unionsautonomen – Einwilligungsbegriff der DS-GVO zumindest die ersten beiden Stufen in Form der schlichten, einseitigen Einwilligung und der schuldrechtlichen, zeitweise unwiderruflichen Einwilligung zur Verfügung (II).[175]

Abschließend wird herausgearbeitet, warum auch die zeitweise unwiderrufliche Einwilligung zwar regelmäßig Bestandteil eines Vertrags ist, aber dennoch eine Einwilligung i. S. d. Art. 6 Abs. 1 lit. a DS-GVO bleibt (III).

I. Die Grenzen der schlichten, einseitigen Einwilligung

Sofern man der derzeitigen h. A. folgt, lässt der datenschutzrechtliche Einwilligungstatbestand lediglich eine schlichte, einseitige und gemäß Art. 7 Abs. 3 S. 1 DS-GVO generell und jederzeit widerrufliche Einwilligung des Datensubjekts zu.[176] Die Einwilligung entfaltet keinerlei Bindungswirkung und es liegt aus

---

[174] Hierzu oben: Kapitel 3 C.II.2.

[175] Für das deutsche BDSG – vor Anwendbarkeit der DS-GVO – ging *Buchner* davon aus, dass als dritte Stufe auch eine konstitutive Rechtseinräumung am „Recht am eigenen Datum" möglich sei: *ders.* Die informationelle Selbstbestimmung im Privatrecht, 2006, S. 276 ff.

[176] *Langhanke/Schmidt-Kessel,* EuCML 2015, 218 (221); *Metzger,* AcP 216 (2016), 817 (825); *Specht*, JZ 2017, 763, (765); *Langhanke*, Daten als Leistung, 2018, S. 118; *Bunnenberg*, Privates Datenschutzrecht, 2020, S. 37 ff.; *M. Wagner*, Datenökonomie und Selbstdatenschutz, 2020, S. 345.

Sicht eines Verantwortlichen nahe, sein Geschäftsmodell technisch so auszugestalten, dass die Datensubjekte mit den personenbezogenen Daten in Vorleistung gehen müssen.[177] Wie eine solche datenschutzrechtliche Widerruflichkeit dogmatisch ins Schuldrecht eingeordnet werden kann, ist bislang völlig offen.

Gegen die Qualifikation als Naturalobligation[178] spricht deren Ausnahmecharakter. Die Naturalobligation ist regelmäßig eine Konsequenz, wenn der Gesetzgeber den Abschluss bestimmter Rechtsgeschäfte verhindern[179] oder staatlich regulieren will,[180] weil er sie – wie Heiratsvermittlung oder Spiel und Wette – grundsätzlich missbilligt.[181] Der Widerruf des Datensubjekts als eine selbstbestimmte *Gestaltungserklärung* passt nicht in diese Kategorie.[182]

Als weitere Möglichkeit kommt eine Interpretation der Leistung von personenbezogenen Daten als bloßer Realakt in Betracht.[183] Hiermit kompatibel wäre die Einordnung des Widerrufs der datenschutzrechtlichen Einwilligung als auflösende Bedingung für die Inanspruchnahme der Leistungen des Verantwortlichen.[184] Diese dogmatische Einordnung ist mit Blick auf Art. 7 Abs. 3 S. 1 DS-GVO überzeugend, wenngleich sie im Einzelfall einer Korrektur bedarf,[185] insbesondere sofern der Bedingungseintritt durch einen „opportunistischen Widerruf" herbeigeführt wird.[186] Die Einordnung als Realakt hat aber zugleich zur Folge, dass keine stabilen Leistungsbeziehungen entstehen, was diesem Ansatz zurecht den Vergleich mit der „schuldrechtlichen Steinzeit"[187] eingebracht hat.

---

[177] Hierzu bereits oben: A.5.

[178] *Langhanke/Schmidt*-Kessel, EuCML 2015, 218 (221).

[179] Vgl. § 762 Abs. 1 BGB und § 656 Abs. 1 BGB.

[180] Zulässigkeit staatlich genehmigter Lotterie und Ausspielung: § 763 Satz 1 BGB.

[181] *Habersack*, in: MüKo, BGB, 8. Aufl. 2020, § 762, Rn. 1 ff.; *Roth*, in: MüKo, BGB, 8. Aufl. 2020, § 656, Rn. 1 f.

[182] Hierzu bereits *Sattler*, JZ 2017, 1036 (1040).

[183] *Riehm*, in: Pertot (Hrsg.), Rechte an Daten, 2020, S. 175 (195 f.).

[184] So *Rafał Mańko*, Contracts for the supply of digital content and digital services, Bericht des Wissenschaftlichen Dienstes des EU-Parlaments (EPRS) vom 27.11.2017, S. 8 („The report deletes the term *counter-performance*, criticized by the EDPS, and replaces it with the term *condition*"), verfügbar unter http://www.europarl.europa.eu/RegData/etudes/BRIE/2018/614707/EPRS_BRI%282018%29614707_EN.pdf, zuletzt abgerufen am 19.05.2022; Allerdings wird dieser Ansatz nicht vertieft. Ebenso: *EDSA*, Leitlinien 05/2020 zur Einwilligung gemäß Verordnung 2016/679, Version 1.1, v. 04.05.2020, Nr. 37; *Hacker*, ZfPW 2019, 148 (172 ff.); *ders.*, Datenprivatrecht, 2020, S. 228 f.; ähnlich: *Riehm*, in: Pertot (Hrsg.), Rechte an Daten, 2020, S. 194 f.

[185] So für den Fall einer Einordnung als Naturalobligation: *Langhanke/Schmidt-Kessel*, EuCML 2015, 218 (221: „justified breach"). Zu den Grenzen der Widerruflichkeit zudem: *Kilian*, in: Gedächtnisschrift für Steinmüller, 2014, S. 195 (212); *ders.*, CRi 2002, 169 ff. ssq.; *Klement*, in: Simitis/Hornung/Spiecker gen. Döhmann (Hrsg.), Datenschutzrecht, 2019, Art. 7, Rn. 92.

[186] *Hacker*, Datenprivatrecht, 2020, S. 278. In diese Richtung auch bereits: *Buchner*, Die informationelle Selbstbestimmung im Privatrecht, 2006, S. 272 ff.

[187] So *Martin Schmidt-Kessel* in der Diskussion anlässlich des Workshops über Rechte an Daten, 22.02.2019, Universität Bayreuth.

Es wird zunehmend offenkundig, dass eine Beschränkung des datenschutzrechtlichen Einwilligungstatbestand auf die schlichte, einseitige Einwilligung zwar das Reue-Recht aller Datensubjekte „makellos" bewahrt, dabei aber zu den bereits absehbaren und teilweise auch befürworteten Ausweichbewegungen führt. Die „Flucht aus der Einwilligung" in das nationale Schuldrecht (Art. 6 Abs. 1 lit. b DS-GVO)[188] und in die unbestimmte Generalklausel (Art. 6 Abs. 1 lit. f DS-GVO) wird beschleunigt. Damit geht eine unionsweite Rechtsunsicherheit und infolgedessen eine Gefährdung der Ziele aus Art. 1 DS-GVO einher.[189]

Zudem verstößt eine zwingende freie Widerruflichkeit der Einwilligung – jedenfalls im B2B-Verhältnis – gegen das Übermaßverbot und verletzt die unternehmerische (Vertrags-)Freiheit aus Art. 16 GRCh.[190] Somit stellt sich die Frage, ob der datenschutzrechtliche Begriff der Einwilligung auf die schlichte, einseitige und frei widerrufliche Einwilligung begrenzt ist oder infolge einer unionsgrundrechtskonformen teleologischen Reduktion von Art. 7 Abs. 3 S. 1 DS-GVO auch für eine (zeitweise) unwiderrufliche Einwilligung offensteht.

II. Die Einwilligung in der Stufenleiter der Gestattungen

Weil die datenschutzrechtliche Einwilligung unionsrechtsautonom auszulegen ist, kann die deutsche Dogmatik zur Einwilligung lediglich als ein möglicher Anhaltspunkt dienen. Dennoch kann die deutsche Forschung zur allgemeinen Einwilligung[191] und zur ehemals nur harmonisierten datenschutzrechtlichen Einwilligung[192] hilfreich sein, um den abstrakten Begriff der Einwilligung zu konkretisieren und dabei zugleich aufzuzeigen, welche Varianten von Einwilligungen grundsätzlich möglich und im Lichte der Vorgaben der DS-GVO sinnvoll sind.

Die Letztentscheidung darüber, welche dieser nach deutschem Vorverständnis bestehenden Varianten für die unionsautonom zu bestimmende Einwilligung der DS-GVO zur Verfügung stehen, liegt jedenfalls dann beim *EuGH*, sofern man mit hier vertretener Ansicht der Auffassung ist, dass die jederzeitige Widerruflichkeit der Einwilligung gemäß Art. 7 Abs. 3 S. 1 DS-GVO im Einzelfall dispositiv ist,[193] so dass die Art. 4 Nr. 11, Art. 6 Abs. 1 lit. a und Art. 7 ff.

---

[188] Sofern im Rahmen einer – tatbestandlich nicht näher verorteten – Interessenabwägung, das Interesse an einer Bindungswirkung überwiegt, soll nach *Bunnenberg* der Erlaubnistatbestand des Art. 6 Abs. 1 lit. b DS-VO Anwendung finden: *ders.*, Privates Datenschutzrecht, 2020, S. 264 f.

[189] Oben Kapitel 2 C.II. und III. und Kapitel 3 C.II.2 und 5.

[190] Oben B.II.2.

[191] Grundlegend: *Ohly*, Volenti non fit iniuria, 2002, S. 147 ff.

[192] *Buchner*, Die informationelle Selbstbestimmung im Privatecht, 2006, S. 231 ff.

[193] Zu den Voraussetzungen und Grenzen einer solchen Disposition unten Kapitel 5 C.III.3.

DS-GVO nur die Mindestvoraussetzungen an eine schlichte, einseitige und frei widerrufliche Einwilligung etablieren.[194]

Es ist wahrscheinlich, dass der *EuGH* seine Auslegung nicht anhand abstrakter Betrachtungen über die Rechtsnatur der Einwilligung vornehmen wird,[195] sondern anhand der für die Richter unmittelbar und konkret vorhersehbaren Konsequenzen für die Datensubjekte,[196] für die Verantwortlichen und für den freien Verkehr von personenbezogenen Daten im europäischen Binnenmarkt. Um zu verhindern, dass dem *EuGH* – ebenso wie dem europäischen Gesetzgeber – die Reichweite einer undifferenzierten Anwendung der DS-GVO entgeht, beispielsweise indem der Begriff des Datensubjekts („Betroffener") vorschnell oder unbewusst mit dem Begriff des Verbrauchers gleichgesetzt wird, ist es wichtig, diese Konsequenzen frühzeitig und deutlich in Vorlageverfahren aufzuzeigen.[197]

Ausgangspunkt hierfür ist die von *Ansgar Ohly* für das deutsche Privatrecht herausgearbeitete Stufenleiter der Gestattungen und deren anschließende teilweise Übertragung auf die datenschutzrechtliche Einwilligung. In diesem Abschnitt werden zunächst die beiden möglichen Stufen der Einwilligung aufgezeigt, bevor deren konkrete rechtliche Umsetzung anhand der DS-GVO im nächsten Kapitel im Detail herausgearbeitet wird.

Der Abgleich mit der deutschen Dogmatik zur Einwilligung im Privatrecht führt zu einer doppelten Erkenntnis. *Erstens* stehen im Kontext der DS-GVO nicht alle Ebenen der Stufenleiter der Gestattungen zur Verfügung (1). *Zweitens* bietet die vorübergehend unwiderrufliche Einwilligung in Form der schuldrechtlichen Gestattung eine Variante der Einwilligung, mit deren Hilfe sich die Rechtsbeziehung zwischen Verantwortlichem und Datensubjekt stabilisieren lässt, ohne dass damit ein empfindlicher oder sogar irreversibler Kontrollverlust des Datensubjekts einhergeht. (2)

1. Schlichte Einwilligung und schuldrechtliche Gestattung

Der im deutschen Privatrecht amorphe Begriff der Einwilligung kann mit *Ansgar Ohly* als eine Stufenleiter der Gestattungen präzisiert und systematisiert werden. Maßgebliches Kriterium für die Abgrenzung der einzelnen Stufen der

---

[194] So bereits: *Sattler*, JZ 2017, 1036 (1043).

[195] Gegen solche abstrakte Herangehensweise für das deutsche Recht bereits: *Kohte*, AcP 185 (1985), 105 (120).

[196] Insoweit verengt *Bunnenberg* die Perspektive zu stark, indem er die unternehmerisch handelnden Datensubjekte in seiner Untersuchung weitgehend ausblendet: *ders.*, Privates Datenschutzrecht, 2020, S. 240 ff.

[197] Beispielsweise macht der Vorlagebeschluss des *OLG Düsseldorf* diejenigen Konsequenzen nur indirekt und damit unzureichend deutlich, die sich ergeben, sofern der *EuGH* die in Vorlagefrage 2a angeführten Daten als besonders sensible i. S. d. Art. 9 Abs. 1 DS-GVO einordnet. *OLG Düsseldorf*, Vorlagebeschl. v. 24.03.2021, Kart 2/19 (V) = GRUR-RS 2021 8370.

Gestattungen ist die jeweils unterschiedliche Intensität der rechtlichen Bindung[198] und infolgedessen das Ausmaß der Rechtssicherheit mit der sie dem Einwilligungsempfänger ein künftiges Verhalten erlaubt. Lässt man die mit Blick auf die Rechtsfolgen verwandten Rechtsfiguren außen vor,[199] die nicht auf dem Willen des Subjekts, sondern allenfalls auf einer Interpretation seines Verhaltens beruhen, so bleiben im Ergebnis vier Stufen[200] der Gestattung:

Auf der untersten Stufe steht die widerrufliche, einseitige Einwilligung. Sie führt zwar zur Rechtmäßigkeit der gestatteten Handlung, etabliert aber keine Rechtsposition, die vom Willen des Einwilligenden – und sei es nur zeitweise – unabhängig ist. Aus Sicht des Handelnden ist seine Position prekär, weil er keinen durchsetzbaren Anspruch erhält. Infolgedessen ist die widerrufliche, einseitige Einwilligung für wirtschaftlich bedeutende Dispositionen untauglich.[201]

Auf der nächsten Stufe steht die schuldvertragliche Gestattung. Diese ist ein schuldrechtlicher Vertrag mit dem der Gestattende seinem Vertragspartner ein tatsächliches Verhalten erlaubt, das er dem Gestattungsempfänger anderenfalls stets verbieten könnte.[202] Somit vermittelt die schuldvertragliche Gestattung dem Gestattungsempfänger eine vom Willen des Gestattenden unabhängige, obligatorische Rechtsposition, die ihm (vorübergehend) Eingriffe in die Rechte des Gestattenden erlaubt,[203] also auch dann, wenn der Gestattende diesen Eingriff nach aktuellem Willen nicht mehr erlauben würde.

Wiederum eine Stufe höher liegt die Gestattung in Form einer konstitutiven Rechtsübertragung. Sie ermöglicht die Einräumung von gegenständlichen Rechten, deren Ausübung durch den Gestattungsempfänger bleibt jedoch (teilweise) an den Willen des Gestattenden gebunden. Typischerweise vermittelt die konstitutive Rechtsübertragung dem Gestattungsempfänger eine gesicherte Rechtsposition an den vermögenswerten Bestandteilen von Persönlichkeitsrechten.[204]

---

198 *Ohly*, Volenti non fit iniuria, 2002, S. 144.

199 Hierunter fallen die berechtigte GoA, die mutmaßliche Einwilligung, das Handeln auf eigene Gefahr und die Verwirkung und Duldung: *Ohly*, Volenti non fit iniuria, 2002, S. 147.

200 Die potenziell fünfte Stufe der unwiderruflichen Einwilligung lässt sich zwar – insbesondere im Verhältnis zu einem unbestimmten Personenkreis – rechtlich konstruieren, regelmäßig können die hierfür in Betracht kommenden Anwendungsfälle jedoch als schuldvertragliche Gestattung oder als Verzicht qualifiziert werden: Hierzu: *Ohly*, Volenti non fit iniuria, 2002, S. 176.

201 *Ohly*, Volenti non fit iniuria, 2002, S. 176 f.

202 *Ohly*, Volenti non fit iniuria, 2002, S. 165 f.

203 Zur (schwierigen) Abgrenzung zwischen schuldvertraglicher Gestattung und der Einräumung eines gegenständlichen Rechts infolge einer zunehmenden Verdinglichung obligatorischer Rechtspositionen (wohl) als Ausweichbewegung vor dem sachenrechtlichen *numerus clausus*: m. w. N. *Ohly*, Volenti non fit iniuria, 2002, S. 166/169.

204 Zu dieser Unterscheidung *BGH*, Urt. v. 01.12.1999, I ZR 49/97 = GRUR 2010, 709 (712) – *Marlene Dietrich*. Mit Kritik an der Kommerzialisierung von Persönlichkeitsrechten: *Schack*, JZ 2000, 1060 (1062); *Peifer*, Individualität im Zivilrecht, 2001, S. 315 ff./325 ff.

Somit ermöglicht die konstitutive (gebundene)[205] Rechtsübertragung bzw. Rechtseinräumung[206] insbesondere eine ökonomische Verwertung von Urheberrechten (§§ 29 ff. UrhG), des Namensrechts (§ 12 BGB),[207] des Rechts am eigenen Bild (§§ 22 f. KUG) und des allgemeinen Persönlichkeitsrechts (§ 823 Abs. 1 BGB i. V. m. Art. 2 Abs. 1, Art. 1 Abs. 1 GG). Diese Rechtseinräumung kann – insbesondere im Rahmen eines ausschließlichen Nutzungsrechts an einem Immaterialgüterrecht – mit einer eigenen Klagebefugnis des Gestattungsempfängers gegenüber Dritten, mit einem Sukzessionsschutz und einem insolvenzrechtlichen Aussonderungsrecht des Gestattungsempfängers einhergehen. Zugleich verbleiben dem Gestattenden diejenigen persönlichkeitsrechtlich geprägten Rechte, welche – wie beispielsweise diejenigen gemäß § 11 UrhG – die ideellen Interessen schützen.[208]

Auf der letzten Stufe mit der höchsten „Bindungswirkung" und damit eigentlich ein „Grenzfall" der Einwilligung ist die translative Rechtsübertragung. Mit dieser Gestattung überträgt der Gestattende (Veräußerer) das gesamte Recht rückhaltlos auf den Gestattungsempfänger (Erwerber). Letzterer kann alle aus dem Recht folgenden Befugnisse allein ausüben. Der Gestattende hat seine Rechtszuständigkeit vollständig verloren.[209]

Obwohl diese Stufenleiter der Gestattungen von *Ansgar Ohly* im Kontext der deutschen Dogmatik ausgearbeitet wurde und bereits deshalb allenfalls als ein mögliches Modell für einen europäischen „Einwilligungsbegriff" in Betracht kommt, ermöglicht die Stufenleiter einen systematischen Ansatz, der auch für das Verständnis „der" datenschutzrechtlichen Einwilligung gemäß Art. 4 Nr. 11, Art. 6 Abs. 1 lit. a und Art. 7 DS-GVO fruchtbar ist.

Jedenfalls bei einem weiten ökonomischen Verständnis von Handel, sind personenbezogene Daten tatsächlich ein immaterielles Handelsgut.[210] Dennoch scheidet eine translative Übertragung, also eine Veräußerung von personenbezogenen Daten unter vollständigem Verlust aller Befugnisse, aufgrund der persönlichkeitsrechtlichen Wurzel des Datenschutzes aus. Einstweilen bestehen an personenbezogenen Daten keine Immaterialgüterrechte im Sinne eines voll-

---

[205] Hierzu grundlegend: *Forkel*, Gebundene Rechtsübertragungen, 1977, S. 44 ff.; sowie speziell zu Persönlichkeitsrechten: *ders.*, GRUR 1988, 491 ff.

[206] Diese ist „konstitutiv", weil sie ein „Tochterrecht" beim Gestattungsempfänger entstehen lässt, das zuvor – jedenfalls bei isolierter Betrachtung – nicht vorhanden war. Das Stammrecht und die damit verbundenen Befugnisse bleiben beim Gestattenden zurück. Hierzu: *Ohly*, Volenti non fit iniuria, 2002, S. 148. Beispielhaft hierfür ist das Rückrufrecht des Urhebers aus gewandelter Überzeugung (§ 42 Abs. 1 UrhG). Infolgedessen beschreibt der Begriff der Rechtseinräumung den Sachverhalt besser als derjenige, der Rechtsübertragung.

[207] Zur Unterscheidung zwischen einem Namenspersönlichkeitsrecht und einem Namensimmaterialgüterrecht: *Klippel*, Schutz des Namens, 1988, S. 479 ff.

[208] M.w.N. *Ohly*, Volenti non fit iniuria, 2002, S. 148 ff.

[209] *Ohly*, Volenti non fit iniuria, 2002, S. 147.

[210] *Sattler*, in: Perot (Hrsg.), Rechte an Daten, 2020, S. 49 (51 ff.).

ständig übertragbaren „Rechts am eigenen Datum".[211] Während die DS-GVO maßgeblich auf einem Verbot der Datenverarbeitung (Ausschluss) beruht, fehlt ihr – trotz des Anspruchs auf Schadensersatz gemäß Art. 82 Abs. 1 DS-GVO – eine eindeutige Zuweisung von personenbezogenen Daten im Sinne eines absoluten Rechts. Im Unterschied zu den gesetzlichen Erlaubnistatbeständen kommt gerade die Möglichkeit zur Einwilligung einer solchen Zuweisung am nächsten, indem sie eine Rechtszuständigkeit des Datensubjekts begründet. Dennoch ist diese Einwilligung lediglich einer von mehreren Erlaubnistatbeständen und im Ausgangspunkt jederzeit frei widerruflich. Auch die stets verbleibenden Rechte auf Auskunft, Portabilität und Berichtigung sprechen dafür, dass eine echte Übertragung eines gegenständlichen Rechts an personenbezogenen Daten ausgeschlossen ist.

Die konstitutive (gebundene) Rechtseinräumung ist für die vermögenswerten Bestandteile von Persönlichkeitsrechten grundsätzlich anerkannt und hat nach Ansicht von *Ohly* gegenüber der „Verlegenheitslösung" einer bloßen Anreicherung der Einwilligung durch Elemente des Lizenzvertrags[212] den Vorteil einer größeren Einfachheit und Klarheit.[213] Dennoch bleibt zu beachten, dass bereits für das deutsche Recht „jeweils im Einzelfall zu prüfen ist, ob das betreffende Persönlichkeitsinteresse der gebundenen Übertragung zugänglich ist".[214]

Während der Begriff „der" Einwilligung auch im Unionsrecht keine klare dogmatisch Struktur hat, so dass der Wortlaut nicht gegen ein Verständnis spricht, das dem der konstitutiven Rechtseinräumung entspricht, liefert die grundsätzliche Widerruflichkeit der datenschutzrechtlichen Einwilligung (Art. 7 Abs. 3 S. 1 DS-GVO) ein Argument gegen ein solches Verständnis.[215] Zwar vermeidet der europäische Gesetzgeber eine klare Positionierung gegenüber einer Kommerzialisierung von personenbezogenen Daten. Allerdings fehlt es bislang an der Möglichkeit eines Einwilligungsempfängers, die hieraus erlangte Befugnis zur rechtmäßigen Datenverarbeitung i. S. der §§ 413, 398 BGB

---

[211] Hierzu: *Sattler*, in: Bakhoum u. a. (Hrsg.), Personal Data in Competition, Consumer Protection and Intellectual Property Law – Towards a Holistic Approach?, 2018, S. 27 (39 ff.). Mit dem Hinweis auf Art. 567 des Code de Commerce von Luxemburg, der eine Herausgabeanspruch auf die Daten im Fall der Insolvenz des Verantwortlichen kodifiziert: *Jülicher*, ZIP 2015, 2063 (2066); ausführlich für das schweizerische Recht: *Schmidt*, Daten als Vermögensrecht, 2020.

[212] *Ohly*, Volenti non fit iniuria, 2002, S. 160.

[213] Zu den wichtigsten Einwänden gegen eine Anerkennung von konstitutiven Rechtseinräumungen an Persönlichkeitsrechten und zu deren Ablehnung: *Ohly*, Volenti non fit iniuria, 2002, S. 162 ff.

[214] *Ohly*, Volenti non fit iniuria, 2002, S. 164.

[215] M.w.N. *Sattler*, in: Bakhoum u. a. (Hrsg.), Personal Data in Competition, Consumer Protection and Intellectual Property Law – Towards a Holistic Approach?, 2018, S. 27 (39 ff.); a. A. für das BDSG a. F. und somit für eine konstitutive Rechtseinräumung „insbesondere" gegenüber Datentreuhändern: *Buchner*, Die informationelle Selbstbestimmung im Privatrecht, 2006, S. 285 ff./314.

(analog) zu übertragen. Jeder Verantwortliche benötigt eine eigene originäre Einwilligung des Datensubjekts. Zudem mündet eine Datenverarbeitung regelmäßig nicht in Verwertungsformen, die für das Datensubjekt wahrnehmbar sind. Dies unterscheidet die Verwertung von personenbezogenen Daten – trotz der datenschutzrechtlichen Informations- und Auskunftspflichten – grundsätzlich von typischen Verwertungen des Urheberrechts oder des Rechts am eigenen Bild. In diesen Fällen lässt sich die höhere Bindungswirkung einer Gestattung in Form einer konstitutiven Rechtseinräumung gerade mit der größeren Wahrnehmbarkeit der Verwertungshandlungen des Gestattungsempfängers durch den Gestattenden rechtfertigen. Die konkrete Verarbeitung von personenbezogenen Daten bleibt dagegen zumeist virtuell, deshalb verborgen und mündet selten in eine wahrnehmbare Vervielfältigung oder Veröffentlichung.

Die EU-Mitgliedstaaten können gemäß Art. 80 Abs. 1 DS-GVO („Vertretung der betroffenen Person") vorsehen, dass ein Datensubjekt bestimmte Institutionen damit beauftragen kann, in seinem Namen Beschwerden einzureichen und Rechte, einschließlich des Rechts auf Schadensersatz, geltend zu machen. Somit sieht die DS-GVO die *Option* einer gewillkürten Prozessstandschaft unter sehr strengen Anforderungen[216] an den Prozessstandschafter vor. Dass die DS-GVO eine gewillkürte Prozessstandschaft lediglich ermöglicht, spricht dagegen, eine eigenständige Klagebefugnis des Verantwortlichen und Gestattungsempfängers gegenüber Dritten anzunehmen.

Zudem macht Art. 80 Abs. 2 DS-GVO deutlich, dass es dem europäischen Gesetzgeber mit Art. 80 DS-GVO nicht um die Möglichkeit einer Erleichterung der Verwertung von personenbezogenen Daten ging, sondern darum, ein (mutmaßliches) Defizit bei der Durchsetzung der datenschutzrechtlichen Regelungen zu beseitigen. Gemäß Art. 80 Abs. 2 DS-GVO können die Mitgliedstaaten sogar vorsehen, dass jede Institution, welche die Anforderungen an einen Prozessstandschafter erfüllt, auch

> „unabhängig von einem Auftrag der betroffenen Person in diesem Mitgliedstaat das Recht hat, […] eine Beschwerde einzulegen und die in den Artikeln 78 und 79 aufgeführten Rechte in Anspruch zu nehmen, wenn ihres Erachtens die Rechte einer betroffenen Person gemäß dieser Verordnung infolge einer Verarbeitung verletzt worden sind."

Weil es dem Prozessstandschafter gerade verboten ist, aus seiner Beauftragung Gewinne zu erzielen, dient Art. 80 Abs. 1 DS-GVO vorrangig der effektiveren Durchsetzung des Datenschutzrechts und gerade nicht zur Ermöglichung einer arbeitsteiligen Verwertung von personenbezogenen Daten. Obwohl eine gewillkürte Prozessstandschaft im Vergleich zur eigenen Klagebefugnis eines Gestattungsempfängers im Rahmen einer konstitutiven Rechtseinräumung mit

---

[216] Dieser muss gemäß Art. 80 Abs. 1 DS-GVO insbesondere ohne Gewinnerzielungsabsicht sein und satzungsmäßige Ziele im öffentlichen Interesse verfolgen, die im Bereich des Schutzes der Rechte und Freiheiten von betroffenen Personen liegen.

einer „Krücke" vergleichbar sein mag,[217] sieht das europäische Datenschutzrecht bislang lediglich diese Krücke vor. Weil die DS-GVO – jedenfalls explizit – nur eine gewillkürte Prozessstandschaft als Option ermöglicht und keine originäre Klagebefugnis eines Einwilligungsempfängers vorsieht, spricht dies dafür, dass die typischerweise mit einer konstitutiven (gebundenen) Rechtseinräumung einhergehende Intensität der Bindungswirkung – zumindest einstweilen[218] – nicht gewünscht ist. Somit sprechen die besseren Argumente dafür, dass eine translative und eine konstitutive Rechtsübertragung für personenbezogene Daten *de lege lata* ausscheidet.

Infolgedessen bleibt neben der schlichten, einseitigen und jederzeit widerruflichen Einwilligung die Stufe der schuldvertraglichen Gestattung, sofern ein Mindestmaß an rechtlicher Bindungswirkung möglich sein soll. Diese schuldvertragliche Gestattung liegt auf der Stufenleiter der Gestattung unterhalb einer (gegenständlichen) Rechtseinräumung, aber oberhalb der schlichten, einseitigen Einwilligung.[219] Auf Grundlage einer schuldvertraglichen Gestattung könnte die Bereitstellung personenbezogener Daten durch das Datensubjekt als vertraglicher Leistungsgegenstand vereinbart werden. Dennoch blieben die persönlichkeitsrechtlichen Bindungen an das Datensubjekt erhalten und personenbezogene Daten wären insoweit mit anderen vermögenswerten Bestandteilen von Persönlichkeitsrechten vergleichbar.[220]

Gerade mit Blick auf die Funktion der Einwilligung im Kontext von Persönlichkeitsrechten – beispielsweise § 22 KUG – kommt die deutsche Literatur zu der überzeugenden Ansicht, dass nicht nur die schlichte, einseitige und jederzeit widerrufliche Einwilligung möglich ist, sondern zumindest auch eine (zeitweise) bindende schuldvertragliche Gestattung.[221] Überträgt man diesen Ansatz auf die datenschutzrechtliche Einwilligung, dann können personenbezogene Daten – ebenso wie Persönlichkeitsrechte – kommerzialisiert werden, ohne dass deshalb die unverbrüchliche Verbindung zum Datensubjekt abreißt. Diese Verbindung verhindert die gegenständliche Verfügung über personenbezogene Daten. Personenbezogene Daten entwickeln sich infolgedessen nicht zu einem vollständigen Immaterialgüterrecht.[222] Weil keine gegenständlichen Rechte an

---

[217] *Helle*, RabelsZ 60 (1996), 448 (466); *Ohly*, Volenti non fit iniuria, 2002, S. 161.

[218] Eine hiervon zu trennende Frage ist, ob diese Entscheidung dauerhaft Bestand haben kann, sofern Datentransaktionen unter Einsatz von sog. Datentreuhändern künftig rechtspolitisch erwünscht sind. Hierzu sogleich sowie: *Wendehorst/Schwamberger/Grinzinger*, in: Pertot (Hrsg.), Rechte an Daten, 2020, S. 103 ff.; *Kühling*, ZfDR 2021, 1 ff.

[219] *Ohly*, Volenti non fit iniuria, 2002, S. 169 f.

[220] Hierzu: *Beverley-Smith/Ohly/Lucas-Schloetter*, Privacy, Property and Personality 2005, S. 94 ff.; mit Rechtsvergleich zum englischen Recht: *Hofmann*, ZGE 2010, 1 ff.

[221] *Ohly*, Volenti non fit iniuria, 2002, S. 144; m. w. N. *Götting*, in: Loewenheim/Schricker, Urheberrecht, 6. Aufl. 2020, § 22 KUG, Rn. 40 f.; zur Möglichkeit einer konstitutiven (gebundenen) Rechtseinräumung: *Ohly*, Volenti non fit iniuria, 2002, S. 162 ff.

[222] Ebenso: *Zech*, JIPLP 2016, 460 (463); zum US-Recht: *Balganesh*, 160 U. Pa. L. Rev. (2012), 1889; *Samuelson*, 52 Stan. L. Rev. (1999), 1125.

personenbezogenen Daten bestehen, erhält ein Verantwortlicher als Empfänger der Gestattung weder einen gesetzlichen Sukzessionsschutz noch eine eigene Klagebefugnis gegen Dritte.

Indem Art. 4 Nr. 11, Art. 6 und Art. 7 ff. DS-GVO nach hier vertretener Ansicht nur die unionsgrundrechtlich zu gewährleistenden Mindestanforderungen an eine datenschutzrechtliche Einwilligung in Form der schlichten, einseitigen Einwilligung regeln, ist es konsequent, dass Art. 7 Abs. 3 S. 1 DS-GVO *insoweit* eine jederzeitige und voraussetzungslose Widerruflichkeit vorsieht. Somit bildet die schlichte, einseitige Einwilligung den Ausgangspunkt des unionsautonomen Begriffs der datenschutzrechtlichen Einwilligung. Sie liefert dem Verantwortlichen eine Erlaubnis zur rechtmäßigen Datenverarbeitung, verschafft ihm aber kein, auch kein lediglich vorübergehend durchsetzbares Recht gegen den (geänderten) Willen des Datensubjekts.

Die gemäß Art. 7 Abs. 3 S. 1 DS-GVO ermöglichte jederzeitige Reue für die Zukunft verhindert, dass das Datensubjekt sich selbst rechtlich bindet. Im Ergebnis erweitert die schlichte einseitige Einwilligung den Rechtskreis des Verantwortlichen *ad hoc*, ohne ihm eine gesicherte Rechtsposition zu verschaffen. Deshalb könnte sich die Bedeutung der schlichten, einseitigen Einwilligung für eine Verarbeitung von personenbezogenen Daten langfristig in dem von Art. 16 ff. DG-VO vorgesehenen Mechanismen eines Datenaltruismus erschöpfen, der ein typisches Instrument für eine gefälligkeitshalber erteilte Erlaubnis ist. Zudem dient die schlichte, einseitige Einwilligung als Auffangtatbestand, wenn eine schuldrechtliche Gestattung zwar beabsichtigt war, aber fehlgeschlagen ist.[223]

Im Unterschied zu den in der DS-GVO ausdrücklich geregelten Anforderungen an das unionsgrundrechtlich zu gewährleistende Mindestmaß der schlichten, einseitigen und jederzeit widerruflichen Einwilligung führt eine schuldrechtliche Gestattung auf die nächst höher gelegene Stufe der Einwilligungen und damit zu einer schuldrechtlichen *Stabilisierung der Rechtsbeziehung* zwischen Verantwortlichem und Datensubjekt. Infolgedessen kann die schuldrechtliche Gestattung im persönlichkeitsrechtlichen Bereich eine Rechtswahrnehmung im Auftrag des Datensubjekts (Art. 80 Abs. 1 DS-GVO) und eine wirtschaftliche Verwertung ermöglichen.[224]

Die Verwertung erfolgt durch einen zumindest zeitweisen Ausschluss der Widerruflichkeit, so dass hierdurch eine Schwelle für eine Beendigung der Da-

---

[223] Mit weiteren Funktionen der schlichten, einseitigen Einwilligung – außerhalb des datenschutzrechtlichen Kontextes: *Ohly*, Volenti non fit iniuria, 2002, S. 176.

[224] *Dasch*, Die Einwilligung zum Eingriff in das Recht am eigenen Bild, 1990, S. 359; *Helle*, AfP 1985, 94 (94/100); *Götting*, Persönlichkeitsrechte als Vermögensrechte, 1995, S. 142/279. Zur deutlich weitergehenden Kommerzialisierung von Persönlichkeitsrechten im US-Recht: *Shields* v. *Gross*, 448 N.E.2d 108, 461 N.Y.2d 254 (1983); hierzu: *McCarthy*, The Right of Publicity and Privacy, 2. Aufl. 2020, § 10.39.

tenverarbeitung für die zulässige Dauer der Bindungswirkung eingeführt wird. Diese Möglichkeit besteht jedenfalls im Verhältnis zwischen einem Verantwortlichen und einem unternehmerisch handelnden Datensubjekt, dem die Kommerzialisierung von personenbezogenen Daten und seiner sonstigen besonderen Persönlichkeitsrechte dazu dient, eine Einkommensverbesserung zu erzielen. Diese Option besteht aber – in eingeschränktem Maße[225] – auch im Verhältnis zu Verbrauchern, die durch eine solche Kommerzialisierung ihr Budget für den Konsum von – zumeist digitalen – Produkten erweitern.

Auf Grundlage der schuldrechtlichen Gestattung erhält der Verantwortliche im Rahmen des vereinbarten Verarbeitungszwecks ein vom aktuellen Willen des Datensubjekts zeitweise unabhängiges schuldrechtliches Verwertungsrecht. Im *relativen Verhältnis* zwischen Datensubjekt und Verantwortlichem ähneln die Folgen der schuldrechtlichen Gestattung somit einer Rechtseinräumung auf Zeit. Es droht dem Datensubjekt jedoch zu keiner Zeit ein Kontrollverlust, weil die schuldrechtliche Gestattung – im Gegensatz zur translativen Übertragung oder konstitutiven Einräumung von (gegenständlichen) Rechtspositionen – keinen Ansatzpunkt für einen Verkehrsschutz zugunsten (gutgläubiger) Dritter bietet.

2. Die schuldrechtliche Gestattung als Stabilisierung von Beziehungen

Man kann Datensubjekten die Möglichkeit zur wirtschaftlichen Verwertung von personenbezogenen Daten nicht versagen.[226] Dies folgt auf unionsgrundrechtlicher Ebene bereits aus Art. 8 Abs. 2 S. 1 GRCh, der (ausschließlich) die Einwilligung des Datensubjekts explizit garantiert. Ist ein Datensubjekt zudem Unternehmer, so kommt der Ausschluss einer bindenden Disposition erst recht nicht in Betracht.[227] Indem sie die höhere Intensität von rechtlicher Bindung vermeidet, wie sie mit der konstitutiven (gebundenen) Rechtsübertragung einhergeht, bietet die schuldvertragliche Gestattung einen angemessenen Ausgleich zwischen dem Schutz von personenbezogenen Daten und der Privatsphäre gemäß Art. 8 bzw. Art. 7 GRCh einerseits und der Vertragsfreiheit gemäß Art. 16 GRCh und Art. 6 Abs. 3 EUV andererseits. Insbesondere kommt es durch die Möglichkeit zur Erteilung einer Einwilligung in Form der schuldrechtlichen Gestattung nicht zu einer grenzenlosen Kommerzialisierung oder einem Kontrollverlust des Datensubjekts. Dafür sorgen bereits die Anforderungen an eine wirksame Einwilligung. Sie muss zweckbestimmt, informiert und freiwillig sein.

---

[225] Hierzu unten Kapitel 5 C.III.2.c.

[226] Im Kontext anderer Persönlichkeitsrechte tendenziell gegen eine Kommerzialisierbarkeit: *Schack*, AcP 195 (1995) 594 f.; *ders.*, JZ 2000, 1060 (1062); *Peifer*, Individualität im Zivilrecht, 2001, S. 315 ff., 325 f.; *Wandtke*, GRUR 1995, 385 (391).

[227] Oben B.II.2.

Zwar wird die Einwilligung immer wieder als „fiktiv" bezeichnet.[228] Infolge der unionsgrundrechtlichen Gewährleistung der Einwilligung kann sich diese Kritik jedoch nicht auf das „Ob" der Einwilligung beziehen, sondern allenfalls auf die Ausgestaltung derjenigen Anforderungen, die der Gesetzgeber aufgrund des Untermaßverbots aufstellen muss, damit die erlaubende Wirkung der datenschutzrechtlichen Einwilligung typischerweise eine selbstbestimmte Entscheidung des Datensubjekts gewährleistet. Insoweit geht es jedoch um die Sicherung der Voraussetzungen *für* eine autonome Entscheidung des Datensubjekts[229] und nicht um die Grenzen der anschließenden (Selbst-)Bindung *an* diese autonome Entscheidung.

Während die Einwilligung in die Datenverarbeitung in Art. 8 Abs. 2 S. 1 GRCh unionsgrundrechtlich garantiert und in Art. 4 Nr. 11, Art. 6 Abs. 1 lit. a, Art. 7 DS-GVO einfachgesetzlich ausgestaltet wurde, ist gesetzlich nicht eindeutig geregelt, ob das Datensubjekt an eine wirksam erteilte Einwilligung gebunden sein kann. Auf den ersten, oberflächlichen Blick erscheint die jederzeitige Widerruflichkeit der Einwilligung gemäß Art. 7 Abs. 3 DS-GVO als stringenter Ausdruck einer umfassenden Gewährleistung von informationeller Selbstbestimmung zugunsten des Datensubjekts. Soweit dadurch jedoch zugleich die Möglichkeit einer Selbstbindung an eine wirksame, autonome Einwilligung ausgeschlossen wird, handelt es sich dabei um eine Form „paternalistischer Freiheitsmaximierung",[230] sofern sie sich auch über einen anfänglich entgegenstehenden Willen des Datensubjekts hinwegsetzt. Neben den überindividuellen Konsequenzen für den Wettbewerb (unten C.III.2.) spricht die aus der Selbstbestimmung folgende Selbstverantwortung dafür, eine „Einwilligung" mit schuldvertraglicher Bindungswirkung grundsätzlich anzuerkennen, sofern die datenschutzrechtlichen Einwilligungsvoraussetzungen – gerade auch hinsichtlich der Bindungswirkung – vorlagen.

Im Ausgangspunkt gilt, was das *OLG München* auch für das Urheberpersönlichkeitsrecht festgehalten hat. Obwohl das Ende der Verfilmung des Buchs „Die unendliche Geschichte" von *Michael Ende* als Entstellung des ursprünglichen literarischen Werks (§ 14 UrhG) beurteilt wurde, konnte sich der Autor dagegen nicht mehr zur Wehr setzen, weil er einem früheren Drehbuch zugestimmt hatte, in der diese „Entstellung" bereits angelegt gewesen war. Ein Recht zur Reue, weil er seine ursprüngliche Einwilligung zur Verfilmung „nur aus wirtschaftli-

---

[228] *Simitis*, NJW 1998, 2573 (2476); m. w. N. *Rogosch*, Die Einwilligung im Datenschutzrecht, 2013, S. 17 f.; *Radlanski*, Das Konzept der Einwilligung in der datenschutzrechtlichen Realität, 2016, S. 147/212/239; *Buchner/Kühling*, in: Kühling/Buchner (Hrsg.), DS-GVO, 3. Aufl. 2020, Art. 7, Rn. 10; ähnlich: *Veil*, NJW 2018, 3337 (3344).

[229] Hierzu die Abstützungen in Kapitel 6.

[230] Diese allenfalls dann für gerechtfertigt haltend, wenn es um irreversible Eingriffe von existenzieller Bedeutung geht und mit dem zutreffenden Hinweis, dass in diesen Fällen häufig bereits die ursprüngliche Einwilligung nicht informiert oder unfreiwillig erfolgte: *Ohly*, Volenti non fit iniuria, 2002, S. 106.

chen Gründen und gegen seine innere Überzeugung“[231] abgegeben hatte, wurde nicht anerkannt.[232] Derartige subjektive Motive beeinträchtigen grundsätzlich weder die Informiertheit noch die Freiwilligkeit einer Einwilligung. Solange keine irreversiblen und die Existenz bedrohenden Beeinträchtigungen drohen, muss das Datensubjekt mit den Konsequenzen seiner Entscheidung leben. Diese Selbstverantwortung ist die Kehrseite jeder Selbstbestimmung.

Zudem führt die Möglichkeit, durch Disposition über die sog. freie Widerruflichkeit i. S. d. Art. 7 Abs. 3 S. 1 DS-GVO eine schuldvertragliche Bindungswirkung auszulösen, gerade nicht dazu, dass auch andere Beendigungsmöglichkeiten mit *ex nunc*-Wirkung durch eine *generelle* Disposition über die Widerruflichkeit vollständig ausgeschlossen sind.[233] Es existieren selbstverständlich weiterhin Gründe, die bereits einer vorübergehenden, befristeten Disposition über die Widerruflichkeit entgegenstehen können, weil der Schutz der Datensubjekte vor übermäßigen zukünftigen Freiheitsbeschränkungen die Einschränkung der Dispositionsfreiheit über die Widerruflichkeit rechtfertigt. Eine solche Beschränkung kommt insbesondere in Betracht, soweit an der Freiwilligkeit der Disposition, beispielsweise aufgrund einer (relativen) Marktmacht des Verantwortlichen, typischerweise Zweifel bestehen.[234]

Die Rechtsposition des Verantwortlichen wird durch einen zeitweisen Ausschluss der Widerruflichkeit der Einwilligung nicht irreversibel auf Kosten des Datensubjekts verbessert, sondern die Rechtsbeziehung wird lediglich befristet stabilisiert. Das Datensubjekt kann die Einwilligung insbesondere jederzeit *aus wichtigem Grund* widerrufen, so dass der Verantwortliche zwar vor einem schlichten Sinneswandel des Datensubjekts und einem jederzeitigen, grundlosen Widerruf geschützt ist, nicht jedoch vor einem Widerruf, der beispielsweise an eine schwerwiegende Verletzung der Grundsätze einer rechtmäßigen Datenverarbeitung (Art. 5 Abs. 1 DS-GVO) durch den Verantwortlichen anknüpft.[235]

Darüber hinaus bleibt die Kontrolle des Datensubjekts weitgehend bestehen, weil der auf Grundlage einer schuldrechtlichen Gestattung bestehende Leistungsanspruch des Verantwortlichen im Grundsatz nur den Vertragspartner begünstigt. Eine Abtretung des Anspruchs aus der schuldrechtlichen Gestattung durch den Verantwortlichen kommt – anders als für sonstige Persönlichkeitsrechte[236] – jedenfalls für Datensubjekte, die Verbraucher sind, grundsätz-

---

[231] *OLG München*, Urt. v. 01.08.1985, 29 U 2114/85 = GRUR 1986, 460 (463) – *Die unendliche Geschichte*.

[232] Hierzu sowie mit den weiteren Beispielen der Fernsehserie „Big Brother“ und den Grenzen im Fall soziopsychologischer Experimente: *Ohly*, Volenti non fit iniuria, 2002, S. 432 ff.

[233] Hierzu unten Kapitel 5 C.III.3.d.

[234] Unten Kapitel 5 C.III.2.

[235] Kapitel 5 C.III.3.d.

[236] BGHZ 14, 249 – *Cosima Wagner*; *Forkel*, NJW 1993, 3181; *Metzger*, Rechtsgeschäfte über das Droit moral, 2002, S. 47 ff.

lich nicht in Betracht. Vielmehr muss für die Datenverarbeitung eines anderen bzw. weiteren (gemeinsam) Verantwortlichen ebenfalls ein Erlaubnistatbestand vorliegen, beispielsweise eine weitere, ebenfalls nur relativ wirkende Einwilligung durch das Datensubjekt.

Um die Position der Datensubjekte zu stärken und eine effektivere Durchsetzung ihrer Rechte zu gewährleisten, besteht gemäß Art. 80 Abs. 1 DS-GVO die Möglichkeit, eine „Einrichtung, Organisation oder Vereinigung" damit zu beauftragen, die Rechte der Datensubjekte wahrzunehmen und insbesondere das Recht auf Schadensersatz gemäß Art. 82 DS-GVO in Anspruch zu nehmen. Somit sieht die DS-GVO die Möglichkeit zur gewillkürten Prozessstandschaft vor.[237]

Sofern man die Anforderungen an eine solche gewillkürte Prozessstandschaft nicht gemäß Art. 6 Abs. 1 lit. b DS-GVO dem nationalen Schuldrecht und damit insbesondere dem Auftragsrecht überlassen will und jedenfalls soweit besonders sensible personenbezogene Daten betroffen sind, kommt als Grundlage dieser gewillkürten Prozessstandschaft ebenfalls nur eine Einwilligung in Form einer schuldrechtlichen Gestattung unter zeitweisem Ausschluss der Widerruflichkeit für die Dauer der Rechtsverfolgung in Betracht.

Soweit Datensubjekte sich für eine Kommerzialisierung von personenbezogenen Daten unter Einsatz eines Treuhänders entscheiden, liegt es nahe, diesen Treuhänder von Anfang an ebenfalls mit einer befristeten, nicht frei widerruflichen Einwilligung auszustatten. Infolgedessen kann der Treuhänder die Daten entsprechend der Vorgaben des Datensubjekts verwerten und dessen Interessen gemäß Art. 80 Abs. 1 DS-GVO auf Grundlage einer gewillkürten Prozessstandschaft verfolgen.

Allerdings wird an dieser Stelle auch eine wesentliche Grenze der schuldrechtlichen Gestattung offenkundig. Aufgrund der für jede Datenverarbeitung erforderlichen eigenständigen Einwilligung bietet auch die schuldrechtliche Gestattung nur eine wenig effiziente rechtliche Grundlage für eine treuhänderische Verwertung von personenbezogenen Daten.[238] Obwohl die schuldrechtliche Gestattung die Position eines Verantwortlichen im Vergleich zur schlichter, einseitigen und jederzeit widerruflichen Einwilligung stabilisiert,[239] begründet auch die schuldrechtliche Gestattung – im Unterschied zu gegenständlichen Rechtspositionen – nicht denjenigen „einigermaßen sicheren Stand",[240] den ein Treuhänder nach bisherigem Verständnis benötigt, damit ein effizientes arbeits-

---

[237] So für die Durchsetzung von Persönlichkeitsrechten bereits: *BGH*, Urt. v. 14.10.1986, VI ZR 10/86, NJW-RR 1987, 231 – *Nena*.

[238] Hierzu: *Wendehorst/Schwamberger/Grinzinger*, in: Pertot (Hrsg.), Rechte an Daten, 2020, S. 103 ff.; *Kühling*, ZfDR 2021, 1 ff.

[239] Deshalb für eine Einschränkung der Widerruflichkeit der Einwilligung gegenüber Datentreuhändern: *Kühling*, ZfDR 2021, 1 (11).

[240] *Forkel*, GRUR 1988, 491 (493).

teiliges Vorgehen möglich wird. Inwieweit neue technologische Lösungen – insbesondere sog. Personal Information Management Systeme (PIMS)[241] – diese fehlende rechtliche Stabilität bei gleichzeitig geringem kommerziellen Wert der personenbezogenen Daten einzelner Datensubjekte durch Technik kompensieren können, ist bislang noch offen,[242] soll aber sowohl gemäß Art. 12 lit. n und Art. 21 Abs. 3 DG-VO und nach Vorstellung des deutschen Gesetzgebers gemäß § 26 des Gesetzes zur Regelung des Datenschutzes und des Schutzes der Privatsphäre in der Telekommunikation und bei Telemedien (TTDSG) in Zukunft an Bedeutung gewinnen.[243]

III. Das Verhältnis zwischen Einwilligung und Vertrag

Solange die datenschutzrechtliche Einwilligung ausschließlich mit einer schlichten, einseitigen und frei widerruflichen Einwilligung gleichgesetzt wird, ist es möglich, diese widerrufliche Einwilligung als eigenständiges und einseitiges Rechtsgeschäft zu betrachten. Tatsächlich wird in der deutschen Literatur die Ansicht vertreten, die datenschutzrechtliche Einwilligung könne vom schuldrechtlichen Vertrag jedenfalls getrennt werden und sei von diesem abstrakt zu behandeln (1). Unabhängig davon, ob die (unbewusste) Übertragung eines deutschen sachenrechtlichen Sonderwegs auf einen unionsautonom geregelten immateriellen Gegenstand überzeugen kann, ist die zeitweise schuldrechtliche Gestattung zwar datenschutzrechtliche Einwilligung i. S. d. Art. 6 Abs. 1 lit. a DS-GVO, aber dennoch regelmäßig Bestandteil eines Vertrags (2). Diese Einordnung bietet zugleich die geeignete Lösung, um sowohl das Spannungsverhältnis zwischen den beiden Zielen aus Art. 1 DS-GVO als auch das Spannungsverhältnis zwischen DS-GVO und DID-RL im Sinne einer abgestützten informationellen Privatautonomie in unionsgrundrechtskonformer Weise aufzulösen (3).

1. Die Argumente für eine Trennung der Einwilligung vom Vertrag

Auf den ersten Blick spricht gegen eine Einordnung der datenschutzrechtlichen Einwilligung als Bestandteil eines schuldrechtlichen Vertrags, dass der europäische Gesetzgeber mit Art. 6 Abs. 1 lit. b DS-GVO einen eigenständigen vertragsakzessorischen Erlaubnistatbestand geschaffen hat (a). Zudem wird in der

[241] Hierzu: *Kettner/Thorun/Spindler*, Innovatives Datenschutz-Einwilligungsmanagement, Abschlussbericht im Auftrag des BMJV, 07.09.2020.

[242] Zu den ersten Geschäftsmodelle von PIMS: *Bericht der EU-Kommission*, An emerging offer of „personal information management services". Current state of service offers and challenges, 2016, S. 15; *EDSA*, Stellungnahme 09/2016 zu Systemen für das Personal Information Management (PIM), v. 20.10.2016.

[243] Vorschlag für eine Verordnung über europäische Daten-Governance (Daten-Governance-Gesetz), COM(2020) 767 final. Hierzu unten Kapitel 6 B.

deutschen Literatur vertreten, dass für die datenschutzrechtliche Einwilligung und einen schuldrechtlichen Vertrag eine Trennung und Abstraktion möglich sei. Dies lässt sich damit begründen, dass datenschutzrechtliche Erklärungen die Wirksamkeit des Vertrags über die Bereitstellung digitaler Produkte „unberührt" lassen sollen (b).

a) Trennung zwischen Einwilligung und Vertrag in der DS-GVO

Gemäß Art. 6 Abs. 1 lit. b DS-GVO ist eine Datenverarbeitung rechtmäßig, soweit sie für die Erfüllung eines Vertrags erforderlich ist. Allein die Existenz dieses eigenständigen Erlaubnistatbestands neben dem Einwilligungstatbestand spricht zunächst dafür, dass eindeutig zwischen solchen Datenverarbeitungen unterschieden werden kann und muss, die auf Grundlage einer Einwilligung oder vertragsakzessorisch erfolgen.[244] Dabei müsste der zweiseitige Vertrag gemäß Art. 6 Abs. 1 lit. b DS-GVO konsequenterweise *lex specialis* gegenüber der einseitigen Einwilligung sein. Eine schuldrechtliche Gestattung wäre insoweit ein in der DS-GVO jedenfalls nicht explizit geregelter Hybrid zwischen der frei widerruflichen Einwilligung und der vertragsakzessorischen Datenverarbeitung.

Diese Unterscheidung zwischen Einwilligung und Vertrag ist konsequent, sofern man in Art. 6 Abs. 1 lit. b DS-GVO den einschlägigen Erlaubnistatbestand für alle Datenverarbeitungen sieht, soweit personenbezogene Daten als Leistungsgegenstand eines Austauschverhältnisses vereinbart werden. Kurzum: Sofern Verträge über die Verarbeitung von personenbezogenen Daten („Datenlizenzverträge") unter Art. 6 Abs. 1 lit. b DS-GVO fallen würden, käme es insoweit auf eine datenschutzrechtliche Einwilligung nicht mehr an.[245]

Tatsächlich überzeugt diese Trennung zwischen einer frei widerruflichen Einwilligung und einem schuldrechtlichen Vertrag jedoch nicht. Käme Art. 6 Abs. 1 lit. b DS-GVO immer dann zur Anwendung, wenn personenbezogene Daten als synallagmatische Leistung vereinbart werden, wäre der Anwendungsbereich der Einwilligung auf einseitige, schlichte Einwilligungen des Datensubjekts und damit in praktischer Hinsicht auf Gefälligkeiten und die Einwilligung in eine Datenverarbeitung von besonders sensiblen Daten i. S. d. Art. 9 Abs. 1 DS-GVO beschränkt.

---

[244] So (wohl) *Metzger*, in: Lohsse/Schulze/Staudenmayer (Hrsg.), Data as Counter-Performance: Contract Law 2.0?, 2020, S. 25 (34); *Hacker*, Datenprivatrecht, 2020, S. 163; *Leistner/Antoine/Sagstetter*, Big Data, 2021, S. 255.

[245] *Bunnenberg*, Privates Datenschutzrecht, 2020, S. 264 f. In einem zweiten Schritt wird jedoch regelmäßig deutlich, dass die Wertungen des europäischen Gesetzgebers aus Art. 4 Nr. 11 DS-GVO, den Grundsätzen gemäß Art. 5 Abs. 1 DS-GVO und insbesondere Art. 7 Abs. 3 und Abs. 4 DS-GVO dann zumeist „analog" auch bei der Anwendung von Art. 6 Abs. 1 lit. b DS-GVO berücksichtigt werden (müssen); vgl. *Hacker*, Datenprivatrecht, 2020, S. 159/540/264 f.; *Bunnenberg*, Privates Datenschutzrecht, 2020, S. 60 f.

Nach hier vertretener Auffassung dient Art. 6 Abs. 1 lit. b DS-GVO jedoch nur zur Entlastung des Einwilligungstatbestands und hat damit nur Bedeutung für untergeordnete Datenverarbeitungen, die typischerweise mit einem Vertrag einhergehen, der eine Einigung über andere (Haupt-)Leistungspflichten enthält. Soweit personenbezogene Daten als im Synallagma stehender Leistungsgegenstand definiert werden, ist Art. 6 Abs. 1 lit. b DS-GVO nicht anwendbar.[246]

b) Trennung zwischen Einwilligung und Vertrag in der DID-RL

Die DID-RL liefert ein zweites Argument, das dafür sprechen könnte, die Einwilligung jedenfalls vom Vertrag über die Bereitstellung digitaler Produkte strikt zu trennen. Der DID-RL lässt sich die Intention des europäischen Gesetzgebers entnehmen, mit seinen vertragsrechtlichen Vorgaben sowohl das europäische Datenschutzrecht als auch die jeweilige nationale Rechtsgeschäftslehre möglichst unberührt zu lassen. Obwohl Art. 3 DID-RL lediglich den Anwendungsbereich der DID-RL bestimmt, lässt sich diese Vorschrift tatsächlich als impliziter Ansatz für eine vom europäischen Gesetzgeber angestrebte Trennung und Abstraktion zwischen der datenschutzrechtlichen Einwilligung und den sonstigen vertraglichen Vereinbarungen anführen.

Gemäß Art. 3 Abs. 8 und Abs. 10 DID-RL lässt die DID-RL die Bestimmungen der europäischen DS-GVO bzw. die nationalen Bestimmungen über das Zustandekommen, die Wirksamkeit und die Nichtigkeit eines Vertrags „unberührt". Dies stellt ErwG 40 DID-RL nochmals klar. Hiernach soll die DID-RL

> „nicht die Folgen für die von ihr erfassten Verträge regeln, die sich ergeben, wenn der Verbraucher die Einwilligung zur Verarbeitung seiner personenbezogenen Daten widerruft. Solche Folgen sollten weiterhin dem nationalen Recht unterliegen."

Diese Ausführungen dienen als Argument dafür, zwischen der datenschutzrechtlichen Einwilligung und dem schuldrechtlichen Vertrag „in dogmatischer Hinsicht scharf zu unterscheiden",[247] selbst wenn der Vertrag eine Verpflichtung zur Einwilligung bzw. den Zugang zu personenbezogenen Daten als Bedingung für den Anspruch auf Bereitstellung von digitalen Produkten enthalte.

Auch der deutsche Gesetzgeber scheint bei seiner Umsetzung der DID-RL gemäß § 327q Abs. 1 BGB die datenschutzrechtlichen und die schuldrechtlichen Rechtsfolgen klar trennen zu wollen. Hiernach lassen

> „die Ausübung von datenschutzrechtlichen Betroffenenrechten und die Abgabe datenschutzrechtlicher Erklärungen des Verbrauchers nach Vertragsschluss die Wirksamkeit des Vertrags unberührt."

---

[246] Zu den Gründen bereits oben: Kapitel 3 C.I–III.
[247] *Hacker*, Datenprivatrecht, 2020, S. 163.

Im Ergebnis werden dadurch Datenschutzrecht und Vertragsrecht auch im BGB verbal aufgespalten, statt sich um diejenige Synchronisierung zu bemühen, die der europäische Gesetzgeber zunächst versäumt hat und die seither rechtspolitisch sehr umstritten ist.[248] Art. 3 Abs. 8 und Abs. 10 DID-RL sowie § 327q Abs. 1 BGB lassen sich als Versuch einer Trennung und Abstraktion interpretieren, wenngleich es dem deutschen Gesetzgeber nicht gelingen konnte, diese durchzuhalten.[249]

In Übereinstimmung mit dieser (behaupteten) Trennung zwischen datenschutzrechtlicher Einwilligung und dem Vertrag über die Bereitstellung digitaler Produkte existiert eine womöglich unbewusste, jedoch spezifisch deutsche Vorstellung darüber, dass der schuldrechtliche Vertrag, einschließlich der vertraglichen Verpflichtung zur Bereitstellung personenbezogener Daten als Gegenleistung, mit einem Verpflichtungsgeschäft gleichgesetzt werden kann, während die datenschutzrechtliche Einwilligung davon getrennt, jedenfalls aber abstrakt zu behandeln sei.[250] Sie wird eher mit einer Verfügung assoziiert.[251] Richtig an diesem Ansatz ist, dass eine Einwilligung das Rechtsverhältnis zwischen Einwilligendem und Einwilligungsempfänger umgestaltet, indem sie die Rechtsposition des Begünstigten verbessert und deshalb nach dem deutschen – sachenrechtlich und durch *Savigny* geprägten – Verständnis als „verfügungsähnlich" bezeichnet werden kann.[252]

Diese Bezeichnung führt jedoch leicht zu Missverständnissen, weil für die datenschutzrechtliche Einwilligung die beiden Stufen der translativen Rechtsübertragung oder auch nur konstitutiven (gebundenen) Rechtseinräumung gerade nicht zur Verfügung stehen.[253] Eine gegenständliche Wirkung wie die

---

[248] Insofern dient diese Formulierung in § 327q Abs. 1 BGB sicherlich auch dazu, eine Aussage darüber zu vermeiden, ob personenbezogene Daten als vertraglicher Leistungsgegenstand („Daten als Gegenleistung") vereinbart werden können.

[249] In § 327q Abs. 2 (Kündigungsrecht des Unternehmers bei Widerruf der Einwilligung durch den Verbraucher) und § 516a Abs. 1 BGB (Möglichkeit der Typisierung Schenkung, obwohl das Datensubjekt im Gegenzug personenbezogene Daten bereitstellt) wird diese Trennung durchbrochen.

[250] So tendenziell: *Metzger*, AcP 216 (2016), 817 (831 f.); *Metzger*, in: Lohsse/Schulze/Staudenmayer (Hrsg.), Data as Counter-Performance: Contract Law 2.0?, 2020, S. 25 (34: „A possible starting point to conceptualize this question could be the so called 'abstraction principle', one of the basic principle of German civil law" sowie S. 35 „What remains unclear under Article 7(3) GDPR and the DCSD are the further consequences for the contract. Here again, the 'abstraction principle' provides a possible solution. The withdrawal of consent does not affect the validity of the contract". In diese Richtung auch: *Langhanke*, Daten als Leistung, 2018, 163 ff.; *Hacker*, Datenprivatrecht, 2020, S. 162; ebenso (wohl): *Leistner/Antoine/Sagsetter*, Big Data, 2021, S. 255.

[251] *Specht*, JZ 2017, 763 (765: „verfügungsähnlich").

[252] So für die schuldrechtliche Gestattung: *Ohly*, Volenti non fit iniuria, 2002, S. 173 f. Auch das deutsche Schuldrecht kennt gegenständliche Verfügungen, die nicht „dinglich" sind, weil sie keine Sachen (§ 90 BGB) voraussetzen, vgl. § 780 und § 781 BGB.

[253] Hierzu oben C.II.1.

Aufhebung, Übertragung, Belastung oder Inhaltsänderung scheidet bislang mangels „Recht am eigenen Datum“[254] aus. Derartige gegenständliche Verfügungen kommen für personenbezogene Daten derzeit ebenso wenig in Betracht wie ein gutgläubiger Erwerb.

Tatsächlich sollten die missglückten Versuche des europäischen Gesetzgebers zwischen dem Datenschutzrecht und dem Vertragsrecht (in Art. 3 Abs. 8 und Abs. 10 DID-RL) abzugrenzen,[255] nicht überbewertet werden. Zwar soll die DID-RL gemäß Art. 3 Abs. 8 DS-GVO sowohl die DS-GVO (vollständig) als auch gemäß Art. 3 Abs. 10 DID-RL das nationale Vertragsrecht (weitgehend)[256] „unberührt“ lassen. Diese Abgrenzung der Anwendungsbereiche dient jedoch nicht der Einführung eines – dem europäischen Recht unbekannten – Trennungs- und Abstraktionsprinzips zwischen datenschutzrechtlicher Einwilligung und schuldrechtlichem Vertrag. Vielmehr fungieren beide Regelungen als formale Rückversicherung, weil dem europäischen Gesetzgeber bei Verabschiedung der DID-RL zwar die Abgrenzungsschwierigkeiten zur DS-GVO zunehmend bewusst wurden, er sich aber dennoch außer Stande sah, die komplexen rechtlichen Überschneidungspunkte zu synchronisieren. Diese undankbare Aufgabe hat die Legislative an die Judikative delegiert.[257]

Dass unterschiedliche rechtliche Rahmenbedingungen für die Einwilligung (DS-GVO/künftige ePrivacy-VO) und die sonstigen vertraglichen Vereinbarungen – einschließlich der (Haupt-)Leistungspflicht des Verantwortlichen – gelten (harmonisiertes Schuldrecht) ist dem asynchronen, teilweise kompetenzrechtlich determinierten Regulierungsansatz des europäischen Gesetzgebers geschuldet. Die daraus resultierenden Schwierigkeiten würden durch eine strikte Trennung und Abstraktion zwischen Einwilligung (Art. 6 Abs. 1 lit. a DS-GVO) und (Rest-)Vertrag (Art. 6 Abs. 1 lit. b DS-GVO i. V. m. nationalem Schuldrecht) allenfalls nochmals verschärft.

Das Ergebnis einer solchen Trennung zwischen der datenschutzrechtlichen Einwilligung und dem (restlichen) schuldrechtlichen Vertrag würde zwar eine gewisse Immunisierung des nationalen Schuldrechts gegenüber der DS-GVO ermöglichen. In einem anschließenden Schritt müsste diese Trennung und Abstraktion – im Fall eines Widerrufs der Einwilligung – jedoch wieder eingefangen werden. Anderenfalls wäre die freie Widerruflichkeit der Einwilligung durch eine nachteilige vertragliche Haftung gefährdet.[258]

---

[254] Hierzu: *Sattler*, in: Bakhoum u. a. (Hrsg.), Personal Data in Competition, Consumer Protection and Intellectual Property Law – Towards a Holistic Approach?, 2018, S. 27 (39 ff.).

[255] Hierzu bereits oben: Kapitel 3 C.III.1.

[256] Gleiches gilt gemäß Art. 3 Abs. 6 der Richtlinie (EU) 2019/771 des Europäischen Parlaments und des Rates vom 20.05.2019 über bestimmte vertragsrechtliche Aspekte des Warenkaufs, ABl. L 136, S. 28.

[257] *Sattler*, NJW 2020, 3623 ff.

[258] Schuldrechtliche Schadensersatzansprüche (wohl) befürwortend: *Metzger*, JIPITEC 2017, 2 (6 f.); *Leistner/Antoine/Sagstetter*, Big Data, 2021, S. 255; andererseits jedoch S. 273

Während der deutsche Gesetzgeber sich mit § 327q Abs. 1 BGB zunächst um eine vermeintlich klare Trennung der datenschutzrechtlichen Einwilligung und des Vertrags über die Bereitstellung der digitalen Produkte bemüht, werden aus § 327q Abs. 3 und Abs. 2 BGB sofort die Grenzen einer solchen Trennung und Abstraktion offenkundig. Mit § 327q Abs. 3 BGB hat der deutsche Gesetzgeber einen wuchtigen Schlag ausgeführt, um den gordischen Knoten aus Datenschutz- und Schuldrecht zumindest für das B2C-Verhältnis zu lösen. Hiernach sind

„Ersatzansprüche des Unternehmers gegen den Verbraucher wegen einer durch die Ausübung von Datenschutzrechten oder die Abgabe datenschutzrechtlicher Erklärungen bewirkten Einschränkung der zulässigen Datenverarbeitung […] ausgeschlossen."

Damit will der deutsche Gesetzgeber alle vertraglichen oder gesetzlichen Folgeansprüchen ausschließen, dem das Datensubjekt anschließend ausgesetzt wäre und die das Datensubjekt von einem freien Widerruf der Einwilligung abhalten könnten. Somit hat der deutsche Gesetzgeber sich seinerseits einem (zu) restriktiven Verständnis des ErwG 42 S. 5 DS-GVO hingegeben, wonach ein Einwilligungswiderruf nur dann frei ist, wenn er möglich ist, „ohne Nachteile zu erleiden".

Zugleich hat der deutsche Gesetzgeber mit § 327q Abs. 3 BGB jedoch einer Trennung und Abstraktion zwischen der Einwilligung und dem Vertrag insofern für das B2C-Verhältnis eine Absage erteilt, weil der Widerruf der Einwilligung auf jedes vertragliche und gesetzliche Schuldverhältnis durchschlägt und alle Sekundäransprüche des Unternehmers/Verantwortlichen gegen den Verbraucher/Datensubjekt ausschließt. Dadurch ist insbesondere ein vertraglicher Schadenersatzanspruch auf (erneute) Erteilung einer Einwilligung als Naturalrestitution ausgeschlossen (§ 249 Abs. 1 BGB).[259]

Immerhin versucht der deutsche Gesetzgeber mit einem außerordentlichen Beendigungsrecht des Unternehmers gemäß § 327q Abs. 2 BGB einen Ausgleich zwischen einem utopischen Verständnis der freien Widerruflichkeit („ohne Nachteil für das Datensubjekt") und der alltäglichen Realität zu erzielen, in der personenbezogene Daten eine im vertraglichen Synallagma stehende Gegenleistung sind.

Wird eine zunächst *wirksam erteilte* Einwilligung anschließend widerrufen, so ist § 327q Abs. 2 BGB *lex specialis* zu § 139 BGB (analog). § 327q Abs. 2 BGB sieht im Fall eines Widerrufs in Bezug auf Verträge über digitale Produkte vor,

---

(„Ein Schadensersatzanspruch dürfte aber letztlich abzulehnen sein. […] Normativ ist die datenschutzrechtliche Wertung zu beachten, dass ein Widerruf des betroffenen jederzeit und ohne Nachteil möglich sein muss").

[259] Von der teleologischen Reduktion des Art. 7 Abs. 3 S. 1 DS-GVO ist der § 327q Abs. 3 BGB nicht betroffen, weil es infolgedessen für die Dauer der Disposition über die freie Widerruflichkeit bereits an der Abgabe einer datenschutzrechtlichen Erklärung i. S. d. § 327q Abs. 3 BGB fehlt.

dass der Unternehmer den weiterhin wirksamen Vertrag über die Bereitstellung digitaler Produkte ohne Einhaltung einer Frist kündigen kann,

„wenn ihm unter Berücksichtigung des weiterhin zulässigen Umfangs der Datenverarbeitung und unter Abwägung der beiderseitigen Interessen die Fortsetzung des Vertragsverhältnisses bis zum vereinbarten Vertragsende oder bis zum Ablauf einer gesetzlichen oder vertraglichen Kündigungsfrist nicht zugemutet werden kann."

Diese Vorschrift wirft mehr Fragen auf, als Antworten zu geben. Zunächst sieht sie eine kuriose zweifache Interessenabwägung vor.

Der nach einem Einwilligungswiderruf weiterhin zulässige Umfang der Datenverarbeitung dürfte sich regelmäßig aus einer *datenschutzrechtlichen* Interessenabwägung gemäß Art. 6 Abs. 1 lit. f i.V.m. Art. 21 Abs. 1 DS-GVO ergeben.[260] Anschließend fordert § 327q Abs. 2 BGB zu einer noch vageren *generellen* Abwägung der beiderseitigen Interessen in Bezug auf die Fortsetzung des Vertrags auf.[261]

Zudem legt die Formulierung des § 327q Abs. 2 BGB im Umkehrschluss ein Verständnis nahe, wonach es zwischen einem Verbraucher/Datensubjekt und einem Unternehmer/Verantwortlichem möglich sein könnte, den Widerruf der Einwilligung durch das Datensubjekt als ordentlichen, fristgebundenen Kündigungsgrund zu vereinbaren. Im Anschluss hieran bleibt auch die Frage unbeantwortet, ob der Verantwortliche und das Datensubjekt in transparenter Weise *im Vorhinein* vereinbaren können, dass der Widerruf einer datenschutzrechtlichen Einwilligung zu einem Wechsel der Leistungspflicht des Datensubjekts führt, so dass der Vertrag mit dem Widerruf *ex nunc* gegen ein zuvor vereinbartes oder übliches monetäres Entgelt fortgesetzt wird.

Eine solche Option ließe sich mit der restriktiven Auslegung des sog. Kopplungsverbots in Art. 7 Abs. 4 DS-GVO vereinbaren, weil diese von Anfang an vereinbarte Wechselmöglichkeit zumindest eine (nachträgliche) alternative Kontrahierung gegen monetäres Entgelt zugunsten des Datensubjekts eröffnet. Freiwillig wäre der Widerruf deshalb, weil eine bereits anfänglich vereinbarte Option zum Wechsel kein Nachteil des Widerrufs des Datensubjekts i.S.d. ErwG 42 S. 5 DS-GVO sein kann.

Die bislang fehlende Synchronisierung von Datenschutz- und Schuldrecht verdeutlicht, dass der Einwilligungsbegriff der DS-GVO unionsautonom ist und „die" Einwilligung nicht existiert, sondern verschiedene Varianten möglich sind, bzw. möglich sein müssen.

---

[260] Der Widerruf der Einwilligung ist regelmäßig auch als konkludente Widerspruchserklärung i.S.d. Art. 21 Abs. 1 DS-GVO gegen eine Datenverarbeitung auf Grundlage von Art. 6 Abs. 1 lit. f DS-GVO auszulegen. Zu den Konsequenzen für deren Ausgestaltung im Rahmen eines Kontroll-Cockpits, unten Kapitel 6 B.

[261] Mit dem Vorschlag für ein freies Wahlrecht des Verantwortlichen im Fall des Einwilligungswiderrufs: *Buchner*, Die informationelle Selbstbestimmung im Privatrecht, 2006, S. 272 f.

2. Die Einwilligung als Bestandteil vertraglicher Vereinbarungen

Aus Art. 7 Abs. 3 S. 1 DS-GVO lässt sich ableiten, dass der europäische Gesetzgeber im Ausgangspunkt von einer schlichten, einseitigen und widerruflichen Einwilligung ausging. Deshalb wirft die Differenzierung zwischen der jederzeit widerruflichen Einwilligung und der zeitweise bindenden schuldrechtlichen Gestattung eine grundlegende Folgefrage auf.

Nach deutscher Dogmatik handelt es sich bei der schuldrechtlichen Gestattung um ein zweiseitiges Rechtsgeschäft und damit einen Vertrag.[262] Aus der – nur untergeordnet relevanten – deutschen Perspektive stellt sich infolgedessen die Frage, ob der befristete Ausschluss der Widerruflichkeit die Rechtsnatur dieser Einwilligung derart grundlegend verändert, dass es auch zu einer kategorialen Verschiebung innerhalb der Erlaubnistatbestände der DS-GVO kommt. Prägnant: Ist das Ergebnis einer zeitweisen Disposition über die Widerruflichkeit i. S. d. Art. 7 Abs. 3 S. 1 DS-GVO noch eine Einwilligung (Art. 6 Abs. 1 lit. a DS-GVO), ein Hybrid oder bereits ein Vertrag (Art. 6 Abs. 1 lit. b DS-GVO)?

Obwohl auch die Antwort auf diese Frage unionsautonom zu erfolgen hat, ist ein Blick auf die in Deutschland geführte Diskussion über die Rechtsnatur der Einwilligung erneut hilfreich, um diese Abgrenzungsfrage einzuordnen (a).

Im Unterschied zur innerstaatlichen Auseinandersetzung über die Rechtsnatur der Einwilligung hat die Einordnung der unionsautonomen datenschutzrechtlichen Einwilligung im europäischen Mehrebenensystem grundlegende Bedeutung für den einheitlichen Schutz von Datensubjekten und den freien Verkehr von personenbezogenen Daten im Binnenmarkt (b).

a) Der deutsche Streit über die Rechtsnatur der Einwilligung

In Deutschland war und ist umstritten, ob die Einwilligung ein Rechtsgeschäft ist. Wie *Ansgar Ohly* herausgearbeitet hat, beruht dieser Streit über die Rechtsnatur der Einwilligung teilweise auf Missverständnissen.[263] Tatsächlich geht es bei dem abstrakten Streit über die Rechtsnatur der Einwilligung vorrangig um die Frage, ob die allgemeinen Regeln der Rechtsgeschäftslehre für die häufig persönlichkeitsrechtlich determinierten Sachverhalte der Einwilligung angemessen sind. Im Ergebnis führen die Ansichten über die Rechtsnatur jedoch regelmäßig zu vergleichbaren Ergebnissen.

Sofern die Einwilligung als Rechtsgeschäft eingeordnet wird, so werden anschließend Vorschriften der Rechtgeschäftslehre – beispielsweise §§ 107 ff. BGB – teleologisch reduziert, soweit sie den höchstpersönlichen Interessen der Beteiligten im Einzelfall nicht gerecht werden. Sofern die Einwilligung nicht als Rechtsgeschäft eingeordnet wird, wird dies regelmäßig damit begründet, dass

---

[262] *Ohly*, Volenti non fit iniuria, 2002, S. 349.

[263] Ebenso für das deutsche Privatrecht: *Ohly*, Volenti non fit iniuria, 2002, S. 201 ff.

die Regelungen des BGB zu den Willenserklärungen für wirtschaftliche Austauschverhältnisse konzipiert sind und deshalb im persönlichkeitsrechtlichen Kontext unpassend seien.[264] Dennoch werden die Vorschriften der Rechtsgeschäftslehre anschließend punktuell und analog auf die „rechtsgeschäftsähnlichen" Willensbekundungen im Rahmen der Einwilligung angewendet.

Kurzum: Der jeweils gewählte Weg unterscheidet sich, mündet am Ende aber stets in eine modifizierte Anwendung der Vorschriften der Rechtsgeschäftslehre.[265]

b) Die Einwilligung als Instrument der Synchronisierung

Die Erkenntnisse aus dem Streit über die Rechtsnatur der Einwilligung lassen sich – unter umgekehrten Vorzeichen – teilweise auf die DS-GVO übertragen. Die Anwendung der Rechtsgeschäftslehre wurde in Deutschland deshalb kritisiert, weil das BGB im Bereich der Persönlichkeitsrechte erhebliche Defizite aufweist und infolgedessen für die häufig im Kontext von Persönlichkeitsrechten erfolgenden Einwilligungen tendenziell zu verwertungsfreundlich geprägt sei. Diametral hierzu wird die DS-GVO durch persönlichkeitsrechtliche Erwägungen dominiert, weil dem europäischen Gesetzgeber bislang das Bewusstsein für die ökonomische Bedeutung von personenbezogenen Daten fehlte.[266]

Auch für die datenschutzrechtliche Einwilligung stehen zwei Lösungswege offen. Entweder hält man die persönlichkeitsrechtlich geprägte Konstruktion der DS-GVO „sauber" und verlagert die aus dieser Perspektive „schmutzige" Realität der Kommerzialisierung von personenbezogenen Daten mit Hilfe von Art. 6 Abs. 1 lit. b DS-GVO in das nationale Schuldrecht. Alternativ gibt man der unionsweit einheitlichen DS-GVO den Vorzug, indem man Art. 6 Abs. 1 lit. b DS-GVO – mit hier vertretener Auffassung – restriktiv auslegt, so dass vorrangig die detailliert ausgestalteten Anforderungen an die Einwilligung Anwendung finden. Dann ist die datenschutzrechtliche Einwilligung in Form einer schuldrechtlichen Gestattung kein Hybrid zwischen Einwilligung und Vertrag, sondern fällt als schuldrechtliche Gestattung unter den unionsautonomen

---

[264] Hierzu ausführlich: *Ohly*, Volenti non fit iniuria, 2002, S. 210 ff.

[265] Allerdings sind die beiden Wege – teleologische Reduktion der Vorschriften der Rechtsgeschäftslehre oder punktuelle analoge Anwendung dieser Vorschriften nicht gleichwertig, weil der zweite Weg intransparenter und schwieriger vorhersehbar ist: *Ohly*, Volenti non fit iniuria, 2002, S. 206.

[266] Insofern ist es konsequent, dass in der Schweiz mit Art. 19 Abs. 2 ZGB nicht nur deutlicher zwischen wirtschaftlicher Mündigkeit und persönlichkeitsrechtlicher Urteilsfähigkeit unterschieden wird, sondern auch klarer für die Möglichkeit einer zeitweisen Disposition über die Widerruflichkeit der datenschutzrechtlichen Einwilligung plädiert wird: *Thouvenin*, SJZ 113/2017, 21 (31: „nahezu unbestreitbar richtiger, ja als ein geradezu zwingender Schritt"); *Schmidt*, Datenschutz als Vermögensrecht, 2020, 146 f.; ebenso mit Blick auf die DS-GVO und § 22 KUG: *Götting*, in: Schricker/Loewenheim, Urheberrecht, § 22 KUG, Rn. 40 f.; a. A. *Specht/Bienemann*, K&R 2018, 22 (23).

Begriff der Einwilligung i. S. d. Art. 4 Nr. 11 DS-GVO i. V. m. Art. 6 Abs. 1 lit. a DS-GVO.

Langfristig könnten – insoweit ähnlich dem Streit über die Rechtsnatur der Einwilligung für das deutsche Recht – beide Wege potenziell zu sehr ähnlichen Ergebnissen führen. Dennoch ist die Einordnung im europäischen Mehrebenensystem nicht mit dem deutschen Rechtstreit über die Rechtsnatur der Einwilligung vergleichbar.

Ordnet man – entgegen hier vertretener Ansicht – die zeitweise unwiderrufliche Einwilligung als schuldrechtliche Gestattung dem unionsautonomen Begriff des Vertrags und damit Art. 6 Abs. 1 lit. b DS-GVO zu, so würden beide Ziele aus Art. 1 DS-GVO solange grundlegend gefährdet, bis die im Kontext der Einwilligung durch die DS-GVO getroffenen Wertungen bei der Anwendung des nationalen Schuldrechts der Mitgliedstaaten analog und unionsweit einheitlich angewendet werden. Insofern ist es konsequent, dass sowohl *Philipp Hacker* als auch *Jan Niklas Bunnenberg* bereits gefordert haben, den Wertungen aus Art. 7 DS-GVO auch innerhalb des jeweils nationalen Schuldrechts mittels analoger Anwendung zur Geltung zu verhelfen bzw. diese im Rahmen der Prüfung der Erforderlichkeit gemäß Art. 6 Abs. 1 lit. b DS-GVO entsprechend zu berücksichtigen.[267] Dieser Weg ist jedoch auf eine (hyper-)komplexe Rekonstruktion der Wertungen der DS-GVO innerhalb des nationalen Schuldrechts angewiesen[268] und wird eine künftige europäische Harmonisierung oder Vereinheitlichung des „Datenschuldrechts" erfordern.

Ordnet man dagegen auch die zeitweise unwiderrufliche Einwilligung dem unionsautonomen Begriff der Einwilligung und somit Art. 4 Nr. 11 DS-GVO i. V. m. Art. 6 Abs. 1 lit. a DS-GVO zu, so kann man die vorrangig persönlichkeitsrechtlich geprägten Anforderungen an die Einwilligung durch eine vergleichsweise schlichte teleologische Reduktion von Art. 7 Abs. 3 S. 1 DS-GVO nachträglich für privatrechtliche Austauschverträge sensibilisieren.

Trotz ihrer Nähe zur schuldrechtlichen Gestattung und damit zum rechtsgeschäftlichen Vertrag hat die Einordnung einer zeitweise unwiderruflichen Einwilligung als datenschutzrechtliche Einwilligung i. S. d. Art. 6 Abs. 1 lit. a DS-GVO wesentliche Vorteile. Diese Vorteile korrespondieren weitgehend mit denjenigen, die auch für einen allgemeinen Vorrang der Einwilligung sprechen.[269] Während die Einordnung der zeitweise unwiderruflichen datenschutzrechtlichen Einwilligung als Vertrag ebenfalls dem individualrechtlichen Charakter des Schutzes von personenbezogenen Daten gerecht würde, sprechen die Systematik der DS-GVO, vor allem aber die einheitliche und unionsautonome

---

[267] *Hacker*, Datenprivatrecht, 2020, S. 159/183 ff./540/264 f.; *Bunnenberg*. Privates Datenschutzrecht, 2020, S. 60 f.

[268] Oben unter Kapitel 3 A.I.; *Hacker*, Datenprivatrecht, 2020, S. 540 ff.; sowie die „schuldrechtliche Lösung" bei *Bunnenberg*, Privates Datenschutzrecht, 2020, S. 53 f.

[269] Oben A.I. und unten Kapitel 5 B.

Rechtsauslegung und -anwendung dafür, die Anforderungen der DS-GVO an die Einwilligung und nicht das nationale und allenfalls im B2C-Verhältnis teilweise harmonisierte nationale Schuldrecht zum Ausgangspunkt zu wählen.

Die detailliert und unionsweit einheitlich ausgestalteten Anforderungen an eine datenschutzrechtliche Einwilligung bieten eine klare Orientierung und legen demjenigen die Argumentationslast auf, der – wie hier vorgeschlagen – von diesen Anforderungen *praeter legem* abweichen möchte. Wer hingegen den Einwilligungsbegriff der DS-GVO auf die jederzeit widerrufliche Einwilligung beschränkt und eine Verpflichtung zur Bereitstellung personenbezogener Daten nur über Art. 6 Abs. 1 lit. b DS-GVO i. V. m. dem durch eine analoge Anwendung von Art. 7 DS-GVO modifizierten nationalen Schuldrecht für möglich hält, riskiert damit eine Überforderung der nationalen Datenschutzbehörden und Gerichte und infolgedessen eine große Diskrepanz zwischen den nationalen Lösungswegen.

Obwohl die DS-GVO mit Art. 6 Abs. 1 lit. b DS-GVO potenziell die Möglichkeit eröffnet hat, aus der Einwilligung und damit auch aus der DS-GVO zu fliehen, führt dieser Weg entweder und bestenfalls über den Umweg einzelfallbezogener Rechtsprechung auf Grundlage des jeweils nationalen Schuldrechts oder über künftiges Sekundärrecht wieder zu einer Angleichung der unionsweiten Rechtslage. Kurz- und mittelfristig ist die Vorhersehbarkeit der Rechtslage im jeweiligen Mitgliedstaat jedoch für Datensubjekte und Verantwortliche beträchtlich eingeschränkt. Infolgedessen gefährdet der Weg über Art. 6 Abs. 1 lit. b DS-GVO die Verwirklichung der in Art. 1 DS-GVO niedergelegten Ziele eines hohen Schutzes der Datensubjekte bei gleichzeitig möglichst freiem Verkehr von personenbezogenen Daten im Binnenmarkt.

Somit verspricht eine Lösung innerhalb der DS-GVO eine unionsweit einheitliche Lösung und dadurch ein höheres Maß an Rechtssicherheit. Deshalb ist die vorübergehend unwiderrufliche Einwilligung als Einwilligung im Sinne der DS-GVO zu behandeln[270] und ihre Voraussetzungen und Folgen ergeben sich unionweit einheitlich und autonom aus der DS-GVO.

c) Konsequenzen der Ausdifferenzierung des Einwilligungsbegriffs

Im nachfolgenden Kapitel mündet das in Kapitel 2–4 herausgearbeitete Verhältnis zwischen den datenschutzrechtlichen Erlaubnistatbeständen und dem Schuldrecht in einen Vorschlag für ein Stufenmodell der abgestützten informa-

[270] Eine hiervon zu trennende Frage ist, ob es im Rahmen eines Vorlageverfahrens gelingt, dem EuGH die Konsequenzen dieser Zuordnung bewusst zu machen. Gelingt dies nicht und beschränkt der EuGH den Tatbestand der Einwilligung auf eine stets widerrufliche Einwilligung, so bleibt immerhin der Weg über Art. 6 Abs. 1 lit. b DS-GVO und das nationale Schuldrecht, soweit keine besonders sensiblen Daten verarbeitet werden. Für Datenverarbeitungen im B2B-Verhältnis verstößt dieser Weg jedoch gegen Art. 16 GRCh i. V. m. Art. 52 Abs. 1 S. 2 GRCh (oben: B.III.).

tionellen Privatautonomie, das auf einem Vorrang der Einwilligung beruht. Vorab werden jedoch die wesentlichen Konsequenzen offengelegt, die mit der zweifachen Abstufung der datenschutzrechtlichen Einwilligung einhergehen.

Kommt man mit der hier vertretenen Auffassung zu der Ansicht, dass der europäische Gesetzgeber mit der DS-GVO einerseits die gemäß Art. 8 Abs. 1 GRCh, Art. 7 GRCh und Art. 16 AEUV unionsgrundrechtlich zu gewährleistenden Mindestanforderungen an eine Einwilligung der Datensubjekte etabliert hat, andererseits aber die traditionellen Möglichkeiten einer Kommerzialisierung der vermögenswerten Bestandteile der Persönlichkeitsrechte und den Einfluss der DS-GVO auf diese Rechtspraxis übersehen hat, so spricht dies für das Erfordernis einer flexiblen Anwendung von Art. 7 Abs. 4 DS-GVO (Freiwilligkeit der Einwilligung) und für die Möglichkeit zur teleologischen Reduktion von Art. 7 Abs. 3 S. 1 DS-GVO (sog. freie Widerruflichkeit der Einwilligung). Letztere ermöglicht grundsätzlich eine Disposition über die Widerruflichkeit der Einwilligung.[271]

Dies hat zur Folge, dass Art. 7 Abs. 3 S. 1 DS-GVO *nicht* mehr als strikte *abstrakt-generelle Wahlbeschränkung* zu verstehen ist, *sondern* als *Standard-Option*, von der jedoch durch die Beteiligten abgewichen werden kann.[272] Eine Abwahl dieser Standard-Option durch eine zeitweise Disposition über die sog. freie Widerruflichkeit der Einwilligung hat jedoch mehrere Voraussetzungen und ist – zum Schutz des Datensubjekts – im Verhältnis zu solchen Verantwortlichen ausgeschlossen, die im relevanten Bereich nach Feststellung einer Kartellbehörde über eine besondere Marktmacht verfügen.[273] Somit ist eine Auslegung und Anwendung von Art. 7 Abs. 3 S. 1 und Abs. 4 DS-GVO möglich, mit der die informationelle Privatautonomie der Datensubjekte materiell abgestützt und zugleich das Risiko reduziert wird, dass die Anforderungen an die Widerruflichkeit und die Freiwilligkeit sich faktisch vorrangig als Marktzutrittsbarrieren auswirken.

Denjenigen Verantwortlichen, die über keine besondere Marktmacht verfügen, bietet eine zeitweise Disposition über die Widerruflichkeit der Einwilligung durch ein Datensubjekt zumindest eine gewisse Planungssicherheit für ein

---

[271] Im Ergebnis ebenfalls für eine Einschränkbarkeit der Widerruflichkeit: *Kilian*, in: Garstka/Coy (Hrsg.), Gedächtnisschrift für Steinmüller, 2014, S. 195 (212); sowie im Kontext von § 22 KUG: *Götting*, in: Schricker/Loewenheim, Urheberrecht, 6. Aufl. 2020, § 22, Rn. 40 f. Ähnlich zum BDSG a. F.: *Gola/Klug/Körffer*, in: *Gola/Schomerus* (Hrsg.), BDSG 2015, § 4a, Rn. 39. Für eine Beschränkung der Widerruflichkeit gemäß dem Grundsatz von Treu und Glauben: *Buchner*, Die Informationelle Selbstbestimmung im Privatrecht, 2006, S. 270 f.; nach *Klement* ist die Widerruflichkeit „zur Vermeidung einer Primärrechtswidrigkeit […] durch allgemeine Rechtsgrundsätze des Unionsrechts und das nationale Schuldvertragsrecht einzuschränken", *ders.* in: Simitis/Hornung/Spiecker gen. Döhmann (Hrsg.), Datenschutzrecht, 2019, Art. 7, Rn. 92.

[272] Zum Verhältnis zwischen Wahlhilfen und Wahlbeschränkungen: *Schmolke*, Grenzen der Selbstbindung im Privatrecht, 2014, S. 258 ff.

[273] Hierzu Kapitel 5 C.III.2.a.

Geschäftsmodell, das auf dem Austausch von digitalen Produkten gegen einen Zugang zu personenbezogenen Daten beruht.

Infolgedessen *kann* für nicht-marktmächtige Verantwortliche der *Anreiz* entstehen, eine datenschonende Gestaltung zu wählen, um langfristige Vertragsbeziehungen zu Datensubjekten einzugehen. Dadurch könnte es diesen Verantwortlichen gelingen, ihren langfristigen Markterfolg zu sichern und mit den Plattformen mit besonderer Marktmacht mittelfristig zu konkurrieren, so dass ein Konditionenwettbewerb einsetzt, weil diese entweder ebenfalls (zusätzlich) auf datenschonendere Geschäftsmodelle einschwenken oder zumindest befürchten müssen, dass ihre Marktposition sich allmählich verschlechtert.

Gleichwohl sind die Verantwortlichen, denen die Möglichkeit zur befristeten Abbedingung der Widerruflichkeit gemäß Art. 7 Abs. 3 S. 1 DS-GVO grundsätzlich offensteht, *nicht gezwungen*, ein datenschonendes Geschäftsmodell zu wählen. Deshalb bedeutet die grundsätzliche Möglichkeit einer zeitweisen Disposition über Art. 7 Abs. 3 S. 1 DS-GVO noch nicht, dass diese Disposition für nicht-marktmächtige Verantwortliche stets und voraussetzungslos zur Verfügung stehen sollte.

Wie in Kapitel 5 herausgearbeitet wird, bleibt eine Disposition über die Widerruflichkeit von den Umständen des Einzelfalls abhängig, die über den Grundsatz der Datenverarbeitung nach Treu und Glauben gemäß Art. 5 Abs. 1 lit. a Var. 2 DS-GVO stets berücksichtigt werden müssen. Insbesondere bleibt die Möglichkeit zum außerordentlichen Widerruf infolge einer Pflichtverletzung des Verantwortlichen von dem zeitweisen Ausschluss der sog. freien Widerruflichkeit unberührt.[274]

D. Fazit

Es ist eine wesentliche Herausforderung für die hier vorgeschlagene Differenzierung zwischen der schlichten, einseitigen und jederzeit widerruflichen Einwilligung und der zeitweise bindenden Einwilligung in Form einer schuldrechtlichen Gestattung, dass der Begriff der Einwilligung auch im Unionsrecht unterkomplex und undifferenziert ist.[275] Dennoch hat die Unterscheidung zwischen der schlichten, einseitigen und jederzeit grundlos widerruflichen Einwilligung und der befristeten schuldrechtlichen Gestattung überwiegend Vorteile.

Erstens eröffnet sie einen Weg, deutlicher zwischen Otto-Normal-Datensubjekten und unternehmerisch handelnden Datensubjekten zu unterscheiden und dadurch die DS-GVO unionsgrundrechtskonform auszulegen.[276]

---

[274] Unten Kapitel 5 C.III.b-d.

[275] Ebenso für das deutsche Privatrecht: *Ohly*, Volenti non fit iniuria, 2002, S. 161 f.

[276] Die Lösung über eine Anwendung von Art. 6 Abs. 1 lit. b DS-GVO im B2B-Verhältnis

Zweitens, und dies mag auf den ersten Blick paradox erscheinen, trägt die hier vorgeschlagene Differenzierung zwischen den datenschutzrechtlichen Einwilligungstatbeständen gerade zum Schutz der Datensubjekte bei. Sie bietet eine rechtliche Stabilisierung der Beziehung zwischen Datensubjekten und nicht-marktmächtigen Verantwortlichen und fördert dadurch – unter Bedingung von Wettbewerb – die Entwicklung von Geschäftsmodellen, welche die Datensubjekte nicht in Vorleistung zwingen müssen. Die infolge eines zeitweisen Ausschusses der Widerruflichkeit aus Sicht von Verantwortlichen gewonnene Planbarkeit kann zumindest potenziell dafür genutzt werden, um personenbezogene Daten zu verwerten, dabei aber auf eine langfristige Geschäftsbeziehung mit Datensubjekten zu setzen und deshalb ein höheres Datenschutzniveau anzubieten. Infolge dieser Stabilisierung der Rechtsbeziehung zwischen Verantwortlichem und Datensubjekt sind die Verantwortlichen nicht gezwungen, die personenbezogenen Daten sofort zu verwerten, um dem Widerruf der Einwilligung zuvorzukommen und die damit potenziell einhergehenden Kosten einer Erfüllung des Anspruchs aus Art. 20 DS-GVO zu decken.[277]

Drittens erhöht die Möglichkeit, das Widerrufsrecht unter bestimmten Voraussetzungen ausschließen zu können, die Transparenz und Rechtssicherheit für alle Beteiligten. Sofern Datensubjekte unter bestimmten Voraussetzungen unionweit und auf Grundlage der DS-GVO vorübergehend über die Widerruflichkeit der Einwilligung disponieren können, hat dies wesentliche Vorteile gegenüber der von *Hacker*, *Buchner* und *Langhanke/Schmidt-Kessel* vorgesehenen einzelfallbezogenen Korrektur eines „opportunistischen Widerrufs" wegen Rechtsmissbrauchs[278] oder der von *Bunnenberg* vorgeschlagenen gerichtlichen Entscheidung, die – auf Grundlage einer vagen und generellen Interessenabwägung im Einzelfall – erst *ex post* beurteilt, ob die Datenverarbeitung auf Grundlage einer widerruflichen Einwilligung nach Maßgabe der DS-GVO unrechtmäßig oder auf Basis eines wirksamen bindenden Vertrags nach Maßgabe des jeweils nationalen Schuldrechts rechtmäßig ist.[279]

---

begünstigt eine uneinheitliche Rechtslage in den Mitgliedstaaten und gefährdet das Ziel des freien Verkehrs von personenbezogenen Daten. Zudem müsste das Tatbestandsmerkmal der „Erforderlichkeit" in Art. 6 Abs. 1 lit. b DS-GVO teleologisch reduziert werden, weil anderenfalls alle Leistungsvereinbarungen in B2B-Verträge einer Angemessenheitskontrolle unterfallen würden.

[277] Mit dem Hinweis, dass die durch Art. 20 DS-GVO verursachten Kosten das Interesse an einem längerfristigen Vertragsverhältnis begründen: *Schweitzer/Peitz*, Datenmärkte in der digitalisierten Wirtschaft: Funktionsdefizite und Regelungsbedarf? ZEW Discussion Paper No. 17-043 2016, S. 50; *dies.*, NJW 2018, 275 (280); mit der Einschätzung, dass Art. 20 DS-GVO eine Marktzutrittsbarriere begründet: *Kerber*, JIPITEC 2018, 318 (326 f.); *Gal/Aviv*, Journal of Competition Law and Economics 2020, 349 (351 f./386 ff.).

[278] So *Hacker*, Datenprivatrecht, 2020, S. 278; zuvor: *Buchner*, Die informationelle Selbstbestimmung im Privatrecht, 2006, S. 270 f.; *Langhanke/Schmidt-Kessel*, EuCML 2015, 218 (221).

[279] So *Bunnenberg*, Privates Datenschutzrecht, 2020, S. 264 f.

Die hier vorgeschlagene unionsrechtsfreundliche, flexiblere Auslegung des Einwilligungsbegriffs der DS-GVO hat jedoch eine wesentliche Voraussetzung: Der *EuGH* müsste sich ernsthaft am Doppelziel der DS-GVO und der durch Art. 3 Abs. 1 S. 2 DID-RL zum Ausdruck kommenden Wertung orientieren, wonach personenbezogene Daten nicht nur tatsächlich ein Leistungsgegenstand sind, sondern diese Realität auch rechtlich abgebildet werden muss. Ein klares Bewusstsein hierfür würde sicherstellen, dass der *EuGH* sich von einer Haltung distanziert, die bisweilen von Datenschutzbehörden eingenommen wird. Beeinflusst durch ihre institutionelle Funktion als Daten*schutz*behörden und als Europäischer Daten*schutz*ausschuss, ziehen sich diese Institutionen tendenziell vorschnell auf die für eine Abwägung nicht mehr zur Verfügung stehende Garantie der Menschenwürde zurück.[280] Im Anschluss bewerten sie eine Vereinbarung von personenbezogenen Daten als synallagmatischer Leistungsgegenstand („Gegenleistung") vorschnell als ethische Grenzüberschreitung. Die Menschenwürde mündet in diesem Fall in einer Leugnung von Autonomie und läuft Gefahr, das jeweilige ethische Verständnis der Autoren über die Selbstbestimmung des Datensubjekts zu stellen. Die Garantie der Menschenwürde kann und sollte allenfalls in extremen Fällen der Freiheitsbeschränkung herangezogen werden.[281] Insbesondere leidet ihre wichtige Reservefunktion, wenn die Begründung mit der Menschenwürde sich nach kurzer Zeit lediglich als argumentative Abkürzung oder als Ausdruck einer schnell wandelbaren ethischen Überzeugung einer (Richter-)Mehrheit herausstellt.

Die Verarbeitung von personenbezogenen Daten als Grundlage für eine personalisierte Werbeansprache hat typischerweise gerade keine irreversiblen, die Existenz des Datensubjekt gefährdenden Beeinträchtigungen zur Folge (hierzu oben: C.II.2.). Sollte der Gesetzgeber in besonderen Konstellationen zu einer anderen Einschätzung kommen, so stehen ihm dafür spezifischere und damit mildere Mittel zur Verfügung als ein generelles Verbot einer Disposition über die Widerruflichkeit.[282]

Bei der unionsgrundrechtlich garantierten Einwilligung in die Datenverarbeitung handelt es sich qualitativ weder um eine digitale Version des von *John Stuart Mill* angeführten Extrembeispiels des Selbstverkaufs in die Sklaverei noch ist sie mit dem vom ehemaligen europäischen Datenschutzbeauftragten, *Giovanni Buttarelli*, angeführten Organhandel[283] vergleichbar. Weder sind die

---

[280] Ebenso zu undifferenziert: *M. Wagner*, Datenökonomie und Selbstdatenschutz, 2020, S. 345 („Denn die Reversibilität bildet einen der wesentlichen Bausteine des informationellen Schutzes der Menschenwürdegarantie").

[281] Ebenso m. w. N. und mit weiteren Beispielen: *Ohly*, Volenti non fit iniuria, 2002, S. 103 ff.

[282] Bereits aufgrund der bestehenden Schwierigkeiten bei der Abgrenzung zwischen personenbezogenen und besonders sensiblen personenbezogenen Daten (hierzu oben Kapitel 2 C.I.3.), ist es nicht sinnvoll, eine Disposition über die freie Widerruflichkeit im Fall einer Verarbeitung von besonders sensiblen personenbezogen Daten *per se* auszuschließen.

[283] Rede von *Giovanni Buttarelli* (EU-Datenschutz-Beauftragter), verfügbar unter https://

Folgen einer lediglich vorübergehend nicht frei widerruflichen Einwilligung derart gravierend noch sind sie irreversibel (vgl. Art. 17 und Art. 20 DS-GVO).

Im Gegenteil: Soweit Art. 7 Abs. 3 S. 1 DS-GVO auch eine zeitweise Disposition über die Widerruflichkeit der Einwilligung durch unternehmerisch handelnde Datensubjekte ausschließt, greift die Vorschrift in unverhältnismäßiger Weise in die unternehmerische (Vertrags-)Freiheit ein.[284] Art. 7 Abs. 3 S. 1 DS-GVO ist ohne eine teleologische Reduktion – jedenfalls im B2B-Verhältnis – gemäß Art. 16 i. V. m. Art. 52 Abs. 1 S. 2 GRCh primärrechtswidrig.[285]

edps.europa.eu/sites/edp/files/publication/17-01-12_digital_content_directive_sd_en.pdf, zuletzt abgerufen am 19.05.2022.

[284] Insbesondere ist „die Erziehung zu einem tugendhaften Leben […] nicht Aufgabe des Privatrechts": *Ohly*, Volenti non fit iniuria, 2002, S. 431. Eine Aufgabe des Privatrechts darin sehend, der Kommerzialisierung von Persönlichkeitsaspekten entgegenzuwirken: *Schack*, JZ 2000, 1060 (1062); *Peifer*, Individualität im Zivilrecht, 2001, S. 292 f.

[285] Ebenso: *Klement*, in: Simitis/Hornung/Spiecker gen. Döhmann (Hrsg.), Datenschutzrecht, 2019, Art. 7, Rn. 92.

5. Kapitel

Stufenmodell der Erlaubnistatbestände

In den vorausgegangenen Kapiteln wurde das nachfolgend vorgeschlagene Stufenmodell der Erlaubnistatbestände bereits mehrfach angedeutet. Als Quintessenz der Analyse lässt sich ein Stufenmodell der datenschutzrechtlichen Erlaubnistatbestände ableiten,[1] wobei in diesem Zusammenhang nochmals die wesentlichen Argumente genannt werden, die bereits in Kapitel 2–4 detailliert begründet wurden. Dieses Stufenmodell verwirklicht die abgestützte informationelle Privatautonomie, ermöglicht die geforderte „Ertüchtigung der Einwilligung“[2] und korrigiert im Wege der unionsgrundrechtskonformen Auslegung nachträglich die „fehlende vertragsrechtliche Unterfütterung“ der DS-GVO.[3] Das nachfolgend vorgeschlagene Stufenmodell ist durch eine Zunahme an informationeller Privatautonomie geprägt. Das Ziel der Ermöglichung von informationeller Privatautonomie beeinflusst auf allen drei Stufen die jeweiligen Anforderungen an die Rechtsmäßigkeit der Datenverarbeitung.

Das Stufenmodell beginnt auf der untersten Stufe mit der Interessenabwägung (Art. 6 Abs. 1 lit. f DS-GVO) und somit mit demjenigen Erlaubnistatbestand, der am wenigsten geeignet ist, die informationelle Privatautonomie zu gewährleisten. Um seine informationelle Privatautonomie auszuüben, muss das Datensubjekt einer Datenverarbeitung auf Grundlage der Interessenabwägung gemäß Art. 21 Abs. 1 DS-GVO widersprechen. Weil Art. 6 Abs. 1 lit. f DS-GVO somit einen aktiven *Opt-Out* voraussetzt, sollte die Interessenabwägung – diametral zur derzeitigen Praxis[4] – restriktiv ausgelegt und angewendet werden (A).

Auf der nächsten Stufe folgt die vertragsakzessorische Datenverarbeitung (Art. 6 Abs. 1 lit. b DS-GVO). Die Datenverarbeitung beruht in diesem Fall immerhin mittelbar auf derjenigen Willenserklärung des Datensubjekts, die zum Vertragsschluss geführt hat. Deshalb verwirklicht Art. 6 Abs. 1 lit. b DS-GVO die informationelle Privatautonomie akzessorisch zur allgemeinen Vertragsautonomie. Dennoch ist der Anwendungsbereich des Erlaubnistatbestands deshalb eng begrenzt, weil die Datenverarbeitung zur Vertragserfüllung gerade erforderlich sein muss.

---

[1] Dieses findet sich in sehr groben Zügen auch in dem Beitrag: *Sattler*, in: Lohsse/Schulze/Staudenmayer (Hrsg.), Data as Counter-Performance? 2020, S. 223 (245).

[2] Mit dieser Forderung: *Leistner/Antoine/Sagstetter*, Big Data, 2021, S. 403.

[3] *Staudenmayer*, ZEuP 2019, 663 (676).

[4] Hierzu: *Leistner/Antoine/Sagstetter*, Big Data, 2021, S. 280.

Während eine Datenverarbeitung gemäß Art. 6 Abs. 1 lit. b DS-GVO eine *rechtsgeschäftliche* Grundlage hat, beruht die Generalklausel der Interessenabwägung gemäß Art. 6 Abs. 1 lit. f DS-GVO auf einem *gesetzlichen* Erlaubnistatbestand. Insofern stehen beide Tatbestände streng genommen nur dann in einem Subsidiaritätsverhältnis zueinander, wenn zwischen Datensubjekt und Verantwortlichem ein Vertrag besteht.

Um der informationellen Privatautonomie des Datensubjekts Vorrang einzuräumen, sollte der Erlaubnistatbestand des Art. 6 Abs. 1 lit. b DS-GVO – wie in Kapitel 3 D. ausgeführt – deshalb restriktiv ausgelegt werden, weil anderenfalls die detaillierteren Anforderungen an die Einwilligung über die in Art. 6 Abs. 1 lit. b DS-GVO enthaltene Öffnung für das nationale Schuldrecht unterlaufen werden könnten und auf diesem Weg weder ein unionsweit einheitliches Schutzniveau noch ein freier Verkehr personenbezogener Daten im Binnenmarkt erreicht werden können (B).

Weil die Möglichkeit in eine Datenverarbeitung einzuwilligen durch Art. 8 Abs. 2 S. 1 GRCh unionsgrundrechtlich garantiert ist und die Einwilligung die Entscheidungsfreiheit und die Präferenzen des Datensubjekts in den Mittelpunkt stellt, steht die Einwilligung auf der obersten Stufe der (abgestützten) informationellen Privatautonomie. Sie muss aber nach hier vertretener Ansicht zusätzlich mit Hilfe einer primärrechtskonformen Auslegung von Art. 7 Abs. 4 DS-GVO und einer teleologischen Reduktion von Art. 7 Abs. 3 S. 1 DS-GVO durch die Judikative flexibilisiert werden. Der europäische Gesetzgeber hat bei Verabschiedung der DS-GVO deren Konsequenzen für die Verwertung der vermögenswerten Bestandteile der Persönlichkeitsrechte übersehen und eine jederzeitige und vertraglich nicht abdingbare Widerruflichkeit der Einwilligung würde die Vertragsfreiheit der Verantwortlichen und Datensubjekte unangemessen beschränken und deshalb gegen den Verhältnismäßigkeitsgrundsatz verstoßen (C). Abschließend werden die herausgearbeiteten Besonderheiten des Stufenmodells der Erlaubnistatbestände in einem Überblick zusammengefasst (D).

A. Erste Stufe: Enge Auslegung der Interessenabwägung

Im Privatrechtsverhältnis führt eine Datenverarbeitung auf Grundlage einer Interessenabwägung gemäß Art. 6 Abs. 1 lit. f DS-GVO zu einem starken Ausmaß an Heteronomie. Deshalb dient die Interessenabwägung nach hier vertretener Auffassung als Auffangtatbestand (I).[5] Zudem steht die derzeitige Rege-

[5] Diese Subsidiarität verhindert jedoch nicht, dass Art. 6 Abs. 1 lit. f DS-GVO ein Rückschritt zu vorherigen, spezifischeren Regelungen des nationalen Rechts ist: *Marsch*, Das Europäische Datenschutzgrundrecht, 2018, S. 267/372.

lung vor mehreren wesentlichen Herausforderungen. Paradoxerweise ist Art. 6 Abs. 1 lit. f DS-GVO teilweise zu weit und teilweise zu eng geraten. Soweit der Erlaubnistatbestand der Interessenabwägung zu eng geraten ist, sollte Art. 6 Abs. 1 lit. f DS-GVO *de lege ferenda* erweitert werden.[6] Dies betrifft insbesondere die Verarbeitung von besonders sensiblen personenbezogen Daten, wenn die eigentlich vorrangige Einwilligung nicht oder nur unter unverhältnismäßigem Aufwand erreichbar ist (II).

I. Art. 6 Abs. 1 lit. f DS-GVO als Schrittmacher

Die Subsidiarität von Art. 6 Abs. 1 lit. f DS-GVO gegenüber einer vertragsakzessorischen Datenverarbeitung und gegenüber der Einwilligung beruht – nach hier vertretener Auffassung[7] – auf der Grundannahme, dass die Willensbekundungen eines Datensubjekts, die von einem Verantwortlichen unter verhältnismäßigem Aufwand zu erreichen ist, grundsätzlich auch eingeholt werden sollte.[8]

Obwohl die berechtigten Interessen eines Verantwortlichen oder eines Dritten rechtliche,[9] wirtschaftliche oder immaterielle Interessen sein können,[10] sollte eine Subsidiarität gegenüber der Einwilligung jedenfalls dann greifen, wenn die Datenverarbeitung eigenständigen kommerziellen Interessen des Verantwortlichen oder Dritter dient.[11] In diesem Fall kommt eine Verarbeitung

---

[6] Hierzu: Kapitel 2 C.I.3.

[7] Oben Kapitel 2 D.

[8] Offen ist insoweit weiterhin, ob die (künftige) ePrivacy-VO im Kontext der personalisierten Werbung auf Grundlage von Cookies Ausnahmen zur Notwendigkeit einer Einwilligung vorsieht, vgl. ErwG 21 des Vorschlags der EU-Kommission für eine Verordnung über die Achtung des Privatlebens und den Schutz personenbezogener Daten in der elektronischen Kommunikation und zur Aufhebung der Richtlinie 2002/58/EG, COM(2017) 10 final; siehe dazu die Stellungnahme: *Artikel-29-Datenschutzgruppe*, Opinion 01/2017 on the Proposed Regulation for the ePrivacy Regulation (2002/58/EC), WP 247, 2017; ferner *Engeler/Felber*, ZD 2017, 251; *Maier/Schaller*, ZD 2017, 373.

[9] Zur Vorgängernorm des Art. 7 lit. f Datenschutz-RL: *EuGH*, Urt. v. 04.05.2017, C-13/16 = EuZW 2017, 912 – *Rīgas satiksme*; für die Gewährleistung von IT-Sicherheit als ein legitimer Zweck: *EuGH*, Urt. v. 19.10.2016, C-582/14, NJW 2016, 3579 (3580) – *Breyer/Deutschland*; sowie ErwG 49 S. 1 DS-GVO.

[10] Vgl. *Artikel-29-Datenschutzgruppe*, Stellungnahme 06/2014 zum Begriff des berechtigten Interesses des für die Verarbeitung Verantwortlichen gemäß Artikel 7 der Richtlinie 95/46/EG, WP217, 09.04.2014, S. 31 f.

[11] So für §§ 22 f. KUG und Art. 6 Abs. 1 lit. f DS-GVO zuletzt der BGH im Rahmen der Prüfung der Wiederholungsgefahr für einen Unterlassungsanspruch wegen Verletzung von § 22 KUG: *BGH*, Urt. v. 21.01.2021, I ZR 207/19 = GRUR 2021, 643 (Rn. 21–24) – *Urlaubslotto*. Hierbei bestätigte der *BGH* die Bewertung der Vorinstanz dahingehend, dass für eine Abwägung gemäß Art. 6 Abs. 1 lit. f DS-GVO keine anderen Interessen und grundrechtlich geschützten Positionen einzustellen seien als in eine Abwägung am Maßstab der §§ 22, 23 KUG, wobei es nicht auf die Grundrechte des Grundgesetzes, sondern die vorrangig anzuwendende GRCh ankomme: ebda., Rn. 38 ff.

auf Grundlage von Art. 6 Abs. 1 lit. b DS-GVO – nach hier vertretener Ansicht[12] – ebenfalls nicht in Betracht.

Die Einwilligung ist – trotz der bekannten kognitiven Defizite von Menschen[13] – das vorrangige Mittel zur Verwirklichung und Ausübung von informationeller Privatautonomie und ermöglicht grundsätzlich eine Gestaltung der rechtlichen Beziehungen zum Verantwortlichen. Zudem setzt die Subsidiarität der Interessenabwägung einen Anreiz dafür, den Willen des Datensubjekts als Ausdruck von informationeller Privatautonomie ernst zu nehmen, so dass es im Interesse der Verantwortlichen ist, Datensubjekte frühzeitig – insbesondere in Form eines *Kontroll-Cockpit* zur Abgabe datenschutzrechtlicher Erklärungen[14] – einzubeziehen, um selbst von den Vorteilen einer – vorübergehend bindenden – Einwilligung zu profitieren.

Wie bereits ausgeführt, sollte die Interessenabwägung im Privatrechtsverhältnis weitgehend auf die Funktion eines Schrittmachers reduziert werden. Solange es tatsächlich und rechtlich ausgeschlossen ist, dass alle Datensubjekte dazu verpflichtet werden, über standardisierte Schnittstellen – beispielsweise im Smartphone – ständig und überall die eigene Datenschutzpräferenz zu kommunizieren, bleiben sowohl die Möglichkeiten zur automatisierten Einwilligung als auch zum präventiven Widerspruch gemäß Art. 21 DS-GVO begrenzt. Infolgedessen wird die Anwendung von Art. 6 Abs. 1 lit. f DS-GVO durch die Gerichte auf absehbare Zeit festlegen, welches Mindestmaß an Datenverarbeitungen durch Privatrechtsubjekte[15] ein Datensubjekt als Mitglied einer sozio-technischen Gesellschaft im Sinne einer Standardauswahl erwarten muss.[16]

Als Kehrseite ihrer Flexibilität, die eine interessengerechte Lösung nach den jeweiligen Umständen des Einzelfalls ermöglicht, birgt die Auslegung und Anwendung von Art. 6 Abs. 1 lit. f DS-GVO großes Potenzial für Rechtsunsicherheit und kann sowohl den Schutz der Datensubjekte als auch den freien Verkehr personenbezogener Daten im Binnenmarkt empfindlich gefährden. Weil über die Interessenabwägung gemäß Art. 6 Abs. 1 lit. f DS-GVO zunächst der Verantwortliche in einem internen Prozess und im Anschluss hieran Datenschutz-

---

[12] M.w.N. oben Kapitel 3 D.

[13] Hierzu: *Simitis*, NJW 1998, 2573 (2476); m. w. N. *Rogosch*, Die Einwilligung im Datenschutzrecht, 2013, S. 17 f.; *Radlanski*, Das Konzept der Einwilligung in der datenschutzrechtlichen Realität, S. 147, 212, 239; *Buchner/Kühling*, in: Kühling/Buchner (Hrsg.), DS-GVO, 2020, Art. 7, Rn. 10; ähnlich: *Veil*, NJW 2018, 3337 (3344).

[14] Hierzu unten Kapitel 6 B.

[15] Gemäß Art. 6 Abs. 1 S. 2 DS-GVO steht die Interessenabwägung nicht für die von Behörden in Erfüllung ihrer Aufgaben vorgenommene Verarbeitung zur Verfügung.

[16] Auch der Vorschlag eines „Rechts auf datenerhebungsfreie Produkte" als individuelle Exit-Option (*Becker*, JZ 2017, 171 (175 ff.); *Hacker*, Datenprivatrecht, 2020, S. 642 f.) findet durch die Entwicklungen des IoT – jedenfalls im öffentlichen Raum und im Kontext von Beschäftigungsverhältnissen – schnell seine Grenzen. Infolgedessen müsste dieser Vorschlag durch ein „Recht auf datenerhebungsfreie Räumlichkeiten" ergänzt werden. In diese Richtung: *Raue*, NJW 2019, 2425 (2426 f.).

behörden und Gerichte über die (mutmaßlichen) Interessen von Datensubjekten entscheiden, sollte dessen Anwendung primär dann in Betracht kommen, wenn eine Einwilligung unerreichbar oder mit einem unverhältnismäßigen Aufwand verbunden ist.[17]

Infolgedessen kommt eine Interessenabwägung insbesondere immer dann zur Anwendung, wenn zwar personenbezogene Daten verarbeitet werden, diese Verarbeitung aber aufgrund der Art der Daten, der Vielzahl der Personenbezüge (Multi-Relationalität), der Dauer der Datenverarbeitung und des Verarbeitungszwecks typischerweise keine hohen Risiken für die individuellen Datensubjekte auslöst, während eine vorherige Einholung der Einwilligung die Verarbeitung zusätzlicher personenbezogener Daten voraussetzt, so dass sich entweder das Verarbeitungsrisiko infolgedessen erhöhen oder diese Einwilligungseinholung – beispielsweise aufgrund der Multi-Relationalität der Daten – für den Verantwortlichen einen Aufwand verursachen würde, der zum Risiko und Zweck der Datenverarbeitung offensichtlich außer Verhältnis steht.

Gegen diese allgemeine Subsidiarität der Interessenabwägung gegenüber der Einwilligung lässt sich zwar einwenden, dass damit der Anwendungsbereich des Art. 6 Abs. 1 lit. f DS-GVO ebenso unbestimmt ist wie die eigentliche Interessenabwägung. Tatsächlich folgt diese Rechtsunsicherheit aber bereits aus dem unbestimmten und flexiblen Tatbestand. Zudem hat der europäische Gesetzgeber die Möglichkeit zur Einwilligung zwar gemäß Art. 8 Abs. 2 S. 1 GRCh garantiert, aber keine explizite Vorrangregelung getroffen. Infolgedessen besteht ohnehin die Notwendigkeit, die Erlaubnistatbestände des Art. 6 Abs. 1 DS-GVO voneinander abzugrenzen. Zugleich hat diese Subsidiarität der Interessenabwägung gegenüber der Einwilligung den Vorteil, dass sie dem Verantwortlichen eine eindeutige Struktur an die Hand gibt. Ist er sich unsicher, ob eine Interessenabwägung ausreicht und ist die Datenverarbeitung für den Verantwortlichen von besonderem Interesse, so steht ihm die Einwilligung als rechtssicherer Weg offen, zumal die – hier vertretene – Möglichkeit zum zeitweisen Ausschluss der sog. freien Widerruflichkeit der Einwilligung die Rechtssicherheit und damit die Planungsmöglichkeit für den Verantwortlichen grundlegend erhöht.

II. Wesentliche Herausforderungen für die Interessenabwägung

Wie bereits in Kapitel 2 ausgeführt, ist die Interessenabwägung gemäß Art. 6 Abs. 1 lit. f DS-GVO zugleich zu weit und zu eng geraten. Die Vorschrift ist zu weit geraten, sofern sie eine Datenverarbeitung im Rahmen eines Profiling für personalisierte Werbung ermöglichen kann und diese Werbung auf Grundlage

[17] Großzügiger: *Leistner/Antoine/Sagsetter*, Big Data, 2021, S. 281.

eines Werbenetzwerks erfolgt (1). Zudem sollte die Informationspflicht über das Widerspruchsrecht im Einzelfall restriktiv ausgelegt werden (2).

Dagegen ist Art. 6 Abs. 1 lit. f DS-GVO zu eng ausgefallen, weil er nicht auf die Verarbeitung von besonders sensiblen personenbezogenen Daten angewendet werden kann (3). Während die beiden ersten Herausforderungen durch eine restriktive Auslegung von Art. 6 Abs. 1 lit. f bzw. Art. 21 Abs. 4 DS-GVO gemeistert werden können, setzt letztere eine Änderung der DS-GVO voraus.

1. Keine personalisierte Werbung durch Werbenetzwerke

Wie in Kapitel 2 analysiert, ist Art. 6 Abs. 1 lit. f DS-GVO ein Rückschritt gegenüber der deutschen Rechtslage nach dem BDSG a. F. Der Vorteil der Flexibilität der generalklauselartigen Interessenabwägung wurde nicht durch Maßnahmen ergänzt, die den Nachteil dieser Flexibilität in Form von großer Rechtsunsicherheit ausgleichen. Es fehlt eine Liste an Regelbeispielen oder eine Liste mit Kriterien, die den Anwendungsbereich des Art. 6 Abs. 1 lit. f DS-GVO konkretisieren.

Die Suche nach Anhaltspunkten, die dabei helfen könnten, den Anwendungsbereich der Interessenabwägung für das Privatrechtsverhältnis zu präzisieren, führt über einen Umkehrschluss zu Art. 21 Abs. 2 Hs. 2 DS-GVO und über den ErwG 47 S. 7 DS-GVO zur Datenverarbeitung für Direktwerbung, einschließlich Profiling. Infolgedessen scheint die Interessenabwägung auf den ersten Blick ausgerechnet dann eine Rechtsgrundlage für eine Datenverarbeitung zu bieten, wenn mit Hilfe von *tracking*-Werkzeugen, beispielsweise *Cookies*, Nutzerprofile erstellt werden und diese für personalisierte Werbung genutzt werden.

Wie in Kapitel 2 ausführlich begründet, sollte der Begriff der Direktwerbung, der auf dem technischen Stand vor über zwei Jahrzehnten in Art. 13 ePrivacy-RL (2002) eingeführt wurde, restriktiv ausgelegt werden. Die Vorarbeiten zu Art. 13 ePrivacy-RL und damit auch der hieraus hervorgegangene Begriff der Direktwerbung entstammen (auch) technologisch betrachtet einem anderen Jahrtausend. Die Möglichkeiten der Verhaltensbeobachtung auf Grundlage der aktuellen *tracking*-Werkzeuge, die ein über die Grenzen von Telemedien und Endeinrichtungen hinausgehendes Profiling ermöglichen, sind mit denjenigen Sachverhalten nicht mehr vergleichbar, die dem Gesetzgeber bei Verabschiedung der ePrivacy-RL mit dem Begriff der Direktwerbung ursprünglich vor Augen standen.

Eine restriktive Auslegung von Direktwerbung, die diese Entwicklungsgeschichte des Begriffs berücksichtigt, findet eine Stütze in ErwG 47 S. 2 DS-GVO. Hiernach ist eine bereits bestehende Kundenbeziehung zwischen Datensubjekt und Verantwortlichen ein wesentliches Kriterium, das eine Datenverarbeitung auf Grundlage einer Interessenabwägung begünstigen kann.

Auch die *EU-Kommission* geht (mittlerweile) von einem engen Verständnis des Begriffs der Direktwerbung auf Grundlage von Profiling aus. Aus ErwG 52 DMA-Vorschlag[18] geht hervor, dass insbesondere sehr große Plattformen die wesentlichen Kriterien für eine personalisierte Werbung gegenüber den Datensubjekten – ausdrücklich vor Erteilung der Einwilligung – offenlegen sollen. Gemäß ErwG 61 sollen jedenfalls *Gatekeeper* i. S. d. DMA-Vorschlags im Rahmen des Ersuchens um diese Einwilligung für ein Profiling besondere Transparenzpflichten beachten. Zudem soll die Zusammenführung von personenbezogenen Daten aus den zentralen Plattformdiensten eines *Gatekeepers* mit personenbezogenen Daten aus anderen von ihm oder von Dritten angebotenen Diensten nach Ansicht der *EU-Kommission* zukünftig ausschließlich auf Grundlage eine Einwilligung möglich sein, Art. 5 lit. a DMA-Vorschlag.

Damit sprechen die Entstehungsgeschichte des Begriffs „Direktwerbung", der ErwG 47 S. 2 DS-GVO und der Fokus auf die Einwilligung im DMA-Vorschlag dafür, dass die Interessenabwägung gemäß Art. 6 Abs. 1 lit. f DS-GVO nur dann als Rechtsgrundlage für eine auf Profiling basierende Direktwerbung in Betracht kommt, wenn diese ausschließlich innerhalb einer bereits bestehenden Kundenbeziehung zwischen *dem* Verantwortlichen und dem Datensubjekt erfolgt und auf *gleiche und ähnliche* Produkte *dieses* Verantwortlichen beschränkt ist.

Dagegen steht Art. 6 Abs. 1 lit. f DS-GVO nicht für eine personalisierte Werbung zur Verfügung, die auf den aktuell gängigen Werbenetzwerke – beispielsweise *Facebook Custom Audience* oder der jeweiligen Werbe-ID von *Apple* und *Alphabet* (*Google*) beruhen. Dies gilt selbst dann, wenn an diesem Werbenetzwerk nur (gemeinsam) Verantwortliche beteiligt wären, zu denen das Datensubjekt jeweils eine selbstständige Kundenbeziehung unterhält. Derartige Werbenetzwerke sind für eine Datenverarbeitung als Grundlage von personalisierter Werbung – unabhängig vom Status des Verantwortlichen als *Gatekeeper* i. S. d. DMA-Vorschlags – stets auf eine jeweils eigenständige Einwilligung des Datensubjekts gegenüber den jeweils (gemeinsam) Verantwortlichen angewiesen.

Insofern kommt der *VGH München*[19] im Fall von *Facebook Custom Audience* im Rahmen der Interessenabwägung zwar zum richtigen Ergebnis, er hätte aber – nach hier vertretener Ansicht – keine Interessenabwägung prüfen müssen. Sinnvoll wäre es stattdessen gewesen, dem *EuGH* die Frage vorzulegen, ob für eine solche Datenverarbeitung überhaupt eine Interessenabwägung in Betracht kommt oder aber – wie hier vertreten und durch den DMA-Vorschlag bestätigt – eine Einwilligung erforderlich ist.

---

[18] Vorschlag der EU-Kommission für eine Verordnung über bestreitbare und faire Märkte im digitalen Sektor (Gesetz über digitale Märkte, kurz: DMA-Vorschlag), v. 15.12.2020, COM(2020) 842 final.

[19] *VGH München*, Beschl. v. 26.09.2018, 5 CS 18.1157 = NVwZ 2019, 171 (Rn. 27 f.).

2. Begrenzung der Informationspflicht aus Art. 21 Abs. 4 DS-GVO

Die gemäß Art. 21 Abs. 4 DS-GVO bestehende Informationspflicht über das Widerspruchsrecht ist im Einzelfall zu weit geraten. Weil die Interessenabwägung gerade als Auffangtatbestand in Betracht kommt, wenn eine Einwilligung des Datensubjekts unerreichbar oder mit einem im Verhältnis zur Datenverarbeitung unangemessenen Aufwand verbunden ist, hat dies auch Auswirkungen auf die Pflicht des Verantwortlichen, die Datensubjekte über deren Widerspruchsrecht zu informieren.

Gemäß Art. 21 Abs. 4 DS-GVO müssen Verantwortliche die Datensubjekte „spätestens zum Zeitpunkt der ersten Kommunikation" ausdrücklich auf deren Widerspruchsrecht hinweisen. Diese Vorgabe ist bestenfalls vage und weder Art. 21 Abs. 4 DS-GVO noch die Erwägungsgründe präzisieren den zeitlichen Zusammenhang zwischen der Datenverarbeitung und der Informationspflicht des Verantwortlichen.

Zunächst legt der Wortlaut des Art. 21 Abs. 4 DS-GVO nahe, dass der Verantwortliche das Datensubjekt jederzeit über das Widerspruchsrecht informieren *darf*, dies aber spätestens mit der ersten Kommunikation tun *muss*. Diese Wortwahl, die ein zeitliches Moment („spätestens") mit einem Verhalten („Kommunikation") kombiniert, legt ein Verständnis nahe, wonach der Begriff der Kommunikation einen zweiseitigen Informationsaustausch meint, der unabhängig von der Übermittlung der Information über das Widerspruchsrecht stattfindet. Nur bei dieser Interpretation ergibt es einen Sinn, dass der Verantwortliche das Datensubjekt jedenfalls *anlässlich dieser Kommunikation* mit einem anderen Inhalt auch darüber informieren muss, inwieweit dem Datensubjekt ein Widerspruchsrecht zusteht.

Es ist offenkundig, dass ein Verantwortlicher die Kommunikation mit dem Datensubjekt nicht bewusst vermeiden darf, um seine Pflicht gemäß Art. 21 Abs. 4 DS-GVO zeitlich hinauszuzögern oder ganz zu vermeiden. Dies folgt bereits aus den Grundsätzen der Transparenz und der Verarbeitung nach Treu und Glauben, Art. 5 Abs. 1 lit. a DS-GVO. Damit dürfte Art. 21 Abs. 4 DS-GVO im Ergebnis so zu verstehen sein, dass der Verantwortliche das Datensubjekt über dessen Widerspruchsrecht unverzüglich und ohne schuldhaftes Zögern informieren muss. Erfolgt diese Information nicht als eigenständiger Hinweis, so ist die Grenze der Unverzüglichkeit jedenfalls überschritten, sobald eine anderweitige Kommunikation zwischen Datensubjekt und Verantwortlichem stattfindet und diese nicht zum Anlass genommen wird, um das Datensubjekt sogleich über ein ihm zustehendes Widerspruchsrecht zu informieren.

Weil nach hier vertretener Auffassung eine Datenverarbeitung auf Grundlage einer Interessenabwägung insbesondere dann in Betracht kommt, wenn eine Einwilligung unerreichbar oder – insbesondere aufgrund einer Multi-Relationalität der Daten – jedenfalls im Verhältnis zum individuellen Risiko mit unan-

gemessenen Anstrengungen verbunden wäre, sollte diese Unerreichbarkeit oder Unverhältnismäßigkeit der Einwilligung auch Auswirkungen auf die Erfüllung der Informationspflicht gemäß Art. 21 Abs. 4 DS-GVO haben.

Wie bereits ausgeführt,[20] gehört es zu den aktuell größten Herausforderungen für die Verwirklichung der informationellen Privatautonomie, dass mit dem Fortschreiten des IoT eine ubiquitäre Datenverarbeitung einhergeht. Infolgedessen werden zunehmend Daten verarbeitet, ohne dass es einem Verantwortlichen zumutbar wäre, jedes Datensubjekt über diese Datenverarbeitung und das gemäß Art. 21 Abs. 4 DS-GVO bestehende Widerspruchsrecht zu informieren. Die Bedingung von vernetzten Endeinrichtung, beispielsweise industriellen Roboter, Sprachassistenten wie *Alexa* oder *Echo* oder komplexen Infotainment-Systemen in Kfz, soll schnell und mühelos möglich sein. Deshalb werden die jeweils berechtigten Nutzer dieser Endeinrichtungen nicht mehr zur Eingabe einer Benutzerkennung und eines Passworts aufgefordert. Stattdessen erfolgen sowohl die Prüfung der Nutzungsberechtigung als auch die anschließende Steuerung der Endeinrichtung in wachsendem Ausmaß über die Sprache, die Mimik und die Gestik von Datensubjekten.[21]

Dies hat zur Folge, dass die Sensoren von solchen vernetzten Endeinrichtungen, einschließlich Kamera und Mikrophon, permanent sehr kurze automatisierte Bild- oder Sprachabgleiche vornehmen müssen und diese Daten zumindest für die Dauer des Abgleichs mit den berechtigten Nutzern verarbeiten, bevor diese gemäß Art. 17 Abs. 1 lit. a DS-GVO unverzüglich wieder zu löschen sind. Soweit diese Datenverarbeitung ausschließlich dem Abgleich und damit der Feststellung der Nutzungsberechtigung dient, kann diese Verarbeitung der personenbezogenen Daten auf Grundlage einer Interessenabwägung erfolgen, soweit die Verarbeitung gerade (besonders sensible) personenbezogene Daten betrifft, die nicht den jeweils zur Nutzung berechtigten Vertragspartner,[22] sondern Dritte identifizieren.[23]

Soweit dieser Abgleich der physiognomischen Eigenarten oder Sprache eines Datensubjekts nur kurzzeitig zur Verifizierung der Nutzungsberechtigung erfolgt, kann es auf eine Informationspflicht gemäß Art. 21 Abs. 4 DS-GVO nicht

---

[20] Oben Kapitel 2 C.I.3.b.

[21] Laut einer Studie nutzte ein Viertel der Deutschen im Jahr 2019 sprachaktivierte Assistenten: *Arnold u. a.*, Any Sirious Concerns Yet? – An Empirical Analysis of Voice Assistants' Impact on Consumer Behavior and Assessment of Emerging Policy Challenges, Working Paper, 2019, S. 8 (https://ssrn.com/abstract=3426809, zuletzt abgerufen am 19.05.2022).

[22] Insoweit kommt Art. 6 Abs. 1 lit. b DS-GVO zur Anwendung.

[23] Soweit die Anbieter einer solchen Endeinrichtung, diese Datenerhebungen jedoch nutzen, um die Qualität der eigenen Spracherkennungs-Software zu verbessern, dient diese Datenverarbeitung einem eigenständigen kommerziellen Interesse des Verantwortlichen, so dass es nach hier vertretener Auffassung der Einwilligung der Datensubjekte bedarf. Hierzu: *Wissenschaftliche Dienste* – Deutscher Bundestag, Zulässigkeit der Transkribierung und Auswertung von Mitschnitten der Sprachsoftware „Alexa" durch Amazon, WD 10 – 3000 – 032/19, Sachstand, 2019, S. 9.

mehr ankommen.[24] Diese Pflicht kann entweder entfallen, indem man Art. 21 Abs. 4 DS-GVO teleologisch reduziert, weil eine nachträgliche Information – d. h. nach dem Löschen der Daten – als bloße Förmelei überflüssig ist. Alternativ besteht die Möglichkeit, die Informationspflicht bereits deshalb entfallen zu lassen, weil es bereits an derjenigen (anderen) Kommunikation zwischen Verantwortlichem und Datensubjekt fehlt, an welche die Informationspflicht des Art. 21 Abs. 4 DS-GVO (spätestens) anknüpft.

3. Sensible personenbezogene Daten und Interessenabwägung

Bereits in Kapitel 2 wurde herausgearbeitet, dass mit der zunehmenden Verbreitung von vernetzten Endeinrichtungen des sog. IoT, die durch Sprache, Gestik oder Mimik gesteuert werden, auch das Ausmaß der Verarbeitung von personenbezogenen Daten steigt.

Dabei tritt zunehmend der Sachverhalt auf, dass ein Datensubjekt in Gegenwart von Sensoren über Angelegenheiten spricht, die als besonders sensible personenbezogene Daten dem besonderen Schutz gemäß Art. 9 Abs. 1 DS-GVO unterfallen. Zumindest sofern das Datensubjekt aus Sicht eines vernünftigen Erwartungshorizonts davon ausgehen muss, dass es sich zu diesem Zeitpunkt im Empfangsbereich von sprachgesteuerten Endeinrichtungen befindet, liegt es nahe, über eine künftige Ergänzung von Art. 9 Abs. 2 DS-GVO nachzudenken.[25]

Eine solche Ergänzung des Art. 9 Abs. 2 DS-GVO um eine Möglichkeit der Interessenabwägung ist nach hier vertretener Auffassung der transparentere Weg als der alternative Vorschlag, wonach bereits der Begriff der besonders sensiblen personenbezogenen Daten in Art. 9 Abs. 1 DS-GVO teleologisch reduziert werden soll, indem das ungeschriebene und zudem schwer nachweisbare subjektive Tatbestandsmerkmal der Auswertungsabsicht des Verantwortlichen hineingelesen wird.[26] Gleichwohl bietet letztere Möglichkeit eine Lösung, die *de lege lata* gegebenenfalls offensteht, bis eine Anpassung der DS-GVO erfolgt.

Die zweite notwendige Erweiterung des Anwendungsbereichs der Interessenabwägung betrifft die Verarbeitung von besonders sensiblen personenbezogenen Daten als Trainingsdaten für ML.[27] Trotz des Vorrangs der Einwilligung

---

[24] A. A. (wohl) *Martini*, in: Paal/Pauly (Hrsg.), DS-GVO, 2021, Art. 21, Rn. 66 (Hinweis hat wegen Art. 13 Abs. 2 lit. b DS-GVO bereits „zum Zeitpunkt der Erhebung" zu erfolgen.

[25] Nicht sinnvoll ist ein nationaler Alleingang, wie ihn der deutsche Gesetzgeber mit § 27 Abs. 1 BDSG für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke beschritten hat.

[26] Hierfür: *Schulz*, in: Gola (Hrsg.), DS-GVO, Art. 9, Rn. 11; *Scholz*, in: Simitis/Hornung/Spiecker gen. Döhmann (Hrsg.), Datenschutzrecht, 2019, Anhang 1 zu Art. 6, Rn. 101. Diese Möglichkeit ausdrücklich als Abgrenzungskriterium erwähnend: *OLG Düsseldorf*, Vorlagebeschl. v. 24.03.2021, Kart 2/19 (V) = GRUR-RS 8370 (Rn. 38 „Klärungsbedürftig ist auch, ob die Verwendungsabsicht für die Beurteilung von Bedeutung ist").

[27] Als Argument hierfür kann zudem der in ErwG 159 DS-GVO weite und damit personen- und institutionsunabhängigen Begriff der Forschung i. S. d. DS-GVO herangezogen

sind Konstellationen denkbar, in denen die Einholung einer bestimmten und informierten Einwilligung aufgrund der Anzahl der Datensubjekte (potentielle Multi-Relationalität) unerreichbar ist oder jedenfalls für den ausschließlichen Zweck eines Training von ML unverhältnismäßige Kosten verursacht.[28]

Infolge des weiten Begriffs der besonders sensiblen personenbezogenen Daten und aufgrund der technischen Grenzen einer rechtssicheren Anonymisierung im Kontext von ML, ist es nach hier vertretener Ansicht erforderlich, eine Datenverarbeitung von besonders sensiblen personenbezogenen Daten für das Trainieren von ML zu ermöglichen. Allerdings muss diese Ermöglichung durch strenge Anforderungen an die Datensicherheit, durch technische und organisatorische Maßnahmen und die Einhaltung geeigneter Garantien gemäß Art. 89 Abs. 1 DS-GVO flankiert werden.[29] Zudem ist es notwendig, diese Datenverarbeitung unter strenge behördliche Aufsicht zu stellen.

Die Vorschläge zur Klassifizierung und Zertifizierung, die von der *Datenethikkommission* in ihrer Empfehlung für einen risikoadaptierten Regulierungsansatz in Bezug auf den Einsatz von KI gemacht wurden[30] und die über die insoweit lediglich groben Vorschläge der *EU-Kommission*[31] hinausgehen, lassen sich auf das Trainieren von ML, einschließlich der Verarbeitung von besonders sensiblen personenbezogenen Daten übertragen, solange der Verantwortliche in der Lage und willens ist, das Trainieren von ML technisch, personell und organisatorisch eindeutig von der späteren Anwendung des trainierten Systems zu trennen.

B. Zweite Stufe: Enge Auslegung der Vertragsakzessorietät

Wie bereits erläutert und hier nur kurz zusammengefasst, sprechen überzeugende Gründe dafür, Art. 6 Abs. 1 lit. b DS-GVO restriktiv auszulegen (I). Dennoch bleiben zumindest zwei Konstellationen, die künftig der besonderen Aufmerksamkeit bedürfen.

---

werden: *Spindler*, DB 2016, 937 (939); *Geminn*, DuD 2018, 640 (643); *Roßnagel*, ZD 2019, 157 (159); *Gutachten der Datenethikkommission*, 2019, S. 124.

[28] Einen Hybrid aus einer weiten Einwilligung („meta consent") für die Forschungszwecke und einer Interessenabwägung für anschließende Konkretisierungen andeutend: *Gutachten der Datenethikkommission*, 2019, S. 127: („Wenn die Daten anschließend für ein konkretes Forschungsvorhaben genutzt werden sollen, wird der Datengeber hierüber vorab informiert und erhält die Möglichkeit, dieser konkreten Datennutzung zu widersprechen.").

[29] *Art. 29-Datenschutzgruppe*, Opinion 03/2013 on purpose limitation, S. 28; *Roßnagel*, ZD 2019, 157 (161); zur Auslegung der Zweckkompatibilität i. R. v. Art. 89 Abs. 4 DS-GVO: *Werkmeister/Schwaab*, CR 2019, 85 (86 f.).

[30] *Gutachten der Datenethikkommission*, 2019, S. 173 ff. (177).

[31] Mit der lediglich dreifachen Unterscheidung möglicher KI-Systeme: Vorschlag der EU-Kommission für eine Verordnung zur Festlegung harmonisierter Vorschriften für Künstliche Intelligenz, v. 21.04.2021, COM(2021) 206 final.

Erstens ist bislang noch offen, ob es möglich ist bzw. sein sollte, personenbezogene Daten gemäß Art. 6 Abs. 1 lit. b DS-GVO zu verarbeiten, wenn diese Datenverarbeitung dazu dient, eine Leistung – wie vereinbart – zu personalisieren (II). *Zweitens* könnten die Datenverarbeitungen auf Grundlage von Art. 6 Abs. 1 lit. b DS-GVO künftig zunehmen, sofern eine steigende Anzahl an Dienstleistern bei der Durchführung von Verträgen einbezogen wird (III).

I. Grundsatz: Beschränkung auf unterstützende Verarbeitungen

Wie in Kapitel 3 herausgearbeitet, sprechen zumindest drei Argumente dafür, den Erlaubnistatbestand des Art. 6 Abs. 1 lit. b DS-GVO eng auszulegen. Art. 6 Abs. 1. lit. b DS-GVO ist der Tatbestand mit der geringsten datenschutzrechtlichen Regelungsdichte.[32] Das ist zwar konsequent, weil er gerade auf das Schuldrecht der Mitgliedstaaten verweist.

Allerdings hat dies *erstens* zur Folge, dass die spezifischen und detaillierteren Vorgaben der DS-GVO zur Einwilligung potenziell unterlaufen werden, wenn Art. 6 Abs. 1 lit. b DS-GVO umfangreich zur Anwendung kommt. Dies ist ein wesentliches Argument dafür, selbst dann vom Erfordernis einer Einwilligung auszugehen, wenn diese – aufgrund einer zeitweisen Disposition über die Widerruflichkeit – nach deutscher Dogmatik als schuldrechtliche Gestattung und damit als Vertrag einzuordnen wäre.[33]

Zweitens ist die vereinheitlichende Wirkung der DS-GVO umso geringer, je häufiger Datenverarbeitungen auf Grundlage von Art. 6 Abs. 1 lit. b DS-GVO i. V. m. dem jeweils nationalen Schuldrecht erfolgen.[34] Trotz bestehender unionsweiter Harmonisierung im Bereich des Verbraucherrechts, insbesondere durch die Klausel-RL, hängt die Anwendung von Art. 6 Abs. 1 lit. b DS-GVO von der jeweiligen Auslegung des nationalen Schuldrechts durch die jeweiligen nationalen Datenschutzbehörden und Gerichte ab.[35] Zwar ist es nicht ausge-

---

[32] Es sind insoweit nur die Informationspflichten gemäß Art. 12 ff. DS-GVO als Spezifizierung des Grundsatzes der Transparenz zu beachten.

[33] Dies wurde oben in Kapitel 4 C.III.2 abgelehnt.

[34] Dies etwas vernachlässigend: *Hacker*, Datenprivatrecht, 2020, S. 159/264 f./540; *Bunnenberg*, Privates Datenschutzrecht, 2020, S. 60 f., *Leistner/Antoine/Sagstetter*, Big Data, 2021, S. 266. Letztere sprechen die Problematik jedoch an: S. 268 („Ziel sollte es aber durchaus sein, im Überschneidungsbereich von Vertrags-, Datenschutz- und Verbraucherrecht *wertungsmäßig kohärente Lösungen* zu finden" [Hervorhebung im Original]).

[35] Dann stellt sich die Frage, ob ein Datensubjekt sich nach nationalem Recht zur Leistung von personenbezogenen Daten verpflichten kann und inwieweit die gesetzgeberischen Wertungen aus Art. 7 Abs. 3 und Abs. 4 DS-GVO im nationalen Vertragsrecht zu berücksichtigen sind. Die gleiche Frage stellt sich im Verhältnis zwischen der Geschäftsfähigkeit gemäß §§ 104 ff. BGB und der datenschutzrechtlichen Einwilligungsfähigkeit gemäß Art. 8 DS-GVO. Kurzum: Je häufiger und umfangreicher die Datenverarbeitungen auf Grundlage von Art. 6 Abs. 1 lit. b DS-GVO erfolgt, desto geringer ist die harmonisierende Wirkung der DS-GVO

schlossen, dass diese nationalen Institutionen aufgrund des unionsrechtlichen Äquivalenz- und Effektivitätsgrundsatzes weitreichende Bezüge zu den Grundsätzen der rechtmäßigen Datenverarbeitung herstellen (Art. 5 Abs. 1 DS-GVO) und auf Grundlage häufiger Vorabentscheidungsverfahren zum *EuGH* oder mittels Kohärenzverfahren (Art. 63 ff. DS-GVO) langfristig zu einer angeglichenen Rechtslage bzw. behördlichen Aufsichtspraxis gelangen.

Wahrscheinlicher ist es jedoch, dass nach einer Zeit der disparaten Rechtsentwicklung der freie Verkehr personenbezogener Daten derart beeinträchtigt wird, dass der europäische Gesetzgeber das Schuldrecht der Mitgliedstaaten nicht nur mit Blick auf die Bereitstellung digitaler Produkte (DID-RL), sondern auch hinsichtlich der vertraglichen Aspekte einer Bereitstellung von personenbezogenen Daten als Leistungsgegenstand (voll-)harmonisieren müsste.

Drittens steht Art. 6 Abs. 1 lit. b DS-GVO unter dem Vorbehalt der Verhältnismäßigkeit („soweit zur Erfüllung erforderlich"). Je nach Auslegung dieses Tatbestandsmerkmals durch die nationalen Gerichte und letztlich durch den *EuGH* bleibt die Öffnung der DS-GVO für das jeweilige nationale Schuldrecht wiederum so eng, dass Art. 6 Abs. 1 lit. b DS-GVO keine geeignete Grundlage für die Mitgliedstaaten bietet, um auf dieser Basis einen eigenen schuldrechtlichen Rahmen für solche Verträge zu entwickeln, die personenbezogene Daten als Leistungsgegenstand vorsehen.

Kurzum: Einerseits ist Art. 6 Abs. 1 lit. b DS-GVO aufgrund des Verhältnismäßigkeitsvorbehalts zu eng; unter diesem Vorbehalt der Verhältnismäßigkeit lässt sich kein Wettbewerb zwischen den nationalen schuldrechtlichen Regelungen initiieren, der alternative Modelle für privatrechtliche Datenverträge hervorbringt.[36] Andererseits ist Art. 6 Abs. 1 lit. b DS-GVO so weit, dass die Rechtssicherheit und infolgedessen die Verwirklichung der Ziele aus Art. 1 DS-GVO gefährdet sind.

Dies spricht im Ergebnis dafür, den Anwendungsbereich von Art. 6 Abs. 1 lit. b DS-GVO auf solche Datenverarbeitungen zu begrenzen, die keinen eigenständigen kommerziellen Zweck haben,[37] sondern lediglich zur Erfüllung von solchen vertraglich geschuldeten Leistung erforderlich sind, die gerade nicht durch eine Verarbeitung von personenbezogen Daten geprägt sind.[38] Daten-

---

im Privatrecht und desto weiter in die Ferne rückt der gemäß Art. 1 Abs. 3 DS-GVO angestrebte freie Verkehr von personenbezogenen Daten in der Union.

[36] Zu diesem Vorteil eines Entdeckungsverfahrens, oben, Kapitel 3 B.I.

[37] Gegen eine Anwendbarkeit von Art. 6 Abs. 1 lit. b DS-GVO für den Fall, dass der Verantwortliche mit der Datenverarbeitung einen – grundsätzlich zu vermutenden – kommerziellen Zweck verfolgt: *von Westphalen/Wendehorst*, BB 2016, 2179 (2184 f.); *Wendehorst*, in: Lohsse/Schulze/Staudenmayer (Hrsg.), Data as Counter-Performance – Contract Law 2.0, 2020, 193 (201); *Buchner/Petri*, in: Kühling/Buchner, DS-GVO/BDSG, 3. Aufl. 2020, Art. 6, Rn. 40.

[38] Ebenso: *Langhanke/Schmidt-Kessel*, EuCML 2015, 218 (221), wonach die Funktion von Art. 6 Abs. 1 lit. b DS-GVO darin besteht, Datenverarbeitungen von lediglich unterstützen-

verarbeitungen, die im Rahmen der Vertragsdurchführung üblich und deshalb für Datensubjekte vernünftigerweise zu erwarten sind, werden auch Bestandteil des jeweiligen gedanklichen Mitbewusstsein bei Abschluss des Vertrags. In diesem Fall wäre eine Einwilligung überflüssig.

Infolgedessen dient Art. 6 Abs. 1 lit. b DS-GVO nach hier vertretener Auffassung der Entlastung des Einwilligungstatbestandes und damit indirekt der Entlastung von Verantwortlichen und Datensubjekten. Dagegen kommt Art. 6 Abs. 1 lit. b DS-GVO nicht als Grundlage in Betracht, sofern ein Anbieter digitale Produkte bereitstellt und dieses Angebot durch eine Verwertung von personenbezogenen Daten für eine personalisierte Werbung finanziert.[39] Allerdings hält Art. 6 Abs. 1 lit. b. DS-GVO – trotz dieser restriktiven Auslegung – in zwei Konstellationen noch Herausforderungen bereit.

II. Erste Herausforderung: Personalisierung digitaler Produkte

Wie bereits ausgeführt,[40] sprechen die Argumente, die für eine enge Auslegung von Art. 6 Abs. 1 lit. b DS-GVO angeführt wurden, auch dagegen, eine Personalisierung der vertraglich vereinbarten (Haupt-)Leistung vertragsakzessorisch zu erlauben.[41] Anderenfalls hätten es gerade diejenigen Verantwortlichen, die besonders umfangreich Daten verarbeiten, beispielsweise *Meta Platforms* (*Facebook*), in der Hand, im Rahmen von AGB zunächst alle Bestandteile und Funktionen ihrer Kommunikationsplattform transparent zu beschreiben und diese anschließend zur vertraglichen (Haupt-)Leistung zu erklären. Infolgedessen würden diese Vereinbarungen einer *praxistauglichen* Kontrolle der Angemessenheit des Synallagmas entgehen.[42] Alle beschriebenen Datenverarbeitungen würden Teil der vertraglichen Leistung und die Datenverarbeitung wäre zur

---

dem Charakter zu erlauben („ancillary activities"); a. A. *Facebook*, das *LG Wien* und das *OLG Wien*, hierzu: *ÖOGH*, Vorlagebeschl. v. 22.07.2021, 6 Ob 56/21k – *Schrems* [*III*] (Rn. 44 ff.). Für eine Anwendung von Art. 6 Abs. 1 lit. b DS-GVO, wenn ein Datensubjekt sich – nach Abwägung der Interessen – verbindlich dazu verpflichtet hat, personenbezogene Daten bereitzustellen: *Bunnenberg*, Privates Datenschutzrecht, 2020, S. 39/282/303.

[39] *EDSA*, Leitlinien 02/2019 zur Verarbeitung personenbezogener Daten gemäß Artikel 6 Absatz 1 Buchstabe b DSGVO im Zusammenhang mit der Bereitstellung von Online-Diensten für betroffene Personen, Nr. 53; a. A.: *DSK* Kurzpapier Nr. 3, Verarbeitung personenbezogener Daten für Werbung, 2018, S. 2 a. E. („Bei ‚kostenlosen' Dienstleistungsangeboten, die die Nutzer mit der Zustimmung für eine werbliche Nutzung ihrer Daten ‚bezahlen' […] muss diese vertraglich ausbedungene Gegenleistung des Nutzers bei Vertragsabschluss klar und verständlich dargestellt werden. Nur dann besteht keine Notwendigkeit mehr für eine Einwilligung").

[40] Oben Kapitel 3 C.III.2 und 3.

[41] A. A. mit der Grenze eines „verobjektivierenden Maßstabs": *Leistner/Antoine/Sagstetter*, Big Data, 2021, S. 265 f.

[42] Oben Kapitel 2 C.I.2.e.

Erfüllung dieses Vertrags über die Nutzung der Kommunikationsplattform *Facebook* erforderlich.[43]

Infolgedessen würden die strengen Voraussetzungen an eine wirksame Einwilligung gerade bei solchen Geschäftsmodellen leerlaufen, die durch eine besonders umfangreiche Datenverarbeitung geprägt sind. Nur soweit die Daten eindeutig nicht der Funktionsweise der Kommunikationsplattform, sondern ausschließlich der Ermöglichung von personalisierter Werbung dienen, wäre insoweit noch eine Einwilligung erforderlich.

Eine solche Abgrenzung, zu welcher der (europäische) Gesetzgeber selbst nicht in der Lage war, ist im Einzelfall jedoch sehr schwierig (1). Im Ergebnis entscheidet diese Abgrenzung darüber, ob eine Datenverarbeitung noch vertragsakzessorisch erforderlich ist oder bereits darüber hinausgeht und damit Teil der vertraglichen Gegenleistung wird, auch darüber, ob ein Vertrag dem Anwendungsbereich der DID-RL bzw. §§ 327 ff. BGB unterfällt (2).

1. Kern der Abgrenzungsschwierigkeit

Die Abgrenzung zwischen einer Datenverarbeitung, die noch erforderlich ist, um eine Kommunikationsplattform wie *Facebook* zu betreiben oder die Trefferliste einer Suchmaschine (auch) nach der mutmaßlichen Relevanz für den Nutzer zu sortieren, und einer Datenverarbeitung die vorrangig der Ermöglichung von personalisierter Werbung dient, ist eine komplexe, einzelfallabhängige Herausforderung. In diesem Zusammenhang besteht stets die Gefahr, dass ein Verantwortlicher sein Angebot derart gestaltet, dass eine personalisierte Leistung, einschließlich einer personalisierten Werbeansprache des Datensubjekts zum Bestandteil der vertraglich geschuldeten (Haupt-)Leistung des Verantwortlichen wird und infolgedessen unter Art. 6 Abs. 1 lit. b DS-GVO fällt. Weil Art. 6 Abs. 1 lit. b DS-GVO gerade für solche Verantwortliche attraktiv ist, die eine personalisierte Leistung anbieten und weil die Personalisierung von Leistungen stetig zunimmt, wird diese Abgrenzungsfrage künftig noch an Bedeutung gewinnen.[44]

---

[43] Das *LG* Wien und das *OLG Wien* hielten ein solches Vorgehen von *Facebook* auf Grundlage von Art. 6 Abs. 1 lit. b DS-GVO für rechtmäßig. Hierzu: *OLG Wien*, Urt. v. 07.12.2020, GZ 11 R 153/20f, 11 R 154/20b-99 S. 28. Zum weiteren Verlauf des Verfahrens: *ÖOGH*, Vorlagebeschl. v. 22.07.2021, 6 Ob 56/21k – *Schrems* [*III*] (Rn. 44 ff.). Auch die zuständige irische Datenschutzbehörde scheint *Facebooks* Ansicht einstweilen zu teilen, dass keine Einwilligung erforderlich ist, sondern die von *Facebook* durchgeführten Datenverarbeitungen auf Grundlage von Art. 6 Abs. 1 lit. b DS-GVO erfolgen können: *Irische Datenschutzbeauftragte*, Entscheidungsentwurf, Case Reference: IN-18-5-5, v. 06.10.2021, S. 39 („Finding 2") (zeitweise abrufbar unter https://noyb.eu/sites/default/files/2021-10/IN%2018-5-5%20Draft%20Decision%20of%20the%20IE%20SA.pdf, zuletzt abgerufen am 19.05.2022).

[44] Eine Rechtfertigung auf Grundlage von Art. 6 Abs. 1 lit. b DS-GVO versucht beispielsweise *Facebook*: Mit Zweifeln hieran: *OLG Düsseldorf*, Vorlagebeschl. v. 24.03.2021, Kart 2/19 (V), Rn. 40; sowie *ÖOGH*, Vorlagebeschl. v. 22.07.2021, 6 Ob 56/21k (Rn. 8 ff.) – *Schrems*

Bislang ist völlig offen, inwieweit eine Datenverarbeitung zur Personalisierung von digitalen Produkten erforderlich und deshalb gemäß Art. 6 Abs. 1 lit. b DS-GVO erlaubt ist und ab wann eine Datenverarbeitung hierüber hinausgeht, damit zur Gegenleistung wird und deshalb einer Einwilligung bedarf. Diese Abgrenzungsschwierigkeiten und die dadurch entstehenden Gefahren für die informationelle Privatautonomie sind ein wesentlicher Grund dafür, warum die Anwendung von Art. 6 Abs. 1 lit. b DS-GVO ausschließlich auf unterstützende Datenverarbeitungen begrenzt werden sollte.[45]

2. Keine Lösungsvorschläge durch den Gesetzgeber

Brisant ist diese Abgrenzungsfrage insbesondere deshalb, weil von ihrer Beantwortung auch abhängt, ob die DID-RL bzw. deren Umsetzung in §§ 327 ff. BGB anwendbar sind. Leider gingen weder der europäische Gesetzgeber[46] noch der deutsche Gesetzgeber bei Verabschiedung der DID-RL bzw. deren Umsetzung im BGB auf die Möglichkeit von personalisierten digitalen Produkten ein. Ausgangspunkt sind vielmehr jeweils solche Konstellationen, in denen ein Datensubjekt personenbezogene Daten nicht für die Personalisierung der digitalen Produkte, sondern als Alternative zum monetären Entgelt bereitstellt. In letzterem Fall sind die personenbezogenen Daten gerade nicht zur Erfüllung des Vertrags erforderlich. In ersterem ist dagegen vertraglich eine Personalisierung geschuldet, deren Erfüllung die Verarbeitung von personenbezogenen Daten voraussetzt.

Nicht eindeutig ist der Fall, sofern ein Unternehmer personalisierte digitale Produkte anbietet – beispielsweise das Streaming von Musik nach bisheriger Präferenz des Verbrauchers (automatisch generierte Playlist) – und diese lediglich als kostenloses Lockangebot vorsieht oder dauerhaft über ausschließlich generische Werbung finanziert.[47] Weil die Bereitstellung der personenbezogenen Daten dann keine Gegenleistung ist, spricht dies im Ausgangspunkt gegen eine Anwendbarkeit der DID-RL bzw. der §§ 327 ff. BGB.

[III]); a. A. noch die Berufungsinstanz: *OLG Wien*, Urt. v. 07.12.2020 (nicht rechtskräftig), GZ 11 R 153/20f, 11 R 154/20b-99 S. 27 f.

[45] A. A. *Mackenrodt/Wiedemann*, ZUM 2021, 89 (98). Sie versuchen, eine Trennung zwischen solchen personenbezogenen Daten einzuziehen, ohne die ein auf Kommunikation ausgerichtetes soziales Netzwerk nicht funktionieren kann (insoweit: Art. 6 Abs. 1 lit. b DS-GVO) und solchen Daten, die Werbezwecken dienen (insoweit: Art. 6 Abs. 1 lit. a DS-GVO). Allerdings ist schon zweifelhaft, ob die Verarbeitung des „Profilfotos, des Geburtsdatums, der Heimatstadt etc." notwendig ist, um ein Nutzerprofil anzulegen. Zudem kann das Profilfoto bereits ein besonders sensibles Datum sein, sofern es Hinweise auf die rassische Herkunft oder die Gesundheit des Datensubjekts i. S. d. Art. 9 Abs. 1 DS-GVO enthält, so dass dessen Verarbeitung auf Grundlage von Art. 6 Abs. 1 lit. b DS-GVO ausscheidet.

[46] Hierzu bereits oben Kapitel 3 C.III.1.

[47] Zu diesen Fällen der „atypischen Schenkung" bereits oben Kapitel 3 C.III.1.

Allerdings lässt es Art. 3 Abs. 1 S. 2 DID-RL seinem Wortlaut nach ausreichen, wenn „der Verbraucher dem Unternehmer personenbezogene Daten bereitstellt".[48] Noch ambivalenter ist § 516a Abs. 1 BGB, der von einer Schenkung des Unternehmers ausgeht, sofern dieser sich verpflichtet,

dem Verbraucher digitale Produkte zu schenken, und der Verbraucher dem Unternehmer personenbezogene Daten nach Maßgabe des § 327 Absatz 3 bereitstellt oder sich hierzu *verpflichtet*".[49]

Mit § 516a Abs. 1 BGB scheint der deutsche Gesetzgeber den Anwendungsbereich der DID-RL erweitern zu wollen. Gemäß Art. 3 Abs. 1 Hs. 2 DID-RL ist der Anwendungsbereich der DID-RL jedoch auf entgeltliche Vereinbarungen, also solche mit Geld oder personenbezogene Daten als Gegenleistung beschränkt.

Die DID-RL regelt nicht den Fall, dass ein *personalisiertes* digitales Produkt „im Austausch" gegen Aufmerksamkeit für generische Werbung angeboten wird. Folglich ging der deutsche Gesetzgeber bei der Umsetzung der DID-RL über deren Vorgaben hinaus, indem er diesen „atypische Schenkungsfall" in § 516a BGB ausdrücklich regelt und in diesem Fall die speziellen (strengeren) Gewährleistungsrecht der §§ 327 ff. BGB für anwendbar erklärt hat.

Somit ist § 516a Abs. 1 BGB aufgrund der vollharmonisierender Wirkung der DID-RL gemäß Art. 4 a. E. DID-RL unionsrechtswidrig, es sei denn, es handelt sich hierbei um einen Anwendungsfall des Art. 3 Abs. 4 DID-RL. Hiernach gilt die DID-RL

nicht für digitale Inhalte, die gegen eine andere Leistung als Geld bereitgestellt werden, soweit der Anbieter vom Verbraucher personenbezogene Daten verlangt, deren Verarbeitung für die Erfüllung des Vertrags oder die Erfüllung rechtlicher Anforderungen unbedingt erforderlich ist, und er diese Daten nicht in einer mit diesem Zweck nicht zu vereinbarenden Weise weiterverarbeitet."

Weil die DID-RL für eine derartige Konstellation keine Vorgaben macht, würde es dem deutschen Gesetzgeber freistehen, in § 516a Abs. 1 BGB die Anforderungen der DID-RL auch auf eine derart „atypische Schenkung" auszuweiten, ohne deshalb gegen das – nur für den Anwendungsbereich der DID-RL geltende – Verbot aus Art. 4 DID-RL zu verstoßen.[50]

---

[48] Auch gemäß § 327 Abs. 3 BGB sind die §§ 327 ff. BGB „auch auf Verbraucherverträge über die Bereitstellung digitaler Produkte anzuwenden, bei denen der Verbraucher dem Unternehmer personenbezogene Daten bereitstellt oder sich zu deren Bereitstellung verpflichtet".

[49] [Hervorhebung durch den Verfasser].

[50] Eine hiervon zu trennende Frage ist jedoch, ob eine Schenkung von digitalen Produkten durch einen Unternehmer nach deutschem Recht vorliegen kann, soweit der Verbraucher sich gemäß § 516a Abs. 1 Var. 2 BGB gegenüber dem Unternehmer dazu verpflichtet, personenbezogene Daten bereitzustellen.

Offen bleibt zudem die Frage, wie es sich auf die vertragliche Pflicht des Unternehmers zur Personalisierung von digitalen Produkten auswirkt, wenn der Verbraucher für diese digitalen Produkte ein monetäres Entgelt zahlt, oder in die Verwertung von personenbezogenen Daten zu anderen Zwecken einwilligt, dann aber für diese Personalisierung der digitalen Produkte nur mangelhafte personenbezogene Daten bereitstellt.[51]

Weder der europäische Gesetzgeber (DID-RL) noch der deutsche Gesetzgeber sahen sich in der Lage, hierfür eine Lösung vorzuschlagen. Sogar im Fall einer vorsätzlichen Schlechtleistung durch das Datensubjekt schließt § 327q Abs. 3 BGB alle Ersatzansprüche des Unternehmers kategorisch aus. Eine Schlechtleistung des Datensubjekts ließe sich allenfalls als konkludenter Widerruf der Einwilligung auslegen, um dem Verantwortlichen – nach einer umfassenden Interessenabwägung – wenigstens das Beendigungsrecht gemäß § 327q Abs. 2 BGB zu eröffnen.

Weil dieses Ergebnis nicht überzeugt, sind die Gerichte gezwungen, die durch eine Realitätsflucht des Gesetzgebers („Personenbezogene Daten dürfen keine Gegenleistung sein") entstandenen Lücken und Widersprüche unter Rückgriff auf den Grundsatz einer Datenverarbeitung nach Treu und Glauben (Art. 5 Abs. 1 lit. a Var. 2 DS-GVO) zu korrigieren und den allgemeinen unionsrechtlichen Grundsatz von Treu und Glauben auch zulasten von Datensubjekte anzuwenden,[52] um dem Verantwortlichen im Einzelfall einen Anspruch auf den ihm entstandenen Vertrauensschaden zu gewähren.[53]

---

[51] Diese Frage ist völlig offen, weil sowohl DID-RL als auch §§ 327 ff. BGB – insbesondere § 327q Abs. 1 BGB – nur Konstellationen im Blick hatten, im Rahmen derer die Datenverarbeitung ausschließlich auf Grundlage einer Einwilligung oder einer Interessenabwägung erfolgt.

[52] Der datenschutzrechtliche Grundsatz einer Datenverarbeitung nach Treu und Glauben (Art. 5 Abs. 1 lit. a Var. 2 DS-GVO) verpflichtet gemäß Art. 5 Abs. 2 DS-GVO nur den Verantwortlichen und nicht das Datensubjekt. Grundlegend zum Grundsatz von Treu und Glauben: *EuGH*, Urt. v. 03.09.2009, C-489/07 = EuZW 2009, 694 (Rn. 26) – *Messner*. *Riesenhuber*, System und Prinzipien des Europäischen Vertragsrechts, 2003, S. 398 ff.; *Stempel*, Treu und Glauben im Unionsprivatrecht, 2016, S. 268 ff., 310 f.; *Metzger*, Extra legem, intra ius. Allgemeine Rechtsgrundsätze im Europäischen Privatrecht, 2009, S. 348 f.; spezifisch zum Grundsatz des Rechtsmissbrauchs: *EuGH*, Urt. v. 12.03.1996, C-441/93 = WM 1996, 1530 (Rn. 69) – *Pafitis*; *EuGH*, Urt. v. 12.05.1998, C-367/96 = EuZW 1999, 57 (Rn. 20) – *Kefalas*; hierzu: *Schmidt-Kessel*, in: Jud u. a. (Hrsg.), Prinzipien des Privatrechts und Rechtsvereinheitlichung, 2001, S. 61 (79 f.).

[53] Diese Rechtsfolge entspricht dem Ansatz, der für den Fall eines entsprechend § 42 UrhG (gewandelte Überzeugung) begründeten Einwilligungswiderrufs in die kommerzielle Nutzung des Rechts am eigenen Bild (§ 22 KUG) vertreten wird: Hierzu: *Dasch*, Die Einwilligung zum Eingriff in das Recht am eigenen Bild, 1990, S. 87; *Helle*, AfP 1985, 93 (101); *Canaris*, AcP 184 (1984) 201 (223 f.); *Götting*, in: Schricker/Loewenheim, Urheberrecht, 6. Aufl. 2020, § 22 KUG, Rn. 41; ohne Auseinandersetzung mit § 327q Abs. 3 BGB für einen Aufwendungsersatz: *Leistner/Antoine/Sagstetter*, Big Data, 2021, S. 272/275.

III. Zweite Herausforderung: Einbeziehung von Dienstleistern

Eine weitere Herausforderung entsteht dadurch, dass die Anzahl der Dienstleister, die vom Verantwortlichen und Vertragspartner des Datensubjekts einbezogen werden, kontinuierlich zunimmt. Weil es für Art. 6 Abs. 1 lit. b DS-GVO lediglich darauf ankommt, dass das Datensubjekt selbst Partei des Vertrags ist, zu dessen Erfüllung die Datenverarbeitung erforderlich ist, kann der Vertragspartner des Datensubjekts in diesen Vertrag grundsätzlich nicht nur Verrichtungs-, sondern auch Erfüllungsgehilfen einbeziehen.[54]

Aufgrund einer zunehmenden arbeitsteiligen Ausdifferenzierung nimmt die Anzahl der Vertragsverhältnisse ab, in denen die personenbezogenen Daten von Verbrauchern ausschließlich durch den Vertragspartner verarbeitet werden. Zudem bemühen sich seit einigen Jahren zahlreiche Anbieter darum, in die Abwicklung von (Fernabsatz-)Verträgen einbezogen zu werden. Längst sind es nicht mehr nur traditionelle Logistikanbieter und Banken, sondern andere Dienstleister für die Vertrags- und Zahlungsabwicklung – beispielsweise *Klarna*, *Paypal*, *Paydirekt*, *Apple-Pay*, *Alipay* –, die im Rahmen der Vertragsabwicklung einbezogen werden (wollen). Sofern künftig auch sog. Kryptowährungen von Unternehmen als (Gegen-)Leistung akzeptiert werden, kommen zusätzliche Unternehmen als Intermediäre hinzu.

Infolgedessen wird der Druck zugunsten einer großzügigeren Auslegung von Art. 6 Abs. 1 lit. b DS-GVO umso mehr steigen, je größer die Anzahl der in die Vertragserfüllung einbezogenen Personen ist und je komplexer die zur Vertragserfüllung erforderlichen Datenverarbeitungen werden. Zwar dient die Anforderung, dass eine Datenverarbeitung für die Vertragserfüllung erforderlich sein muss, dazu, den Tatbestand des Art. 6 Abs. 1 lit. b DS-GVO gegenüber der Einwilligung abzugrenzen. Allerdings dürfte die Beurteilung, welche Datenverarbeitungen nach dem objektiven Empfängerhorizont im Zusammenhang mit einer Vertragserfüllung zu erwarten sind, durch die faktische Zunahme der Anzahl der Beteiligten ausgedehnt werden. Infolgedessen wächst das Risiko, dass insbesondere Logistikunternehmen und Anbieter von Diensten zur Zahlungsabwicklung versuchen werden – als Erfüllungsgehilfen und Auftragsverarbeiter des Verantwortlichen – über Art. 6 Abs. 1 lit. b DS-GVO einen rechtmäßigen Zugang zu personenbezogenen Daten zu erlangen und diesen anschließend gemäß Art. 6 Abs. 1 lit. f DS-GVO zusätzlich für eigene Zwecke zu verarbeiten. Kombiniert mit einer weiten Auslegung der „Direktwerbung“

[54] Nicht gemeint sind solche Verträge, die weitere Verarbeitungszwecke (Marktanalyse) durch Dritte zulassen. Diese unterfallen dem Anwendungsbereich von Art. 6 Abs. 1 lit. b DS-GVO bereits deshalb nicht, weil insoweit zwei (gemeinsam) Verantwortliche existieren, die jeweils eigene wirtschaftliche Ziele verfolgen und deshalb für ihre Datenverarbeitung jeweils einen eigenen Erlaubnistatbestand benötigen. Hierzu: *EuGH*, Urt. v. 29.07.2019, C-40/17 = GRUR 2019, 958 (Rn. 132 f.) – *Fashion ID*.

i. S. d. Art. 21 Abs. 2 Hs. 2 DS-GVO und ErwG 47 S. 7 DS-GVO bestünde die Gefahr, dass diesen Dienstleistern – entgegen hier vertretener Auffassung[55] – sogar der Weg zu einem rechtmäßigen Profiling für eigene Werbezwecke[56] gemäß Art. 6 Abs. 1 lit. f DS-GVO offensteht.[57]

Jedenfalls aus der Perspektive eines Vorfeldschutzes, den Datenschutzbehörden bisweilen einnehmen, liegt es deshalb nahe, zu hinterfragen, ob und inwieweit eine strategische und sukzessive Kombination aus Art. 6 Abs. 1 lit. b und lit. f DS-GVO die Risiken für Datensubjekte kontinuierlich erhöht. Diese Entwicklung ist weitgehend unproblematisch, sofern man die Möglichkeit zur personalisierten Direktwerbung auf Grundlage von Art. 6 Abs. 1 lit. f DS-GVO – mit hier vertretener Auffassung – auf ähnliche Produkte und auf eine bereits bestehende Kundenbeziehung zwischen dem Datensubjekt und dem Verantwortlichen beschränkt. Dabei ist zu beachten, dass solche Dienstleister auch dann noch Erfüllungsgehilfen des Verantwortlichen bleiben, wenn das Datensubjekt selbst zwischen einer vorgegebenen Auswahl an Erfüllungsgehilfen des Verantwortlichen, beispielsweise für die Logistik (*Hermes*, *DHL*, *UPS*) oder die Zahlungsabwicklung (*Paypal*, *Paydirekt*, *Apple-Pay*) auswählt.

Nach dem hier vertretenen, engen Verständnis von Art. 6 Abs. 1 lit. b DS-GVO bleiben diese Dienstleister somit Erfüllungsgehilfen des Verantwortlichen und des Vertragspartners des Datensubjekts, werden deshalb nicht zu eigenständigen Vertragspartnern des Datensubjekts und diese Dienstleister können infolgedessen den Art. 6 Abs. 1 lit. f DS-GVO nicht als Begründung für ein eigenes Profiling als Grundlage für Direktwerbung gegenüber dem Datensubjekt heranziehen. Wer durch den Verantwortlichen lediglich in die Abwicklung eines Vertrages mit dem Datensubjekt einbezogen wurde, steht in keiner eigenen Kundenbeziehung zum Datensubjekt i. S. d. ErwG 47 S. 2 DS-GVO. Infolgedessen muss ein Dienstleister des Verantwortlichen für jede Datenverarbeitung, die über seine vertragliche Pflicht zur Leistungserbringung gegenüber dem Verantwortlichen hinausgeht, eine eigene wirksame Einwilligung des Datensubjekts einholen.

---

[55] Oben A.II.1. sowie Kapitel 2 C.I.2.b.

[56] Als Beispiel hierfür können die derzeit gängigen Angebote traditioneller Banken für Girokonten dienen. So wird die Führung eines Girokontos, ohne monetäre Gegenleistung, an die Bedingung geknüpft, dass der Kontoinhaber eine monatliche Mindestanzahl von Transaktionen unter Nutzung von *Apple Pay* oder *Google Pay* durchführt. Dieses Geschäftsmodell ist für *Apple und Google* ökonomisch sinnvoll, weil beide die Transaktionsdaten der Kontoinhaber anderweitig effizient monetisieren und einen Betrag an die kontoführende Bank zahlen. Mittelfristig dürfte dieses Modell auch dazu dienen, die – attraktiven – Kunden für die eigene Bank von *Apple und Google* abzuwerben.

[57] Zusätzlich kann es das Ziel sein, einen Zugang zu strukturierten – nicht notwendig nur personenbezogenen – Daten zu erlangen, um diese als Trainingsdaten für ML zu verwenden. Hierzu: *Zech*, GRUR 2015, 1151 (1152); *Schweitzer/Peitz*, Datenmärkte in der digitalisierten Wirtschaft: Funktionsdefizite und Regelungsbedarf, ZEW Discussion Paper No. 17–043, 2017, S. 15 ff. (http://ftp.zew.de/pub/zew-docs/dp/dp17043.pdf, zuletzt abgerufen am 19.05.2022).

C. Dritte Stufe: Flexibilisierung des Einwilligungstatbestands

Als Konsequenz des hier vertretenen Vorrangs der Einwilligung im Privatrechtsverhältnis kommt diesem Erlaubnistatbestand eine zentrale Bedeutung für die Verarbeitung von personenbezogenen Daten zu.[58] Zunächst werden die Gründe für eine unionsgrundrechtskonforme Flexibilisierung des Einwilligungstatbestands nochmals kurz zusammengefasst (I). Wesentliche Folge dieser Flexibilisierung ist die Anerkennung von personenbezogenen Daten als Leistungsgegenstand. Diese setzt voraus, dass das sog. Kopplungsverbot in Art. 7 Abs. 4 DS-GVO (Freiwilligkeit der Einwilligung) im Sinne eines generalklauselartigen Berücksichtigungsgebots ausgelegt (II) und die Widerruflichkeit der Einwilligung gemäß Art. 7 Abs. 3 S. 1 DS-GVO jedenfalls – aber nicht nur – im B2B-Verhältnis teleologisch reduziert wird (III).

I. Gründe für eine Flexibilisierung

Wie bereits im vorherigen Kapitel ausgeführt, *müssen* das sog. Kopplungsverbot (Art. 7 Abs. 4 DS-GVO) und die sog. freie Widerruflichkeit der Einwilligung (Art. 7 Abs. 3 S. 1 DS-GVO) flexibilisiert werden. Hierfür gibt es drei Gründe.

Erstens wurde bei Verabschiedung der DS-GVO die langjährige Tradition einer Verwertung der vermögenswerten Bestandteile von Persönlichkeitsrechten übersehen. Dadurch greift eine strenge Auslegung des Einwilligungstatbestands in unverhältnismäßiger Weise in die gemäß Art. 8 Abs. 2 S. 1 GRCh garantierte Möglichkeit zur Einwilligung, in das allgemeine europäische Grundrecht der Vertragsfreiheit (Art. 6 Abs. 3 EUV) und in die unternehmerische (Vertrags-)Freiheit (Art. 16 GRCh) von Verantwortlichen und unternehmerisch handelnden Datensubjekten ein. Insbesondere wird die unternehmerische Freiheit von jenen Verantwortlichen durch eine strenge Auslegung von Art. 7 Abs. 3 S. 1 und Abs. 4 DS-GVO unverhältnismäßig beeinträchtigt, die – im Gegensatz zu den jeweils in spezifischen Märkten dominanten *GAFAM* – nicht über eine marktmächtige Position verfügen, sondern als KMU einem intensiven Wettbewerb ausgesetzt sind.[59]

Zweitens verhindert eine sog. freie Widerruflichkeit, dass die Einwilligung das Rechtsverhältnis zwischen Datensubjekt und Verantwortlichem stabilisieren kann. Die Einwilligung bietet den Verantwortlichen keine Verlässlichkeit und es besteht keine Möglichkeit, auf Grundlage einer Einwilligung längerfris-

[58] Für eine Verarbeitung von besonders sensiblen personenbezogenen Daten scheidet eine vertragsakzessorische Datenverarbeitung und die Verarbeitung auf Grundlage einer Interessenabwägung *de lege lata* von vornherein aus, Art. 9 Abs. 2 DS-GVO.

[59] Die ebenfalls allgemein für die Anforderungen der DS-GVO andeutend: *Evaluationsbericht DS-GVO der EU-Kommission*, COM(2020) 264 final, S. 12/19 ff.

tige Planungen anzustellen. Dies erschwert zugleich Geschäftsmodelle, die auf eine geringere Kommerzialisierung von personenbezogenen Daten setzen und für solche Geschäftsmodelle, die auf einer treuhänderischen Verwertung von personenbezogenen Daten beruhen (sollen).[60]

Drittens setzt bzw. verstärkt eine jederzeitige Widerruflichkeit der Einwilligung einen Anreiz zur Flucht aus der Einwilligung. Jedenfalls solange die Anwendung und Auslegung von Art. 6 Abs. 1 lit. b und lit. f DS-GVO – mangels Konkretisierung durch den europäischen Gesetzgeber oder durch den *EuGH* – mit großer Rechtsunsicherheit verbunden sind, bleibt die Datenverarbeitung auf Grundlage der Vertragsakzessorietät oder der Interessenabwägung aus Sicht des Verantwortlichen deshalb attraktiver als die Einholung einer Einwilligung, weil sie dann keinen jederzeitigen Widerruf befürchten müssen. Die sog. freie Widerruflichkeit der Einwilligung, die zugunsten des Datensubjekts gedacht war, führt eindeutig zu Strategien der Vermeidung der Einwilligung durch die Verantwortlichen.[61]

II. Flexibilisierung der Freiwilligkeit der Einwilligung

Sinn und Zweck des Art. 7 Abs. 4 DS-GVO ist es, das Tatbestandsmerkmal der Freiwilligkeit i. S. d. Art. 4 Nr. 11 DS-GVO zu konkretisieren. Obwohl Art. 7 Abs. 4 DS-GVO zu den in Rechtsprechung und Literatur heftig umstrittenen Regelungen der DS-GVO gehört,[62] ist eine Flexibilisierung des sog. Kopplungsverbots aus Art. 7 Abs. 4 DS-GVO aufgrund des insoweit mehrdeutigen Wortlauts vergleichsweise leicht möglich.

Nach hier vertretener Auffassung und in Übereinstimmung mit der wohl h. A. in der privatrechtlichen Literatur muss bei der Beurteilung der Freiwilligkeit einer Einwilligung gemäß Art. 7 Abs. 4 DS-GVO *lediglich berücksichtigt* werden,[63] ob der Verantwortliche die Erfüllung eines Vertrags gerade von der Einwilligung in eine Datenverarbeitung abhängig gemacht hat, obwohl diese Verarbeitung für die Erfüllung des Vertrags nicht erforderlich ist.

Mit anderen Worten: Art. 7 Abs. 4 DS-GVO mahnt den Verantwortlichen *ex ante* und die Datenschutzbehörden und Gerichte *ex post* zur Aufmerksamkeit, sofern Verantwortliche einen Vertragsabschluss und eine Einwilligung miteinander kombinieren, obwohl die Durchführung des Vertrags eine solche Einwilligung nicht zwingend voraussetzt. Dieses Verständnis lässt sich bereits ErwG

---

[60] Hierzu zuletzt: *Kühling*, ZfDR 2021, 1 (11).

[61] Zum Wechsel von einer Einwilligung auf Art. 6 Abs. 1 lit. b durch *Facebook* infolge der Anwendbarkeit der DS-GVO: *ÖOGH*, Vorlagebeschl. v. 22.07.2021, 6 Ob 56/21k – *Schrems* [*III*] (Rn. 7 f.).

[62] Oben Kapitel 4 A.II.4. und Kapitel 4 B.I.1.

[63] Hierzu oben Kapitel 4 B.I.2.

43 S. 1 DS-GVO entnehmen, der als Beispiel für eine Unfreiwilligkeit der Einwilligung eine Situation benennt, in der zwischen Datensubjekt und Verantwortlichem ein klares Ungleichgewicht besteht und es infolgedessen unwahrscheinlich ist, dass das Datensubjekt die Einwilligung freiwillig erteilt hat.

Im Ergebnis hält Art. 7 Abs. 4 DS-GVO Verantwortliche somit zu einer Trennung von Vertrag und Einwilligung an und fordert im Fall einer Verknüpfung der Erklärungen dazu auf, zu prüfen, ob diese Kombination aus Vertrag und Einwilligung womöglich nur deshalb vom Datensubjekt akzeptiert wird, weil das Datensubjekt dem Verantwortlichen im Einzelfall derart *strukturell* („Ungleichgewicht") oder *situativ* („aller Umstände") unterlegen ist, dass dessen Willensbekundung rechtlich nicht mehr als Ausdruck von Selbstbestimmung gewertet werden darf.

Für eine Flexibilisierung des datenschutzrechtlichen Einwilligungstatbestands folgt hieraus ein großes Potenzial dafür, den Freiwilligkeitsbegriff in Abhängigkeit von den Umständen des Einzelfalls abzustufen. Weil die Kehrseite dieser Flexibilität ein höheres Ausmaß an Rechtsunsicherheit sein kann, sollte der *EDSA* auf Grundlage von Art. 70 Abs. 1 S. 2 lit. e DS-GVO auch für die Bewertung der Freiwilligkeit i. S. d. Art. 7 Abs. 4 DS-GVO (unverbindliche) Leitlinien entwickeln. Zudem können Verbände und andere Vereinigungen Verhaltensregelungen nach Art. 40 Abs. 2 lit. a DS-GVO (faire und transparente Verarbeitung) ausarbeiten.

Allerdings dürfte kaum eine Aussicht auf Erfolg bestehen, wenn Verbände solche Verhaltensregelungen gemäß Art. 40 Abs. 5 DS-GVO den jeweils zuständigen Aufsichtsbehörden zur Genehmigung vorlegen. Gleiches gilt für die Möglichkeit, dass die *EU-Kommission* derartige Verhaltensregelungen gemäß Art. 40 Abs. 9 DS-GVO für verbindlich erklärt. Weder die Aufsichtsbehörden noch die *EU-Kommission* werden sich aus der Deckung wagen, solange der *EuGH* keine Grundsatzentscheidung zur Auslegung von Art. 7 Abs. 4 DS-GVO gefällt hat.[64] Dennoch ist es aus Sicht der Verbände und ihrer Mitglieder sinnvoll, solche Verhaltensregelungen als Handreichung für die Bewertung der Freiwilligkeit einer Einwilligung auszuarbeiten.

In diesen Verhaltensregelungen können Kriterien aufgelistet werden, die bei der Einschätzung der Freiwilligkeit helfen. Hierfür kommen mehrere Kriterien in Betracht, die aus dem Unionsrecht bereits bekannt sind und die infolgedessen lediglich mit Blick auf die spezifischen Ziele des Art. 1 DS-GVO angewendet werden müssen.

Als erstes und wichtigstes Beurteilungskriterium sollte die Position des Verantwortlichen auf dem jeweiligen Markt berücksichtigt werden (1). Anschließend bieten die für den Verantwortlichen erkennbaren Eigenschaft des Daten-

[64] Zur Verletzung der Vorlagepflicht gemäß Art. 267 Abs. 3 AEUV durch den *ÖOGH* (Urt. v. 31.08.2018, 6 OB 140/18 H): oben Kapitel 4 B.I.

subjekts ein weiteres wesentliches Beurteilungskriterium (2). Zudem kommt es entscheidend auf die konkreten situativen Umstände an, die zur Erteilung der Einwilligung geführt haben (3).

Mit Hilfe dieser Kriterien ist es im Ergebnis möglich, Art. 7 Abs. 4 DS-GVO *flexibel* anzuwenden. Infolgedessen kann die Vorschrift ihren unbestreitbaren wettbewerbspolitischen Zweck erfüllen, ohne zugleich Marktzutrittsbarrieren zu etablieren und ohne pauschal und damit in unverhältnismäßiger Weise in die Grundrechte der potenziell sehr unterschiedlichen Verantwortlichen und Datensubjekte einzugreifen (4).

1. Kriterium: Marktmacht des Verantwortlichen

ErwG 43 S. 1 DS-GVO nennt ein zwischen dem Datensubjekt und dem Verantwortlichen bestehendes klares Ungleichgewicht als ein im Rahmen der Beurteilung der Freiwilligkeit zu berücksichtigendes wesentliches Kriterium. Weil in diesem Kontext aber lediglich das Beispiel einer Behörde als Verantwortlicher angeführt wird, lässt sich aus ErwG 43 S. 1 DS-GVO für das Privatrechtsverhältnis wenig Substantielles ableiten. Im Gegenteil: Die ausschließliche Erwähnung einer Behörde als möglicher Verantwortlicher ist ein deutlicher Hinweis darauf, dass der europäische Gesetzgeber die privatrechtlichen Konsequenzen von Art. 7 Abs. 4 DS-GVO allenfalls unvollständig bedacht hat. Die offensichtlichen Überschneidungspunkte, die sich aus der Anforderung an die Freiwilligkeit einer Einwilligung gemäß Art. 7 Abs. 4 DS-GVO und dem kartellrechtlichen Verbot eines Missbrauchs einer marktbeherrschenden Stellung ergeben, hat der europäische Gesetzgeber entweder gänzlich übersehen. Alternativ war ihm das Spannungsverhältnis zwar bewusst, aber er sah sich nicht in der Lage, einen produktiven Beitrag zur Lösung dieses, durch Art. 7 Abs. 4 DS-GVO verursachten Konflikts zu leisten.[65] Infolgedessen bleibt die Synchronisierung von Art. 7 Abs. 4 DS-GVO und Art 102 AEUV (§§ 19 ff. GWB) – bestenfalls[66] – den Kartellbehörden und anschließend den auf das Kartellrecht spezialisierten Gerichten überlassen.[67]

---

[65] Mit dem Hinweis, dass auch zwischen dem Wortlaut von Art. 7 Abs. 4 und ErwG 43 ein Spannungsverhältnis besteht: *ÖOGH*, Urt. v. 31.08.2018, 6 Ob 140/18h = ZD 2019, 72 (Rn. 46).

[66] Im Idealfall kommen kartellrechtliche Beurteilung und datenschutzrechtliche Beurteilung zu einem synchronen Ergebnis. Diese für den Beschluss des *BGH* (Beschl. v. 23.06.2020, KVR 69/19 = NZKart 2020, 863 – *Facebook*.) annehmend: *Mackenrodt/Wiedemann*, ZUM 2021, 89 (101: „Das Freiwilligkeitserfordernis verpflichtet Facebook also datenschutzrechtlich zu eben der Wahlmöglichkeit, die der BGH aus kartellrechtlichen Erwägungen für geboten hält"); diesbezüglich skeptisch: *Körber*, NZKart 2019, 187 (191/193); *Lohse*, NZKart 2020, 292 (294).

[67] Allerdings besteht zunächst die Frage, ob und inwieweit eine (nationale) Kartellbehörde eine datenschutzrechtliche Prüfung – neben den gemäß Art. 51 ff. DS-GVO vorgesehenen

Nach hier vertretener Auffassung etabliert Art. 7 Abs. 4 DS-GVO ein *Gebot zur Berücksichtigung* der Position des Verantwortlichen auf dem spezifischen Markt (c). Dieses Verständnis setzt jedoch voraus, dass sich aus Art. 7 Abs. 4 DS-GVO weder ein strenges, anbieterbezogenes Kopplungsverbot (a) noch ein marktbezogenes Kopplungsverbot (b) ableiten lässt.

a) Strenges anbieterbezogenes Kopplungsverbot

Das restriktivste Verständnis von Art. 7 Abs. 4 DS-GVO im Sinne eines sog. strengen Kopplungsverbots stellt bei der Beurteilung der Freiwilligkeit der Einwilligung nur auf das konkrete Angebot des jeweiligen Verantwortlichen ab. Danach ist eine Einwilligung bereits dann als unfreiwillig zu beurteilen, wenn die Datenverarbeitung nicht für die Vertragserfüllung erforderlich ist – insoweit gilt der Erlaubnistatbestand des Art. 6 Abs. 1 lit. b DS-GVO – und der Verantwortliche seine Leistungen nicht ebenfalls gegen Zahlung eines monetären Entgelts anbietet.[68]

Diese strenge datenschutzrechtliche Auffassung stützt sich regelmäßig auf eine bemerkenswerte Aussage in ErwG 42 S. 5 DS-GVO. Hiernach sei von einer freien Wahl des Datensubjekts nur dann auszugehen, wenn es in der Lage ist, die Einwilligung zu verweigern, „ohne Nachteile zu erleiden".[69] Versteht man diese Aussage wörtlich, obwohl es nach den Gesetzen der Logik naheliegt, dass jede menschliche Entscheidung stets mit Nachteilen verbunden ist, so käme eine Einwilligung für die derzeit ubiquitären Geschäftsmodelle mehrseitiger Plattformen nicht in Betracht. Ein Angebot von (werbefinanzierten) digitalen Produkten ausschließlich im Austausch gegen eine Einwilligung in die Verarbeitung von personenbezogenen Daten würde stets an der fehlenden Freiwilligkeit der Einwilligung gemäß Art. 7 Abs. 4 DS-GVO scheitern. Nur sofern der Anbieter eine vergleichbare Leistung auch anbietet, ohne dass das Datensubjekt in die Datenverarbeitung einwilligen muss, entsteht eine Wahlmöglichkeit des Datensubjekts und eine unter diesen Bedingungen erteilte Einwilligung kann deshalb freiwillig sein. Dieses alternative Angebot dürfte regelmäßig die Zahlung eines Geldbetrags voraussetzen.

Denkt man dieses Verständnis von Art. 7 Abs. 4 DS-GVO als strenges anbieterbezogenes Kopplungsverbot mit seiner Pflicht zur alternativen Kontrahie-

---

Aufsichtsbehörden – durchführen kann: Hierzu die Vorlagefragen 1 und 7 des *OLG Düsseldorf*, Vorlagebeschl. v. 24.03.2021, Kart 2/19 (V), Rn. 28 ff. bzw. 69 ff.

[68] So *Albrecht/Jotzo*, Das neue Datenschutzrecht der EU, 2016, S. 70; *Krohm/Müller-Peltze*, ZD 2017, 551 (553); *Golland*, MMR 2018, 130 (134 f.); als Regelung der Vermutung mangelnder Freiwilligkeit: *M. Wagner*, Datenökonomie und Selbstdatenschutz, 2020, S. 333 ff., 341 f.). Zu dieser Möglichkeit auch: *Metzger*, AcP 216 (2016), 817 (823); *Dix*, ZEuP 2017, 1 (7 f.). Dagegen: *Bräutigam*, MMR 2012, 635 (626).

[69] Gleiches soll für die Freiwilligkeit des Widerrufs der Einwilligung gelten. Dazu unten C.III.2.a.

rung gegen Geldzahlung konsequent zu Ende, so müsste auch die Angemessenheit der alternativ geforderten monetären Gegenleistung überprüft werden. Nur durch eine solche Preiskontrolle könnte sichergestellt werden, dass die Zahlung des geforderten Geldbetrags aus Sicht der Datensubjekte eine echte Alternative zur Einwilligung ist. Bleibt einem Datensubjekten dagegen lediglich die Wahl zwischen einem unangemessenen monetären Entgelt oder der Einwilligung in die Verarbeitung personenbezogener Daten, so müsste eine Auslegung des Art. 7 Abs. 4 DS-GVO als strenges, anbieterbezogenes Kopplungsverbot konsequenterweise in die Unfreiwilligkeit der erteilten Einwilligung münden.[70]

b) Marktbezogenes Kopplungsverbot

Auf der nächsten, etwas abgeschwächten Stufe wird Art. 7 Abs. 4 DS-GVO etwas weiter ausgelegt. Eine Einwilligung wäre demnach unfreiwillig, wenn auch kein anderes Unternehmen eine Leistung bereithält, die aus Sicht des Datensubjekts ein Substitut darstellt und für deren Inanspruchnahme entweder weniger personenbezogene Daten verwertet werden oder stattdessen eine Geldzahlung verlangt wird.[71] Auch bei einem marktbezogenen Verständnis ist die Nähe des Art. 7 Abs. 4 DS-GVO zur kartellrechtlichen Marktdefinition und -abgrenzung offenkundig.

Ein solches marktbezogenes Verständnis ließe sich mit dem Argument begründen, dass dieses auch dem § 28 Abs. 3b BDSG a. F. zugrunde lag[72] und noch immer in § 95 Abs. 5 TKG niedergelegt ist. Die Abweichung im Wortlaut dieser Vorschriften, die ein marktbezogenes Verständnis der Freiwilligkeit zum Ausdruck bringen, kann jedoch sowohl als Argument für ein strengeres, anbieterbezogenes Verständnis als auch für eine flexiblere Anwendung von Art. 7 Abs. 4 DS-GVO im Sinne eines Gebots zur Berücksichtigung der Marktsituation (dazu sogleich) gedeutet werden. Fest steht insoweit nur, dass der europäische Gesetzgeber diesbezüglich weder in Art. 7 Abs. 4 noch in ErwG 43 DS-GVO eine klare Entscheidung treffen wollte oder konnte.

An einem Beispiel lässt sich der Unterschied zum strengen, anbieterbezogenen Verständnis verdeutlichen. Enthielte Art. 7 Abs. 4 DS-GVO ein marktbe-

---

[70] Hierfür: *Golland,* MMR 2018, 130 (134 f.); *Hacker*, Datenprivatrecht, 2020, S. 190.

[71] M.w.N. *Golland*, MMR 2018, 130 (134 f.).

[72] Gemäß § 28 Abs. 3b BDSG a. F. durfte die „verantwortliche Stelle […] den Abschluss eines Vertrags nicht von einer Einwilligung des Betroffenen […] abhängig machen, wenn dem Betroffenen ein anderer Zugang zu gleichwertigen vertraglichen Leistungen ohne die Einwilligung nicht oder nicht in zumutbarer Weise möglich ist". Hierzu: *Gierschmann*, ZD 2016, 51 (54); *Dammann*, ZD 2016, 307 (311); *Wolff*, in: Brink/Wolff (Hrsg.), BeckOK DatenschutzR, 28. Ed. 2015, Art. 28 BDSG (a. F.), Rn. 170–172. Zu weiteren Vorschriften, die ein marktbezogenes Kopplungsverbot enthielten: *Buchner*, Die informationelle Selbstbestimmung im Privatrecht, 2006, S. 264 ff.

zogenes Kopplungsverbot, so könnte *Meta Platforms* (*Facebook*) die Nutzung seines internetbasierten Kommunikationsmittels *WhatsApp* (sog. over the top, kurz: OTT-Provider*) datenschutzrechtlich* wirksam von der Einwilligung in die intensive Datenverarbeitung abhängig machen, sofern die (wohl) weniger datenintensiven OTT-Kommunikationsdienste wie *Signal* oder *Threema* oder– im Fall einer weiten Marktabgrenzung – sogar die zahlungspflichtigen Kommunikationsmittel in Form von *SMS/MMS* als Substitute für den Dienst von *WhatsApp* gelten würden.[73]

c) Art. 7 Abs. 4 als generalklauselartiges Berücksichtigungsgebot

Sowohl ein strenges anbieterbezogenes Kopplungsverbot, das ausschließlich auf das Angebot des jeweiligen Verantwortlichen abstellt und diesem damit eine Pflicht zur alternativen Kontrahierung gegen ein (angemessenes) monetäres Entgelt auferlegt als auch das marktbezogene Kopplungsverbot, das zusätzlich die Möglichkeiten zum Ausweichen auf eine Leistung von Wettbewerbern einbezieht, sind mit zwei schwerwiegenden Herausforderungen konfrontiert.

Erstens setzen beide Ansätze eine gerichtliche Kontrolle der Angemessenheit von mindestens zwei Angeboten voraus (aa). *Zweitens* führt die Anwendung des Kriteriums der Marktmacht als strenges anbieterbezogenes oder als marktbezogenes Kopplungsverbot zu grundlegenden unionweiten Kompetenzkonflikten zwischen den jeweiligen Datenschutzbehörden und den jeweiligen Kartellbehörden (bb).

Beide Herausforderungen lassen sich nach hier vertretener Ansicht *de lege lata* nur sinnvoll lösen, indem das Kriterium der Freiwilligkeit *kartellrechtsakzessorisch* und infolgedessen *asymmetrisch* angewandt wird (cc).

aa) Keine Angemessenheitskontrolle der Leistungsbeziehung

Welche Schwierigkeiten es birgt, wenn die nationalen Datenschutzbehörden und Gerichte gezwungen sind, den synallagmatischen Hauptgegenstand auf seine Angemessenheit zu überprüfen, wurde bereits im Kontext der vertragsakzessorischen Datenverarbeitung gemäß Art. 6 Abs. 1 lit. b DS-GVO heraus-

---

[73] Eine verengte Marktabgrenzung, die nur „kostenlose" Kommunikationsdienste berücksichtigt, ist i. R. v. Art. 7 Abs. 4 DS-GVO nicht möglich. Fraglich könnte zudem sein, ob E-Mails ein Substitut für Echtzeitkommunikation sind oder bereits einen anderen Kommunikationsmarkt darstellen; zur Unterscheidung: *Sieber*, in: Hoeren/Sieber/Holznagel, MMR-HdB, Teil 1, Technische Grundlagen, Rn. 117 ff.; gegen solches Verständnis (wohl): Anordnung des *HmbBfDI* gegen *Facebook*: Verbot der Weiterverarbeitung von WhatsApp-Nutzerdaten durch *Facebook*, Pressemitteilung v. 11.05.2021: „Die Zustimmung erfolgt weder transparent noch freiwillig. Das gilt in besonderer Weise für Kinder", (https://datenschutz-hamburg.de/pressemitteilungen/2021/05/2021-05-11-facebook-anordnung, zuletzt abgerufen am 19.05.2022).

gearbeitet.[74] Diese Schwierigkeiten lassen sich unmittelbar auf die Überprüfung der Freiwilligkeit einer Einwilligung übertragen, sofern die Freiwilligkeit im Sinne eines strengen anbieterbezogenen oder auch nur eines marktbezogenen Kopplungsverbots ausgelegt wird.

Erstens müssen die Datenschutzbehörden und Gerichte das geforderte monetäre Entgelt mit dem Wert der Verarbeitung von personenbezogenen Daten auf Grundlage der Einwilligung vergleichen. Ein Verständnis von Art. 7 Abs. 4 DS-GVO als strenges *anbieterbezogenes* Kopplungsverbot würde die Verantwortlichen immerhin dazu zwingen, ihre Leistung alternativ mit einem monetären Preisschild zu versehen. Dies würde womöglich den vom Verantwortlichen durchschnittlich erwarteten Mindestwert von personenbezogenen Daten offenbaren und Behörden und Gerichte hätten mit diesen monetären Preisen zumindest einen ersten Anhaltspunkt für die Angemessenheitskontrolle, weil sie infolgedessen (vermeintlich) ähnliche Leistungsangebote unterschiedlicher Verantwortlicher vergleichen könnten. Somit führt ein strenges anbieterbezogenes Kopplungsverbot zu einer Ausweitung der Information über die jeweiligen Leitungsangebote der Verantwortlichen. Dennoch bliebe es schwierig, die Angemessenheit der synallagmatischen Leistungsversprechen inhaltlich zu überprüfen.

Festzuhalten ist, dass die Freiwilligkeit nicht allein deshalb gefährdet wird, weil ein Verantwortlicher die Einwilligung mit (anderen) vertraglichen Klauseln verknüpft und Datensubjekte sich einen Zugang zu diesen Leistungen wünschen[75] oder die Einwilligung lediglich ein höheres Maß an Komfort und Bequemlichkeit ermöglicht.[76] Infolgedessen ist eine Einwilligung auch nicht allein deshalb unfreiwillig, weil die alternativen Angebote objektiv weniger attraktiv oder teurer sind.[77] Letztlich hängt die Angemessenheit im Einzelfall von zahlreichen Faktoren ab, einschließlich der subjektiven Datenschutz-Präferenzen und der jeweiligen Kaufkraft eines Datensubjekts, die sowohl individuell als auch durch das durchschnittliche Einkommensniveau in einem EU-Mitgliedstaat geprägt werden.

Sofern man Art. 7 Abs. 4 DS-GVO als *marktbezogenes* Kopplungsverbot versteht, hätte dies zwar einerseits den Vorteil, dass die Angemessenheitsprüfung automatisch die Angebote anderer Wettbewerber als Maßstab miteinbeziehen könnte. Hierbei besteht jedoch die Schwierigkeit, dass im ersten Schritt komplexe Marktabgrenzungen durchgeführt werden müssen, um die Substituier-

---

[74] Kapitel 3 C.I.2.e.

[75] So: *Metzger*, AcP 216 (2016), 817 (823); *Buchner*, DuD 2010, 39 (41).

[76] A. A. und für eine Anwendung unabhängig von einer Angewiesenheit des Datensubjekts auf die Leistung: *Hacker*, Datenprivatrecht, 2020, S. 192 („Datenschutz und Wahlfreiheit sollten nicht dort enden, wo die Freizeitgestaltung beginnt").

[77] *Schweitzer/Fetzer/Peitz*, Digitale Plattformen: Bausteine für einen künftigen Ordnungsrahmen, Discussion Paper, No. 16-042, S. 21 f.; *Buchner*, Die Informationelle Selbstbestimmung, 2006, S. 265 f.

barkeit der Produkte jeweils bewerten zu können. Erst anschließend kann der monetäre Preis für ein anerkanntes Substitut zumindest einer (Evidenz-)Kontrolle unterzogen werden,[78] um beurteilen zu können, ob dieses alternative Angebot gegen Zahlung eines monetären Preises angemessen ist. Nur sofern das Substitut zu einem angemessenen monetären Preis verfügbar ist, wäre die Entscheidung zugunsten einer Einwilligung in die Datenverarbeitung und gegen das Angebot mit Geldzahlungspflicht freiwillig i. S. d. Art. 7 Abs. 4 DS-GVO.

Unabhängig davon, ob man Art. 7 Abs. 4 DS-GVO als anbieterbezogenes oder lediglich als marktbezogenes Kopplungsverbot interpretiert, setzt die praktische Anwendung dieser beiden Herangehensweisen einen Bewertungsmaßstab für den jeweiligen Einzelfall voraus. Bereits an dieser Stelle wird offenkundig, dass die praktische Umsetzung eines solchen Kopplungsverbots einen sehr komplexen Tatsachenvortrag und eine hohe ökonomische Beurteilungskompetenz voraussetzt.[79] Sowohl das Verständnis als anbieterbezogenes als auch eine Auslegung als marktbezogenes Kopplungsverbots laufen deshalb (erneut) auf ökonomische Sachverständigengutachten oder – mit *Philipp Hacker* – auf die Zugrundelegung einer hypothetischen Verhandlungssituation zwischen durchschnittlichen Referenzakteuren hinaus[80] und enden damit in einem aufwändigen Verfahren, das im Ergebnis tendenziell auf eine Anmaßung von Wissen durch den jeweiligen juristischen Entscheider hinausläuft. Verantwortungsbewusste Gerichte vermeiden es, unter dem Mantel der rechtlichen Angemessenheit inzident über Preise zu entscheiden.[81]

Die *zweite* Herausforderung dieses Ansatzes lässt sich anhand des Verfahrens des *BKartA* gegen *Facebook* (jetzt: *Meta Platforms*) illustrieren. Dieses verdeutlicht zugleich, dass nicht einmal die auf das Kartellrecht und ökonomische Marktabgrenzungsfragen spezialisierten Institutionen darüber einig sind, wie Art. 7 Abs. 4 DS-GVO im kartellrechtlichen Kontext zu interpretieren ist.[82]

---

[78] Für die Vorgängervorschrift: *Buchner*, Die informationelle Selbstbestimmung im Privatrecht, 2006, S. 266 („Es kann daher im Ergebnis für die Frage der Zumutbarkeit immer nur auf eine *abstrakte* Zumutbarkeit ankommen, es muss dem Einzelnen überhaupt zumutbar sein, einen in seinem Kernangebot vergleichbaren Dienst in Anspruch zu nehmen. Da dieser alternative Dienst *vergleichsweise* teurer oder schlechter ist, spielt dagegen eine Rolle") [Hervorhebungen im Original].

[79] A. A. *Golland*, MMR 2018, 130 (134 f.). Die praktischen Schwierigkeiten erkennend, aber mit einem (hyper)komplexen Anwendungsvorschlag: *Hacker*, Datenprivatrecht, 2020 S. 190/486 ff./646 f.

[80] *Hacker*, Datenprivatrecht, 2020, S. 474; hierzu bereits oben Kapitel 3 C.I.2.e.

[81] Dies ist auch der Grund dafür, warum Gerichte sich mit einer monetären Bewertung oder sogar Bezifferung von patentrechtlichen FRAND-Lizenzen zurückhalten, obwohl die Verfahrensbeteiligten regelmäßig jeweils Angebot vorlegen, so dass insoweit eine bessere Beurteilungsgrundlage besteht, als im Kontext des Datenschutzrechts. Hierzu: *BGH*, Urt. v. 05.05.2020, KZR 36/17 = GRUR 2020, 961 (Rn. 73–81) – *FRAND-Einwand* (m. Anm. *Picht*).

[82] Leider musste der *BGH* sich aufgrund der von ihm verfolgten Schadenstheorie mit dieser Frage weder vertieft auseinandersetzen noch eine Vorlage zum *EuGH* erwägen: *BGH*, Beschl. v. 23.06.2020, KVR 69/19 = NZKat 2020, 473 (Rn. 107) – *Facebook*.

So kam das *BKartA* zu der Einschätzung, dass die Freiwilligkeit gemäß Art. 7 Abs. 4 DS-GVO „jedenfalls" dann fehle, wenn der Einwilligungsempfänger eine marktbeherrschende Stellung habe.[83] Dieser Ansicht ist das *OLG Düsseldorf* im Kontext des Missbrauchstatbestands (§ 19 GWB) mit der Auffassung entgegengetreten, dass es sich bei Art. 7 Abs. 4 DS-GVO um eine datenschutzrechtliche und keine kartellrechtliche Vorschrift handele.[84] Zudem habe das *BKartA* verkannt, dass – trotz der für Teile des Angebots bestehenden marktbeherrschenden Stellung von *Facebook*[85] – niemand gezwungen sei, einen Vertrag mit *Facebook* einzugehen.[86] Infolgedessen sei auch die im Rahmen des Vertragsschlusses erforderliche Erteilung einer Einwilligung nicht unfreiwillig.[87]

Die Entscheidungen von *BKartA* und *OLG Düsseldorf* haben unmissverständlich offengelegt, dass die Auslegung von Art. 7 Abs. 4 DS-GVO weitreichende Konsequenzen für das Kartellrecht hat.[88] Unverkennbar basiert Art. 7 Abs. 4 DS-GVO – ebenso wie der Anspruch auf Portabilität von personenbezogenen Daten (Art. 20 DS-GVO) – maßgeblich auf wettbewerbspolitischen Überlegungen.[89] Beide Vorschriften sind gleichsam kartellrechtlich geprägte Vorposten innerhalb des Datenschutzrechts. Infolgedessen steht die Anwendung von Art. 7 Abs. 4 DS-GVO stets in einer Wechselbeziehung zum kartellrechtlichen Verbot des Missbrauchs einer marktbeherrschenden Stellung.

bb) Freiwilligkeit als Ursache kompetenzieller Konflikte

Obwohl das Kartellverfahren des *BKartA* gegen *Facebook* (jetzt: *Meta Platforms*) immerhin innerhalb des durch Sonderzuständigkeiten geprägten kartell-

---

[83] *BKartA*, Beschl. v. 06.02.2019 (B6–22/16) Rn. 621 ff./646.

[84] *OLG Düsseldorf*, Beschl. v. 26.08.2019, VI-Kart 1/19 (V), BeckRS 2019, 18837 Rn. 67; sowie Vorlagefrage 6 des *OLG Düsseldorf*, Vorlagebeschl. v. 24.03.2021, Kart 2/19 (V), Rn. 68 (hierbei aber nicht auf Art. 7 Abs. 4, sondern direkt auf die Freiwilligkeit i. S. d. Art. 4 Nr. 11 DS-GVO abstellen).

[85] *BKartA*, Beschl. v. 06.02.2019 (B6–22/16) Rn. 413: mehr als 90 % Marktanteil von Facebook auf dem relevanten Markt; sowie: Rn. 417: „Lediglich Facebook.com bietet sämtliche Funktionalitäten zur Abbildung eines virtuellen sozialen Raumes an".

[86] So zuvor bereits: *Körber*, NZKart 2019, 187 (191).

[87] *OLG Düsseldorf*, Beschl. v. 26.08.2019, VI-Kart 1/19 (V), BeckRS 2019, 18837 Rn. 69 und 75.

[88] Der Beschluss des *BKartA* in Sachen *Facebook* (Beschl. v. 06.02.2019 (B6–22/16)) wurde deshalb kritisiert, weil er über die Bande des Datenschutzrechts den kartellrechtlichen Missbrauchstatbestand mit Blick auf das Merkmal der Ausbeutung und der Kausalität aufweicht: *Körber*, NZKart 2019, 187 (191 f.); *Lohse*, NZKart 2020, 292. Der BGH vertritt nun eine „normative" Kausalität (BGH, Beschl. v. 23.06.2020, KVR 69/19 = NZKart 2020, 863 – *Facebook*). Mit der Reform des § 19(a) durch die 10. GWB-Novelle hat der Gesetzgeber die strengere, vom *OLG Düsseldorf* geforderte Verhaltenskausalität zwischen der Marktmacht und der Durchführung der wettbewerbsschädigenden Handlung, abgelehnt: Zum ganzen *Mackenrodt/Wiedemann*, ZUM 2021, 89 (94).

[89] Skeptisch gegenüber diesem wettbewerbsrechtlichen Ansatz des Art. 20 DS-GVO innerhalb des Datenschutzrechts: *Hennemann*, PinG 2017, 5 (5 f.).

rechtlichen Behörden- und Gerichtsstrangs geblieben ist, haben die unterschiedlichen Entscheidungen von *BKartA*, *OLG Düsseldorf*[90] und *BGH*[91] eindrücklich offengelegt, dass Art. 7 Abs. 4 DS-GVO nicht nur der Kristallisationspunkt von materiell-rechtlichen Spannungen zwischen Kartell- und Datenschutzrecht ist, sondern auch einen kompetenziellen Konflikt heraufbeschwört.[92]

Zwar lässt sich vertreten, dass Art. 7 Abs. 4 DS-GVO ein mikroökonomischer Ansatz zugrunde liegt, weil er auf jede einzelne Einwilligung anwendbar ist. Insoweit unterscheidet er sich von Art. 102 AEUV und §§ 19 f. GWB, mit denen vorrangig makroökonomische Ziele verfolgt werden. Sofern aber die Anforderungen an die Freiwilligkeit gemäß Art. 7 Abs. 4 DS-GVO nicht nur in kontradiktorischen Zivilprozessen, sondern auch durch Datenschutzbehörden, Kartellbehörden und Verwaltungsgerichte geprüft und Verstöße zudem kollektiv durch Verbände über das UKlaG[93] und womöglich über §§ 3a, 8 Abs. 3 Nr. 1 UWG noch zusätzlich durch Mitbewerber durchgesetzt werden können,[94] überschneiden sich die Anwendungsbereiche und Zuständigkeiten in erheblichem Ausmaß.

Aus strenger kartellrechtlicher Perspektive ist ein derart rigoroser Ansatz wie ein anbieterbezogene Kopplungsverbot bislang nur für einen monopolistischen Markt plausibel, auf dem aus Sicht der Nachfrager keinerlei Substitute zur Verfügung stehen[95] und sofern Güter betroffen sind, die zur zivilisatorischen Daseinsvorsorge zählen.[96] Je strengere Anforderungen an eine Freiwilligkeit im Sinne des Art. 7 Abs. 4 DS-GVO gestellt werden, desto geringer wird die Bedeutung der spezifischeren Tatbestandsvoraussetzungen von §§ 19, 19a, 20 GWB bzw. Art. 102 AEUV für solche Verträge, die personenbezogene Daten als Leistungsgegenstand vorsehen.[97]

---

[90] *OLG Düsseldorf*, Beschl. v. 26.08.2019, VI-Kart 1/19 (V), BeckRS 2019, 18837 Rn. 69 und 75.

[91] *BGH* (Kartellsenat), Beschl. v. 23.06.2020, KVR 69/19 = NZKart 2020, 473 – *Facebook II*.

[92] Hierzu aus kartellrechtlicher Perspektive: *Körber*, NZKart 2019, 187 (193 ff).

[93] *BGH*, Beschl. v. 28.05.2020, I ZR 186/17 (KG) = GRUR 2020, 896 (Rn. 33 ff.) – *App-Zentrum*.

[94] Zum hierüber bestehenden Streit: *Köhler*, WRP 2018, 1269 (1269); gegen eine lauterkeitsrechtliche Klagebefugnis von Mitbewerben: *LG Bochum*, K&R 2018, 737; *LG Wiesbaden*, K&R 2019, 281; *LG Magdeburg*, K&R 2019, 210; *LG Stuttgart*, WRP 2019, 1089 (Rn. 13 ff.); *Köhler*, ZD 2018, 337; *ders.*, WRP 2019, 1279; *Ohly*, GRUR 2019, 686; *Spittka* GRUR-Prax. 2019, 4. Für eine Klagebefugnis von Mitwerbern: *OLG Hamburg*, WRP 2018, 1510 (Rn. 25); *OLG Naumburg*, GRUR 2020, 210; *Uebele,* GRUR 2019, 694 ff.

[95] Deshalb für eine Begrenzung des Art. 7 Abs. 4 DS-GVO auf Fälle, in denen der Verantwortliche ein Monopolist ist: *Plath*, in: Plath (Hrsg.), DSGVO/BDSG, 2018, Art. 7, Rn. 19 f.; *Schneider*, Datenschutz nach der EU-Datenschutz-Grundverordnung, 2019, S. 166; *Schulz*, in: Gola (Hrsg.), DS-GVO, 2018, Art. 7, Rn. 27/29.

[96] Für eine Liste mit aus ihrer Sicht relevanten Leistungen der zivilisatorischen Grundversorgung für die ein strenges Kopplungsverbot gelten müsse: *Roßnagel/Pfitzmann/Garstka*, Modernisierung des Datenschutzrechts, Gutachten im Auftrag des Bundesministeriums des Inneren, 2001, S. 93.

[97] Nicht überzeugen können die oberflächlichen Ausführungen des *BGH*, wonach sowohl das Recht auf informationelle Selbstbestimmung und DS-GVO als auch das nationale Ver-

Umgekehrt sollte eine datenschutzrechtliche Einwilligung im Einzelfall dann unfreiwillig sein, wenn sie auf dem Missbrauch einer marktbeherrschenden Stellung beruht. Dies ist bereits der Fall, wenn der Verantwortliche die Einwilligung des Datensubjekts als sonstige Geschäftsbedingungen gemäß Art. 102 S. 2 lit. a AEUV erzwingt. Dennoch hätte es nicht geschadet, diesen kartellrechtlichen Sachverhalt in ErwG 43 DS-GVO als das offensichtliche, vom Datenschutzrecht unabhängige Beispiel einer unfreiwilligen Einwilligung zu erwähnen.[98]

Allein die Existenz von Art. 7 Abs. 4 DS-GVO und der Wortlaut von ErwG 43 S. 1 DS-GVO sprechen somit dafür, dass wettbewerbsrechtliche und -politische Erwägungen bereits unterhalb der kartellrechtlichen Schwelle eines Missbrauchs einer marktbeherrschenden Stellung zur Unfreiwilligkeit der Einwilligung führen können („in Anbetracht aller Umstände in dem speziellen Fall").[99] Allerdings führt bereits diese Selbstverständlichkeit zu der Schwierigkeit, die jeweiligen institutionellen Zuständigkeiten zwischen Kartell- und Datenschutzrecht abzugrenzen.

Während der *BGH* davon ausgeht, dass das *BKartA* das Datenschutzrecht berücksichtigen kann,[100] hat das *OLG Düsseldorf* an dieser Rechtsaufassung Zweifel und sieht einen potenziellen Konflikt zur Zuständigkeitsregelung gemäß Art. 56 Abs. 1 DS-GVO.[101] Zudem habe Deutschland der *EU-Kommission* die § 19 und § 32 GWB nicht gemäß Art. 86 Abs. 2 DS-GVO als Vorschriften mitgeteilt, die neben der DS-GVO andere Sanktionen für datenschutzrechtliche

---

tragsrecht und die DS-GVO nebeneinander anwendbar sind. Sowohl für die Einwilligung als auch die vertragsakzessorische Datenverarbeitung macht die DS-GVO die wesentlichen Vorgaben, *direkt* über die detaillierten Tatbestandsvoraussetzungen der Einwilligung und die „Erforderlichkeit" i. R. v. Art. 6 Abs. 1 lit. b DS-GVO und indirekt über die zu beachtenden Grundsätze der rechtmäßigen Datenverarbeitung (Art. 5 Abs. 1 DS-GVO). Der Versuch des BGH, das nationale Vertragsrecht gegenüber der DS-GVO zu immunisieren, ist nachvollziehbar, hätte aber gemäß Art. 267 Abs. 3 AEUV einer Vorlage zum *EuGH* bedurft; *BGH*, Beschl. v. 23.06.2020, KVR 69/19 = NZKart 2020, 863 (109) – *Facebook*. Diese erfolgt nun durch Vorlagefrage 3 des *OLG Düsseldorf*, Vorlagebeschl. v. 24.03.2021, Kart 2/19 (V). Das Verfahren wird vom EuGH unter dem Aktenzeichen C-252/21 geführt.

[98] Mit dieser Auffassung nun: *OLG Düsseldorf*, Vorlagebeschl. v. 24.03.2021, Kart 2/19 (V) Rn. 68. Zu weit geht jedoch eine Auslegung, wonach die wettbewerbliche Situation und insbesondere die Marktmacht des Verantwortlichen im Rahmen von Art. 7 Abs. 4 nicht zu berücksichtigen sei: *Stemmer*, in: Brink/Wolff (Hrsg.), BeckOK DatenschutzR, 28. Ed. 2018, Art. 7 DS-GVO, Rn. 44 f.; *Golland*, MMR 2018, 130 (132 f.).

[99] Ebenso: *Heckmann/Paschke*, in: Ehmann/Selmayr (Hrsg.), DS-GVO, 2018, Art. 7, Rn. 52; *Buchner*, WRP 2019, 1243 (1245); *ders.*, WRP 2018, 1283 (1286); *ders./Kühling*, in: Kühling/Buchner (Hrsg.), 2020, Art. 7, Rn. 52 f.; *Klement*, in: Simitis/Hornung/Spiecker gen. Döhmann (Hrsg.), Datenschutzrecht, 2019, Art. 7, Rn. 62; *Ingold*, in: Sydow (Hrsg.), DS-GVO, 2018, Art. 7, Rn. 33; *Hacker*, Datenprivatrecht, 2020, S. 188 f.

[100] *BGH*, Beschl. v. 23.06.2020, KVR 69/19 = NZKart 2020, 863 (Rn. 126) – *Facebook*.

[101] Das OLG Düsseldorf hat diese offenen Abgrenzungsfragen nun zurecht dem *EuGH* vorgelegt: Vorlagefragen 1 und 7 des *OLG Düsseldorf*, Vorlagebeschl. v. 24.03.2021, Kart 2/19 (V). Das Verfahren wird vom *EuGH* unter dem Aktenzeichen C-252/21 geführt.

Verstöße vorsehen.[102] Sollte das *BKartA* neben der datenschutzrechtlich zuständigen und bereits aktiv gewordenen *Irischen Datenschutzbehörde* ebenfalls Verstöße gegen die DS-GVO prüfen und anschließend mit den Mitteln des Kartellrechts sanktionieren können, so würde dies schwierige Fragen zur Abgrenzung und Hierarchie aufwerfen, für die mit der Verpflichtung zur loyalen Zusammenarbeit aus Art. 4 Abs. 3 EUV[103] lediglich ein sehr abstrakter Grundsatz zur Verfügung steht.

Diesen Bedenken des *OLG Düsseldorf* ist hinzuzufügen, dass es nicht genügt, wenn Datenschutz- und Kartellrecht irgendwann potenziell beim *EuGH* zusammengeführt werden. Vielmehr ist es erforderlich, die jeweilige Zuständigkeit und Kompetenz entweder klar zu trennen oder bereits auf der jeweils nationalen Ebene in einer Behörde zu bündeln.[104]

Dieses Erfordernis ist in Deutschland seit dem 01.01.2021 umso dringlicher geworden, weil § 19a Abs. 2 Nr. 4a GWB nunmehr dem *BKartA* ausdrücklich die Befugnis einräumt,[105] es einem Unternehmen mit überragender marktübergreifender Bedeutung für den Wettbewerb zu untersagen,

„die Nutzung von Diensten davon abhängig zu machen, dass Nutzer der Verarbeitung von Daten aus anderen Diensten des Unternehmens oder eines Drittanbieters zustimmen, ohne den Nutzern eine ausreichende Wahlmöglichkeit hinsichtlich des Umstands, des Zwecks und der Art und Weise der Verarbeitung einzuräumen."

Gerade weil diese institutionellen Abgrenzungsschwierigkeiten nicht neu sind, ist es verblüffend, dass die DS-GVO über dieses Spannungsverhältnis wortlos hinweggeht.[106] Offenkundig ist zudem, dass die Bedeutung des Kartellrechts im Bereich der Verarbeitung von personenbezogenen Daten umso merklicher zurückgeht, je strengere Maßstäbe die Datenschutzbehörden und Gerichte an die Freiwilligkeit einer Einwilligung gemäß Art. 7 Abs. 4 DS-GVO anlegen (dürfen).[107]

---

[102] *OLG Düsseldorf*, Vorlagebeschl. v. 24.03.2021, Kart 2/19 (V), Rn. 28 f.

[103] *OLG Düsseldorf*, Vorlagebeschl. v. 24.03.2021, Kart 2/19 (V), Rn. 30.

[104] *Fanta*, Europas Behörden wollen Datenschutz und Wettbewerbsrecht verheiraten; Netzpolitik, 10.07.2019 (https://netzpolitik.org/2019/europas-behoerden-wollen-datenschutz-und-wettbewerbsrecht-verheiraten/, zuletzt abgerufen am 19.05.2022). Mit Skepsis gegenüber dieser Möglichkeit: *Körber*, NZKart 2019, 187 (194 f.).

[105] Auf Grundlage des neuen § 19a Abs. 1 GWB hat das *BKartA* zuletzt ein Verfahren gegen *Apple* eingeleitet: Pressemitteilung v. 21.06.2021 (https://www.bundeskartellamt.de/SharedDocs/Meldung/DE/Pressemitteilungen/2021/21_06_2021_Apple.html, zuletzt abgerufen am 19.05.2022).

[106] Die „Wettbewerbsbehörden" werden nur beispielhaft im Kontext einer Datenübermittlungen aufgrund wichtiger Gründe des öffentlichen Interesses erwähnt (ErwG 112 S. 1 DS-GVO.

[107] Dies verdeutlicht die Anordnung des *HmbBfDI* gegen Facebook: Verbot der Weiterverarbeitung von WhatsApp-Nutzerdaten durch *Facebook*, Pressemitteilung v. 11.05.2021: „Ferner erfolgt die Zustimmung nicht aus freien Stücken, da WhatsApp die Einwilligung in die neuen Bestimmungen als Bedingung für die Weiternutzung der Funktionalitäten des Dienstes einfordert", (https://datenschutz-hamburg.de/pressemitteilungen/2021/05/2021-05-11-facebook-anordnung, zuletzt abgerufen am 19.05.2022).

Der kartellrechtliche Zusammenhang von Art. 7 Abs. 4 DS-GVO spricht dafür, dass eine Auslegung als *generelles*, anbieterbezogenes Kopplungsverbot ausscheidet, weil diese Auslegung die Voraussetzungen der europäischen und nationalen kartellrechtlichen Missbrauchstatbestände deutlich unterschreitet. Art. 7 Abs. 4 DS-GVO würde jede Kopplung zwischen (anderen) vertraglichen Klauseln und der datenschutzrechtlichen Einwilligung als missbräuchlich behandeln, völlig unabhängig von den jeweiligen sektorspezifischen Marktstrukturen und davon, ob ein Verantwortlicher eine überragende marktübergreifende Bedeutung für den Wettbewerb i. S. d. § 19a Abs. 1 S. 2 GWB hat. Eine solche Auslegung als *generelles*, anbieterbezogenes Kopplungsverbot würde jeden Versuch einer Abgrenzung der Zuständigkeit zwischen Datenschutz- und Kartellbehörden unterlaufen. Zudem ist eine solche Auslegung weder mit der Gewährleistung der unionsgrundrechtlich gewährten Vertragsfreiheit noch mit der unternehmerischen Freiheit vereinbar.[108]

Es würde für die Wahrung der Verhältnismäßigkeit auch nicht genügen, dass der Verantwortliche dieses strenge Kopplungsverbot immerhin „durch Vertragsgestaltung oder die Eröffnung einer monetären Alternative […] aushebeln" könnte.[109] Zumindest die Ausweichmöglichkeit über Art. 6 Abs. 1 lit. b DS-GVO – die nach hier vertretener Auffassung zudem nicht zur Verfügung steht[110] – würde die gemäß Art. 8 Abs. 2 S. 1 GRCh unionsgrundrechtlich garantierte Möglichkeit zur Einwilligung für das Privatrechtsverhältnis weitgehend aushöhlen. Zunehmend würde eine gerichtliche Interessenabwägung gemäß Art. 6 Abs. 1 lit. f DS-GVO über die Rechtmäßigkeit von Geschäftsmodellen entscheiden. Zudem wären nach diesem Verständnis *alle* Verantwortlichen dazu gezwungen, einen zusätzlichen Antrag zu unterbreiten, der keine datenschutzrechtliche Einwilligung, sondern eine Geldzahlung vorsieht.

Obwohl nach hier vertretener Auffassung eine Auslegung von Art. 7 Abs. 4 DS-GVO als *generelles* anbieterbezogenes oder marktbezogenes Kopplungsverbot abzulehnen ist, weil dieses Verständnis die Datenschutzbehörden und Gerichte überfordert und zu einer problematischen Doppelzuständigkeit für Kartell- und Datenschutzrecht führen würde,[111] bleibt die Marktmacht des Verantwortlichen dennoch *ein* wesentliches Kriterium für die Beurteilung der Freiwilligkeit einer Einwilligung.

---

[108] So auch *Heckmann/Paschke*, in: Ehmann/Selmayr (Hrsg.), DSGVO, 2. Aufl. 2018, Art. 7, Rn. 95/97/99; *Schulz*, in: Gola (Hrsg.), DS-GVO, 2018, Art. 7, Rn. 24; *Lohse*, NZKart 2020, 292 (294).

[109] In dieser Möglichkeit sieht *Hacker* einen Grund dafür, warum trotz des (strengen) Kopplungsverbots noch ein schonender Ausgleich zwischen den beteiligten Grundrechten und Interessen möglich sei: *ders.*, Datenprivatrecht, 2020, S. 194.

[110] Zur (auch) hier vertretenen restriktiven Auslegung der vertragsakzessorischen Datenverarbeitung bereits oben, Kapitel 3 D.

[111] *Körber*, NZKart 2020, 187 (194 f.).

cc) Kartellrechtsakzessorische und asymmetrische Anwendung

Sofern Art. 7 Abs. 4 DS-GVO nicht faktisch die Schwelle des kartellrechtlichen Missbrauchstatbestands für solche Geschäftsmodelle absenken soll, die den Zugang zu personenbezogenen Daten als (Gegen-)Leistung vorsehen, liegt es nahe, seine Anwendung auf individuelle Einwilligungen zu begrenzen und eher flexible Anforderungen an die Freiwilligkeit zu stellen. Deshalb sind bei der Auslegung und Anwendung von Art. 7 Abs. 4 DS-GVO die Konsequenzen für den kartellrechtlichen Missbrauchstatbestand – nach hier vertretener Ansicht – zwingend zu berücksichtigen.[112]

Eine wesentliche Herausforderung für die Synchronisierung von Kartellrecht und Datenschutzrecht entsteht, sofern Datenschutzbehörden und nicht auf Fragen des Kartellrechts spezialisierte Behörden und Spezialkammern der Gerichte sich berufen fühlen, im Rahmen von Art. 7 Abs. 4 DS-GVO eigene Marktanalysen vorzunehmen oder das Fehlen der Freiwilligkeit der Einwilligung pauschal mit einer starken Marktposition des Verantwortlichen zu begründen.

Um dies zu verhindern, muss es aus formal kompetenziellen und spezifisch fachlichen Gründen zunächst der jeweiligen nationalen Kartellbehörde bzw. der *EU-Kommission* überlassen bleiben, die Marktmacht eines Verantwortlichen zu beurteilen, bevor die Datenschutzbehörden das Kriterium der Marktmacht heranziehen können, um die Freiwilligkeit einer Einwilligung maßgeblich mit *dieser Begründung* abzulehnen.

Infolgedessen kann das Kriterium der Marktmacht die Unfreiwilligkeit i. S. d. Art. 7 Abs. 4 DS-GVO auch nur begründen, *soweit* eine Kartellbehörde die Marktmacht für den relevanten Markt ausdrücklich festgestellt hat oder diese aufgrund einer abgeschlossenen Sektor- oder Marktuntersuchung des *BKartA* bzw. der *EU-Kommission* zumindest eine sehr hohe Plausibilität hat.[113]

Dieses restriktive Verständnis von Art. 7 Abs. 4 DS-GVO, wonach diese Vorschrift kein generelles Kopplungsverbot etabliert, sondern lediglich dazu auffor-

---

[112] Ebenfalls für eine Berücksichtigung der Marktmacht, allerdings im Rahmen einer freien Abwägung der Interessen und Grundrechte/-freiheiten der Beteiligten: *Engeler*, ZD 2018, 55 (58 f.); *Klement*, in: Simitis/Hornung/Spiecker gen. Döhmann (Hrsg.), Datenschutzrecht, 2019, Art. 7, Rn. 58.

[113] Eine zusätzliche Ausnahme kommt in Betracht, sofern eine Aufsichtsbehörde von der Dringlichkeit einer Anordnung ausgeht und mit Blick auf die Ziele der DS-GVO begründet. Somit ist auch die Anordnung des *HmbBfDI* gegen *Facebook* mit dem hier vertretenen Ansatz einer kartellrechtsakzessorischen, asymmetrischen Anwendung von Art. 7 Abs. 4 DS-GVO zu vereinbaren, wenngleich die Argumente „Datenleck" und „bevorstehende Bundestagswahl" sachlich nicht weiterführen: *HmbBfDI*, Verbot der Weiterverarbeitung von WhatsApp-Nutzerdaten durch *Facebook*, Pressemitteilung v. 11.05.2021: „Ferner erfolgt die Zustimmung nicht aus freien Stücken, da *WhatsApp* die Einwilligung in die neuen Bestimmungen als Bedingung für die Weiternutzung der Funktionalitäten des Dienstes einfordert", (https://datenschutz-hamburg.de/pressemitteilungen/2021/05/2021-05-11-facebook-anordnung, zuletzt abgerufen am 19.05.2022).

dert, eine strukturelle Unterlegenheit des Datensubjekts aufgrund der Marktmacht des Verantwortlichen *kartellrechtsakzessorisch* zu berücksichtigen, wird durch aktuelle Gesetzgebungsinitiativen der *EU-Kommission* bestätigt.

Gemäß Art. 1 Abs. 7 DMA-Vorschlag wäre die *EU-Kommission* vorrangig dafür zuständig, Anbieter von zentralen Plattformdiensten i.S.d. Art. 2 Abs. 2 DMA-Vorschlag[114] bei Vorliegen der Voraussetzungen gemäß Art. 3 DMA-Vorschlag als sog. *Gatekeeper* zu benennen. Eine Benennung als *Gatekeeper* soll nach den Vorschlägen der *EU-Kommission* gemäß Art. 5 lit. a DMA-Vorschlag zur Folge haben, dass der *Gatekeeper* in Bezug auf seine zentralen Plattformdienste[115] keine personenbezogenen Daten und Endnutzerdaten zusammenführen darf, es sei denn, dem Datensubjekt bzw. dem Endnutzer wurde

„diesbezüglich gemäß [DS-GVO] eine Wahl gegeben […] und er [hat] eingewilligt".[116]

Weil diese Formulierung nicht nur auf die datenschutzrechtliche Einwilligung und deren Voraussetzungen Bezug nimmt, sondern zusätzlich ausdrücklich die Bedeutung einer Wahlmöglichkeit betont, spricht dies dafür, dass auch die *EU-Kommission* den Art. 7 Abs. 4 DS-GVO nicht als generelles strenges Kopplungsverbot auffasst. Nur bei diesem Verständnis wäre das Tatbestandsmerkmal erforderlich, wonach gerade im Fall der Einwilligung gegenüber einem *Gatekeeper* – zusätzlich zu den datenschutzrechtlichen Anforderungen an die Freiwilligkeit (Art. 7 Abs. 4 DS-GVO) – zudem eine Wahlmöglichkeit bestehen muss.[117]

Dieses Ergebnis wird durch den DSA-Vorschlag der *EU-Kommission*[118] nochmals bestätigt. Hiernach sollen (große) Online-Plattformen gemäß Art. 29 Nr. 1 DSA-Vorschlag dazu verpflichtet sein, ihre Leistungen auch in einer Variante ohne Profiling i.S.d. Art. 4 Nr. 4 DS-GVO anzubieten. Hieraus kann im

---

[114] Hierunter fallen: Online-Vermittlungsdienste, Online-Suchmaschinen, Online-Dienste sozialer Netzwerke, Video-Sharing-Plattform-Dienste, nummernunabhängige interpersonelle Kommunikationsdienste, Betriebssysteme, Cloud-Computing-Dienste, Werbedienste, einschließlich Werbenetzwerken, Werbebörsen und sonstiger Werbevermittlungsdienste, die von dem Betreiber eines der zuvor genannten zentralen Plattformdienste betrieben werden.

[115] Hierzu: Art. 3 Abs. 7 DMA-Vorschlag.

[116] Vergleiche insoweit den Wortlaut von § 19a Abs. 2 Nr. 4a GWB „die Nutzung von Diensten davon abhängig zu machen, dass Nutzer der Verarbeitung von Daten aus anderen Diensten des Unternehmens oder eines Drittanbieters *zustimmen*, *ohne* den Nutzern eine *ausreichende Wahlmöglichkeit* hinsichtlich des Umstands, des Zwecks und der Art und Weise der Verarbeitung einzuräumen" [Hervorhebung durch den Verfasser].

[117] Andererseits steht die Bezugnahme auf die DS-GVO vor den Anforderungen „Wahl" und „Einwilligung", so dass diese Vorschrift mit dem Hinweis auf eine Wahlmöglichkeit auch Art. 7 Abs. 4 DS-GVO meinen könnte. Dann wäre dieser Hinweis allerdings deshalb überflüssig, weil die Wahlmöglichkeit als Teil der Freiwilligkeit bereits im (komplexen) Begriff der Einwilligung enthalten wäre.

[118] Vorschlag der EU-Kommission für eine Verordnung über einen Binnenmarkt für digitale Dienste (Gesetz über digitale Dienste oder kurz: DSA), v. 15.12.2020, COM(2020) 825 final.

Umkehrschluss gefolgert werden, dass sich eine solche generelle Pflicht zum alternativen Angebot nach Ansicht der *EU-Kommission* noch nicht *de lege lata* aus Art. 7 Abs. 4 DS-GVO ergibt.

Art. 4 Abs. 3 DMA-Vorschlag sieht vor, dass die *EU-Kommission* die Liste der *Gatekeeper* und ihrer zentralen Plattformdienste veröffentlichen und laufend aktualisieren muss. Diese Liste könnte nicht nur von den Kartellbehörden herangezogen werden, um zu überwachen, ob die *Gatekeeper* die geplanten Verpflichtungen des DMA-Vorschlags einhalten. Vielmehr könnten auch Datenschutzbehörden und Gerichte mit der widerleglichen Vermutung arbeiten, dass die Einwilligung in die Datenverarbeitung gegenüber einem von der *EU-Kommission* gelisteten *Gatekeeper* grundsätzlich nur dann gemäß Art. 7 Abs. 4 DS-GVO freiwillig ist, wenn *dieser Gatekeeper* selbst auch einen alternativen Zugang gegen ein monetäres Entgelt zur Verfügung stellt (sog. anbieterbezogenes Kopplungsverbot).[119] Infolgedessen würde die Nennung in der Liste der *Gatekeeper* zu einer Synchronisierung der kartellrechtlichen und datenschutzrechtlichen Beurteilung führen. Dieser Ansatz im DMA-Vorschlag der *EU-Kommission* würde mit dem hier gemachten Vorschlag einer *kartellrechtsakzessorischen* Anwendung des Kriteriums der Marktmacht im Rahmen von Art. 7 Abs. 4 DS-GVO korrespondieren.

Dies gilt jedoch nicht für das umgekehrte Verhältnis: Nur weil eine Geschäftspraktik eines Verantwortlichen auf Grundlage einer Einwilligung durch eine Datenschutzbehörde oder ein Gericht für datenschutzrechtlich zulässig erachtet wurde, hat dies keine Konsequenzen für die kartellrechtliche Beurteilung als Missbrauch einer marktbeherrschenden Stellung bzw. als Verstoß gegen die Pflicht aus Art. 5 lit. a DMA-Vorschlag.[120] Diese Beurteilung ist weiterhin ausschließlich und abschließend dem *BKartA* bzw. der *EU-Kommission* vorbehalten und kann nicht durch die Anwendung und Auslegung von Art. 7 Abs. 4 DS-GVO präjudiziert werden. Allerdings steht es den Kartellbehörden offen, bereits gefestigte datenschutzrechtliche Argumente zu verwerten, solange dadurch keine eigenständige und abweichende Auslegung und Anwendung des Datenschutzrechts im kartellrechtlichen Verfahren etabliert wird.[121] Die Arbeitsteilung zwischen Kartellbehörden und Datenschutzbehörden erfolgt also *einseitig zwingend*, indem Datenschutzbehörden und Gerichte bei der Beurteilung der Freiwilligkeit i. S. d. Art. 7 Abs. 4 DS-GVO auf die von den Kartellbehörden geprüfte Marktmacht eines Verantwortlichen zurückgreifen müssen.

---

[119] Oben C.II.1.a.

[120] *Buiten*, Journal of Antitrust Enforcement 2020, 1 (9) (https://doi.org/10.1093/jaenfo/jnaa041, zuletzt abgerufen am 19.05.2022); *BGH*, Beschl. v. 23.06.2020, KVR 69/19 = NZKart 2020, 863 (Rn. 99) – *Facebook*.

[121] Zur Gefahr, dass die Kartellbehörden, das erst in Erstehung begriffene Datenschutzrecht „eigenmächtig" und ohne Vorlage(pflicht) zum *EuGH* auslegen: *Körber*, NZKart 2020, 187 (194 f.).

Dieses Vorgehen ermöglicht es, die Zuständigkeit von Kartellbehörden und Datenschutzbehörden auf Basis der fachlichen Kompetenz besser voneinander abzugrenzen und stellt mit dem – von den Kartellbehörden geprüften – Kriterium der Marktmacht einen sachlichen Grund dafür zur Verfügung, den Art. 7 Abs. 4 DS-GVO *kartellrechtsakzessorisch* und infolgedessen *asymmetrisch* anzuwenden.

Asymmetrisch ist dieser Ansatz deshalb, weil zwar KMU regelmäßig, d. h. abgesehenen von anderen Ursachen, die Zweifel an der Freiwilligkeit begründen, digitale Produkte im Austausch gegen eine Einwilligung in eine Verarbeitung von personenbezogenen Daten anbieten können. Im Gegensatz dazu, können sich aber insbesondere *GAFAM* und andere gelistete *Gatekeeper* (DMA-Vorschlag) bzw. Unternehmen mit überragender marktübergreifender Bedeutung für den Wettbewerb (GWB) nur auf eine freiwillige Einwilligung für die Nutzung ihrer zentralen Plattformdienste berufen, soweit sie ihre hierauf basierenden Leistungen zugleich auch im Austausch gegen ein monetäres Entgelt anbieten, das zumindest einer groben Evidenzkontrolle auf dessen Angemessenheit standhält.

Mit diesem *kartellrechtakzessorischen* und *asymmetrischen* Ansatz wird der wettbewerbspolitische Zweck des Art. 7 Abs. 4 DS-GVO verwirklicht, aber die Entscheidung über das Vorliegen von Marktmacht verbleibt dennoch bei den fachlich kompetenten nationalen Kartellbehörden und der *EU-Kommission*.[122] Weil die Feststellung des *BKartA* über die Eigenschaft als Unternehmen mit überragender marktübergreifender Bedeutung für den Wettbewerb gemäß § 19a Abs. 1 S. 3 GWB auf fünf Jahre befristet ist und die künftig geplante Benennung als *Gatekeeper* durch die *EU-Kommission* gemäß Art. 4 Abs. 1 bzw. Abs. 2 DMA-Vorschlag jederzeit, zumindest aber nach zwei Jahren überprüfbar ist, wird die Marktdynamik ausreichend berücksichtigt.

Gegenüber einem *generellen* anbieter- oder marktbezogenen Kopplungsverbot hat diese *kartellrechtsakzessorische*, *asymmetrische* Anwendung von Art. 7 Abs. 4 DS-GVO zudem den Vorteil, dass sie keine Marktzutrittsbarriere für KMU und neue datenbasierte Geschäftsmodelle etabliert. Im Gegenteil: Solange und soweit weder das *BKartA* festgestellt hat, dass ein Verantwortlicher ein Unternehmen „mit überragender marktübergreifender Bedeutung für den Wettbewerb" i. S. d. § 19a Abs. 1 S. 2 Nr. 4 GWB ist,[123] noch die *EU-Kommission* den Verantwortlichen als *Gatekeeper* i. S. d. Art. 3 DMA-Vorschlag benannt

[122] Zum Verhältnis zwischen den nationalen und europäischen Behörden vgl. Art. 1 Abs. 7 DMA-Vorschlag der *EU-Kommission*. „Die nationalen Behörden erlassen keine Entscheidungen, die einem von der Kommission nach dieser Verordnung erlassenen Beschluss zuwiderlaufen würden. Hinsichtlich der Durchsetzungsmaßnahmen arbeiten die Kommission und die Mitgliedstaaten eng zusammen und stimmen sich eng ab".

[123] Gesetz zur Änderung des Gesetzes gegen Wettbewerbsbeschränkungen für ein fokussiertes, proaktives und digitales Wettbewerbsrecht 4.0 und anderer Bestimmungen (GWB-Digitalisierungsgesetz) v. 18.01.2021, BGBl. I, S. 2 ff.

hat, kommt dem Verantwortlichen mit Blick auf die Einwilligung eine Flexibilität zugute, die *GAFAM* für eine Vielzahl ihrer Geschäftsbereiche gerade nicht mehr zur Verfügung steht. Dieser Ansatz hat zudem indirekte Folgen für den Erwerb von Unternehmen mit datenbasierten Geschäftsmodellen, weil eine Unternehmensübernahme durch *GAFAM* häufig dazu führen wird, dass auch der von *GAFAM* übernommene Verantwortliche fortan der *kartellrechtsakzessorischen* Auslegung von Art. 7 Abs. 4 DS-GVO unterliegt. Mit der Übernahme von *WhatsApp* durch *Facebook* hätte es bei einer strengen kartellrechtsakzessorischen Auslegung von Art. 7 Abs. 4 DS-GVO nahegelegen, dass eine Einwilligung gegenüber *WhatsApp* nur noch freiwillig erfolgen kann, sofern *WhatsApp* seine Dienste ebenfalls gegen ein – jedenfalls nicht evident unangemessenes – monetäres Entgelt anbietet.

Kurzum: Unabhängig von der Fusionskontrolle sollte die Übernahme eines erfolgreichen, aber selbst noch nicht marktmächtigen Unternehmens i. S. d. § 19a Abs. 1 S. 2 Nr. 4 GWB durch ein marktmächtiges Unternehmen bzw. einen *Gatekeeper* zu einer strengeren Anwendung von Art. 7 Abs. 4 DS-GVO führen. Hierdurch fördert die *kartellrechtsakzessorische*, *asymmetrische* Anwendung von Art. 7 Abs. 4 DS-GVO den Wettbewerb und hilft dabei, dass grundrechtlich zu gewährleistende Untermaß zugunsten der informationellen Privatautonomie (Art. 8 GRCh) sicherzustellen, ohne dabei unverhältnismäßig in die ebenfalls zu gewährleistende unternehmerische Freiheit (Art. 16 GRCh) und das allgemeine Grundrecht der Vertragsfreiheit (Art. 6 Abs. 3 EUV) einzugreifen.

Diese *kartellrechtsakzessorische* und *asymmetrische* Anwendung von Art. 7 Abs. 4 DS-GVO steht im Einklang mit § 19a Abs. 2 Nr. 4 lit. a GWB und Art. 5 lit. a DMA-Vorschlag. Zudem bietet sie einstweilen ein milderes Mittel im Vergleich zu der beiderseits des Atlantiks zunehmend in Erwägung gezogenen gesetzlich angeordneten Desintegration großer Plattformbetreiber.[124]

Gleichwohl stellen sich schwerwiegende Abgrenzungsfragen, solange es nicht gelingt, die wettbewerbsrechtlichen und durch Kartellbehörden initiierten Verfahren (Art. 102 AEUV, § 19 ff. GWB)[125] mit den initiierten datenschutzrechtlichen Dringlichkeitsverfahren der Datenschutzbehörden (Art. 66

[124] Vgl. den (nachgebesserten) Antrag des *FTC* gegen *Facebook* vom 19.08.2021, Case No.: 1:20-cv-03590-JEB (https://www.ftc.gov/system/files/documents/cases/ecf_75-1_ftc_v_facebook_public_redacted_fac.pdf, zuletzt abgerufen am 19.05.2022); *Hoppe/Riecke*, Kartellamtschef Mundt bezeichnet Zerschlagung von Tech-Riesen als „letztes Mittel", Handelsblatt, 18.03.2021 (https://www.handelsblatt.com/politik/international/digitalkonzerne-kartellamtschef-mundt-bezeichnet-zerschlagung-von-tech-riesen-als-letztes-mittel/27014042.html, zuletzt abgerufen am 19.05.2022); *FAZ* „Reif für eine große Zerschlagung", Interview mit Florian Ederer v. 05.08.2021 (https://www.faz.net/aktuell/wirtschaft/tech-konzerne-laut-yale-oekonom-reif-fuer-eine-zerschlagung-17470011.html, zuletzt abgerufen am 19.05.2022).

[125] Zuletzt *OLG Düsseldorf*, Beschl. v. 24.03.2021 – Kart 2/19 (V). Das Verfahren wird vom EuGH unter dem Aktenzeichen C-252/21 geführt.

Abs. 1 DS-GVO)[126] vor den Verwaltungsgerichten zu synchronisieren, obwohl für beide die Auslegung der Freiwilligkeit gemäß Art. 7 Abs. 4 DS-GVO entscheidungserheblich ist und beide eine Verfügungen zur Untersagung einer Zusammenführung von (unterschiedlichen) personenbezogenen Daten innerhalb eines Konzerns als Rechtsfolge vorsehen.[127]

2. Kriterium: Eigenschaften des Datensubjekts

In Übereinstimmung mit Art. 8 GRCh und Art. 16 AEUV zielt die DS-GVO auf den Schutz des Datensubjekts, also eines menschlichen Individuums ab. Insofern ist es auf den ersten Blick konsequent, dass die DS-GVO grundsätzlich keine weiteren Differenzierungen enthält, die an spezifische Eigenschaften einer natürlichen Person anknüpfen. Eine Ausnahme von diesem undifferenzierten Ansatz bildet die besondere Berücksichtigung von Kindern (a).

Zudem fordert der europäische Gesetzgeber in ErwG 43 S. 1 DS-GVO ausdrücklich dazu auf, ein klares Ungleichgewicht zwischen Datensubjekt und Verantwortlichem zu berücksichtigen. Dies zwingt dazu, bei der Beurteilung der Freiwilligkeit einer Einwilligung die Umstände des Einzelfalls und damit auch andere persönliche Eigenschaften von Datensubjekten zu beachten. Es liegt deshalb nahe, zumindest zu berücksichtigen, ob das Datensubjekt als Verbraucher oder Unternehmer handelt (b).

a) Einwilligung durch Kinder

Die DS-GVO kennt nur eine besondere Unterkategorie von Datensubjekten. Gemäß Art. 8 Abs. 1 DS-GVO ist die Einwilligungsfähigkeit von Kindern im Bereich von Diensten der Informationsgesellschaft auf das vollendete 16. Lebensjahr herabgesetzt und kann durch die Mitgliedstaaten gemäß Art. 8 Abs. 3 DS-GVO nochmals auf das 13. Lebensjahr reduziert werden.[128] Im Gegensatz zu dieser Erleichterung der Einwilligung durch Herabsetzung des Alters für die Einwilligungsfähigkeit wird im Rahmen der Interessenabwägung (Art. 6 Abs. 1 lit. f DS-GVO), der Verhaltensregeln (Art. 40 Abs. 2 lit. g DS-GVO) und der

---

[126] So: *HmbBfDI*, Hamburger Dringlichkeitsverfahren gegen *Facebook* im Zusammenhang mit den neuen WhatsApp-Nutzungsbedingungen eröffnet, Pressemitteilung v. 13.04.2021 (https://datenschutz-hamburg.de/pressemitteilungen/2021/04/2021-04-13-facebook, zuletzt abgerufen am 19.05.2022).

[127] Ohne unionsweite Klärung von Art. 7 Abs. 4 DS-GVO: Anordnung des *HmbBfDI* gegen Facebook: Verbot der Weiterverarbeitung von WhatsApp-Nutzerdaten durch Facebook, Pressemitteilung v. 11.05.2021: „Ferner erfolgt die Zustimmung nicht aus freien Stücken, da WhatsApp die Einwilligung in die neuen Bestimmungen als Bedingung für die Weiternutzung der Funktionalitäten des Dienstes einfordert", (https://datenschutz-hamburg.de/pressemitteilungen/2021/05/2021-05-11-facebook-anordnung, zuletzt abgerufen am 19.05.2022).

[128] Hierzu Kapitel 4 A.II.1.

Aufgaben der Aufsichtsbehörden (Art 57 Abs. 1 lit. b S. 2 DS-GVO) die besondere Schutzbedürftigkeit von Kindern herausgestellt. Auch für die Beurteilung der Freiwilligkeit einer Einwilligung kann es von Bedeutung sein, ob das einwilligende Datensubjekt ein Kind ist.

Indem ErwG 43 S. 1 DS-GVO dazu auffordert, ein klares Ungleichgewicht zwischen Datensubjekt und Verantwortlichem zu berücksichtigen, öffnet er den Tatbestand der Freiwilligkeit nicht nur für eine Berücksichtigung der Marktstruktur (Kartellrecht), sondern auch für das konkrete Marktverhalten (UWG). Anders formuliert: Die abstrakte Altersgrenze für die Einwilligungsfähigkeit in Art. 8 Abs. 1 DS-GVO schließt es nicht aus, das Alter darüber hinaus als ein Kriterium für ein Ungleichgewicht zwischen Verantwortlichem und Datensubjekt im Rahmen der Prüfung der Freiwilligkeit im konkreten Einzelfall zu berücksichtigen.

Sofern minderjährige Datensubjekte auch Verbraucher sind, so dass das Verhalten des Verantwortlichen im Vorfeld der Einwilligung auch an den Anforderungen der Richtlinie 2005/29/EG vom 11.05.2005 über unlautere Geschäftspraktiken im binnenmarktinternen Geschäftsverkehr zwischen Unternehmen und Verbrauchern (UGP-RL)[129] zu messen ist (hierzu sogleich: 3.), kann die Minderjährigkeit dieser Datensubjekte dann bei der Beurteilung der Freiwilligkeit einbezogen werden, wenn sich die geschäftliche Handlung vorrangig an Minderjährige richtet oder sich faktisch besonders auf diese auswirkt und dies für einen Unternehmer vernünftigerweise vorhersehbar ist. Wie sich aus ErwG 19 UGP-RL ergibt, zählen zu den berücksichtigungsfähigen Eigenschaften insbesondere das Alter oder die Leichtgläubigkeit einer Person in Bezug auf eine Geschäftspraxis oder ein Produkt.

Während die Einwilligungsfähigkeit gemäß Art. 8 Abs. 1 DS-GVO eine eindeutige und klare Altersgrenze kennt[130] und damit eine formelle Voraussetzung für die Einwilligung zieht, legt ErwG 43 S. 1 DS-GVO ein Verständnis der Freiwilligkeit der Einwilligung nahe, das stärker dazu dient, die Einwilligung im Einzelfall zu „materialisieren". Dies hat zur Folge, dass es der DS-GVO zwar im Grundsatz nicht darum geht, das Verhalten des Verantwortlichen am Markt zu regeln[131] und beispielsweise dessen aggressive Praktiken dadurch zu sanktionieren, dass die Freiwilligkeit der Einwilligung entfällt und

---

[129] ABl. v. 11.06.2005, 149, S. 22 ff.

[130] Diese steht ihrerseits gemäß Art. 8 Abs. 3 DS-GVO in einem Spannungsverhältnis zur Geschäftsfähigkeit nach dem jeweils nationalen Recht.

[131] So aus der umgekehrten Perspektive, also mit dem Fokus auf der umstrittenen Frage, ob bzw. unter welchen (ggfs. zusätzlichen) Voraussetzungen Verstöße gegen datenschutzrechtliche Bestimmungen zu lauterkeitsrechtlichen Ansprüchen durch Mitbewerber führen können, jeweils m. w. N.: *Köhler*, WRP 2018, 1269 ff.; *ders.* in: Köhler/Bornkamm/Feddersen (Hrsg.), UWG, 39. Aufl. 2021, § 3a, Rn. 1.40 ff.; *Ohly*, GRUR 2019, 868 (892). Zur diesbezüglichen Vorlage an den EuGH: *BGH*, Beschl. v. 28.05.2020 – I ZR 186/17 = GRUR 2020, 896 ff. – *App-Zentrum*.

anschließend ein Bußgeld aufgrund der rechtswidrigen Datenverarbeitung verhängt wird. Weil die Freiwilligkeit der Einwilligung jedoch eine Tatbestandsvoraussetzung ist, muss sie – anders als die Wirksamkeit einer Willenserklärung im Fall einer Drohung (gemäß § 123 Abs. 1 BGB wirksam, aber anfechtbar) – von Amts wegen geprüft werden. Dies hat zur Folge, dass die Freiwilligkeit zwar eine spezifisch datenschutzrechtliche Voraussetzung ist. Sie kann jedoch aufgrund von Verhaltensweisen entfallen, die ebenfalls Gegenstand von lauterkeitsrechtlichen Regelungen sind. Insofern ist es zwar richtig, dass die aggressive geschäftliche Handlung ein Umstand ist, der im Datenschutzrecht nicht abschließend berücksichtigt wird. Es bleibt insoweit ein eigener Regelungsbereich mit autonomen Kriterien für unlauteres Verhalten nach dem UWG.[132] Allerdings folgt daraus umgekehrt kein Verbot, ein (auch) originär lauterkeitsrechtlich relevantes Verhalten im Rahmen der Beurteilung der Freiwilligkeit einer Einwilligung zu berücksichtigen.

Dies hat zur Folge, dass das Verhalten eines Verantwortlichen die Freiwilligkeit der Einwilligung entfallen lässt und darüber hinaus – bei Ausnutzung einer Machtposition durch den Unternehmer – eine aggressive geschäftliche Handlung gegenüber einem Verbraucher i. S. d. von § 4a Abs. 1, Abs. 2 S. 2 und S. 3 UWG sein *kann*.[133] Obwohl ErwG 43 S. 1 DS-GVO die strukturelle Unterlegenheit eines Datensubjekts gegenüber dem Verantwortlichen als wesentlichen Umstand für die Beurteilung der Freiwilligkeit der Einwilligung nennt, muss bei der Beurteilung eines Sachverhalts somit zwischen der lauterkeitsrechtlichen und der datenschutzrechtlichen Bewertung differenziert werden. Zugleich sperrt die datenschutzrechtliche Beurteilung der Freiwilligkeit einer individuellen datenschutzrechtlichen Einwilligung nicht die Anwendung des UWG (Art. 4 Abs. 4 UGP-RL).[134]

Dies lässt sich anhand des Sachverhalts illustrieren, der dem *BGH*-Urteil „Nordjob-Messe" zugrunde lag. Auf einer Job-Messe für Jugendliche wurde ein Gewinnspiel angeboten, an dem Jugendliche nur teilnehmen konnten, wenn sie zahlreiche personenbezogene Daten preisgaben. Der *BGH* sah darin eine lauterkeitsrechtlich unzulässige Ausnutzung der Unerfahrenheit von jugendlichen Verbraucher durch den Unternehmer.[135] Obwohl die Verknüpfung der Teilnahme an einem Gewinnspiel mit einer datenschutzrechtlichen Einwilligung für (personalisierte) Werbemaßnahmen grundsätzlich nicht gegen das Kopplungsverbot des Art. 7 Abs. 4 DS-GVO verstößt,[136] dürften die der UGP-

[132] *Ohly*, GRUR 2019, 868 (892).

[133] Hierzu: *Ohly*, GRUR 2019, 868 (892).

[134] Für eine solche Sperrwirkung in Bezug auf die spezifischen datenschutzrechtlichen Informationspflichten aus Art. 13, 14 DS-GVO: *Ohly*, GRUR 2019, 868 (893).

[135] So noch zu § 4 UWG a. F.(2004): *BGH*, GRUR 2014, 682 – *Nordjob-Messe*; vgl. auch *OLG Frankfurt a. M.*, GRUR 2005, 785 – *Skoda-Autokids-Club*.

[136] Mit sehr knapper Begründung: *OLG Frankfurt a. M.*, Urt. v. 27.06.2019 – 6 U 6/19 = ZD 2019, 507 (Rn. 12).

RL zugrundeliegenden Wertungen des europäischen Gesetzgebers auch für die Beurteilung der Freiwilligkeit i.S.d. Art. 7 Abs. 4 DS-GVO ausschlaggebend sein, solange daraus ein Ungleichgewicht zwischen Verantwortlichem und Datensubjekt folgt, dass nicht ausschließlich mit dem Alter des Datensubjekts begründet wird.[137]

Umgekehrt kann aus der Unfreiwilligkeit einer datenschutzrechtlichen Einwilligung nicht automatisch auf das Vorliegen einer unzulässigen Beeinflussung i.S.d. Art. 9 Abs. 1 lit. c UGP-RL bzw. § 4a Abs. 1 S. 2 Nr. 3 UWG geschlossen werden. Während § 4a Abs. 1 S. 3 UWG die Ausnutzung einer Machtposition des Unternehmers gegenüber einem Verbraucher *voraussetzt*, ist für die Beurteilung der Freiwilligkeit lediglich dem Umstand einer „klaren Unterlegenheit" des Datensubjekts *Rechnung zu tragen*, ErwG 43 S. 1 DS-GVO.

Zwar spricht der gemäß Art. 8 Abs. 1 GRCh unionsgrundrechtlich gewährleistete besondere Schutz des Datensubjekts im Ausgangspunkt für eine strenge Auslegung der Freiwilligkeit, weil es insoweit nicht lediglich um die wirtschaftlichen Interessen eines Kindes als Marktteilnehmer geht. Eindeutig ist das Verhältnis zwischen datenschutzrechtlicher Freiwilligkeit und lauterkeitsrechtlicher Bewertung als aggressive Handlung jedoch schon deshalb nicht, weil Art. 8 Abs. 1 DS-GVO jedenfalls 16-Jährige als Erwachsene im Sinne des Datenschutzrechts behandelt, ohne dass hieraus automatisch Konsequenzen für die Beurteilung im Rahmen des Art. 5 Abs. 3 UGP-RL bzw. des § 4a Abs. 2 S. 3 UWG folgen.[138]

b) Unternehmerisch handelnde Datensubjekte

Abgesehen von der ausdrücklichen Erwähnung von Kindern enthält die DS-GVO keine Anknüpfungen an die persönlichen Eigenschaften von Datensubjekten. Diese indifferente Herangehensweise ist ein Rückschritt im Vergleich zu dem (bisherigen) Schutz der Persönlichkeit durch das nationale Recht der Mitgliedstaaten und hat gravierende Nachteile. Eine wesentliche Konsequenz ist, dass unternehmerisch handelnde Datensubjekte von der DS-GVO im Aus-

[137] Aufgrund der in Art. 8 Abs. 1 DS-GVO getroffenen Wertung, scheidet das Alter der Datensubjekte ab Vollendung des 16. Lebensjahres – ohne Hinzutreten anderer besonderer Umstände – als Argument für eine Unfreiwilligkeit aus, soweit der Verantwortliche Dienste der Informationsgesellschaft anbietet.

[138] Mit der Erwartung, diese Altersabsenkung werde auch Druck auf die Altersgrenzen für die Geschäftsfähigkeit ausüben: *Klement*, in: Simitis/Hornung/Spiecker gen. Döhmann (Hrsg.), Art. 8, Rn. 33. Zudem stellt sich die Frage, inwieweit aus dem datenschutzrechtlichen Begriff des Kindes als einer Person bis zum 16. Geburtstag (Art. 8 Abs. 1 DS-GVO) etwas für den gleichlautenden Begriff im sonstigen europäischen Sekundärrecht – beispielsweise Nr. 28 des Anhang I der UGP-RL – folgt. Nochmals komplexer wird die Antwort auf diese Frage ausfallen, wenn man auch die durch die datenschutzrechtliche Öffnungsklausel des Art. 8 Abs. 3 DS-GVO ermöglichte Definition von Kindern als Personen zwischen 0 und 13 Jahren über den Anwendungsbereich der DS-GVO ausdehnen würde.

gangspunkt ebenso behandelt werden wie diejenigen Datensubjekte, die Verbraucher sind.

Allerdings bedeutet diese Undifferenziertheit nicht, dass typische Eigenschaften von Personengruppen oder die – für einen Verantwortlichen erkennbaren – individuellen Eigenschaften eines Datensubjekts bei der Auslegung und Anwendung von Art. 7 Abs. 4 DS-GVO unberücksichtigt bleiben, ErwG 43 S. 1 DS-GVO. Handelt eine natürliche Person unternehmerisch und kommerzialisiert ihre Persönlichkeitsrechte, beispielsweise im Rahmen einer Tätigkeit als sog. Influencer für unterschiedliche Unternehmen oder als traditioneller Werbeträger für ein Unternehmen oder Produkt, so muss Art. 7 Abs. 4 DS-GVO sehr zurückhaltend angewendet werden. Die in diesem Kontext regelmäßig stattfindende Verarbeitung personenbezogener Daten trifft ein unternehmerisch handelndes Datensubjekt und die Einwilligung wird in diesem Fall vom Datensubjekt bewusst und zielgerichtet eingesetzt, um Einkommen oder andere ökonomische Vorteile zu erzielen. Unternehmerisch handelnde Datensubjekt sind gegenüber Verantwortlichen *prima facie* nicht schutzwürdig und Datenschutzbehörden und Gerichte dürfen nicht über Bande spielen, indem sie anhand des Tatbestandsmerkmals der Freiwilligkeit gemäß Art. 7 Abs. 4 DS-GVO zu einer regelmäßigen Prüfung der Angemessenheit der synallagmatischen Leistungsbeziehung im B2B-Verhältnis kommen.

Erfolgt die datenschutzrechtliche Einwilligung im B2B-Verhältnis, so sind die personenbezogenen Daten regelmäßig Teil des vertraglichen Synallagmas und das unternehmerisch handelnde Datensubjekt erhält im Austausch als (Gegen-)Leistung ein monetäres Honorar oder eine andere Leistung. Für diese vom europäischen Gesetzgeber bei Verabschiedung der DS-GVO mutmaßlich übersehene Konstellation ist eine strenge Auslegung von Art. 7 Abs. 4 DS-GVO unangemessen.

Sofern man der hier vertretenen restriktiven Auslegung von Art. 6 Abs. 1 lit. b DS-GVO folgt oder sofern auch besonders sensible personenbezogene Daten i. S. d. Art. 9 Abs. 1 DS-GVO verarbeitet werden – hierfür kann die Verarbeitung eines Portraitfotos bereits ausreichen –, kommt es auf die Einwilligung des unternehmerisch handelnden Datensubjekts zwingend an, so dass Art. 7 Abs. 4 DS-GVO im B2B-Verhältnis erst recht lediglich als Gebot zur Berücksichtigung der Umstände des Einzelfalls interpretiert werden muss.

Eine Auslegung von Art. 7 Abs. 4 DS-GVO im Sinne eines anbieterbezogenen oder auch nur marktbezogenen Kopplungsverbots[139] würde unverhältnismäßig in die unternehmerische (Vertrags-)Freiheit der beteiligten Unternehmer eingreifen und wäre deshalb gemäß Art. 52 Abs. 1 S. 2 GRCh unionsgrundrechtwidrig. Deshalb ist Art. 7 Abs. 4 DS-GVO – jedenfalls – im B2B-Verhältnis und sofern der Verantwortliche nicht von einer Kartellbehörde als markt-

[139] Oben C.II.2.b.

mächtiges Unternehmen gelistet wird, zwingend als generalklauselartiges Berücksichtigungsgebot auszulegen, um mit dem Unionsprimärrecht vereinbar zu sein.

3. Kriterium: Situationsadäquates Verhalten des Verantwortlichen

Wie bereits in Bezug auf minderjährige Datensubjekte angesprochen, kann im Rahmen der Beurteilung der Freiwilligkeit einer Einwilligung auf die im Unionsrecht bereits seit Jahren bekannten Kriterien der UGP-RL zurückgegriffen werden.[140]

Zwar ist dabei zu berücksichtigen, dass bereits die vollharmonisierende UGP-RL nur im B2C-Anwendung findet und individuelle Verbraucher aufgrund der Umsetzung im UWG selbst bislang nicht klagebefugt waren.[141] Dieser besondere lauterkeitsrechtliche Rahmen schließt es aber nicht aus, die im unionsrechtlichen Lauterkeitsrecht zum Ausdruck gebrachten Wertungen auch bei der Beurteilung der Freiwilligkeit einer Einwilligung durch unternehmerisch handelnde Datensubjekte zu berücksichtigen. Führen diese Wertungen zu einer Unfreiwilligkeit der Einwilligung, so kann dies in eigene datenschutzrechtliche Ansprüche des Datensubjekts auf Unterlassung[142] und auf Schadensersatz münden.

Weil eine Beeinträchtigung des Datensubjekts durch eine Nötigung, einschließlich körperlicher Gewalt, ganz offensichtlich die Freiwilligkeit einer Einwilligung ausschließt, ist vorrangig die in Art. 9 Abs. 1 lit. c UGP-RL genannte unzulässige Beeinflussung interessant. Im Rahmen der Beurteilung, ob eine Beeinflussung unzulässig ist, sind entsprechend Art. 9 Abs. 1 lit. a UGP-RL der Zeitpunkt, der Ort, die Art oder die Dauer ihres Einsatzes zu berücksichtigen. Entsprechend Art. 9 Abs. 1 lit. c UGP-RL ist es hierbei insbesondere

---

[140] ABl. v. 11.06.2005, 149, S. 22 ff.

[141] Zur Änderung dieses Grundsatzes: Art. 3 Ziff. 5 der Richtlinie (EU) 2019/2161 v. 27.11.2019 zur Änderung der Richtlinie 93/13/EWG des Rates und der Richtlinien 98/6/EG, 2005/29/EG und 2011/83/EU des Europäischen Parlaments und des Rates zur besseren Durchsetzung und Modernisierung der Verbraucherschutzvorschriften der Union (Omnibus-Richtlinie – ABl. v. 18.12.2019, L 328 S. 7 ff.), der die UGP-Richtlinie um einen neuen Artikel 11a ergänzt, welcher die EU-Mitgliedstaaten dazu verpflichtet, Verbrauchern Zugang zu angemessenen und wirksamen Rechtsbehelfen, einschließlich Ersatz des entstandenen Schadens zu gewährleisten. Diese Vorgabe ist durch § 9 Abs. 2 S. 1 UWG-E des Gesetzesentwurfs der Bundesregierung zur Stärkung des Verbraucherschutzes im Wettbewerbs- und Gewerberecht vom 20.01.2021 umgesetzt worden.

[142] Die Grundlage für einen solchen Anspruch ist bislang noch offen: Umstritten ist, ob Art. 79 Abs. 1 DS-GVO einen Unterlassungsanspruch des Datensubjekts begründet (dafür: *VG Regensburg*, BeckRS 2020, 19361, Ls. 2) oder den Unterlassungsanspruch aus den §§ 823, 1004 BGB zumindest nicht sperrt (dafür: *LG Frankfurt a. M.*, Urt. v. 18.09.2020, 2-27 O 100/20 GRUR-RS 2020, 28899 (Rn. 1 f.); *LG Hamburg*, Urt. v. 04.09.2020, 324 S 9/19BeckRS 2020, 23277 (Rn. 21); *LG München I*, Urt. v. 07.11.2019, 34 O 13123/19 = ZD 2020, 204 (Rn. 28 f.).

von Bedeutung, ob vom Verantwortlichen eine konkrete Unglückssituation oder andere Umstände von solcher Schwere ausgenutzt werden, dass diese das Urteilsvermögen des Datensubjekts beeinträchtigen können.

In Anhang I Nr. 24–31 UGP-RL (sog. schwarze Liste) hat der europäische Gesetzgeber mehrere Verhaltensweisen von Unternehmern erfasst, die im Verhältnis zu Verbrauchern als aggressive Geschäftspraktiken stets unzulässig sind. Obwohl diese nicht auf die datenschutzrechtliche Einwilligung eingehen, haben sie den Zweck, die Entscheidungsfreiheit von Verbrauchern zu schützen und können deshalb im Rahmen von Art. 7 Abs. 4 DS-GO argumentativ herangezogen werden, sofern das Datensubjekt zugleich Verbraucher ist.

Obwohl die Beispiele der schwarzen Liste der UGP-RL weder auf die Besonderheiten von digitalen Sachverhalten noch auf Fälle im Kontext von personenbezogenen Daten ausgerichtet sind, können ihnen doch Wertungen des europäischen Gesetzgebers entnommen werden, die sich auch auf die datenschutzrechtliche Einwilligung übertragen lassen.

Beispielsweise erklärt Nr. 24 Anhang I UGP-RL (bzw. Nr. 25 Anhang UWG) es für aggressiv und unzulässig, wenn ein Unternehmer den Eindruck erweckt, der Verbraucher könne die Räumlichkeiten ohne Vertragsabschluss nicht verlassen. Gemäß Nr. 6 lit. b Anhang I UGP-RL (bzw. Nr. 6 Anhang UWG) ist es eine unzulässige aggressive geschäftliche Handlung, wenn ein Unternehmer den Verbraucher zum Kauf eines Produkts zu einem bestimmten Preis auffordert, sich dann aber weigert, eine Bestellung für das beworbene Produkt anzunehmen oder dieses innerhalb einer vertretbaren Zeit zu liefern. Gemäß Nr. 6 lit. c Anhang I UGP-RL ist es zudem unzulässig, wenn statt des beworbenen Artikels ein fehlerhaftes Exemplar in der Absicht präsentiert wird, stattdessen ein anderes Produkt abzusetzen (sog. „*bait-and-switch*"-Technik).

Grundsätzlich passen weder Nr. 24 noch Nr. 6 Anhang I UGP-RL für digitale Austauschverhältnisse. Die Anwendung der beiden Tatbestände ist jedenfalls ursprünglich auf die analoge Welt beschränkt. Ferner verbietet sich eine entsprechende Anwendung für diese gemäß § 3 Abs. 3 UWG stets unzulässigen geschäftlichen Handlungen, die keine anschließende Interessenabwägung zulassen. Zudem ist die Suggestion, ein Verbraucher sei physisch eingesperrt (Nr. 24 Anhang I UGP-RL) in qualitativer Hinsicht nicht mit einer Situation vergleichbar, in der einem Verbraucher im digitalen Umfeld suggeriert wird, er müsste eine Einwilligung erklären, um Zugang zu digitalen Produkten zu erlangen.

Dennoch lässt sich den Regelungen eine zugrundeliegende Wertung des europäischen Gesetzgebers entnehmen, die sich auf die Gestaltung von Webseiten und insbesondere auf die Umstände der Erteilung der Einwilligung in eine Datenverarbeitung auf Grundlage von *tracking* (*cookies*, *finger printing* etc.) übertragen lässt, sofern die Anzeigen im Browser eingefroren und unscharf gestellt wird, die Datensubjekte zur Einwilligung in *third-party-tracking* aufgefordert

werden („Allen Cookies zustimmen") und alternative Nutzungsmöglichkeiten der Webseite nur über kaum erkennbare und verschlungene digitale Pfade erreichbar sind. Infolgedessen ist es nicht ausgeschlossen, dass Manipulationsversuche und die Suggestion einer Drucksituation im Einzelfall zu einer unzulässigen Beeinflussung im Sinne des § 4a Abs. 1 Nr. 3, S. 3 UWG führen kann und die Freiwilligkeit der Einwilligung gemäß Art. 7 Abs. 4 DS-GVO deshalb ebenfalls ausgeschlossen ist.[143]

Allerdings bestehen hierfür enge Grenzen. Nur weil die Digitalisierung – vermeintlich – neue Varianten aggressiver geschäftlicher Handlungen hervorbringt, sollten die über Jahrzehnte gewachsenen Einsichten aus der analogen Welt nicht leichtsinnig über Bord geworfen werden. Obwohl die Möglichkeiten zur Beeinflussung im digitalen Umfeld tatsächlich eigenständig zu analysieren und zu bewerten sind, sollten die von der Rechtsprechung ursprünglich zu § 1 UWG a. F. entwickelten Fallgruppe des sog. physischen Kaufzwangs[144] und des sog. übertriebenen Anlockens[145] nicht vorschnell aus der lauterkeitsrechtlichen Mottenkiste hervorgekramt und unreflektiert auf digitale Sachverhalte angewendet werden, nur weil Erkenntnisse über die menschliche Entscheidungspsychologie auch im digitalen Umfeld durch Unternehmen in eigenem Interesse und zur Erlangung einer Einwilligung in die Datenverarbeitung genutzt werden.

Sinnvoll erscheint es dagegen, den Anhang der UGP-RL bzw. des § 3 Abs. 3 UWG (schwarze Liste) dahingehend zu überprüfen, ob bestimmte Praktiken gegenüber Verbrauchern[146] als stets unzulässige geschäftliche Handlungen definiert werden sollten oder ob es insoweit genügt, wenn die Gerichte diese im Einzelfall anhand von § 4a Abs. 1 Nr. 2 und Nr. 3 UWG überprüfen.

Als Illustration für ein Verhalten des Verantwortlichen, dass nicht mehr situationsadäquat ist und deshalb die Freiwilligkeit der Einwilligung ausschließt, kann eine abgewandelte Reaktion von *Tesla* im Vorfeld des Hurrikans *Irma* dienen.

Tesla nutzt ein nicht nur in der Automobilbranche übliches Modell der gezielten Preisdifferenzierung. Hierfür wird die technisch verfügbare höhere Leistung eines Kfz beim Kauf oder Leasing einer günstigeren Modellvariante mithilfe der Steuerungs-Software gezielt gedrosselt.

---

[143] Hier überschneidet sich die Freiwilligkeit mit der Informiertheit der Einwilligung (Art. 4 Nr. 11 DS-GVO) und dem Grundsatz der Transparenz (Art. 5 Abs. 1 lit. a DS-GVO).

[144] Hierzu: *Leistner*, ZGE 2009, 3 (24 ff.); *Scherer*, WRP 2005, 672; *Steinbeck*, WRP 2008, 865; sowie: *Sosnitza*, in: Ohly/Sosnitza, UWG, 7. Aufl. 2016, § 4a, Rn. 21–24.

[145] Nach der Aufgabe dieser Fallgruppe durch die Rechtsprechung nur noch auf die grundsätzliche Rationalität der Nachfrageentscheidung abstellend: *Köhler*, GRUR 2003, 729, (736); *Ohly*, GRUR 2004, 889 (897); *Sosnitza*, in: Ohly/Sosnitza, UWG, 7. Aufl. 2016, § 4a, Rn. 66 f.

[146] Zu den begrifflich bereits negativ konnotierten sogenannten „Dark Pattern" als Versuche der Einflussnahme auf Entscheidungen der Datensubjekte: *Martini/Drews/Seeliger/Weinzierl*, ZfDR 2021, 47 (57/62 f.).

Laut Medienberichten[147] erreichte *Tesla* im September 2017 die Anfrage eines Kunden, wonach diesem eine Batterie-Reichweite von ca. 30 Meilen fehlte, um die in Vorbereitung auf den Hurrikan behördlich festgelegte Evakuierungszone zu verlassen. Daraufhin übermittelte *Tesla* im Weg der Fernwartung ein *software-gesteuertes Upgrade* auf alle Fahrzeuge, die sich innerhalb oder in der Nähe der behördlich festgelegten Evakuierungszone befanden. Dieses ermöglichte den Kunden des günstigeren, durch Software technisch gedrosselten Fahrzeugs die Nutzung der vollständigen technischen Leistungskapazität der Batterie für sechs Tage, bevor die Batteriekapazität – mittels *software-gesteuerten Downgrade* – wieder auf die Standardleistung von ca. 80 % gedrosselt wurde.

Dieser Sachverhalt lässt sich dahingehend fiktiv variieren, dass *Tesla* anlässlich einer Katastrophenwarnung alle Nutzer im Katastrophengebiet kurz vor Eintritt der Naturkatastrophe kontaktiert und diesen über das Infotainment-System des Kfz eine kurzfristige Reichweitensteigerung im Austausch gegen eine umfassende(re) Einwilligung in die Verarbeitung von personenbezogenen Daten anbietet. Obwohl *Tesla* auf dem Markt der (elektrisch betriebenen) Kfz keine marktbeherrschende Stellung hat und jedenfalls einige Tage vor Eintritt des vorhergesagten Ereignisses andere Verkehrsmittel zur Verfügung gestanden hätten, ist es überzeugend, die Freiwilligkeit der Einwilligung in einer solchen Situation, einer absehbar und unmittelbar bevorstehenden Naturkatastrophe auf Grundlage von Art. 7 Abs. 4 DS-GVO abzulehnen.

Bietet *Tesla* die vorübergehende Reichweitensteigerung dagegen nicht nur im Austausch gegen eine umfassende Einwilligung, sondern auch gegen ein monetäres Entgelt an, das nicht evident unangemessen ist, so spricht dies dafür, dass auch eine umfassende Einwilligung der Datensubjekte trotz des unmittelbar drohenden Hurrikans freiwillig erfolgt.

4. Fazit

Im Ergebnis bietet Art. 7 Abs. 4 DS-GVO nach hier vertretener Auffassung Raum für eine umfassende Interessenabwägung unter Berücksichtigung der Umstände des Einzelfalls.[148] Dagegen ist die Vorschrift nicht der richtige Ort, um wettbewerbspolitische Antworten auf diejenigen komplexen Herausforderungen zu finden, die derzeit durch direkte und indirekte Netzwerkeffekte auf

---

[147] *Liptak*, Tesla extended the range of some Florida vehicles for drivers to escape Hurricane Irma, The Verge, 10.09.2017.

[148] Ebenso: *Heckmann/Paschke*, in: Ehmann/Selmayr (Hrsg.), DS-GVO, 2018, Art. 7, Rn. 52; *Buchner*, WRP 2019, 1243 (1245); *ders.*, WRP 2018, 1283 (1286); *ders./Kühling*, in: Kühling/Buchner (Hrsg.), 2020, Art. 7, Rn. 52 f.; *Klement*, in: Simitis/Hornung/Spiecker gen. Döhmann (Hrsg.), Datenschutzrecht, 2019, Art. 7, Rn. 62; *Ingold*, in: Sydow (Hrsg.), DS-GVO, 2018, Art. 7, Rn. 33; *Hacker*, Datenprivatrecht, 2020, S. 188 f.

mehrseitigen Plattformen ausgelöst werden.[149] Weil Art. 7 Abs. 4 DS-GVO weitere Kriterien zur Bewertung der Freiwilligkeit zulässt, wird die Bewertung der Marktmacht des Verantwortlichen und deren Folgen für eine Bündelung der Einwilligung mit (anderen) vertraglichen Klauseln gegebenenfalls nicht als alleiniges Argument benötigt.

Nach hier vertretener Ansicht ergibt sich insbesondere mit Blick auf die sog. *Marktmacht* als Kriterium für die Freiwilligkeit der Einwilligung eine wesentliche Flexibilisierung der Anwendung von Art. 7 Abs. 4 DS-GVO. Zunächst löst Art. 7 Abs. 4 DS-GVO keine widerlegliche Vermutung dahingehend aus, dass eine Verknüpfung einer Einwilligung mit (anderen) vertraglichen Vereinbarungen stets zur Unfreiwilligkeit der Einwilligung führt.[150] Eine solche Vermutung lässt sich zwar damit begründen, dass sie das grundsätzliche Verarbeitungsverbot aus Art. 6 Abs. 1 und Art. 9 Abs. 1 DS-GVO lediglich fortführt, greift aber unverhältnismäßig in das allgemeine Grundrecht der Vertragsfreiheit (Art. 6 Abs. 3 EUV),[151] in die unternehmerische Freiheit von Verantwortlichen und unternehmerisch handelnden Datensubjekten (Art. 16 GRCh) und in die unionsgrundrechtlich garantierte Möglichkeit zur Einwilligung (Art. 8 Abs. 2 S. 1 GRCh) ein.[152] Jedenfalls eine Auslegung als *generelles* anbieterbezogenes oder *generelles* marktbezogenes Kopplungsverbot ist mit der informationellen Privatautonomie nicht vereinbar.

Die Ablehnung einer Auslegung als *generelles* anbieterbezogenes oder marktbezogenes Kopplungsverbot bedeutet jedoch nicht, dass eine Einwilligung insbesondere gegenüber *GAFAM* leicht über die Hürde des Art. 7 Abs. 4 DS-GVO hinwegkommt. Die flexible Auslegung der Freiwilligkeit hat vielmehr den Vorteil, dass Art. 7 Abs. 4 DS-GVO *kartellrechtsakzessorisch* und damit im Ergebnis *asymmetrisch* angewendet werden kann. Sachlicher Grund für diese asymmetrische Anwendung ist die festgestellte – evident hohe – Marktmacht des Verantwortlichen als ein schwer widerlegliches Indiz für ein „klares Ungleichgewicht" (ErwG 43 S. 1 DS-GVO). Somit kann die Marktmacht als wesentliches Kriterium für die Annahme einer Unfreiwilligkeit der Einwilligung grundsätzlich herangezogen werden.

---

[149] *Crémer/de Montjoye/Schweitzer*; Competition policy for the digital era, 2019, 54 ff.; speziell zu personenbezogenen Daten: *Peitz/Schweitzer*, NJW 2018, 275 (276 ff.).

[150] Für eine solche Vermutung, aber regelmäßig ohne Bewusstsein für das Spannungsverhältnis zum Kartellrecht: *Albrecht*, CR 2016, 88 (91); *Dammann*, ZD 2016, 307 (311); *Ernst*, ZD 2017, 110 (112); *Gierschmann*. in: Gierschmann/Schlender/Stentzel/Veil (Hrsg.), DS-GVO, 2017, Art. 7, Rn. 62; Stemmer, in: Brink/Wolff (Hrsg.), BeckOK DatenschutzR, 28. Ed. 1.05.2018, Art. 7, Rn. 46; *Hacker*, ZfPW 2019, 148 (183); *ders*., Datenprivatrecht, 2020, S. 190 f.

[151] Soweit Grundrechtsträger ein Unternehmen ist, wird die Vertragsfreiheit zudem durch Art. 16 GRCh gewährleistet: *EuGH*, Urt. v. 18.07.2013, C-426/11 = EuZW 2013, 747 (Rn. 32) – *Alemo-Herron*.

[152] So im Ergebnis auch: *Engeler*, ZD 2018, 55 (56); *Klement*, in: Simitis/Hornung/Spiecker gen. Döhmann (Hrsg.), Datenschutzrecht, 2019, Art. 7, Rn. 59; *Mackenrodt/Wiedemann*, ZUM 2021, 89 (100 f.).

Zwar ist es Datenschutzbehörden und Gerichten aufgrund der Unbestimmtheit von Art. 7 Abs. 4 DS-GVO gesetzlich nicht versagt, ihre tatsächlichen oder eingebildeten makroökonomischen Kompetenzen unter Beweis zu stellen. Es wäre jedoch sinnvoll, wenn diese Beurteilung durch Spezialisten mit wettbewerbsrechtlichem und ökonomischem Sachverstand erfolgt und nicht durch Mitarbeiter der Datenschutzbehörden oder Richter am Amts- oder Verwaltungsgericht.[153]

Deshalb sollte es nach hier vertretener Auffassung zunächst der jeweiligen nationalen Kartellbehörde und der *EU-Kommission* überlassen bleiben, die absolute oder relative Marktmacht eines Verantwortlichen „mit überragender marktübergreifender Bedeutung für den Wettbewerb" i.S.d. § 19a Abs. 1 S. 2 Nr. 4 GWB bzw. die Eigenschaft als *Gatekeeper* im Sinne von Art. 3 DMA-Vorschlag festzustellen.

Erst und nur im Anschluss hieran, können Datenschutzbehörden und Gerichte in datenschutzrechtlichen Prozessen die Marktmacht des Verantwortlichen als entscheidendes Kriterium für die Beurteilung der Freiwilligkeit der Einwilligung i.S.d. Art. 7 Abs. 4 DS-GVO heranziehen. Damit verbleibt die Entscheidung über das Vorliegen und die Reichweite einer Marktmacht des Verantwortlichen bei den fachlich kompetenten nationalen Kartellbehörden und der *EU-Kommission*.[154]

Gegenüber einem *generellen* strengen Kopplungsverbot hat diese *kartellrechtsakzessorische*, *asymmetrische* Anwendung von Art. 7 Abs. 4 DS-GVO zudem den Vorteil, dass sie keine Marktzutrittsbarriere für KMU und neue datenbasierte Geschäftsmodelle etabliert. Im Gegenteil: Solange und soweit weder das *Bundeskartellamt* festgestellt hat, dass ein Verantwortlicher ein Unternehmen „mit überragender marktübergreifender Bedeutung für den Wettbewerb" i.S.d. § 19a Abs. 1 S. 2 Nr. 4 GWB ist,[155] noch die *EU-Kommission* den Verantwortlichen (künftig) als *Gatekeeper* i.S.d. Art. 3 des DMA-Vorschlags benannt hat, kommt dem Verantwortlichen mit Blick auf die Einwilligung eine Flexibilität zugute, die *GAFAM* für einige ihrer Geschäftsfelder gerade nicht mehr zur Verfügung stehen dürfte.

---

[153] Dies wirft schwierige Fragen zur Abgrenzung der jeweiligen Zuständigkeit auf, die über die Bestimmung der jeweils national zuständigen datenschutzrechtlichen Aufsichtsbehörde hinausgehen: Hierzu nun erste Vorlagefrage des *OLG Düsseldorf*, Beschl. v. 24.03.2021, Kart 2/19 (V), Rn. 27 ff. Vom *EuGH* geführt unter C-252/21.

[154] Zum vagen Verhältnis zwischen den nationalen und europäischen Behörden vgl. Art. 1 Abs. 7 des DMA-Vorschlags der *EU-Kommission*. „Die nationalen Behörden erlassen keine Entscheidungen, die einem von der Kommission nach dieser Verordnung erlassenen Beschluss zuwiderlaufen würden. Hinsichtlich der Durchsetzungsmaßnahmen arbeiten die Kommission und die Mitgliedstaaten eng zusammen und stimmen sich eng ab".

[155] Gesetz zur Änderung des Gesetzes gegen Wettbewerbsbeschränkungen für ein fokussiertes, proaktives und digitales Wettbewerbsrecht 4.0 und anderer Bestimmungen (GWB-Digitalisierungsgesetz) v. 18.01.2021, BGBl. I S. 2 ff.

Zusammengefasst: Die *kartellrechtsakzessorische*, *asymmetrische* Anwendung von Art. 7 Abs. 4 DS-GVO fördert den Wettbewerb und hilft dabei, das grundrechtlich zu gewährleistende Untermaß der informationellen Privatautonomie (Art. 8 GRCh) sicherzustellen, ohne dabei unverhältnismäßig in die ebenfalls zu gewährleistende unternehmerische Freiheit (Art. 16 GRCh) und das allgemeine Grundrecht der Vertragsfreiheit (Art. 6 Abs. 3 EUV) einzugreifen. Diese Vorgehensweise steht im Einklang mit § 19 Abs. 2 Nr. 4 lit. a GWB und Art. 5 lit. a DMA-Vorschlag und bietet – jedenfalls aus spezifisch datenschutzrechtlicher Perspektive – einstweilen ein milderes Mittel im Vergleich zu der beiderseits des Atlantiks zunehmend in Erwägung gezogenen Desintegration großer Plattformbetreiber.[156]

Mit Blick auf das Kriterium der besonderen *Eigenschaften von Datensubjekten* ist die DS-GVO weitgehend indifferent. Das einzige, ausdrücklich erwähnte Differenzierungskriterium sind Kinder, Art. 8 Abs. 1 DS-GVO. Der Ansatz des europäischen Gesetzgebers, für alle natürlichen Personen einen einheitlichen Schutz der personenbezogenen Daten zu gewährleisten, ist auf den ersten Blick konsequent und lässt sich mit Art. 8 Abs. 1 GRCh und Art. 16 AEUV begründen. Allerdings hat der europäische Gesetzgeber dabei verkannt,[157] dass die DS-GVO auch unternehmerisch handelnde Datensubjekte und deren bewusste Kommerzialisierung von personenbezogenen Daten erfasst. Die Verwertung der vermögenswerten Bestandteile von Persönlichkeitsrechten umfasst traditionell auch die Verarbeitung von besonders sensiblen personenbezogenen Daten i. S. d. Art. 9 Abs. 1 DS-GVO. Infolgedessen können diese Verwertungshandlungen nur auf Grundlage einer Einwilligung erfolgen. Deshalb müssen die Voraussetzungen der Einwilligung – jedenfalls im B2B-Verhältnis – großzügiger ausgelegt werden.

---

[156] Vgl. den (nachgebesserten) Antrag des *FTC* gegen *Facebook* vom 19.08.2021, Case No.: 1:20-cv-03590-JEB (https://www.ftc.gov/system/files/documents/cases/ecf_75-1_ftc_v_facebook_public_redacted_fac.pdf, zuletzt abgerufen am 19.05.2022); *Hoppe/Riecke*, Kartellamtschef Mundt bezeichnet Zerschlagung von Tech-Riesen als „letztes Mittel", Handelsblatt, 18.03.2021 (https://www.handelsblatt.com/politik/international/digitalkonzerne-kartellamtschef-mundt-bezeichnet-zerschlagung-von-tech-riesen-als-letztes-mittel/27014042.html, zuletzt abgerufen am 19.05.2022).

[157] Eine Einordnung von Verträgen über die Verwertung von Persönlichkeitsrechten, einschließlich der Verarbeitung von personenbezogenen Daten unter die (bezahlte) Meinungsfreiheit der Öffnungsklausel gemäß Art. 85 Abs. 1 DS-GVO ist nach hier vertretener Ansicht nicht sinnvoll, oben Kapitel 3 D.; sowie *EuGH*, C-131/12 = NJW 2014, 2257 (Rn. 85) – *Google Spain*. Mit Blick auf die vermögensrechtlichen Bestandteile von Persönlichkeitsrechten ebenfalls zu undifferenziert: *Marsch*, Das Europäische Datenschutzgrundrecht, 2018, S. 366: „Für den aus grundrechtlicher Perspektive besonders bedeutsamen und durch die jeweilige Rechtskultur in den Mitgliedstaaten stark geprägten Konflikt zwischen Datenschutzrecht und Persönlichkeitsrechtsschutz auf der einen und den Kommunikationsfreiheiten auf der anderen Seite nimmt das europäische Datenschutzsekundärrecht seinen Harmonisierungsanspruch schließlich in erheblichem Maße zurück".

Ein Verständnis von Art. 7 Abs. 4 DS-GVO als generalklauselartiges Berücksichtigungsgebot ermöglicht es, das *situationsadäquate* Verhalten des Verantwortlichen bei der Beurteilung der Freiwilligkeit der Einwilligung einzubeziehen. In diesem Zusammenhang können die Fallgruppen der Nr. 6 und Nr. 24 ff. Anhang I UGP-RL und die Rechtsprechung zur aggressiven Geschäftspraxis (Art. 9 UGP-RL bzw. § 4a UWG) erste Anhaltspunkte und argumentative Stützen bereitstellen, gleichwohl bleibt hier erheblicher Spielraum für die Argumentation am Einzelfall.

III. Flexibilisierung der Widerruflichkeit der Einwilligung

Wie in Kapitel 4 ausgeführt, kommt eine sog. freie – also frist- und grundlose – Widerruflichkeit einem voraussetzungslosen Reue-Recht für die Zukunft gleich. Ein sachlicher Grund für eine Meinungs- und Verhaltensänderung muss nicht genannt werden. Legt man dieses weite – und derzeit in der Literatur nahezu einhellig vertretene – Verständnis des Art. 7 Abs. 3 S. 1 DS-GVO zu Grunde, so darf der Widerruf keinerlei nachteilige Folgen für das Datensubjekt auslösen. Hiernach wäre der Widerruf nur dann frei, wenn der Widerrufende auch keine Pflicht zur Zahlung von Schadens- oder von Wertersatz befürchten müsste.[158]

Nach herrschender Ansicht etabliert Art. 7 Abs. 3 S. 1 DS-GVO eine *generelle* Widerruflichkeit jeder datenschutzrechtlichen Einwilligung. Sofern die Notwendigkeit, einen Ausschluss der Widerruflichkeit im Einzelfall zuzulassen, überhaupt anerkannt wird, fehlen bislang überzeugende Lösungswege.

Der von *Benedikt Buchner* für das BDSG a. F. gemachte und von *Philipp Hacker* für die DS-GVO übernommene Vorschlag, im Einzelfall eine Datenverarbeitung trotz des Widerrufs der Einwilligung auf Grundlage von Art. 6 Abs. 1 lit. f DS-GVO[159] zuzulassen, handelt sich alle Rechtsunsicherheiten ein, die mit der Interessenabwägung verbunden sind. Für eine Verarbeitung von besonders sensiblen personenbezogenen Daten bietet dieser Vorschlag ohnehin keine Option, weil Art. 6 Abs. lit. f DS-GVO für eine solche Datenverarbeitung nicht anwendbar ist.

---

[158] *v. Westphalen/Wendehorst*, BB 2016, 2179 (2184): „Das Vertragsrecht darf dabei die Ausübung datenschutzrechtlicher Rechte und Behelfe auch nicht indirekt erschweren, etwa durch Verpflichtungen zum Schadens- oder Wertersatz." Dieses Verständnis liegt auch § 327q Abs. 3 BGB zugrunde. Hiernach sollen alle Ersatzansprüche eines Unternehmers gegen einen Verbraucher ausgeschlossen sein, sofern die Einschränkung der ursprünglich zulässigen Datenverarbeitung auf der Ausübung von Datenschutzrechten beruht. a. A. zuvor (wohl) *Metzger*, JIPITEC 2017, 2 (6 f.) und zumindest *de lege ferenda*: *Leistner/Antoine/Sagstetter*, Big Data, 2021, S. 272 f.

[159] So *Buchner*, Die informationelle Selbstbestimmung im Privatecht, 2006, S. 272 ff.; *Hacker*, Datenprivatrecht, 2020, S. 278.

Auch der Vorschlag von *Jan Niklas Bunnenberg*, von der widerrufenen Einwilligung nachträglich auf Art. 6 Abs. 1 lit. b DS-GVO zu wechseln, sofern ausnahmsweise im Rahmen einer Interessenabwägung das Bindungsinteresse des Verantwortlichen das Widerrufsinteresse des Datensubjekts überwiegt,[160] ist – nach hier vertretener restriktiver Auslegung von lit. b DS-GVO – nicht möglich. Ohnehin müsste diese Ausnahme im B2B-Verhältnis eher die Regel sein. Zudem käme auch diese Option für besonders sensible Daten nicht in Betracht, weil auch Art. 6 Abs. 1 lit. b für solche Datenverarbeitungen nicht anwendbar ist.

Weil der Übergang zwischen personenbezogenen Daten und besonders sensiblen personenbezogenen Daten unscharf ist[161] und diese Qualifikation – beispielsweise mit einem Portraitfoto – leicht erreicht wird, muss für die Konstellationen, in denen ein jederzeitiger, grundloser Widerruf der Einwilligung die Rechtmäßigkeit der fortgesetzten Datenverarbeitung nicht beenden soll, ein Lösungsweg gefunden werden, der auch dann greift, wenn Daten i. S. d. Art. 9 Abs. 1 DS-GVO verarbeitet werden. Deshalb muss eine Option gefunden werden, die unmittelbar an den Tatbestand der Einwilligung und damit an die Möglichkeit zum Widerruf anknüpft.[162]

Im Grundsatz kommt der Ausschluss eines Widerrufs in Betracht, sofern dieser zur Unzeit erfolgt.[163] So kann die Begrenzung der Widerruflichkeit auf Grundlage von Treu und Glauben zu einer gerechten Lösung im Einzelfall führen. Wegen des Vorrangs des Unionsrechts kommt hierfür nicht § 242 BGB zur Anwendung, sondern der Grundsatz von Treu und Glauben muss unionsrechtlich hergeleitet werden.[164] Allerdings geht diese Notlösung über die General-

---

[160] Dies wäre eine mögliche Weiterentwicklung des Ansatzes von: *Bunnenberg*, Privates Datenschutzrecht, 2020, 265 f.

[161] Hierzu die Vorlageverfahren: *OLG Düsseldorf*, Vorlagebeschl. v. 24.03.2021 – Kart 2/19 (V) = NZKart 2021, 306 (Rn. 45: „Klärungsbedürftig ist auch, ob die Verwendungsabsicht für die Beurteilung [als besonders sensibles personenbezogenes Datum] von Bedeutung ist"); sowie: *ÖOGH*, Vorlagebeschl. v. 22.07.2021, 6 Ob 56/21k – *Schrems* [*III*].

[162] Hierfür spricht zudem die Notwendigkeit, die Widerruflichkeit der Einwilligung im Verhältnis zwischen Datensubjekten und sog. Datentreuhändern einschränken zu können: *Kühling*, ZfDR 2021, 1 (11).

[163] *Langhanke/Schmidt-Kessel*, EuCML 2015, 218 (221); in diese Richtung (wohl) auch: *Leistner/Antoine/Sagstetter*, Big Data, 2021, S, 272 f.

[164] Grundlegend zum Grundsatz von Treu und Glauben: *EuGH*, Urt. v. 03.09.2009, C-489/07 = EuZW 2009, 694 (Rn. 26) – *Messner*; *Riesenhuber*, System und Prinzipien des Europäischen Vertragsrechts, 2003, S. 398 ff.; *Stempel*, Treu und Glauben im Unionsprivatrecht, 2016, S. 268 ff., 310 f.; *Metzger*, Extra legem, intra ius. Allgemeine Rechtsgrundsätze im Europäischen Privatrecht, 2009, S. 348 f.; spezifisch zum Grundsatz des Rechtsmissbrauchs: *EuGH*, Urt. v. 12.03.1996, C-441/93 = WM 1996, 1530 (Rn. 69) – *Pafitis*; *EuGH*, Urt. v. 12.05.1998, C-367/96 = EuZW 1999, 57 (Rn. 20) – *Kefalas*; hierzu: *Schmidt-Kessel*, in: Jud u. a. (Hrsg.), Prinzipien des Privatrechts und Rechtsvereinheitlichung, 2001, S. 61 (79 f.). Der Grundsatz der Datenverarbeitung nach Treu und Glauben ist nach dem Wortlaut von Art. 5 Abs. 1 DS-GVO nicht zugunsten von Verantwortlichen und Auftragsverarbeitern anwendbar.

klausel mit Rechtsunsicherheit einher. Zudem bietet sie keine angemessene Reaktion für das Problem, dass dem europäischen Gesetzgeber die sog. freie Widerruflichkeit insgesamt unangemessen weit geraten ist.

Wie bereits ausgeführt, etabliert ein *generelles* Widerrufsrecht eine Marktzutrittsbarriere für solche Verantwortlichen, die als KMU ebenfalls auf das derzeit sehr erfolgreiche Geschäftsmodell einer mehrseitigen Plattform setzen wollen, die auf Grundlage von personalisierter Werbung finanziert wird.[165] Infolgedessen ist es plausibel, dass die Auslegung von Art. 7 Abs. 3 S. 1 DS-GVO als ein *generelles* Widerrufsrecht insbesondere *GAFAM* faktisch begünstigt, weil diese Unternehmen zumindest teilweise Produkte anbieten, die – maßgeblich infolge von Netzwerkeffekten – aus Sicht der Datensubjekte nicht oder nur sehr schwer substituierbar sind. Insbesondere *GAFAM* brauchen den Widerruf der Datensubjekte deshalb faktisch nicht zu befürchten.[166]

Weil der europäische Gesetzgeber die Folgen der DS-GVO für Verträge zur Verwertung der vermögenswerten Bestandteile der Persönlichkeitsrechte übersehen hat, wäre es – jedenfalls soweit unternehmerisch handelnde Datensubjekten die Einwilligung in kommerziellem Eigeninteresse einsetzen – ein unverhältnismäßiger Eingriff in die durch Art. 16 GRCh gewährleistete unternehmerische Freiheit von Verantwortlichen und von unternehmerisch handelnden Datensubjekten, sofern es die DS-GVO ihnen verwehrt, vertragliche Dispositionen über die Widerruflichkeit der Einwilligung zu treffen. Deshalb müssen die Gerichte und damit zunächst der *EuGH* auf Grundlage einer teleologischen Reduktion zu einer flexiblen Auslegung und Anwendung von Art. 7 Abs. 3 S. 1 DS-GVO gelangen (1).

Für die Beurteilung, wann eine teleologische Reduktion von Art. 7 Abs. 3 S. 1 DS-GVO in Betracht kommt, stehen grundsätzlich dieselben Kriterien zur Verfügung, die bereits zur Flexibilisierung der Freiwilligkeit der Einwilligung (Art. 7 Abs. 4 DS-GVO) vorgeschlagen wurden (2). Im Gegensatz zu Art. 7 Abs. 4 DS-GVO ist der Wortlaut des Abs. 3 S. 1 DS-GVO jedoch nicht als offene Generalklausel formuliert. Die dadurch zum Ausdruck kommende gesetzgeberische Grundentscheidung zugunsten einer Widerruflichkeit der datenschutzrechtlichen Einwilligung ist zu respektieren. Zwar sind nach dem hier vertretenen Ansatz gerade auch schuldrechtliche Gestattungen für die Datenverarbeitung möglich, die hierfür erforderliche Disposition über die Widerruflichkeit ist jedoch zwingend durch spezifische Maßnahmen zugunsten der Datensubjekte abzustützen (3).[167]

---

[165] *Gal/Aviv*, Journal of Competition Law and Economics 2020, 349 (351 f./386 ff.).

[166] Hierzu oben Kapitel 4 B.II.

[167] Zu weiteren Maßnahmen, die notwendig sind, um die informationelle Privatautonomie abzustützen: Kapitel 6.

1. Teleologische Reduktion von Art. 7 Abs. 3 S. 1 DS-GVO

Die hier vertretene restriktive Auslegung der vertragsakzessorischen Datenverarbeitung (Art. 6 Abs. 1 lit. b DS-GVO) hat zur Folge, dass es den Mitgliedstaaten nicht möglich ist, eine bindende, schuldrechtliche Gestattung der Datenverarbeitung auf Grundlage des nationalen Schuldrechts anzuerkennen.[168] Infolgedessen eröffnet Art. 6 Abs. 1 lit. b DS-GVO kein Feld für mitgliedstaatliche Experimente und die Entwicklung eines nationalen „Datenschuldrechts". Zudem wäre dieses Experimentierfeld mit Blick auf die zu beachtende Erforderlichkeit der Datenverarbeitung für die Vertragserfüllung (Art. 6 Abs. 1 lit. b DS-GVO), die stets anzuwendenden Grundsätze der rechtmäßigen Datenverarbeitung (Art. 5 Abs. 1 DS-GVO), die Beschränkung des Erlaubnistatbestands auf nicht-sensible Daten und die Begrenzung der nationalen Lösung durch die Verpflichtung zur Rücksichtnahme auf das Ziel des freien Verkehrs von personenbezogenen Daten im Binnenmarkt ohnehin sehr eng ausgefallen.[169]

Infolgedessen ist eine ausdrückliche Anerkennung von schuldrechtlichen Gestattungen durch die mitgliedstaatlichen Gesetzgeber auf Grundlage des nationalen Schuldrechts nicht möglich. Weil der Tatbestand der Einwilligung gerade keine Öffnungsklausel für eine abweichende nationale Regelung enthält, setzt die Anerkennung einer zeitweise unwiderruflichen Einwilligung entweder eine ausdrückliche Änderung der DS-GVO voraus (*de lege ferenda*) oder kann – so nach hier vertretener Ansicht – auch *de lege lata* durch eine teleologische Auslegung von Art. 7 Abs. 3 S. 1 DS-GVO *praeter legem* erreicht werden.[170] Dies ist möglich, weil der europäische Gesetzgeber die Bedeutung der DS-GVO zumindest für den unternehmerischen Geschäftsverkehr verkannt und deshalb Regelungen getroffen hat, die durch den Gesetzgeber unbemerkt und damit planwidrig über das beabsichtigte Regelungsziel der DS-GVO hinausschießen.

Eine solche Auslegung der DS-GVO ist zudem nicht nur möglich,[171] sondern zur Wahrung der Vertragsfreiheit und unternehmerischen Freiheit – jedenfalls im B2B-Verhältnis – aufgrund des Verhältnismäßigkeitsgrundsatzes (Art. 52 Abs. 1 S. 2 GRCh) zwingend.[172] Weil der europäische Gesetzgeber die Konsequenzen der DS-GVO für die Verwertung von Persönlichkeitsrechten

---

[168] Anders (wohl) *Bunnenberg*, der jedoch nicht auf die schuldrechtlichen Folgefragen und die dadurch entstehende Gefährdung der Ziele aus Art. 1 DS-GVO eingeht: *ders.*, Privates Datenschutzrecht, 2020, S. 265 f.

[169] Oben Kapitel 3 D.

[170] Zu dieser Möglichkeit allgemein: *Neuer*, in: Riesenhuber (Hrsg.), Europäische Methodenlehre, 4. Aufl. 2021, S. 365, Rn. 28 ff.

[171] *Sattler*, JZ 2017, 1036 (1043 ff.).

[172] Zum unionsrechtlichen Verhältnismäßigkeitsgrundsatz: *EuGH*, Urt. v. 13.04.2000 C-292/97 = BeckRS 2004, 76064 (Rn. 45) – *Karlsson*; *EuGH*, Urt. v. 13.07.1989, Slg. 5/88 = BeckRS 2004, 73224 (Rn. 18) – *Wachauf*; *Trstenjak/Beysen*, EuR 2012, 265 ff.; *Streinz/Michl*, in: Streinz (Hrsg.), EUV/AEUV, 3. Aufl. 2018, GRCh, Art. 52, Rn. 16 ff.

verkannt hat, der Anwendungsbereich von Art. 7 Abs. 3 DS-GVO deshalb zu pauschal und damit zu weit geraten ist, muss dieses Defizit nachträglich durch eine unionsgrundrechtskonforme, teleologische Reduktion korrigiert werden.

2. Kriterien für eine teleologische Reduktion

Die jederzeitige und voraussetzungslose Widerruflichkeit etabliert eine Instabilität der Leistungsbeziehungen, die weniger das Geschäftsmodell von etablierten und *marktmächtigen Verantwortlichen* beeinträchtigen dürfte; deren Dienste sind aus Sicht der Datensubjekte derzeit – jedenfalls zu vertretbaren Wechselkosten – nicht substituierbar (a).

Soweit *unternehmerisch handelnde Datensubjekte* im Rahmen der Kommerzialisierung der vermögensrechtlichen Bestandteile ihrer Persönlichkeitsrechte auch in die Verarbeitung von (besonders sensiblen) personenbezogenen Daten einwilligen, ist die Möglichkeit zur Disposition über die Widerruflichkeit unionsgrundrechtlich zwingend geboten (b).

Soweit *Datensubjekte als Verbraucher* einwilligen und der Verantwortliche weder ein Unternehmen mit überragender marktübergreifender Bedeutung für den Wettbewerb ist noch über die Position eines sog. *Gatekeepers* für zentrale Plattformdienste verfügt, sollte nach hier vertretener Ansicht die Möglichkeit zur zusätzlich abgestützten, vorübergehenden Disposition über die Widerruflichkeit der Einwilligung ermöglicht werden (c).

a) Marktmacht des Verantwortlichen

Marktmächtige Verantwortliche, also Unternehmen mit überragender marktübergreifender Bedeutung für den Wettbewerb i. S. d. § 19a Abs. 1 S. 2 Nr. 4 GWB oder *Gatekeeper* i. S. d. (künftigen) Art. 3 DMA-Vorschlag können ihre Marktposition und Netzwerkeffekte nutzen, um ihre Tätigkeit auf immer neue Geschäftsmodelle und Märkte auszudehnen.[173] Sie brauchen dabei den Widerruf der Einwilligung durch ihre Kunden kaum zu fürchten, weil für ihre Dienste aus Sicht der Datensubjekte (meist) keine adäquaten Substitute von Wettbewerbern angeboten werden.

Infolgedessen dürfte eine *generelle* freie Widerruflichkeit vorrangig die Entwicklungschancen von neuen Anbietern verschlechtern. Beispielsweise werden die Geschäftsmodelle von solchen KMU erschwert, die ebenfalls einen Zugang zu digitalen Produkten verschaffen und im Gegenzug (auch) personenbezogene Daten – beispielsweise für personalisierte Werbung – verwerten. Infolge einer

[173] Hierauf reagiert die *EU-Kommission* mit Art. 12 f. DMA-Vorschlag. Zur Ausnutzung von Marktdominanz für die Erschließung und ggfs. Dominanz auf weiteren Märkten: *Schweitzer*, GRUR 2019, 569 (579 f.).

generellen freien Widerruflichkeit wird solchen Geschäftsmodellen die längerfristige Kalkulationsgrundlage entzogen und damit die Planung erschwert. Zudem scheitert ein Ausweichen auf ein Angebot, das auf die Kommerzialisierung von personenbezogenen Daten verzichtet und stattdessen die Zahlung eines Geldbetrags erfordert, leicht an der durch marktdominante Anbieter genährten Erwartung von Verbrauchern. Verbraucher sind es derzeit noch gewohnt, dass ein „kostenloses" Einstiegsangebot den Zugang zu digitalen Gütern ermöglicht.[174] Daher ist die Verwertung von personenbezogenen Daten für personalisierte Werbung faktisch die Standard-Option zur Finanzierung vieler Geschäftsmodelle geworden, die Zugang zu digitalen Produkten eröffnen (*data processing by default*).

Infolge einer *generellen*, jederzeitigen Widerruflichkeit der Einwilligung dürfte die Zuverlässigkeit der erwarteten Werbeeinnahmen sinken, dies erschwert die ökonomische Bewertung von Geschäftsmodellen neuer Anbieter und gefährdet damit potenziell auch die Grundlage für eine Aufnahme von Fremdkapital. Somit verursacht eine *generelle* Widerruflichkeit vorrangig für neue Anbieter und KMU erhebliche Unsicherheit und etabliert dadurch Marktzutrittsbarrieren. Entgegen der derzeit vom europäischen Gesetzgeber mit dem DMA-Vorschlag verfolgten Ziele könnte sich der Wettbewerbsdruck auf bereits dominante *Gatekeeper* infolge dieser *generellen* Widerruflichkeit der Einwilligung sogar reduzieren. Deshalb ist die Marktmacht des Verantwortlichen ein wesentliches Kriterium für die Beurteilung, ob eine Disposition über Art. 7 Abs. 3 S. 1 DS-GVO gegenüber bestimmten Verantwortlichen in Betracht kommt.

Übernehmen marktmächtige *Gatekeeper* frühzeitig die Mehrheitsanteile an kleineren Anbietern und integrieren deren Geschäftsmodell in ihre eigenen Plattformen, so sinkt die Wahrscheinlichkeit eines Einwilligungswiderrufs durch die Datensubjekte wiederum. Deshalb liegt es nach hier vertretener Ansicht nahe, das Kriterium der Marktmacht – ebenso wie im Rahmen des Art. 7 Abs. 4 DS-GVO – auch für die Widerruflichkeit der Einwilligung fruchtbar zu machen. Dies hat zur Folge, dass die Widerruflichkeit zwar grundsätzlich zur Disposition des Datensubjekts stehen kann, so dass auch zeitweise unwiderrufliche Einwilligungen in die Verarbeitung von personenbezogenen Daten möglich sind.

Die hierfür erforderliche teleologische Reduktion des Art. 7 Abs. 3 S. 1 DS-GVO kommt jedoch in *kartellrechtsakzessorischer* und somit *asymmetrischer* Anwendung nicht in Betracht, sofern das Widerrufsrecht eines Datensubjekts gerade im Verhältnis zu einem Verantwortlichen beschränkt werden soll, der

[174] Für eine Möglichkeit, die (Teil-)Finanzierung des Geschäftsmodells durch personalisierte Werbung ohne Einwilligung und stattdessen auf Grundlage einer Interessenabwägung (Art. 6 Abs. 1 lit. f DS-GVO) zuzulassen: *Peitz/Schweitzer*, NJW 2018, 275 (277); sowie zur Datenschutz-RL von 1995: *Art. 29 Data Protection Working Group*, Opinion 06/2014, WP 217, S. 25–26.

nach Auffassung des *Bundeskartellamts* über eine überragende marktübergreifende Bedeutung für den Wettbewerb verfügt (§ 19a Abs. 1 S. 2 Nr. 4 GWB) oder nach Ansicht der *EU-Kommission* die Position eines *Gatekeepers* über zentrale Plattformdienste innehat (Art. 3 DMA-Vorschlag).[175]

Zwar lässt sich an diesem Ansatz kritisieren, dass er die Ausgestaltung der datenschutzrechtlich determinierten Beziehung zwischen Verantwortlichem und Datensubjekt von der Prüfung durch Kartellämter abhängig macht, so dass die Datenaufsichtsbehörden und Gerichte auf die Arbeit dieser Wettbewerbsbehörden und deren Bemühen um eine klare Abgrenzung von Märkten und Produkten angewiesen sind. Allerdings ist dieses arbeitsteilige Vorgehen nach hier vertretener Ansicht erforderlich, sofern eine spezialisierte, einheitliche und somit rechtssichere Anwendung des Kriteriums der Marktmacht erreicht werden soll. Im Übrigen bleibt es den Aufsichtsbehörden und Gerichten unbenommen, aufgrund der Umstände des konkreten Einzelfalls einen Widerruf aus wichtigem Grund anzuerkennen (hierzu unten 3.d), ohne dass es auf die Marktmacht des Verantwortlichen ankommt.

Zudem ist eine solche *kartellrechtsakzessorische*, *asymmetrischer* Auslegung und Anwendung von Art. 7 Abs. 3 S. 1 DS-GVO erneut ein milderes Mittel, als eine zwangsweise Entflechtung derjenigen Dienste,[176] die von marktmächtigen Verantwortlichen auch im Austausch gegen den Zugang zu personenbezogenen Daten angeboten werden. Zugleich wird das Risiko vermieden, dass eine *generelle* Widerruflichkeit der Einwilligung sich faktisch primär als Marktzutrittsbarriere auswirkt. Stattdessen wird die Widerruflichkeit der Einwilligung zum wesentlichen Instrument der Verwirklichung von informationeller Privatautonomie und fördert zugleich den Wettbewerb auf dem Markt der Anbieter von digitalen Produkten, die ihr Geschäftsmodell auf der Grundlage mehrseitiger Plattformen betreiben.

b) Unternehmerisch handelnde Datensubjekte

Eine *generelle* Widerruflichkeit der Einwilligung beschränkt die zivilrechtliche Möglichkeit zum Abschluss und zur Durchführung von Verträgen als Grundlage für eine Stabilisierung von privatrechtlich organisierten Leistungsbeziehungen. Dadurch greift Art. 7 Abs. 3 S. 1 DS-GVO in die unionsgrundrechtlich anerkannte allgemeine Vertragsfreiheit (Art. 6 Abs. 3 EUV)[177] und in die spezi-

[175] Zur Notwendigkeit einer Abgrenzung der Zuständigkeiten zwischen Kartell- und Datenschutzbehörden, Oben: C.II.2.c.bb.

[176] Zum Gedanken der internen Entflechtung: *Mundt*, NZKart 2019, 117; sowie das (bislang nicht erfolgreiche) Verfahren der Federal Trading Commission (FTA) gegen *Facebook* mit dem potenziellen Ergebnis einer Abtrennung von *WhatsApp* und *Instagram* von *Facebook* (https://www.ftc.gov/system/files/documents/cases/051_2021.01.21_revised_partially_redacted_complaint.pdf, zuletzt abgerufen am 19.05.2022).

[177] *EuGH*, Urt. v. 18.07.2007, C-277/05 = EuZW 2007, 706 (Rn. 21) – *Société thermale*

fische Vertragsfreiheit im unternehmerischen Geschäftsverkehr ein,[178] die als Bestandteil der unternehmerischen Freiheit der Verantwortlichen und der unternehmerisch handelnden Datensubjekte gemäß Art. 16 GRCh zu gewährleisten ist. Deshalb ist Art. 7 Abs. 3 S. 1 DS-GVO nach hier vertretener Ansicht nur dann unionsgrundrechtskonform, sofern er mit Blick auf den Verhältnismäßigkeitsgrundsatz (Art. 52 Abs. 1 S. 2 GRCh)[179] flexibel ausgelegt wird und dadurch ein Verstoß gegen das Übermaßverbot verhindert wird.[180]

Jedenfalls für das B2B-Verhältnis wurde bereits davor gewarnt, dass Art. 7 Abs. 3 S. 1 DS-GVO nur dann mit dem Unionsprimärrecht vereinbar sei, wenn er durch unionsrechtlich anerkannte Grundsätze wie Treu und Glauben und ihre mitgliedstaatlichen Funktionsäquivalente[181] auf das grundrechtskonforme Maß beschränkt wird.[182] Diese Warnung ist überzeugend. Ohne eine solche Einschränkung der Widerruflichkeit wäre im B2B-Verhältnis keine vertragliche Bindungswirkung und damit keine Stabilisierung von Rechtsverhältnissen möglich, obwohl unternehmerisch tätige Datensubjekte – im Gegensatz zu Verbrauchern – regelmäßig[183] nicht, jedenfalls aber in einem geringeren Ausmaß schutzbedürftig sind.[184]

Ohne eine Einschränkung des Art. 7 Abs. 3 S. 1 DS-GVO würde die sog. freie Widerruflichkeit alle Verträge gefährden, in denen sich Prominente, aber auch unbekannte Personen, als Marken- und Produktbotschafter (sog. Testimonial) verpflichten und dabei auch in die Verarbeitung von personenbezogenen Daten

---

d'Eugénie-les-Bains; *EuGH*, Urt. v. 28.04.2009, C-518/06 (Rn. 66); *EuGH*, Urt. v. 19.4. 2012 – C-213/10 = EuZW 2012, 427 (Rn. 45) – *F-Tex SIA/Lietuvos-Anglijos*.

[178] *EuGH*, Urt. v. 18.07.2013, C-426/11 = EuZW 2013, 747 (Rn. 32) – *Alemo-Herron*.

[179] *EuGH*, Urt. v. 13.04.2000 C-292/97 (Rn. 45) = EuGRZ 2000, 524 – *Karlsson*; *EuGH*, Urt. v. 13.07.1989, 5/88 = BeckRS 2004, 73224 (Rn. 18) – *Wachauf*; *Trstenjak/Beysen*, EuR 2012, 265 ff.; *Streinz/Michl*, in: Streinz (Hrsg.), EUV/AEUV, 3. Aufl. 2018, GRCh, Art. 52, Rn. 16 ff.

[180] Oben Kapitel 4 B.II.2. und III.

[181] Allgemein zur Beschränkung der Widerruflichkeit von Einwilligungen durch Vertrag und gemäß § 242 BGB: *Ohly*, Volenti non fit iniuria, 2002, S. 348 ff.

[182] *Klement*, in: Simitis/Hornung/Spiecker gen. Döhmann (Hrsg.), DS-GVO, Art. 7, Rn. 92; die Vorgängervorschrift in § 4a BDSG a. F. für verfassungswidrig haltend: *Giesen*, JZ 2007, 918 (926).

[183] Hiervon bleibt die kartellrechtsakzessorisch zwingende Widerruflichkeit gegenüber einem Unternehmen mit überragender marktübergreifender Bedeutung für den Wettbewerb oder gegenüber einem Gatekeeper unberührt, da das Kriterium der Marktmacht des Verantwortlichen unabhängig davon anzuwenden ist, ob ein einwilligendes Datensubjekt als Unternehmer oder als Verbraucher handelt.

[184] Die Exekutive scheut mittlerweile aber nicht mehr davor zurück, pauschal von einer strukturellen Unterlegenheit bestimmter Unternehmer auszugehen: Gesetzentwurf der Bundesregierung für ein Gesetz zur Umsetzung der DID-RL v. 13.01.2021, S. 95 (zur Umsetzung der Regressansprüche gemäß Art. 22 DID-RL in § 327u BGB: „Dennoch soll zum Schutz des Unternehmers eine zwingende Ausgestaltung vorgenommen werden, da der Unternehmer im Verhältnis zu den Vertriebspartnern in der Regel die strukturell unterlegene Vertragspartei ist").

einwilligen.[185] Eine teleologische Reduktion von Art. 7 Abs. 3 S. 1 DS-GVO ermöglicht es, (weiterhin) rechtsverbindliche Werbe-Vereinbarungen zu treffen, so dass bei Schlecht- oder Nichtleistung des unternehmerisch handelnden Datensubjekts ein Anspruch auf Erfüllung, jedenfalls aber auf Schadensersatz durchgesetzt werden kann[186] und der Verantwortliche ein Recht zur Vertragsbeendigung hat, welche die engen Voraussetzungen nicht beachten muss, die § 327q Abs. 2 BGB derzeit für das B2C-Verhältnis etabliert.

Weil derartige Vereinbarungen weder unter die Öffnungsklausel des Art. 85 Abs. 1 DS-GVO fallen[187] noch der Erlaubnistatbestand der vertragsakzessorischen Datenverarbeitung (Art. 6 Abs. 1 lit. b DS-GVO) greift,[188] sind Verantwortliche und unternehmerisch handelnde Datensubjekte zur Fortsetzung ihrer bisher stabilen Rechtsbeziehungen auf eine zeitweise unwiderrufliche Einwilligung angewiesen.

Hiervon bleibt die Möglichkeit zum außerordentlichen Widerruf als Instrument der Vertragsbeendigung unberührt.[189] Weil die datenschutzrechtliche Einwilligung selbst Bestandteil des (Werbe-, Sponsoring- oder Merchandise-)Vertrags ist, oder zumindest gemeinsam mit dem Vertrag stehen und fallen soll, können ordentliche, jedenfalls aber außerordentliche Kündigungen des Vertrags auch die zeitweise unwiderrufliche Einwilligung in die Datenverarbeitung erfassen.[190]

c) Als Verbraucher handelnde Datensubjekte

Mit Blick auf Datensubjekte, die Verbraucher sind, ist die jederzeitige *generelle* Widerruflichkeit und die damit einhergehende fehlende Bindungswirkung einer datenschutzrechtlichen Einwilligung auf den ersten Blick überzeugend.

---

185 Hierzu: *Sattler*, NJW 2020, 3623 (3627).

186 Dieses Ergebnis wird in der Literatur als sachlich richtig betrachtet, wobei die Vertreter dieser Ansicht die Konsequenzen wegen Art. 7 Abs. 3 S. 1 DS-GVO stets wieder relativieren: *Metzger*, JIPITEC 2017, 2 (6 f.); nur noch für ein Vertragsbeendigungsrecht: *ders.*, in: Lohsse/Schulze/Staudenmayer (Hrsg.), Data as Counter-Performance – Contract Law 2.0? 2020, S. 25 (34 f.); *Leistner/Antoine/Sagstetter*, Big Data, 2021, S. 255 (einerseits für Rücktritt und Schadensersatz) und S. 272 („Ein Schadensersatz dürfte aber letztlich [wegen der Widerruflichkeit der Einwilligung] abzulehnen sein").

187 Sowohl die Vorgängernorm des Art. 9 Datenschutz-RL als auch Art. 85 DS-GVO enthalten als sog. Presseprivileg keine Öffnung für die kommerzielle Verwertung von Persönlichkeitsrechten, weil deren Auslegung zugunsten der Meinungsfreiheit ausdrücklich mit Blick auf journalistische Tätigkeiten erfolgt, ErwG. 153 S. 7 DS-GVO. Für eine Webseite: *EuGH*, Urt. v. 16.12.2008, C-73/07 = EuZW 2009, 108 (Rn. 56) – *Satakunnan Markkinapörssi und Satamedia*). Zudem lehnte der EuGH die Anwendung der Öffnungsklausel auf Datenverarbeitungen i. R. d. Suchmaschine von Google bereits ab: *EuGH*, Urt. v. 13.05.2014, C-131/12 = NJW 2014, 2257 (Rn. 85) – *Google Spain*.

188 Oben Kapitel 4 C.III.2.

189 Nach deutscher Dogmatik handelt es sich insoweit um eine Kündigung aus wichtigem Grund.

190 Hierzu unten d.

Sofern kein anderer Erlaubnistatbestand eingreift, behält das Otto-Normal-Datensubjekt jederzeit die vollständige Entscheidungszuständigkeit über die künftige Verarbeitung der personenbezogenen Daten. Legt man die sog. freie Widerruflichkeit besonders weit aus, so brauchen diese Datensubjekte auch keinerlei langfristigen Konsequenzen durch einen Widerruf befürchten. Sofern ein Widerruf wegen Art. 7 Abs. 3 S. 1 und ErwG 42 S. 5 DS-GVO bzw. § 327q Abs. 3 BGB keinerlei Nachteile und deshalb auch keine Schadens- oder Wertersatzpflichten auslösen darf, scheint die Widerruflichkeit für Datensubjekte rechtlich ausschließlich positive Folgen zu haben.

Dieser Eindruck täuscht jedoch: Weil die jederzeitige Widerruflichkeit der Einwilligung es ermöglicht, dass Leistungsbeziehungen die stabile rechtliche Grundlage jederzeit und einseitig durch das Datensubjekt entzogen werden kann, setzt sie für die Verantwortlichen bestimmte tatsächliche Verhaltensanreize, die zwar diametral zu den mit der DS-GVO verfolgten Zielen stehen, aber dennoch rechtmäßig sind (aa).

Zudem erschwert eine generelle freie Widerruflichkeit die Etablierung von Geschäftsmodellen für Datentreuhänder, obwohl diese nach Vorstellung des europäischen Gesetzgebers dabei helfen sollen, Datensubjekte bei der kontrollierten Verwertung und Bereitstellung von personenbezogenen Daten zu unterstützen (bb).

aa) Freie Widerruflichkeit als Anreiz für die sofortige Verwertung

Infolge der sog. freien Widerruflichkeit ist es aus Sicht der Verantwortlichen sinnvoll, ihre Leistungen nur denjenigen Datensubjekten anzubieten, die mit personenbezogenen Daten in Vorleistung gehen.[191] Zudem ist es konsequent, die personenbezogenen Daten auf Grundlage einer transparenten, aber umfassenden[192] Einwilligung unverzüglich zu monetisieren und dabei auch zahlungsbereite Dritte bzw. weitere (gemeinsam) Verantwortliche einzubeziehen. Widerruft das Datensubjekt später seine Einwilligung, so erfährt dies zunächst nur der unmittelbare Einwilligungsempfänger (erster Verantwortlicher).[193] Dieser ist zwar gemäß Art. 19 S. 1 DS-GVO, Art. 17 Abs. 1 lit. b DS-GVO dazu verpflichtet, die ihm bekannten weiteren Verantwortlichen und Datenempfänger, denen er die personenbezogenen Daten mit Einwilligung des Datensubjekts offengelegt hat, über diesen Einwilligungswiderruf zu informieren. Jeder weitere Verantwortliche prüft auf dieser Grundlage selbst, ob er zur Löschung ver-

[191] Hierzu oben Kapitel 4 A.II.5.

[192] Die Grenze bildet vorrangig der Zweckbindungsgrundsatz (Art. 5 Abs. 1 lit. b DS-GVO) und der Grundsatz einer Datenverarbeitung nach Treu und Glauben (Art. 5 Abs. 1 lit. a Var. 2 DS-GVO).

[193] Vor dieser Relativität des Widerrufs als Risiko für das Datensubjekt warnend: *Simitis*, BDSG, 5. Aufl. 2003, § 4a, Rn. 99; *Buchner*, Die informationelle Selbstbestimmung im Privatrecht, 2006, S. 235.

pflichtet ist. Diese Informationspflicht desjenigen Verantwortlichen, der die personenbezogenen Daten ursprünglich mit Einwilligung des Datensubjekts für weitere (gemeinsam) Verantwortliche eingeholt hat, endet aber, sobald deren Erfüllung mit einem unverhältnismäßigen Aufwand verbunden ist, Art. 19 S. 1 DS-GVO.

Jedenfalls bei unterschiedlichen Ansichten darüber, wann ein Aufwand noch verhältnismäßig ist und solange hierzu keine klare Rechtsprechung existiert, wird es faktisch Sache der Datensubjekte sein, von den weiteren Gliedern der Datenkette jeweils die Löschung der Daten zu verlangen. Das Resultat ist eine Daten-Schnitzeljagd,[194] wobei – je nach Umfang der ursprünglichen erklärten Einwilligung – die Kette der Datenweitergabe so lang ist, dass eine Durchsetzung der Ansprüche des Datensubjekts irrationale Opportunitätskosten verursacht (sog. rationale Apathie). Allerdings können diesem Szenario einer Daten-Schnitzeljagd zwei Einwände entgegengehalten werden:

Erstens muss die ursprüngliche, weitreichende Einwilligung selbst rechtmäßig gewesen sein und in diesem Zusammenhang die spezifischen Anforderungen an die Einwilligung und die generellen Anforderungen an die Grundsätze der rechtmäßigen Datenverarbeitung (Art. 5 Abs. 1 DS-GVO) erfüllen. Zudem benötigt jeder der (gemeinsam) Verantwortlichen jeweils einen Erlaubnistatbestand für die Datenverarbeitung.[195] Sofern die ursprünglichen Einwilligungen die Datenweitergabe an weitere bekannte (gemeinsame) Verantwortliche vorsah, könnten diese Einwilligungen und damit die darauf beruhende Verwertungskette insbesondere am Grundsatz der Transparenz (Art. 5 Abs. 1 lit. a Var. 3 DS-GVO) oder am Grundsatz der Verarbeitung nach Treu und Glauben (Art. 5 Abs. 1 lit. a Var. 2 DS-GVO) scheitern.[196]

Zweitens geht derjenige Verantwortliche, der sich darauf beruft, dass eine Pflicht zur Information der weiteren Verantwortlichen gemäß Art. 19 S. 1 DS-GVO unverhältnismäßig aufwändig sei, das Risiko ein, dass Gerichte zugunsten der Datensubjekte entscheiden und Datenschutzbehörden anschließend vom Verantwortlichen ein hohes Bußgeld fordern. Zudem ist nicht auszuschließen, dass die Datenschutzbehörden bei der Bemessung des Bußgelds für den ersten Verantwortlichen zusätzlich die nachfolgenden Datenverarbeitungen berücksichtigen, die zeitlich nach dem Einwilligungswiderruf noch durch weitere

---

[194] *Sattler*, JZ 2017, 1036 (1040).

[195] *EuGH*, Urt. v. 29.06.2019, C-40/17 = GRUR 2019, 958 (Rn. 132 f.) – *Fashion ID*.

[196] Weil durch die Notwendigkeit zur Abwahl schon keine Einwilligung(en) vorlag(en), musste der BGH sich nicht dazu äußern, ob eine Liste von bis zu 60 potenziellen Verantwortlichen noch mit den Anforderungen an eine wirksame Einwilligung und den Grundsätzen einer rechtmäßigen Datenverarbeitung vereinbar ist: *BGH*, Urt. v. 28.05.2020, I ZR 7/16 = NJW 2020, 2540 (Rn. 32) – *Cookie-Einwilligung II*; skeptisch insoweit: *Spindler*, NJW 2020, 2513 (2514: „Ob mit dieser Entscheidung allerdings tatsächlich ein ‚Mehr' an Datenschutz gewonnen wird, kann mit Fug und Recht bezweifelt werden; vielmehr dürfte die Zahl der anzukreuzenden Kästchen einfach vermehrt werden").

(gemeinsam) Verantwortliche stattfanden, weil der erste Verantwortliche seiner Informationspflicht gemäß Art. 19 S. 1 DS-GVO nicht unverzüglich nachgekommen ist.

Alternativ kann man den Verhältnismäßigkeitsvorbehalt in Art. 19 S. 1 DS-GVO auch für einen gesetzgeberischen Fehler halten, der zu korrigieren ist.[197] Kurzum: Die im Szenario aufgezeigten Schwächen, die Art. 19 S. 1 DS-GVO für die Durchschlagskraft des Art. 7 Abs. 3 S. 1 DS-GVO etabliert und die einen betriebswirtschaftlichen Anreiz für die Einholung möglichst umfassender Einwilligungen und für eine schnelle Weitergabe der personenbezogenen Daten an weitere (gemeinsam) Verantwortliche bieten, sprechen nicht gegen die freie Widerruflichkeit als solche. Vielmehr dürfte Art. 19 S. 1 DS-GVO zu vage ausgefallen sein.

Dennoch setzt Art. 7 Abs. 3 S. 1 DS-GVO weiterhin einen Anreiz für Geschäftsmodelle, bei denen Datensubjekte mit den personenbezogenen Daten in Vorleistung gehen müssen. Diese Vorleistung des Datensubjekts kann der Verantwortliche rechtlich als Bedingung (§ 158 Abs. 1 BGB) und technisch mit Hilfe von Software absichern. Die Leistungsbeziehung wird dadurch in eine feingliedrige Kette aus – für sich jeweils abgeschlossenen – *ad hoc* Mikro-Transaktionen unterteilt. Aus rechtlicher Perspektive wird diese Kette aus technisch determinierten Mikro-Transaktionen bereits mit der „schuldrechtlichen Steinzeit" verglichen,[198] wenngleich die faktische Abwicklung auf Grundlage von maschinenlesbar codierter Information durch diese rechtliche Konstruktion über bedingte Mikro-Transaktionen nicht beeinträchtigt wird.

Dennoch begünstigt diese rechtlich indizierte Unterteilung in atomistische Transaktionen faktisch diejenigen Verantwortlichen, die – wie insbesondere *GAFAM* – aufgrund ihrer Marktposition mit der Konsequenz einer jederzeit generellen Widerruflichkeit besser zurechtkommen. Sollen die wettbewerbspolitischen Vorteile einer Flexibilisierung von Art. 7 Abs. 3 S. 1 DS-GVO realisiert werden, setzt dies voraus, dass auch Datensubjekte, die als Verbraucher handeln, grundsätzlich über die Widerruflichkeit der Einwilligung disponieren können, so dass Verantwortliche auf Basis einer befristeten, aber insoweit bindenden Einwilligung über eine verlässliche Grundlage für die Datenverarbeitungen verfügen. Eine hiervon zu trennende Frage ist, welche Voraussetzungen und Grenzen einer solchen zeitweisen Disposition über die sog. freie Widerruflichkeit i. S. d. Art. 7 Abs. 3 S. 1 DS-GVO zu setzen sind (hierzu sogleich).

---

[197] Es liegt jedenfalls nahe, die Einrede der Unverhältnismäßigkeit dann besonders eng auszulegen, wenn die Datenverarbeitung ausschließlich der unmittelbaren Monetisierung der Daten dient und diese voll automatisiert abläuft. In diesem Fall dürfte es jedenfalls nicht unverhältnismäßig und gemäß Art. 7 Abs. 3 S. 4 DS-GVO sogar geboten sein, dass der Einwilligungsempfänger auch die Information über den Widerruf vollständig automatisieren muss. Infolgedessen würde der Widerruf sofort an alle Datenempfänger weitergeleitet, die ihre Berechtigung zur Verarbeitung aus der ursprünglichen Einwilligung ableiten.

[198] So *Martin Schmidt-Kessel* in der Diskussion anlässlich des Workshops über Rechte an Daten, 22.02.2019, Universität Bayreuth.

bb) Zeitweise bindende Einwilligung und Datenaltruismus

Für den hier vertretenen Ansatz einer Flexibilisierung der Widerruflichkeit auch im B2C-Verhältnis spricht zudem – zumindest[199] – eine aktuelle EU-Verordnung.[200] Gemäß Art. 10 Abs. 1 lit. b DG-VO[201] sollen beaufsichtigte Datenvermittler entstehen, die dabei helfen, eine gemeinsame Nutzung von – ausdrücklich auch personenbezogenen – Daten zu ermöglichen und das durch die Datenverarbeitung vorhandene wirtschaftliche Potenzial in der EU zu nutzen.

Als Grundlage für diese geplante treuhänderische Datenvermittlung sehen Art. 10 Abs. 1 lit. b und Art. 12 lit. n DG-VO primär eine Einwilligung vor. Diese Herangehensweise mit einer zentralen Funktion der Einwilligung gilt auch für das ebenfalls in der DG-VO geregelte Konzept eines Datenaltruismus, Art. 16–25 DG-VO. Das Konzept des Datenaltruismus ist gemäß Art. 2 Nr. 16 DG-VO definiert als

> „die freiwillige gemeinsame Nutzung von Daten auf der *Grundlage der Einwilligung* betroffener Personen zur Verarbeitung der sie betreffenden personenbezogenen Daten […], ohne hierfür ein Entgelt zu fordern oder zu erhalten, das über eine Entschädigung für die ihnen durch die Bereitstellung ihrer Daten entstandenen Kosten hinausgeht, für Ziele von allgemeinem Interesse gemäß dem nationalen Recht, […]." [Hervorhebung durch den Verfasser].

Gemäß ErwG 52 DG-VO soll das Konzept des Datenaltruismus dazu dienen, den Pool derjenigen personenbezogenen Daten zu erweitern, die für Zwecke der Gesundheitsversorgung, der Bekämpfung des Klimawandels und der Verbesserung der Mobilität verarbeitet werden können. Als Grundlage für den Datenaltruismus plant die *EU-Kommission* die Entwicklung eines verbindlichen europäischen Einwilligungsformulars (Art. 25 DG-VO).

In diesem Zusammenhang wird deutlich, dass die *EU-Kommission* die Möglichkeit einer vertragsakzessorischen Datenverarbeitung, beispielsweise in Form eines (entgeltlichen) Auftrags oder eines Schenkungsvertrags weder im Kontext der treuhänderischen Datenvermittlung noch in Bezug auf das Konzept des Datenaltruismus erwähnt. Obwohl die DG-VO – unter Einhaltung der derzeitigen *political correctness* – die Widerruflichkeit der jeweiligen Einwilligung erwähnt,[202] bestehen erhebliche Zweifel, dass sich Organisationen oder

---

[199] Auch der geplante europäische Data Act soll den grenzüberschreitenden Zugang zu personenbezogenen Daten im Binnenmarkt verbessern.

[200] Deshalb sehr kritisch und zu einer Klarstellung auffordernd, dass die DS-GVO Vorrang hat und nicht aufgeweicht werden soll: *EDPB-EDPS*, Joint Opinion 03/2021 on the Proposal for a regulation of the European Parliament and of the Council on European data governance (Data Governance Act oder kurz: DG-VO) v. 11.03.2021, S. 38 f.

[201] Verordnung (EU) 2022/868 v. 30.5.2022 über europäische Daten-Governance und zur Änderung der Verordnung (EU) 2018/1724 (Daten-Governance-Rechtsakt, kurz: DG-VO), ABl. v. 3.6.2022, L 152, S. 1 ff.

[202] Im Kontext des Datenaltruismus: Art. 25 Abs. 3 sowie ErwG 52 DG-VO.

Unternehmen finden werden, die auf der instabilen Rechtsgrundlage einer jederzeit und grundlos widerruflichen Einwilligung ein Geschäftsmodell entwickeln können, dass die erwünschte rechtssichere, aber auch effiziente und effektive Nutzung personenbezogener Daten für die mit der DG-VO angestrebten Zwecke ermöglicht.

Aus der Perspektive des hier vorgeschlagenen Stufenmodells der Erlaubnistatbestände zur Gewährleistung einer abgestützten informationellen Privatautonomie bestehen gute Chancen, dass jedenfalls die treuhänderische Datenvermittlung – vermutlich aber auch das Konzept des Datenaltruismus – wichtige Anwendungsfälle sein werden, die von einer zeitweise unwiderruflichen Einwilligung in Form einer schuldrechtlichen Gestattung profitieren würden.[203]

3. Abstützungen einer Disposition über Art. 7 Abs. 3 S. 1 DS-GVO

Die grundsätzliche Möglichkeit zur Disposition über die Widerruflichkeit der datenschutzrechtlichen Einwilligung gilt weder stets und bedingungslos noch für jedes Datensubjekt gegenüber jedem Verantwortlichen. Sofern eine Kartellbehörde festgestellt hat, dass ein Verantwortlicher in einem Marktsegment eine beherrschende Marktposition hat, ist eine Disposition über die Widerruflichkeit der Einwilligung gegenüber diesem Verantwortlichen ausgeschlossen. Dies gilt unabhängig davon, ob das Datensubjekt ein Verbraucher ist oder unternehmerisch handelt (a).

Selbst für den Fall, dass ein Verantwortlicher nicht über eine derartige Marktposition verfügt, folgt hieraus noch keine generelle Möglichkeit zur Disposition des Datensubjekts über Art. 7 Abs. 3 S. 1 DS-GVO. Vielmehr liegt es auf der Hand, lediglich einen befristeten Ausschluss der sog. freien Widerruflichkeit zuzulassen, sofern ein Datensubjekt zugleich Verbraucher ist (b). Dieser befristete Ausschluss der jederzeitigen und grundlosen Widerruflichkeit sollte zudem nicht automatisch, sondern nur durch eine erneute Entscheidung des Datensubjekts und auch dann wiederum nur mit befristeter Wirkung verlängert werden können (c).

Unabhängig von einer wirksamen Disposition über die Widerruflichkeit bleibt dem Datensubjekt die Möglichkeit, die gestattende Wirkung der Einwilligung jederzeit zu beenden, sofern ein wichtiger Grund besteht (d). Obwohl gegen diese – unionsgrundrechtlich gebotene – Flexibilisierung der Widerruflichkeit ebenfalls der Einwand von erheblicher Rechtsunsicherheit erhoben werden kann, hat sie den Vorteil, dass sie anhand der bestehenden Anforderungen an eine wirksame Einwilligung und unter Heranziehung der Grundsätze der rechtmäßigen Datenverarbeitung und somit unionsautonom und damit unionsweit einheitlich entwickelt werden kann.

---

[203] Dies ebenfalls (über)vorsichtig erwägend: *Kühling*, ZfDR 2021, 1 (11); weitergehend und für eine konstitutive Rechtseinräumung, einschließlich Wahrnehmungsvertrag, für Datentreuhänder: *Buchner*, Die informationelle Selbstbestimmung im Privatrecht, 2006, S. 285 ff./290 f.

a) Keine Disposition gegenüber marktmächtigen Verantwortlichen

Hat eine zuständige Kartellbehörde bereits darüber entschieden, dass der Verantwortliche auf dem relevanten Markt eine marktbeherrschende Position (Art. 102 AEUV bzw. § 19 GWB) innehat bzw. (künftig) ein *Gatekeeper* im Sinne des Art. 3 des DMA-Vorschlags der *EU-Kommission* ist oder hat das *Bundeskartellamt* festgestellt, dass dem Verantwortlichen eine überragende marktübergreifende Bedeutung für den Wettbewerb gemäß § 19a Abs. 1 GWB zukommt, so sollte für Datenschutzbehörden und Gerichte die *unwiderlegliche* Vermutung gelten, dass eine Einschränkung der Widerruflichkeit der Einwilligung unfreiwillig und damit gemäß des Grundsatzes einer Datenverarbeitung nach Treu und Glauben (Art. 5 Abs. 1 lit. a Var. 2 DS-GVO) unwirksam ist.[204]

Durch diese *kartellrechtsakzessorische*, *asymmetrische* Auslegung und Anwendung von Art. 7 Abs. 3 S. 1 DS-GVO wird der Entmachtungsmechanismus des Wettbewerbs[205] gestärkt[206] und es lohnt sich für die Herausforderer, eine langfristige Rechtsbeziehung zu Datensubjekten auf Grundlage eines datenschonenden Geschäftsmodells einzugehen.[207]

Die *kartellrechtsakzessorische* Anwendung von Art. 7 Abs. 3 S. 1 DS-GVO führt dazu, dass die Disposition über die Widerruflichkeit der Einwilligung stets ausscheidet, soweit eine Entscheidung einer Kartellbehörde die bestehende Marktmacht eines Verantwortlichen festgestellt hat. Zudem sollte die Disposition über die Widerruflichkeit bereits dann ausgeschlossen sein, soweit die Angebote von Unternehmen – wie *GAFAM* – Gegenstand aktueller kartellrechtlicher Verfahren sind.

An dieser Stelle werden (erneut) die Nachteile der fehlenden Synchronisierung von Kartell- und Datenschutzrecht deutlich. *De lege ferenda* ist es notwendig, einen Mechanismus vorzusehen, der den Datenschutzbehörden einen Zugang zu der Expertise der jeweiligen Kartellbehörde ermöglicht, sofern eine strukturelle Unterlegenheit des Datensubjekts aufgrund der Marktmacht des Verantwortlichen ernsthaft in Betracht kommt.

De lege lata lässt sich jedoch nicht ausschließen, dass die Datenschutzbehörden und (Verwaltungs-)Gerichte diese Beurteilung – ebenso wie im Rahmen von Art. 7 Abs. 4 DS-GVO – (über-)optimistisch selbst vornehmen (müssen).

---

[204] Die Freiwilligkeit der (widerruflichen) Einwilligung bleibt hiervon jedoch unberührt, soweit die Voraussetzungen aus Art. 7 Abs. 4 DS-GVO erfüllt sind.

[205] *Böhm*, Demokratie und ökonomische Macht, 1961, S. 22.

[206] Insoweit ist diese kartellrechtsakzessorische Auslegung und Anwendung der DS-GVO ein milderes Mittel als eine (interne) Entflechtung von *GAFAM* und ermöglicht zugleich eine flexiblere Anwendung gegenüber KMU. Zu den Entflechtungsbestrebungen: *Mundt*, NZKart 2019, 117. Zur Gefahr einer Überforderung von KMU: *Evaluierungsbericht zur DS-GVO der EU-Kommission*, COM (2020)264 final, S. 12 (19 ff.).

[207] Zu dem bislang fehlenden Anreiz: *Bäcker*, Der Staat 51 (2012), S. 91; *Bunnenberg*, Privates Datenschutzrecht, 2020, S. 241 f.

b) Befristung der Unwiderruflichkeit im B2C-Verhältnis

Obwohl die DS-GVO nicht danach differenziert, ob ein Datensubjekt Verbraucher ist oder seinerseits unternehmerisch handelt, ist diese Unterscheidung für die Möglichkeit zur Disposition über die Widerruflichkeit essentiell.[208] Verfügt der Verantwortliche nicht über eine marktmächtige Position im Sinne des Kartellrechts (sonst greift Kriterium a), so steht Art. 7 Abs. 3 S. 1 DS-GVO einer transparenten Disposition über die Widerruflichkeit jedenfalls durch unternehmerisch handelnde Datensubjekte nach hier vertretener Ansicht grundsätzlich nichts im Wege. Als Abstützung bleiben die Vereinbarung von ordentlichen Beendigungsrechten und der außerordentliche Widerruf der Einwilligung (unten d).

Spannender und besonders umstritten dürfte jedoch die hier vorgeschlagene Möglichkeit zur Disposition über die Widerruflichkeit der Einwilligung sein, soweit sie das Rechtsverhältnis zwischen einem als Verbraucher handelnden Datensubjekt und einem Verantwortlichen betrifft, der über keine marktmächtige Stellung verfügt. Aus Art. 7 Abs. 3 S. 1 DS-GVO folgt – trotz der hier vertretenen Möglichkeit zur teleologischen Reduktion – unzweifelhaft die grundsätzliche Entscheidung des europäischen Gesetzgebers, dem Datensubjekt für die Zukunft eine möglichst umfassende und dauerhafte Möglichkeit zur Wiederherstellung der Entscheidungszuständigkeit einzuräumen.

Diese gesetzgeberische Entscheidung und die Gewährleistungspflicht aus Art. 8 Abs. 1 GRCh sorgen dafür, dass im B2C-Verhältnis lediglich eine befristete Disposition über die Widerruflichkeit der datenschutzrechtlichen Einwilligung möglich ist. Während also die Möglichkeit zur befristeten Disposition sicherstellt, dass das Untermaß der allgemeinen Vertragsfreiheit (Art. 6 Abs. 3 EUV) gewährleistet wird, würde die Anerkennung einer dauerhaft und stets bindenden Disposition über die Widerruflichkeit der Einwilligung das gemäß Art. 8 Abs. 1 GRCh zu gewährleistende Untermaß zum Schutz personenbezogener Daten unterschreiten. Infolgedessen können der Gesetzgeber und – soweit infolge einer Delegation zulässig – die Gerichte über die Höchstdauer, die Voraussetzungen und möglichen Grenzen entscheiden, die für eine solche zeitliche Disposition über die sog. freie Widerruflichkeit zu beachten sind.[209]

---

[208] Immerhin ging der Berichterstatter des Europäischen Parlaments für die DS-GVO davon aus, dass die Verbrauchereigenschaft eines Datensubjekts ein im Rahmen der Interessenabwägung (Art. 6 Abs. 1 lit. f DS-GVO) zu berücksichtigendes Kriterium ist: *Albrecht*, CR 2016, 88 (91). Die fehlende Differenzierungen der DS-GVO führt zu grundlegenden Abgrenzungsfragen zwischen Datenschutz- und Verbraucherschutzrecht: Vorlagefrage zur Auslegung und Anwendbarkeit von § 8 Abs. 3 Nr. 3 UWG bzw. §§ 1, 2 Abs. 2 S. 1 Nr. 11, 3 Abs. 1 S. 1 Nr. 1 UKlaG trotz der Regelung von spezifischen Rechtsbehelfen in Art. 80 Abs. 1 und Abs. 2, Art. 84 DS-GVO: *BGH*, Beschl. v. 28.05.2020, I ZR 186/17 = GRUR 2020, 896 – *App-Zentrum*.

[209] Neben den nachfolgend angeführten Abstützungen ist es beispielsweise denkbar, zusätzliche Formerfordernisse oder Mechanismen zu verlangen. So ist es beispielsweise sinnvoll, dass eine befristete Disposition über die Widerruflichkeit nur durch ein *Double-Opt-In-*

Weil dem europäischen Gesetzgeber das Bewusstsein für die Folgen einer stets frei widerruflichen Einwilligung fehlte und die Konsequenzen für die Verwertung der vermögenswerten Bestandteile von Persönlichkeitsrechten übersehen wurden, enthält die DS-GVO auch keine Regelung über eine angemessene Dauer für eine wirksame Disposition über die Widerruflichkeit. Somit fällt diese Aufgabe gemäß Art. 2 EUV und Art. 19 Abs. 1 UAbs. 1 Satz 2 EUV einstweilen in den richterlichen Beurteilungsspielraum bei der Auslegung und Anwendung des Sekundärrechts.

Gesetzliche Grundlage für die richterrechtlich zu setzenden Grenzen einer privatrechtsensiblen Auslegung und Anwendung der DS-GVO ist der generalklauselartige Grundsatz einer Datenverarbeitung nach Treu und Glauben gemäß Art. 5 Abs. 1 lit. a Var. 2 DS-GVO.

Mangels spezifischer gesetzgeberischer Ansätze ist die Bemessung der rechtmäßigen Befristung einer Disposition über die Widerruflichkeit schwierig. Diese Fristsetzung muss einen Ausgleich zwischen der Gewährleistung des Schutzes von personenbezogenen Daten und der Privatsphäre und der Gewährleistung der Vertragsfreiheit schaffen. Hinzu kommt, dass eine Disposition über die Widerruflichkeit der Einwilligung auch dem Ziel dient, Marktzutrittsbarrieren für KMU zu verhindern[210] und für neue, insbesondere datenschonende Geschäftsmodelle eine stabilere und verlässlichere rechtliche Grundlage zu schaffen.

Solange eine sinnvolle Abgrenzung zwischen personenbezogenen Daten und besonders sensiblen personenbezogenen Daten noch nicht gelungen ist, einfache Portraitfotos und die Protokollierung von Besuchen von oder Eingaben auf bestimmten Webseiten[211] potenziell bereits als besonders sensibles personenbezogenes Datum zu beurteilen ist und der deutsche Gesetzgeber danach strebt, diese Unterscheidung mit Blick auf die verfügbaren Erlaubnistatbestände aufzuweichen,[212] spricht dies dagegen, *per se* eine kürzerer Zeitspanne für eine Disposition über die freie Widerruflichkeit vorzusehen, sofern auch besonders sensible personenbezogene Daten verarbeitet werden. Gleichwohl ist es plausibel, dass der zeitweise Ausschluss der freien Widerruflichkeit insbesondere im Bereich von Gesundheitsdaten oder genetischen Daten potenziell mit hohen Risiken verbunden ist.[213]

Verfahren und unter Verwendung von E-Mail rechtmäßig ist, so dass dieser gewünschte „Medienbruch", den Nutzungsvorgang bewusst unterbricht, um die Bedeutung dieser Disposition über Art. 7 Abs. 3 S. 1 DS-GVO herauszustellen (Warnfunktion).

[210] *Evaluationsbericht der EU-Kommission zur DS-GVO*, COM(2020) 264 final, S. 12/19 ff.

[211] Vorlagefrage 2a des *OLG Düsseldorf*, Vorlagebeschl. v. 24.03.2021 – Kart 2/19 (V), GRUR-RS 2021, 8370 (Rn. 37 ff.).

[212] Gemäß § 27 Abs. 1 BDSG soll eine Verarbeitung von besonders sensiblen personenbezogenen Daten „abweichend" von Art. 9 Abs. 1 DS-GVO für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke auch auf Grundlage einer (qualifizierten) Interessenabwägung und damit ohne Einwilligung zulässig sein.

[213] Weil eine Verarbeitung dieser besonders sensiblen Kategorien von personenbezogenen Daten nicht nur besondere technische und organisatorische Maßnahmen des Verantwort-

Mit dem Ziel über eine praktische Konkordanz einen Ausgleich zwischen den unionsgrundrechtlichen Gewährleistungspflichten aus Art. 8, Art. 7, Art. 16 GRCh und Art. 6 Abs. 3 EUV zu schaffen, liegt es auf der Hand, lediglich eine kurzzeitige Disposition über die Widerruflichkeit der Einwilligung anzuerkennen.

Ausgehend von ihrem Zweck, die informationelle Privatautonomie anzuerkennen und ein Mindestmaß an Stabilität für die Rechtsbeziehung zwischen Datensubjekt und Verantwortlichem zu ermöglichen, ist eine kurze Zeitspanne von wenigen Monaten regelmäßig ausreichend. Für eine solche kurze Zeitspanne spricht zudem die Möglichkeit, dass der Verantwortliche sich anschließend um einen erneuten, wiederum befristeten Ausschluss der Widerruflichkeit bemühen kann.

c) Keine stillschweigende Verlängerung des Widerrufsausschlusses

Indem Art. 7 Abs. 3 S. 1 DS-GVO von einer freien Widerruflichkeit ausgeht und diese dazu dient, die Entscheidungszuständigkeit des Datensubjekts über den unionsgrundrechtlich gewährleisteten Schutz von personenbezogenen Daten dauerhaft zu sichern, spricht dies gegen die Möglichkeit einer „automatischen", also stillschweigenden Verlängerung der Disposition über Art. 7 Abs. 3 S. 1 DS-GVO im B2C-Verhältnis.

Insbesondere liefert § 309 Nr. 9 b BGB bzw. Nr. 1 lit. h des Anhangs der Klausel-RL, der für entgeltliche Dauerschuldverhältnisse im B2C-Verhältnis lediglich eine „bindende stillschweigende Verlängerung des Vertragsverhältnisses um jeweils mehr als ein Jahr" ausschließt kein zwingendes Argument für oder gegen die Möglichkeit einer stillschweigenden Verlängerung der Bindungswirkung der datenschutzrechtlichen Einwilligung.[214] Schon der bloße Vergleich mit den in § 309 Nr. 9b BGB geregelten, bloße monetäre Nachteile betreffenden Sachverhalten verbietet sich, weil die persönlichkeitsrechtlichen Bestandteile von personenbezogenen Daten für die Beurteilung der Rechtmäßigkeit einer stillschweigenden Verlängerung des Ausschlusses des freien Widerrufs ausschlaggebend sind.

Gegen eine stillschweigende Verlängerung spricht zudem, dass – nach hier vertretener Auffassung – der Vorrang der Einwilligung für Datenverarbeitungen im Privatrechtsverhältnis zu beachten ist und die DS-GVO damit struktu-

---

lichen voraussetzt, sondern auch ein Vertrauen in die Zuverlässigkeit des Verantwortlichen, können begründete Zweifel an dieser Zuverlässigkeit auch zu erleichterten außerordentlichen Beendigungsrechten führen, hierzu sogleich unter d.

[214] Auch aus der im – gescheiteren – Art. 85 lit. v GEKR vorgesehenen maximalen erstmaligen Bindungsdauer von einem Jahr eines Vertrages über die Bereitstellung digitaler Inhalte lässt sich nichts für die datenschutzrechtliche Einwilligung ableiten, da diese Regelung nur Verträge gegen monetäres Entgelt berücksichtigt hätte.

rell von einem *Opt-In* ausgeht. Dadurch wird die originäre Entscheidungszuständigkeit des Datensubjekts abgesichert. Ein *Opt-Out* kommt gemäß Art. 21 Abs. 1 DS-GVO gerade nur im Fall einer Interessenabwägung und damit in Konstellationen zur Anwendung, in denen eine Einwilligung unerreichbar oder mit unverhältnismäßigem Aufwand verbunden ist.[215]

Diese grundlegende Entscheidung zugunsten eines *Opt-In* spricht dafür, ein *Opt-In* als Strukturprinzip des Datenschutzrechts dauerhaft aufrechtzuerhalten. Infolgedessen ist der Ausschluss der jederzeitigen und voraussetzungslosen Widerruflichkeit im B2C-Verhältnis sowohl bei dem erstmaligen als auch bei einem nachfolgenden Ausschluss der freien Widerruflichkeit stets durch eine sog. *sunset clause* zu befristen.[216] Ebenso wie ein Schweigen oder die Untätigkeit des Datensubjekts nicht als Einwilligung gewertet werden können (ErwG 32 S. 3 DS-GVO), darf das Schweigen eines Datensubjekts auch nicht zu einer automatischen Verlängerung einer Disposition über die sog. freie Widerruflichkeit der Einwilligung führen.

Hat der Verantwortliche ein Interesse an einem längeren Ausschluss der freien Widerruflichkeit, so muss er sich vor Ablauf der Frist um einen erneuten, wiederum befristeten Ausschluss der Widerruflichkeit i. S. d. Art. 7 Abs. 3 S. 1 DS-GVO durch das Datensubjekt bemühen. Diese Notwendigkeit zum wiederkehrenden *Re-Opt-In* kombiniert die Vorteile der Widerruflichkeit der Einwilligung mit den Vorteilen einer befristeten Stabilisierung der Leistungsbeziehung zwischen einem nicht-marktbeherrschenden Verantwortlichem und einem Datensubjekt, das Verbraucher ist. Zugleich erhöht die Notwendigkeit, den befristeten Ausschluss der Widerruflichkeit periodisch erneut einzuholen, den Wettbewerbsdruck, weil ein Datensubjekt nur dann erneut in den zeitweisen Ausschluss auf die Widerruflichkeit einwilligen wird, wenn der nicht-marktmächtige Verantwortliche dem Datensubjekt einen Vorteil gegenüber der anderenfalls nach Fristablauf automatisch wieder auflebenden, jederzeitig widerruflichen datenschutzrechtlichen Einwilligung bieten kann.

Die Kombination aus einer zwingenden Befristung und der Möglichkeit zur erneuten Disposition über einen zeitweisen Ausschluss der Widerruflichkeit hat einen weiteren wesentlichen Vorteil. Sie ermöglicht eine zeitnahe, wiederkehrende Anpassungsmöglichkeit an eine mittlerweile veränderte Wettbewerbslage. War ein Verantwortlicher im Zeitpunkt der befristeten Disposition über die sog. freien Widerruflichkeit nicht marktmächtig und verändert sich diese Position dahingehend, dass dieser Verantwortliche nach Ansicht einer Kartellbehörde mittlerweile marktbeherrschend ist und deshalb – beispielswei-

---

[215] Oben Kapitel 2 D.

[216] Dies bereits für die datenschutzrechtliche Einwilligung erwägend: *Spindler*, NJW-Beilage 2012, 98 (100: „Die zeitliche Gültigkeit einer Einwilligung sollte periodisch erneuert werden, in aller Regel alle zwei bis vier Jahre, um zu verhindern, dass Nutzer an früher erteilten Einwilligungen trotz veränderter Umstände und Risikobewusstseins festgehalten werden").

se infolge eines Unternehmenszusammenschlusses – in die Liste der *Gatekeeper* bzw. Unternehmen mit überragender marktübergreifender Bedeutung für den Wettbewerb aufgenommen wurde, so kann dies zu einem außerordentlichen Widerruf der Einwilligung berechtigen.[217] Zudem ist es dem – nun marktmächtigen – Verantwortlichen ab diesem Zeitpunkt nicht mehr möglich, einen erneuten Ausschluss der Widerruflichkeit i. S. d. Art. 7 Abs. 3 S. 1 DS-GVO zu erlangen. Mit dem Auslaufen des befristeten Ausschlusses der freien Widerruflichkeit kann die Datenverarbeitung durch den marktmächtigen Verantwortlichen wiederum nur auf Grundlage der ursprünglich jederzeit und voraussetzungslos widerruflichen Einwilligung i. S. d. Art. 7 Abs. 3 S. 1 DS-GVO bzw. – soweit einschlägig – auf Basis eines gesetzlichen Erlaubnistatbestands fortgesetzt werden.

Umgekehrt wird ein befristeter Ausschluss der freien Widerruflichkeit grundsätzlich möglich, sofern ein Verantwortlicher nach (erneuter) Prüfung durch die zuständige Kartellbehörde kein *Gatekeeper* bzw. kein Unternehmen mit überragender marktübergreifender Bedeutung für den Wettbewerb mehr ist.[218] Indem der Ausschluss des Widerrufsrechts von Anfang an befristet ist, reduzieren sich zugleich die irreparablen Nachteile für einen Verantwortlichen, sofern er unzutreffender Weise als marktmächtig qualifiziert wurde und dies erst später durch Gerichtsurteil korrigiert wird.

d) Jederzeitiger Widerruf aus wichtigem Grund

Die Möglichkeit über die sog. freie Widerruflichkeit i. S. d. Art. 7 Abs. 3 S. 1 DS-VO befristet disponieren zu können, dient insbesondere dazu, die informationelle Privatautonomie der Datensubjekte ernst zu nehmen und die Leistungsbeziehungen zwischen Datensubjekten und solchen Verantwortlichen zu stabilisieren, die nicht marktmächtig sind. Dennoch sind mannigfaltige Gründe denkbar, warum ein Datensubjekt seine Einwilligung – trotz wirksamer Disposition über die freie Widerruflichkeit – im Einzelfall dennoch *außerordentlich* widerrufen kann.

Wenngleich die Gründe für einen außerordentlichen Widerruf hier nicht abschließend behandelt werden, lassen sich diese Gründe zumindest in einem ersten Schritt grob danach unterscheiden, ob sie aus der Sphäre des Verantwortlichen (aa) oder aus der Sphäre des Datensubjekts stammen (bb).

---

[217] Zu weiteren Gründen für einen außerordentlichen Widerruf der Einwilligung trotz Disposition über die sog. freie Widerruflichkeit gemäß Art. 7 Abs. 3 S. 1 DS-GVO sogleich unter d.

[218] Die Feststellung des *Bundeskartellamts* über die Eigenschaft als Unternehmen „mit überragender marktübergreifender Bedeutung für den Wettbewerb" ist gemäß § 19a Abs. 1 S. 3 GWB auf fünf Jahre befristet. Die künftig geplante Benennung als Gatekeeper durch die *EU-Kommission* ist gemäß Art. 4 Abs. 1 bzw. Abs. 2 DMA-Vorschlag jederzeit, zumindest aber nach zwei Jahren überprüfbar.

aa) Widerrufsgründe aus der Sphäre des Verantwortlichen

Das mit der Disposition über die sog. freie Widerruflichkeit verbundene Ziel einer Stabilisierung der Leistungsbeziehungen tritt insbesondere dann in den Hintergrund, wenn der Verantwortliche oder sein Auftragsverarbeiter die datenschutzrechtlichen Pflichten für eine rechtmäßige Datenverarbeitung (Art. 5 DS-GVO) oder die datenschutzrechtlichen Pflichten zum Schutz der IT-Sicherheit (Art. 32 und Art. 25 DS-GVO) verletzen. In diesem Fall kann das Datensubjekt seine Einwilligung außerordentlich und damit auch während der befristeten Disposition über die sog. freie Widerruflichkeit jederzeit widerrufen. Die Berechtigung des Datensubjekts darüber hinaus auch gemäß Art. 82 DS-GVO Schadensersatz zu verlangen, sollte durch einen solchen außerordentlichen Widerruf der Einwilligung – ebenso wie nach deutschem Schuldrecht (§ 314 Abs. 4 BGB) – nicht ausgeschlossen sein.

Zudem kommt ein Widerruf aus wichtigem Grund auch dann grundsätzlich in Betracht, wenn ein Verantwortlicher oder sein Auftragsverarbeiter das Ziel eines erfolgreichen Angriffs durch Hacker geworden ist oder Sicherheitslücken aufgetreten sind und das Datensubjekt infolgedessen das Vertrauen in eine sichere Datenverarbeitung durch den Verantwortlichen in begründeter Weise verloren hat. Ob der außerordentliche Widerruf der Einwilligung, verbunden mit der Geltendmachung des Anspruchs auf Datenportabilität gemäß Art. 20 DS-GVO, als Reaktion auf die Benachrichtigung über ein solches Ereignis tatsächlich sinnvoll ist,[219] hat für diese rechtliche Beurteilung keine Bedeutung.

Den bislang genannten Gründen für einen außerordentlichen Widerruf der Einwilligung ist gemeinsam, dass der Grund hierfür aus der Sphäre des Verantwortlichen stammt, sei es, weil dieser nachweislich und schuldhaft Pflichten verletzt oder weil er – auch unverschuldet – das Ziel eines erfolgreichen Hackerangriffs geworden ist. Fraglich ist jedoch, ob auch Gründe, die in der Person des Datensubjekts liegen oder anderweitig aus dessen Sphäre stammen, einen außerordentlichen Widerruf der Einwilligung ermöglichen können.

bb) Widerrufsgründe aus der Sphäre des Datensubjekts

Zunächst spricht die hier vertretene Möglichkeit zur lediglich kurzfristigen Disposition über die sog. freie Widerruflichkeit im B2C-Verhältnis dafür, allenfalls bei ganz gravierenden, persönlichen Gründen des Datensubjekts einen au-

[219] Ein solches Verhalten ist aufgrund des Vertrauensverlusts in den bisherigen Vertragspartner nachvollziehbar. Allerdings offenbaren Datensubjekte ihre personenbezogenen Daten durch einen Wechsel des Verantwortlichen zusätzlich gegenüber mindestens einem weiteren Unternehmen. Es besteht insoweit die Gefahr, dass Datensubjekte die langfristig mit einer zusätzlichen Weitergabe von personenbezogenen Daten einhergehenden Risiken für weitere künftige Datenlecks und Datenschutzverstöße systematisch unterschätzen: *Romanowski/Acquisti*, 24 Berkeley Tech.L.J. (2009), 1061 (1064).

ßerordentlichen Widerruf der Einwilligung zuzulassen. Im Grundsatz gilt: Je leichter ein außerordentlicher Widerruf der Einwilligung aus Gründen möglich ist, die lediglich aus der Sphäre des Datensubjekts stammen, desto stärker nähert sich das Recht zum außerordentlichen Widerruf wieder der sog. freien Widerruflichkeit i. S. d. Art. 7 Abs. 3 S. 1 DS-GVO an.

Deshalb kommt ein solcher außerordentlicher Widerruf im B2C-Verhältnis nur in Betracht, sofern wesentliche, insbesondere persönlichkeitsrechtlich geschützte Interessen durch die Datenverarbeitung beeinträchtigt werden und sofern ein Abwarten bis zum Ablauf des befristeten Ausschlusses der freien Widerruflichkeit dem Datensubjekt nicht zumutbar ist. Diese erhöhte Schwelle für ein außerordentliches Widerrufsrecht aus Gründen, die ausschließlich aus der Sphäre des Datensubjekts stammen, hat zugleich den Vorteil, dass die Überwindung dieser Schwelle ein Argument dafür liefert, mögliche Schadens- oder Wertersatzansprüche des Verantwortlichen infolge eines solchen außerordentlichen Widerrufs – jedenfalls im B2C-Verhältnis – auszuschließen, obwohl der Grund für den außerordentlichen Widerruf ausschließlich aus der Sphäre des Datensubjekts stammt. Infolgedessen ist ein solches außerordentliches Widerrufsrecht auch mit dem in § 327q Abs. 3 BGB geregelten Ausschluss von Ersatzansprüchen des Unternehmers gegen einen Verbraucher vereinbar.

Im B2B-Verhältnis kommt eine andere, flexiblere Beurteilung in Betracht. Soweit im B2B-Verhältnis auch ein längerfristiger Ausschluss der sog. freien Widerruflichkeit gemäß Art. 7 Abs. 3 S. 1 DS-GVO möglich ist, gewinnt auch der zwischenzeitliche außerordentliche Widerruf an Bedeutung. Ein Vergleich mit der in Deutschland bestehenden urheberrechtlichen Lösung liegt nahe.[220] Gemäß § 42 Abs. 1 UrhG steht dem Urheber die Option zur Verfügung, ein von ihm eingeräumtes Verwertungsrecht trotz eines wirksamen und bindenden Vertrags wegen gewandelter Überzeugung zurückzurufen.

Dieser Rückruf wird im Kontext einer Verwertung anderer Persönlichkeitsrechte – insbesondere für das Recht am eigenen Bild (§ 22 KUG) – analog angewendet. *Horst-Peter Götting* scheint zudem davon auszugehen, dass diese Möglichkeit auch dann besteht, wenn es bei der Verwertung des Rechts am eigenen Bild – wie mittlerweile der Regelfall – zur Verarbeitung von personenbezogenen Daten i. S. d. Art. 4 Nr. 1 DS-GVO kommt.[221]

Dieser Ansatz führt zwangsläufig zu der Folgefrage, ob dem Verantwortlichen im B2B-Verhältnis – in Abweichung zum Entschädigungsanspruch i. S. d.

---

[220] Hierzu: *Schwartmann/Hentsch*, RDV 2015, 221 (224 f.); ebenfalls das urheberrechtliche Rückrufrecht als möglichen Ansatz *de lege ferenda* erwähnend: *Leistner/Antoine/Sagstetter*, Big Data, 2021, S. 293.

[221] So für den Widerruf der Einwilligung in die kommerzielle Nutzung des Rechts am eigenen Bild (§ 22 KUG): *Götting*, in: Schricker/Loewenheim, Urheberrecht, 6. Aufl. 2020, § 22 KUG, Rn. 41 (wobei „es sich bei Personenbildnissen um personenbezogene Daten handelt" (Rn. 43a a. E.).

Art. 42 Abs. 3 UrhG – auch ein Anspruch gegen das unternehmerisch handelnde Datensubjekt auf Ausgleich (lediglich) desjenigen Schadens zugebilligt werden kann, den der Verantwortliche erlitten hat, weil er auf den befristeten Ausschluss der freien Widerruflichkeit der Einwilligung vertraut hat. Im Fall eines Widerrufs der Einwilligung in die kommerzielle Nutzung des Rechts am eigenen Bild (§ 22 KUG) soll ein solcher Anspruch gemäß § 122 BGB analog gewährt werden.[222]

Dieser deutsche Ansatz kommt für die Verarbeitung von personenbezogenen Daten aufgrund des Vorrangs der DS-GVO zwar nicht zur Anwendung. Die hierin zum Ausdruck kommende Wertung behält – jedenfalls für eine Datenverarbeitung im B2B-Verhältnis – jedoch ihre Überzeugungskraft. Infolgedessen sollten deutsche Gerichte eine sich bietende Gelegenheit nutzen, um dem *EuGH* diesen Weg vorzuschlagen.

Allerdings findet diese Möglichkeit in der DS-GVO keine spezifische gesetzliche Grundlage. Dies führt zu der Frage, ob der Grundsatz einer Datenverarbeitung nach Treu und Glauben als Grundlage für einen solchen Anspruch im Verhältnis zwischen Verantwortlichem und unternehmerisch handelndem Datensubjekt in Betracht kommt.

Gegen eine solche Möglichkeit sprechen sowohl der Wortlaut des Art. 5 als auch die Ziele der DS-GVO. Gemäß Art. 5 Abs. 1 lit. a Var. 2 DS-GVO müssen personenbezogene Daten nach Treu und Glauben *verarbeitet* werden. Ein Bezug zum Verhalten des Datensubjekts wird nicht hergestellt. Dies gilt auch für die anderen Grundsätze der Datenverarbeitung in Art. 5 Abs. 1 DS-GVO. Selbst der Grundsatz der Richtigkeit der personenbezogenen Daten und die daraus folgende Pflicht zur Aktualisierung der Daten gemäß Art. 5 Abs. 1 lit. d DS-GVO richtet sich ausschließlich an den Verantwortlichen und nicht an das Datensubjekt, obwohl letzteres häufig selbst die Quelle fehlerhafter Daten ist. Zuletzt stellt Art. 5 Abs. 2 DS-GVO nochmals abschließend und unmissverständlich klar, dass ausschließlich der „Verantwortliche […] für die Einhaltung des Absatzes 1 verantwortlich [ist]".

Auch die gemäß Art. 1 DS-GVO verfolgten Ziele sprechen gegen einen solchen Anspruch des Verantwortlichen auf Ersatz des Vertrauensschadens gegen das unternehmerisch handelnde Datensubjekt.

Den Interessen der Verantwortlichen an einer rechtmäßigen Datenverarbeitung kommt in der DS-GVO, beispielsweise im Rahmen der Interessenabwägungen und für das Ziel eines freien Verkehrs personenbezogener Daten im Binnenmarkt lediglich mittelbar eine Bedeutung zu. Dies spricht dafür, dass auf den allgemeinen unionsrechtlich anerkannten Grundsatz des Rechtsmissbrauchs[223]

---

[222] *Dasch*, Die Einwilligung zum Eingriff in das Recht am eigenen Bild, 1990, S. 87; *Helle*, AfP 1985, 93 (101); *Canaris*, AcP 184 (1984), 201 (223 f.); *Götting*, in: Schricker/Loewenheim, Urheberrechts, 6. Aufl. 2020, § 22 KUG, Rn. 41.

[223] Grundlegend zum Grundsatz von Treu und Glauben: *EuGH*, Urt. v. 03.09.2009,

zurückzugreifen ist, sofern ein unternehmerisch handelndes Datensubjekt die Einwilligung innerhalb desjenigen Zeitraums außerordentlich widerruft, für den die freie Widerruflichkeit i.S.d. Art. 7 Abs. 3 S. 1 DS-GVO ausgeschlossen wurde und soweit der Widerruf aus Gründen erfolgt, die ausschließlich aus der Sphäre des unternehmerisch handelnden Datensubjekts stammen.

4. Fazit: Abgestützte Abdingbarkeit der sog. freien Widerruflichkeit

In Kenntnis der seit Jahrzehnten geübten Vertragspraxis zur Kommerzialisierung der vermögenwerten Bestandteile von Persönlichkeitsrechten wird die „fehlende vertragsrechtliche Unterfütterung der DS-GVO“[224] offenkundig.

Abgesehen von der engen Öffnungsklausel gemäß Art. 85 Abs. 1 DS-GVO für solche Konstellationen, in denen die Datenverarbeitungen, neben einem (untergeordneten) kommerziellen Zweck, primär im Zusammenhang mit der Meinungs- und Informationsfreiheit stehen (sog. Presseprivileg), hat der europäische Gesetzgeber die Möglichkeit zur kommerziellen Verwertung von Persönlichkeitsrechten verkannt. Dieses Versäumnis wird mit Blick auf die freie Widerruflichkeit besonders deutlich. Dem europäischen Gesetzgeber ist mit Art. 7 Abs. 3 S. 1 DS-GVO ein planwidriger Konstruktionsfehler unterlaufen. Ohne die Möglichkeit zum zeitweisen Ausschluss der sog. freien Widerruflichkeit ist Art. 7 Abs. 3 S. 1 DS-GVO ein unverhältnismäßiger Eingriff in die unternehmerische Freiheit (Art. 16 GRCh) und die informationelle Privatautonomie (Art. 8 Abs. 2 S. 1 DS-GVO). Infolgedessen muss der unbewusst und damit planwidrig zu weit geratene Anwendungsbereich des Art. 7 Abs. 3 S. 1 DS-GVO durch eine privatrechtsensible Auslegung – im B2B-Verhältnis zwingend und nach hier vertretener Ansicht auch im B2C-Verhältnis – teleologisch reduziert werden.

Dieser Vorschlag dürfte auf Kritik stoßen. Die Ablehnung einer solchen teleologischen Reduktion von Art. 7 Abs. 3 S. 1 DS-GVO durch den *EDSA* und den *EDSB* dürfte bereits in deren institutionellem Auftrag und dem jeweiligen Selbstverständnis angelegt sein. Deren Skepsis gegenüber jeder Kommerzialisierung von personenbezogenen Daten ist durch die – berechtigten, aber einseitigen – rechtspolitischen Ziele dieser Institutionen motiviert. Interessanter sind deshalb potenzielle Kritikpunkte, die sich aus privatrechtlicher Perspektive ergeben.

Während die Methodik einer teleologische Reduktion von Art. 7 Abs. 3 S. 1 DS-GVO überzeugen dürfte, sofern man mit hier vertretener Ansicht eine

---

C-489/07 = EuZW 2009, 694 (Rn. 26) – *Messner*. *Riesenhuber*, System und Prinzipien des Europäischen Vertragsrechts, 2003, S. 398 ff.; *Stempel*, Treu und Glauben im Unionsprivatrecht, 2016, S. 268 ff., 310 f.; *Metzger*, Extra legem, intra ius. Allgemeine Rechtsgrundsätze im Europäischen Privatrecht, 2009, S. 348 f.; spezifisch zum Grundsatz des Rechtsmissbrauchs: *EuGH*, Urt. v. 12.03.1996, C-441/93 = WM 1996, 1530 (Rn. 69) – *Pafitis*; *EuGH*, Urt. v. 12.05. 1998, C-367/96 = EuZW 1999, 57 (Rn. 20) – *Kefalas*; hierzu: *Schmidt-Kessel*, in: Jud u.a. (Hrsg.), Prinzipien des Privatrechts und Rechtsvereinheitlichung, 2001, S. 61 (79 f.).

[224] *Staudenmayer*, ZEuP 2019, 663 (676).

planwidrig zu weit geratene Vorschrift wieder unionsrechtskonform einfängt, dürfte es aus privatrechtlicher Perspektive irritieren und beunruhigen, dass die hier vorgeschlagene Möglichkeit einer befristeten Disposition über die sog. freie Widerruflichkeit der Einwilligung und die davon unberührt bleibende Möglichkeit zum außerordentlichen Widerruf aus wichtigem Grund auf den ersten Blick ohne eindeutige Verankerung in der DS-GVO auskommen müssen. Daraus folgt intuitiv die Versuchung, stattdessen auf den generalklauselartigen Art. 6 Abs. 1 lit. f DS-GVO, also – so *Benedikt Buchner* und *Philipp Hacker* – auf die jeweiligen Umstände des Einzelfalls zu setzen, oder den Rückzug auf das bekannte Terrain des jeweils nationalen Schuldrechts (Art. 6 Abs. 1 lit. b DS-GVO) anzutreten (*Jan Niklas Bunnenberg*).

Dieser Versuchung sollte die Judikative nach hier vertretener Ansicht jedoch aus mehreren Gründen widerstehen. Weder ist es ausreichend, die Datenverarbeitung als „Fortsetzung der privatautonomen Gestaltung mit anderen Mitteln“[225] ausnahmsweise auf Grundlage einer Interessenabwägung gemäß Art. 6 Abs. 1 lit. f DS-GVO zu ermöglichen, sofern das Datensubjekt die Einwilligung „opportunistisch“ widerruft.[226] Noch kommt eine Datenverarbeitung auf Grundlage von Art. 6 Abs. 1 lit. b DS-GVO immer dann in Betracht, wenn im Rahmen einer Abwägung im Einzelfall das Interesse des Verantwortlichen an einer vertraglichen Bindung gegenüber dem Interesse des Datensubjekts an einem Widerruf der Einwilligung überwiegt.[227]

Beide Lösungsvorschläge scheitern, soweit auch besonders sensible personenbezogene Daten i. S. d. Art. 9 Abs. 1 DS-GVO verarbeitet werden. Zudem verursachen beide Lösungswege ein erhebliches Ausmaß an Rechtsunsicherheit und enorme Transaktionskosten, weil im Ergebnis nationale Gerichte anhand von schwer zu typisierenden Einzelfällen (Art. 6 Abs. 1 lit. f DS-GVO) oder auf Grundlage des jeweiligen nationalen Schuldrechts (Art. 6 Abs. 1 lit. b DS-GVO) – über die Rechtsmäßigkeit ganzer Geschäftsmodelle entscheiden, ohne dass die Verantwortlichen und Datensubjekte die Möglichkeit haben, dieses Geschäftsmodell selbst vertraglich zu stabilisieren. Sowohl der Schutz der Datensubjekte als auch die Gewährleistung eines freien, grenzüberschreitenden Verkehrs personenbezogener Daten im Binnenmarkt hängen davon ab, ob es der (nationalen) Judikative innerhalb eines angemessenen Zeithorizonts gelingt, einheitliche Maßstäbe zu entwickeln. Die erforderliche Transparenz und Vorhersehbarkeit lassen sich mit diesen Vorschlägen jedoch allenfalls sehr langfristig erreichen.

Weil weder Art. 6 Abs. 1 lit. b noch lit. f DS-GVO eine sinnvolle Option bieten,[228] rückt die Einwilligung und infolgedessen insbesondere die Möglichkeit

---

[225] *Hacker*, Datenprivatrecht, 2020, S. 278.

[226] So: *Hacker*, Datenprivatrecht, 2020, S. 211/279.

[227] Mit diesem Vorschlag: *Bunnenberg*, Privates Datenschutzrecht, 2020, S. 265 f.

[228] *De lege ferenda* bestehen weitere Alternativen. So könnte die Öffnungsklausel des Art. 85 Abs. 1 DS-GVO um kommerzielle Verwertungen von personenbezogenen Daten im

zur vorübergehenden Disposition über die freie Widerruflichkeit gemäß Art. 7 Abs. 3 S. 1 DS-GVO ins Zentrum einer nachträglichen Sensibilisierung der DS-GVO für privatrechtliche Beziehungen.[229]

Art. 7 Abs. 3 S. 1 DS-GVO sollte zwingend sein, sofern der Verantwortliche ein marktmächtiges Unternehmen i. S. d. Kartellrechts ist oder sofern die ursprüngliche Einwilligung lediglich die durch Art. 4 Nr. 11 DS-GVO vorgegebenen Mindestanforderungen erfüllt. Somit bleiben einseitig erteilte Einwilligungen, die lediglich einen Einwilligungsempfänger begünstigen und kein Bestandteil eines synallagmatischen Leistungsaustauschs sind, jederzeit und voraussetzungslos widerruflich. Auf diese Weise gewährleisten Art. 4 Nr. 11 und Art. 7 Abs. 3 S. 1 DS-GVO das gemäß Art. 8 Abs. 1 GRCh und Art. 16 AEUV primärrechtlich gebotene Untermaß zum Schutz von Datensubjekten. Spannend bleibt die Frage, ob diese einseitige, schlichte Einwilligung beispielsweise als Rechtsgrundlage für den gemäß Art. 16 ff. DG-VO geregelten sog. Datenaltruismus ausreichend ist, oder ob selbst das Konzept des Datenaltruismus erst dann Interesse findet, wenn durch einen befristeten Ausschluss der Widerruflichkeit der Einwilligung ein Mindestmaß an Planbarkeit für den Datenempfänger sichergestellt ist.

Dies bedeutet jedoch zugleich, dass von Art. 4 Nr. 11 i. V. m. Art. 7 DS-GVO lediglich die unionsgrundrechtlich zu gewährleistenden *Mindestanforderungen* an eine datenschutzrechtliche Einwilligung i. S. d. Art. 8 Abs. 2 S. 1 GRCh festgelegt werden.[230] Dagegen schließt Art. 4 Nr. 11 DS-GVO Einwilligungen nicht aus, die auf der Stufenleiter der Gestattungen[231] über diese einfache, einseitige Einwilligung hinausgehen.

Weil die in Art. 8 Abs. 2 S. 1 GRCh garantierte Möglichkeit zur Einwilligung eine Disposition über den grundrechtlichen Schutz sogar ausdrücklich vorsieht, trägt er gemeinsam mit dem allgemeinen Grundrecht der Vertragsfreiheit (Art. 6

B2B-Verhältnis erweitert werden. Alternativ könnte Art. 9 Abs. 2 DS-GVO dahingehend ergänzt werden, dass eine Verarbeitung von besonders sensiblen personenbezogenen Daten – jedenfalls im B2B-Verhältnis – auch auf Grundlage von Art. 6 Abs. 1 lit. b DS-GVO ermöglicht wird.

[229] Hierzu bereits: *Sattler*, JZ 2017, 1936 (1041 ff.); *ders.*, in: Lohsse/Schulze/Staudenmayer (Hrsg.), Data as Counter-Performance – Contract Law 2.0? 2020, S. 223 (245). Im Ergebnis ebenfalls für die Möglichkeit einer unwiderruflichen Einwilligung für das Schweizerische Recht: *Thouvenin*, SJZ 113/2017, 21 (31: „nahezu unbestreitbar richtiger, ja als ein geradezu zwingender Schritt"); im Anschluss an beide für das Schweizerische Recht: *Schmidt*, Datenschutz als Vermögensrecht, 2020, S. 146 f.; ebenso mit Blick auf die DS-GVO und § 22 KUG: *Götting*, in: Schricker/Loewenheim, Urheberrecht, § 22 KUG, Rn. 40 f.; a. A. *Specht/Bienemann*, K&R 2018, 22 (23).

[230] So soll gemäß ErwG 32 S. 3 DS-GVO beispielsweise dann keine konkludente Einwilligung i. S. d. Art. 4 Nr. 11 DS-GVO vorliegen, wenn das Datensubjekt lediglich schweigt oder sich untätig verhält. Auch das schlichte Weiterklicken bei einem durch die Voreinstellung automatisch aktivierten Einwilligungs-Kästchen ist hiernach ausdrücklich nicht ausreichend.

[231] Hierzu grundlegend: *Ohly*, Volenti non fit iniuria, 2002, S. 147 ff.; sowie oben Kapitel 4 C.II.

Abs. 3 EUV) und der unternehmerischen Freiheit (Art. 16 GRCh) zur Gewährleistung der informationellen Privatautonomie bei. Auch wenn der Zusammenhang zur Vertragsfreiheit vom *EuGH* bislang meist mit Blick Art. 16 GRCh hergestellt wurde[232] und obwohl die GRCh mit Blick auf die allgemeine Handlungsfreiheit eine mangelhafte Kodifikation ist,[233] lässt sich aus Art. 8 Abs. 2 S. 1 GRCh eine Entscheidung zugunsten von privatautonomen Dispositionen[234] und damit auch zugunsten einer befristeten Disposition über die Widerruflichkeit der Einwilligung entnehmen. Der *EuGH* hat im Anschluss an den *EGMR* die Möglichkeit eines Verzichts auf die Rechtschutzgewährleistung gemäß Art. 47 GRCh und auf den Schutz der Verteidigungsrechte gemäß Art. 48 Abs. 2 GRCh anerkannt.[235] Der *EGMR* hat diesen Verzicht auch für den Schutz des Privatlebens bereits angenommen.[236]

Infolgedessen ermöglicht die hier vorgeschlagene Anerkennung einer befristeten Disposition über die freie Widerruflichkeit eine unionsgrundrechtskonforme und privatrechtssensible Auslegung und Anwendung des datenschutzrechtlichen Einwilligungstatbestands.

Maßgeblicher Vorteil dieses Ansatzes ist, dass eine zeitweise teleologische Reduktion von Art. 7 Abs. 3 S. 1 DS-GVO für eine unionweite und unionsautonome Möglichkeit der Flexibilisierung sorgt und dadurch am besten das konfliktträchtige Doppelziel eines einheitlichen Schutzes von personenbezogenen Daten und eines freien Verkehrs personenbezogener Daten im Binnenmarkt verwirklicht. Zudem werden die individuellen Präferenzen der Datensubjekte und Verantwortlichen ernstgenommen, ohne das gemäß Art. 8 Abs. 1 GRCh zu gewährleistende Untermaß zu unterschreiten. Um sicherzustellen, dass ein ausreichender Schutz von personenbezogenen Daten gewährleistet wird, sind vier wesentliche Anforderungen einzuhalten:

Erstens ist auch[237] für die teleologische Reduktion von Art. 7 Abs. 3 S. 1 DS-GVO eine *kartellrechtsakzessorische*, *asymmetrische* Anwendung erforderlich. Im Verhältnis zu marktmächtigen Verantwortlichen ist eine Disposition über die sog. freie Widerruflichkeit ausgeschlossen. Dies gilt unabhängig davon, ob das Datensubjekt ein Unternehmer oder ein Verbraucher ist.

Zweitens ist ein Ausschluss der sog. freien Widerruflichkeit im B2C-Verhältnis zu befristen. Mangels empirischer Grundlagen, erscheint es im Ausgangs-

---

[232] *EuGH*, Urt. v. 22.01.2013, C-283/11 = MMR 2013, 265 (Rn. 42) – *Sky Österreich*; *EuGH*, Urt. v. 18.07.2013, C-426/11 EuZW 2013, 747 (Rn. 32) – *Alemo-Herron*; *EuGH*, Urt. v. 17.10. 2013, C-101/12 = BeckEuRS 2013, 745488 (Rn. 25) – *Herbert Schaible/Land Baden-Württemberg*.

[233] Oben Kapitel 1 B.IV.

[234] So auch: *Jarass*, ZEuP 2017, 310 (329 f.).

[235] Hierzu: *Jarass*, ZEuP 2017, 310 (328 f.).

[236] *EGMR*, Urt. v. 23.09.2010 – Nr. 1620/03, Rn. 71.

[237] Gleiches gilt für die Beurteilung der Freiwilligkeit einer Einwilligung gemäß Art. 7 Abs. 4 DS-GVO: oben C.II.1.

punkt sinnvoll, einen solchen Ausschluss zunächst jedenfalls nicht länger als für die Dauer von sechs Monaten zu ermöglichen (sog. *sunset clause*).

Drittens ist eine stillschweigende Verlängerung dieser Disposition über die sog. freie Widerruflichkeit ausgeschlossen. Es bedarf einer erneuten ausdrücklichen Erklärung des Datensubjekts, um nochmals über Art. 7 Abs. 3 S. 1 DS-GVO – erneut befristet – wirksam zu disponieren.

Viertens bleibt die Möglichkeit zum außerordentlichen Widerruf aus wichtigem Grund von dieser Disposition über die sog. freie Widerruflichkeit unberührt. Der Grund für den außerordentlichen Widerruf kann sowohl aus der Sphäre des Verantwortlichen als auch aus der Sphäre des Datensubjekts stammen. Anders als im B2C-Verhältnis, kommt im B2B-Verhältnis auch die Möglichkeit in Betracht, dass ein unternehmerisch handelndes Datensubjekt die Einwilligung zwar außerordentlich aus Gründen widerruft, die ausschließlich aus seiner Sphäre stammen – vergleichbar dem urheberrechtlichen Rückruf aus gewandelter Überzeugung –, das unternehmerisch handelnde Datensubjekt ist aber im Anschluss regelmäßig zum Ersatz des Vertrauensschadens verpflichtet.

Diese Abstützungen der informationellen Privatautonomie eröffnen einen Rahmen für die Rechtsgestaltung und bieten eine Option für eine Stabilisierung von Rechtsbeziehungen im Privatrechtsverhältnis, die nur in geringem Ausmaß fehleranfällig ist. Auf Grundlage dieser Abstützungen ist es beispielsweise von vergleichsweise geringer Bedeutung, ob eine wirksame befristete Disposition über die sog. freie Widerruflichkeit für drei oder sechs Monate ermöglicht wird. Der außerordentliche Widerruf bleibt davon unberührt und die – im B2C-Verhältnis stets vorzusehende – Befristung begrenzt von vorherein die potenziellen negativen Konsequenzen, die mit einem solchen befristeten Ausschluss der jederzeitigen und grundlosen Widerruflichkeit einhergehen können.

Abgesehen von der Möglichkeit zur teleologischen Reduktion von Art. 7 Abs. 3 S. 1 DS-GVO bietet die DS-GVO auf den ersten Blick wenige Anknüpfungspunkte für den hier unterbreiteten Vorschlag einer Flexibilisierung des Einwilligungstatbestands. Allerdings eröffnet der europäische Gesetzgeber mit den in Art. 5 DS-GVO geregelten Grundsätzen der Datenverarbeitung die Möglichkeit, die DS-GVO im Wege der Auslegung durch Richterrecht zu konkretisieren und zumindest punktuell weiterzuentwickeln. Diese Option ist deshalb von besonderer Bedeutung, weil die mit unbestimmten Rechtsbegriffen und Generalklauseln gespickte DS-GVO ohne eine solche grundsatzgeleitete Fortentwicklung durch den *EuGH* einerseits Gefahr läuft, zu unbestimmt zu sein. Andererseits besteht jedoch ebenfalls die Gefahr, dass die DS-GVO ohne eine unionsgrundrechtskonforme Auslegung unverhältnismäßig in grundrechtlich geschützte Positionen eingreift.

Die in Art. 5 Abs. 1 DS-GVO geregelten Grundsätze der Datenverarbeitung eröffnen der Judikative eine Möglichkeit, beiden Gefahren Rechnung zu tragen. Dabei kommt dem Grundsatz einer Datenverarbeitung nach Treu und Glauben

gemäß Art. 5 Abs. 1 lit. a Var. 2 DS-GVO schon deswegen eine besondere Bedeutung zu, weil er durch Art. 8 Abs. 2 S. 1 GRCh auch primärrechtlich vorgegeben ist.[238]

Somit handelt es sich bei Art. 5 Abs. 1 lit. a Var. 2 DS-GVO um einen Auffangtatbestand,[239] der insbesondere dann unter Abwägung der betroffenen Interessen eine angemessene Lösung ermöglicht, wenn die spezifischen Abwägungsgebote der DS-GVO nicht zur Anwendung kommen.[240] Infolgedessen eignet sich der Grundsatz einer Datenverarbeitung nach Treu und Glauben als „Scharniernorm",[241] die es ermöglicht, solchen Wertungen bei der Auslegung und Anwendung der DS-GVO Rechnung zu tragen, die in den spezifischen Regelungen nur vage oder überhaupt nicht berücksichtigt wurden.

Im B2C-Verhältnis dient der Rückgriff auf Art. 5 Abs. 1 lit. a Var. 2 DS-GVO nach dem hier vertretenen Vorschlag ausschließlich dazu, die Rechtsposition des Datensubjekts abzustützen. Weil eine teleologische Reduktion von Art. 7 Abs. 3 S. 1 DS-GVO unionsgrundrechtlich zwingend ist, ermöglicht es der Grundsatz einer Datenverarbeitung nach Treu und Glauben im Gegenzug, die Disposition über die Widerruflichkeit zu befristen und dem Datensubjekt gemäß Art. 5 Abs. 1 lit. a Var. 2 DS-GVO im Einzelfall ein außerordentliches Widerrufsrecht zu gewähren. Ohne Zweifel bedeutet eine zeitweise Disposition über die Widerruflichkeit eine Modifikation des Datenschutzrechts, die – solange der europäische Gesetzgeber nicht tätig wird – grundsätzlich durch den *EuGH* vorgenommen werden sollte. Hierfür könnten mehrere Anläufe und damit mehrere Vorlageverfahren erforderlich sein.

D. Übersicht zum Stufenmodell

Abschließend lässt sich das zur Gewährleistung einer abgestützten informationellen Privatautonomie vorgeschlagene Stufenmodell der Erlaubnistatbestände graphisch darstellen. Dabei liegt der Schwerpunkt auf den hier erstmals vorgeschlagenen Besonderheiten (grau unterlegt).

---

[238] Deshalb für eine umfassende Bedeutung des Grundsatzes für die Anwendung der DS-GVO: *Clifford/Ausloos*, 37 Yearbook of European Law 2018, 130.

[239] *Kühling/Klar/Sackmann*, Datenschutzrecht, 4. Aufl. 2018, Art. 5, Rn. 145; *Herbst*, in: Kühling/Buchner (Hrsg.), DS-GVO, 3. Aufl. 2020, Art. 5, Rn. 17; *Frenzel*, in: Paal/Pauly, DS-GVO, 2021, Art. 5, Rn. 20; *Roßnagel*, ZD 2018, 339 (340); *Buchner*, in: Tinnefeld u. a. (Hrsg.), Einführung in das Datenschutzrecht, 7. Aufl. 2020, S. 220 (243).

[240] Für das Privatrechtsverhältnis insbesondere von Relevanz: Art. 6 Abs. 1 lit. f, Art. 7 Abs. 4 und Art. 22 Abs. 3 DS-GVO.

[241] So *Hacker*, Datenprivatrecht, 2020, S. 153 („Scharniernorm"), der sich aber andererseits im Kontext der Einwilligung für einen Vorrang des allgemeinen unionsrechtlichen Rechtsmissbrauchs ausspricht (S. 498), obwohl Art. 5 Abs. 1 lit. a Var. 2 DS-GVO im Kontext einer Datenverarbeitung als *lex specialis* Vorrang einzuräumen ist.

	Bezeichnung	**Funktion**	**Norm**	**B2C**	**B2B**
1. Stufe	Einwilligung	Verwirklichung von informationeller Privatautonomie	Art. 7 III 1	Frei widerrufliche Einwilligung	
			Ausnahme Kartellrechtsakzessorische Anwendung		
				Ist der Verantwortliche marktmächtig?	
			Teleolog. Reduktion Art. 7 III 1	falls (-) Befristete Disposition über die freie Widerruflichkeit (+)	falls (-) Befristete oder dauerhafte Disposition über die freie Widerruflichkeit (+)
				Abstützungen • Befristung • Ausschluss einer stillschweigenden Verlängerung der Disposition • Außerordentlicher Widerruf bleibt unberührt	
			Art. 7 IV	Freiwilligkeit als Berücksichtigungsgebot	
				Ist der Verantwortliche marktmächtig?	
			Art. 7 IV	falls (+) Strenge kartellrechtsakzessorische Anwendung	falls (+) Strenge kartellrechtsakzessorische Anwendung
				Sofern keine Substitute gegen monetäres Entgelt am Markt verfügbar sind: Pflicht des marktmächtigen Verantwortlichen zum Angebot einer alternativen Kontrahierung gegen monetäres Entgelt	

	Bezeichnung	Funktion	Norm	B2C	B2B
2. Stufe	Vertragsakzessorietät	Restriktive Auslegung: Entlastung der Einwilligung	Art. 6 I lit. b	Vermutung eines eigenständigen kommerziellen Zwecks der DV, so dass insoweit eine Einwilligung erforderlich wird.	
3. Stufe	Interessenabwägung	Auffangtatbestand Soweit die Einholung einer Einwilligung unerreichbar oder der damit verbundene Aufwand unter Berücksichtigung der Verarbeitungszwecke unverhältnismäßig ist. Dies gilt insbesondere bei Multi-Relationalität der Personenbezüge, aber lediglich geringen individuellen Risiken für die Datensubjekte.	Art. 6 I lit. f	Restriktive Auslegung von „Direktwerbung“ (Relativität der Schuldverhältnisse) Erweiterungen (*de lege ferenda*) für besonders sensible personenbezogene Daten • Kurzzeitige DV im Kontext des IoT (Steuerung über Gestik/Mimik/Sprache) • Training von ML-Systemen	

Tabelle 1: Stufenmodell der Erlaubnistatbestände

6. Kapitel

Erforderliche Abstützungen der informationellen Privatautonomie

Die Diskussion über notwendige Reformen und Anpassungen der DS-GVO ist so alt wie die DS-GVO selbst. Aus privatrechtlicher Perspektive hat insbesondere *Philipp Hacker* zuletzt den Stand der Diskussion über technische[1] und rechtliche Instrumente[2] zur Unterstützung einer Durchsetzung der individuellen datenschutzrechtlichen Präferenzen zusammengefasst und hierauf aufbauend um eigene Vorschläge ergänzt. Dies ermöglicht es, an dieser Stelle auf diese umfassende Darstellung der Diskussion beiderseits des Atlantiks hinzuweisen, an diese anzuknüpfen und nachfolgend auf dieser Grundlage zwei Vorschläge zu unterbreiten, wie die informationelle Privatautonomie und der hier vertretene Vorrang der Einwilligung im Privatrechtsverhältnis künftig zusätzlich abgestützt werden können.

Diese Maßnahmen sind keine notwendige Voraussetzung, um das hier vorgeschlagene Stufenmodell der Erlaubnistatbestände und insbesondere den Vorrang der Einwilligung zu begründen. Dennoch dienen diese Vorschläge dazu, Datensubjekte besser zu befähigen, ihre informationelle Privatautonomie faktisch wahrzunehmen, ohne sie zu dem zeitintensiven – und wenig attraktiven – „Hobby Datenschutz" zu zwingen und ohne sie durch eine Informationsflut zu überfordern.

Die nachfolgend erwogenen Abstützungen wurden teilweise bereits im vorgeschlagenen Stufenmodell der Erlaubnistatbestände erwähnt. Sie sollen abschließend einen privatrechtlich geprägten Ausblick auf wesentliche Bestandteile einer künftigen Reform bieten. Weil alle Vorschläge bereits im geltenden Datenschutzrecht (DS-GVO, BDSG) – jedoch jeweils nur unvollkommen und mittelbar – angelegt sind, bieten sie eine Möglichkeit zur evolutiven Anpassung des europäischen Datenschutzrechts.

---

[1] Zu sog. Privacy-Enhancing-Technologies und einer Rechtmäßigkeitskontrolle unter Einsatz von Techniken des maschinellen Lernens: *Hacker*, Datenprivatrecht, 2020, S. 553 ff. bzw. S. 566 ff.

[2] Zum Vorschlag eines „Rechts auf datenerhebungsfreie Produkte" als individuelle Exit-Option: *Becker*, JZ 2017, 171 (175 ff.); *ders.*, ZGE 2017, 371 ff.; *Hacker*, Datenprivatrecht, 2020, S. 578 ff./620 ff./642 f. Mit dem Vorschlag eines Rechts auf „datenerhebungsfreie Räumlichkeiten": *Raue*, NJW 2019, 2425 (2426 f.).

Zentraler Begriff der DS-GVO ist das personenbezogene Datum als Information, die sich auf eine identifizierte oder identifizierbare natürliche Person bezieht. Aufgrund dieses Regelungsobjekts ist die DS-GVO konzeptionell kein originärer Bestandteil des europäischen Verbraucher(schutz)rechts. Dennoch setzt der europäische Gesetzgeber mit der DS-GVO eindeutig auf das im Verbraucherrecht dominante sog. Informationsmodell.[3] Die in der DS-GVO etablierten Pflichten der Verantwortlichen und Auftragsverarbeiter sollen die Datensubjekte zu informierten Entscheidungen befähigen.

Unabhängig von der grundlegenden Kritik am Informationsmodell, die sich insbesondere auf verhaltensökonomische Experimente und Studien berufen kann, hat es der europäische Gesetzgeber bislang jedenfalls versäumt, die notwendigen Voraussetzungen dafür zu schaffen, dass die Datensubjekte ihre informationelle Privatautonomie auf Grundlage von Information effektiv wahrnehmen können.[4] Soll das Informationsmodell eine positive Wirkung entfalten, so muss diejenige Information, die zur Ausübung informationeller Privatautonomie benötigt wird, durch unionsweit einheitliche Standards der Informationsaufbereitung und -vermittlung ergänzt werden.

Obwohl die Entwicklung solcher Standards keine originär rechtwissenschaftliche Aufgabe ist, liegt die Einführung einer unionsweit standardisierten Kombination aus einer farblich abgestuften Kennzeichnung einschließlich *Privacy Score* auf der Hand (A).

Darüber hinaus ist die Verwirklichung informationeller Privatautonomie darauf angewiesen, dass Datensubjekte ihre Entscheidungen einfach und effektiv umsetzen können. Dies gilt vorrangig für die Erteilung und den Widerruf der Einwilligung, so dass letztere materiell „ertüchtigt" wird.[5] Dies gilt aber ebenfalls für den Widerspruch gegen eine Datenverarbeitung auf Grundlage einer Interessenabwägung und für die Ansprüche auf Berichtigung, Löschung und Portabilität.

---

[3] Hierzu grundlegend: *Dauner-Lieb*, Verbraucherschutz durch Ausbildung eines Sonderprivatrechts für Verbraucher, 1983, S. 62 ff.; *Drexl*, Die wirtschaftliche Selbstbestimmung des Verbrauchers, 1998, S. 26 ff.; *Fleischer*, ZEuP 2000, 772 (781 ff.); sowie *Ackermann*, ZEuP 2009, 230 (245 ff.).

[4] Mit Blick auf die in Österreich derzeit verwendeten AGB von *Facebook* a. A. und somit von einer ausreichenden Befähigung der Datensubjekte und Verbraucher ausgehend: *OLG Wien*, Urt. v. 07.12.2020 (nicht rechtskräftig), GZ 11 R 153/20f, 11 R 154/20b-99 S. 27: „Das Wesen dieses Facebook-Geschäftsmodells und die damit verknüpften Vertragszwecke […] [(] aus Sicht der Beklagten insbesondere: Erzielung von Einnahmen durch personalisierte Werbung, ermöglicht durch die personenbezogenen Daten der Facebook-Nutzer) wird in den Bedingungen in einer Weise erläutert, die *für jeden auch nur durchschnittlich aufmerksamen Leser leicht verständlich* ist." [Hervorhebung durch den Verfasser]; deutlich skeptischer gegenüber den (zuvor) in Deutschland von *Facebook* verwendeten AGB: *v. Westphalen*, VuR 2017, 323 (328 ff.).

[5] Mit dieser Forderung: *Leistner/Antoine/Sagstetter*, Big Data, 2021, S. 403.

Die praktische Umsetzung dieser Anforderung sollte erleichtert werden, indem die Abgabe datenschutzrechtlicher Erklärungen zentralisiert wird. Hierfür kommen sog. *Kontroll-Cockpits* in Betracht, die als Beispiele für sog. Personal Information Management Systems (PIMS) diskutiert werden. Sie sind ein erster Schritt zur effektiveren Kontrolle und Durchsetzung von Datenschutzpräferenzen (B).

A. Standardisierte Kennzeichnung und Privacy Score

Mit der informierten Einwilligung (Art. 4 Nr. 11 DS-GVO), den umfangreichen Informationspflichten in Art. 7 Abs. 3 S. 3, Art. 21 Abs. 4, Art. 12 ff. DS-GVO und dem allgemeinen Grundsatz der Transparenz gemäß Art. 5 Abs. 1 lit. a Var. 3 DS-GVO setzt der europäische Gesetzgeber auch im Datenschutzrecht weiterhin vorrangig auf das sog. Informationsmodell. Dies ist unionsgrundrechtlich geboten, sofern transparenzfördernde Information geeignet ist, als Wahlhilfe für selbstbestimmte Entscheidungen zu fungieren und deshalb im Vergleich zu Wahlbeschränkungen[6] ein milderes und damit gemäß Art. 52 Abs. 1 S. 2 GRCh vorrangig gebotenes Mittel ist.[7]

Das Informationsmodell als Grundlage für die Verwirklichung von informationeller Privatautonomie ist jedoch von Voraussetzungen abhängig, welche die DS-GVO bislang nicht ausreichend gewährleistet (I). Infolgedessen ist es erforderlich, unionweit einheitliche Standards für die Kennzeichnung von Datenverarbeitungen zu etablieren (II). Zudem bietet diese standardisierte Kennzeichnung künftig einen vergleichsweise aussichtsreichen Anwendungsfall für maschinelles Lernen (III).

I. Fehlende Voraussetzungen für das Informationsmodell

Indem der europäische Gesetzgeber mit der DS-GVO weitgehend auf Wahlhilfen (Informiertheit, Widerruf, Widerspruch) setzt, endet seine Verantwortung nicht mit der *rechtlichen* Konstitution von Informationspflichten, welche die Ausübung dieser Wahlhilfen ermöglichen sollen, sondern er trägt eine Folgenverantwortung dafür, dass mittels dieser Informationspflichten die *tatsächliche* Ausübung dieser Wahlhilfen erleichtert wird.

Weil der europäische Gesetzgeber sich bislang mit der Konstitution von Informationspflichten begnügte, hat er lediglich die erste Hälfte derjenigen Basis

[6] Hierzu: *Schmolke*, Grenzen der Selbstbindung im Privatrecht, 2014, S. 258 ff.

[7] Insbesondere über den allgemeinen Grundsatz der Datenverarbeitung nach Treu und Glauben (Art. 5 Abs. 1 lit. a Var. 2 DS-GVO) hat der Gesetzgeber jedoch Möglichkeiten vorgesehenen, diese Wahlhilfen durch Wahlbeschränkungen zu ergänzen.

geschaffen, die für funktionierende Wahlhilfen erforderlich ist. Ohne Bemühungen um die effektive Vermittlung der Information, können die Informationspflichten ihre Funktion nicht entfalten.[8]

Trotz einer insoweit grundsätzlich bestehenden Einschätzungsprärogative des Gesetzgebers kann er die Augen nicht vor den durch empirische Studien aufgezeigten inhärenten Grenzen des Informationsmodells verschließen. Die Gewährleistungspflicht aus Art. 8 Abs. 1 GRCh und Art. 16 Abs. 1 AEUV ist deshalb erst erfüllt, wenn auch die *Informationsdarstellung* in einer Weise sichergestellt ist, welche die Annahme erlaubt, dass das mit der Informationspflicht verbundene Ziel der Wahlhilfe auch erreicht werden kann. Deshalb ist eine Verpflichtung sinnvoll, wonach komplexe Einwilligungserklärungen und Datenschutzerklärungen mehrstufig aufgebaut sein müssen[9] und ihnen ab einer bestimmten Länge eine Zusammenfassung der wesentlichen Punkte vorangestellt werden muss (sog. *one-pager*).[10]

Allerdings ließ sich in einer ersten Studie auch empirisch nachweisen, dass die Informiertheit der Einwilligung von Datensubjekten nur marginal dadurch gesteigert werden kann, dass die anzugebende Information nicht in langen und unübersichtlichen Einwilligungserklärungen, sondern mehrstufig aufgebaut und zusätzlich konzentriert und übersichtlich auf einer Seite zusammengefasst wird.[11] Das grundlegende Spannungsverhältnis zwischen Vollständigkeit und Verständlichkeit[12] lässt sich allein durch eine Verdichtung der textlichen Darstellung nicht auflösen. Es ist eine mehrstufige Herangehensweise[13] erforderlich, um die Informationsdarstellung und -vermittlung zu verbessern.

Hieraus folgt, dass es nicht genügt, Informationspflichten zu konstituieren und deren textliche Darstellung zu verbessern. Vielmehr ist es zwingend erforderlich, die Information *auch* visuell aufzubereiten und damit leichter zugäng-

---

[8] Mit grundlegenden Zweifeln am Informationsmodell: *Ben-Shahar/Chilton*, 45 Journal of Legal Studies 2016, 41(64 f.); *Hermstrüwer*, 8 JIPITEC 2017, 9 (Rn. 35 f.); *Hacker*, Datenprivatrecht, 2020, S. 588 ff.

[9] Gemäß Art. 22 des Vorschlags für DGA soll ein Datenaltruismus durch Bereitstellung eines modular aufgebauten Einwilligungsformulars gefördert werden.

[10] Für die zusammenfassende Darstellung von AGB und Datenschutzvorgaben auf einer Seite (One Pager): Sachverständigenrat für Verbraucherfragen, Verbraucherrecht 2.0, 2016, 46 f.; *Micklitz*, VuR 2017, 43 (44).

[11] *Conpolicy*, Wege zur besseren Informiertheit – Verhaltenswissenschaftliche Ergebnisse zur Wirksamkeit des One-Pager-Ansatzes und weiterer Lösungsansätze im Datenschutz, v. 28.02.2018, S. 57 f. (https://www.conpolicy.de/data/user_upload/Studien/Bericht_ConPolicy_2018_02_Wege_zur_besseren_Informiertheit.pdf, zuletzt abgerufen am 19.05.2022).

[12] *Bäcker*, in: Kühling/Buchner (Hrsg.), DS-GVO, 3. Aufl. 2020, Art. 12, Rn. 12; *Franck*, in: Gola (Hrsg.), DS-GVO, 2. Aufl. 2018, Art. 12, Rn. 23.

[13] *Article 29 Data Protection Working Group*, Opinion 10/2004 on More Harmonised Information Provisions, WP 100, 2004, S. 8 f.; *Menzel*, DuD 2008, 400 (408); *Kampert*, Datenschutz in sozialen Online-Netzwerken de lege lata und de lege ferenda, 2016, S. 191 f.; m. w. N. *Hacker*, Datenprivatrecht, 2020, S. 580 f.

lich zu machen.[14] Erst infolgedessen kann das Informationsmodell seine Vorteile als milderes Mittel gegenüber Wahlbeschränkungen verwirklichen. Dass es hierbei stets zu Vereinfachungen und Verkürzungen kommt und jede Form einer Klassifizierung zu Abgrenzungsschwierigkeiten und zu Unschärfe führt, spricht nicht gegen eine solche Visualisierung, sondern lediglich dafür, dass diese Instrumente immer wieder evaluiert werden müssen und anschließend gegebenenfalls anzupassen sind.

II. Unionweit einheitliche Kennzeichnung

Mit Blick auf das Doppelziel der DS-GVO, also den Schutz von Datensubjekten vor einer Verarbeitung personenbezogener Daten und die Gewährleistung eines freien Verkehrs von personenbezogenen Daten im Binnenmarkt, ist offensichtlich, dass eine unionweit einheitliche, standardisierte Vorgehensweise nicht nur sinnvoll, sondern notwendig ist.[15] Die Reichweite der in der DS-GVO enthaltenen ersten Ansätze für eine einheitliche Kennzeichnung (1) sind umstritten und nicht ausreichend (2). Sie befähigen Datensubjekte nicht dazu, sich zunächst auf wesentliche und leicht zu verarbeitende Information konzentrieren können.

Obwohl die Entwicklung eines Kennzeichnungssystems anhand umfassender empirischer Tests erfolgen muss und diese Aufgabe damit kein originäres Forschungsgebiet der Rechtswissenschaften ist, legen die Anforderungen der DS-GVO an die Rechtsmäßigkeit einer Datenverarbeitung eine mehrstufige Darstellung der Information nahe, die auf der ersten Informationsstufe eine farbliche Unterscheidung mit einer numerischen Klassifizierung in Form eines sog. *Privacy Score* kombiniert (3) und die Erlaubnistatbestände ins Zentrum dieser Kennzeichnung rückt (4).

1. Rechtsgrundlage für eine unionsweite Standardisierung

Der europäische Gesetzgeber war sich bei Verabschiedung der DS-GVO der mit dem Informationsmodell verbundenen Schwierigkeiten zumindest im Ansatz bewusst. Deshalb hat er in Art. 12 Abs. 7 S. 1 DS-GVO immerhin die Möglichkeit vorgesehen, dass diejenige Information über die Datenverarbeitung, die den Datensubjekten bereitzustellen ist, mit standardisierten Bildsymbolen kombiniert werden *kann*, um die Wahrnehmbarkeit und Verständlichkeit der Information zu verbessern. Sofern die Bildsymbole in elektronischer Form dargestellt werden, müssen sie zudem maschinenlesbar sein, Art. 12 Abs. 7 S. 2 DS-GVO.

---

[14] Für ein sog. privacy nutrition label: *Cranor*, 10 Journal on Telecommunications & High Technology Law 2012, 273.

[15] Zum Fehlen einer einheitlichen Standardisierung und deren Folgen: *Reidenberg* u. a., 96 Washington University Law Review 2019, 1409 (1428 ff.).

Mit dieser Regelung hat der europäische Gesetzgeber zunächst lediglich die Möglichkeit geschaffen, dass die Verantwortlichen ihren Informationspflichten gemäß Art. 12 Abs. 1 S. 1 DS-GVO in präziser, transparenter, verständlicher und leicht zugänglicher Form nachkommen können. Zugleich schien der europäische Gesetzgeber allerdings selbst davon auszugehen, dass die Verantwortlichen von dieser Möglichkeit zu wenig oder falschen Gebrauch machen würden. Dies würde erklären, warum der *EU-Kommission* die Befugnis übertragen wurde, delegierte Rechtsakte zu erlassen und hierdurch selbst aktiv zu werden. Gemäß Art. 12 Abs. 8 DS-GVO i. V. m. Art. 92 DS-GVO kann die *EU-Kommission* in delegierten Rechtsakten (Art. 290 AEUV) diejenige Information bestimmen, die durch solche Bildsymbole dargestellt werden muss und das Verfahren für die Bereitstellung solcher standardisierten Bildsymbole festlegen.

Bislang hat die *EU-Kommission* von dieser seit Mitte 2016 bestehenden Befugnis[16] keinen Gebrauch gemacht. Dadurch gefährdet sie nicht nur die beiden Zielvorgaben aus Art. 1 DS-GVO. Vielmehr wird sie der Aufgabe nicht gerecht, die ihr der europäische Gesetzgeber zugedacht hat. Gemäß ErwG 166 S. 1 DS-GVO soll die Kompetenz zum Erlass delegierter Rechtsakte ausdrücklich genutzt werden, um das Doppelziel aus Art. 1 DS-GVO zu erreichen. Erheblicher als die Vernachlässigung der ihr zugedachten Aufgabe ist jedoch, dass die *EU-Kommission* zunehmend Gefahr läuft, ihre eigenen Gewährleistungspflichten aus Art. 8 Abs. 1 GRCh und Art. 16 Abs. 1 AEUV zu verletzen.

Leider ist nicht nur die *EU-Kommission* untätig geblieben. Weder das *EU-Parlament* noch der *Rat* sind bislang ihrer jeweils eigenen (Reserve-) Gewährleistungspflicht nachgekommen. Gemäß Art. 92 Abs. 3 S. 1 DS-GVO kann sowohl das *EU-Parlament* als auch der *Rat* die Übertragung der Befugnis an die *EU-Kommission* widerrufen und dadurch das Verfahren zur Bereitstellung von standardisierten Bildsymbolen wieder an sich ziehen. Das bisherige Fehlen solcher Bildsymbole legt nahe, dass die europäischen Institutionen mit der DS-GVO zwar stark auf das Informationsmodell setzen (Art. 12 ff. DS-GVO) und sich der immanenten Beschränkungen des Informationsmodells aufgrund der beschränkten Kapazitäten textlicher Informationsverarbeitung von Menschen bewusst sind (Art. 12 Abs. 7 DS-GVO). Allerdings vernachlässigen sie ihre jeweilige Folgenverantwortung, die mit dem Informationsmodell einhergeht und die in ErwG 166 S. 1 und Art. 92 Abs. 2 und Abs. 3 DS-GVO ihren Ausdruck gefunden hat. Die europäischen Institutionen handeln oder genauer: unterlassen es, die Informationsdarstellung und Informationsvermittlung zugunsten von Datensubjekten zu verbessern.

Auch der *EDSA* hat bislang keine Stellungnahme zu möglichen Bildsymbolen i. S. d. Art. 12 Abs. 7 DS-GVO abgegeben. Diese Stellungnahme soll zwar gemäß Art. 70 Abs. 1 lit. r DS-GVO „für die Kommission" erfolgen. Dennoch

[16] Art. 92 Abs. 2 DS-GVO.

setzt eine solche Stellungnahme nicht voraus, dass die *EU-Kommission* bereits einen Vorschlag für einen delegierten Rechtsakt i. S. d. Art. 12 Abs. 8 DS-GVO unterbreitet hat. Der *EDSA* könnte also auch selbst die Initiative ergreifen und eine Stellungnahme nutzen, um eigene, unverbindliche Vorschläge zu formulieren und damit die Bitte an die *EU-Kommission* zu verbinden, endlich Vorschläge auszuarbeiten.

2. Reichweite der Rechtsgrundlage für eine Standardisierung

Derzeit ist umstritten, ob die in Art. 12 Abs. 8 i. V. m. Art. 92 Abs. 2 DS-GVO enthaltende Befugnis der *EU-Kommission* sich in der Bestimmung der mittels Bildsymbolen darzustellenden Information und der Etablierung eines Verfahrens erschöpft[17] oder ob die *EU-Kommission* selbst konkrete Bildsymbole ausgestalten und festlegen kann. Der Wortlaut von Art. 12 Abs. 7 und Abs. 8 DS-GVO, der bereits *standardisierte* Bildsymbole voraussetzt und ErwG 166 DS-GVO, welcher der *EU-Kommission* ausdrücklich die Verantwortung dafür zuweist, die Ziele der DS-GVO und die Unionsgrundrechte mit Hilfe der Befugnis zum Erlass delegierter Rechtsakte zu wahren, sprechen beide dafür, dass sich aus Art. 12 Abs. 8 DS-GVO zumindest eine Annexkompetenz der *EU-Kommission* dafür ableiten lässt, solche Bildsymbole auch selbst zu entwickeln und festzulegen.[18]

Unabhängig von der bisherigen Untätigkeit der europäischen Institutionen, bestehen jedoch auch Zweifel, ob solche Bildsymbole i. S. d. Art. 12 Abs. 7 DS-GVO ausreichen. Selbst wenn die *EU-Kommission* von ihrer Kompetenz Gebrauch machen würde, wäre dadurch nicht sichergestellt, dass im Ergebnis auch sinnvolle, leicht verständlich und dennoch sachlich zutreffende Bildsymbole entstehen,[19] die eine effektive Wahlhilfe für Datensubjekte sind. Dies liegt einerseits an der grundsätzlichen Schwierigkeit, die mit der Ausgestaltung und Festlegung von solchen Bildsymbolen verbunden ist und andererseits daran,

---

[17] So: *Dix*, in: Simitis/Hornung/Spiecker gen. Döhmann (Hrsg.), Datenschutzrecht, 2019, Art. 12, Rn. 41; *Pohle/Spittka*, in: Taeger/Gabel (Hrsg.), DS-GVO/BDSG, 3. Aufl. 2019, Art. 12, Rn. 29; *Bäcker*, in: Kühling/Buchner (Hrsg.), DS-GVO, 2020, Art. 12, Rn. 24.

[18] Ebenso: *Artikel-29-Datenschutzgruppe*, Leitlinien für Transparenz gemäß der Verordnung 2016/679, WP 260 rev.01, 2018, S. 30; *Heckmann/Paschke*, in: Ehmann/Selmayr (Hrsg.), DS-GVO, 2. Aufl. 2018, Art. 12, Rn. 57; *Efroni u. a.*, 5 European Data Protection Law Review 2019, 352 (360); *Hacker*, Datenprivatrecht, 2020, S. 587.

[19] Zur Gestaltung von Bildsymbolen: *Cranor*, 10 Journal on Telecommunications & High Technology Law 2012, 273 (293 ff.); *Conpolicy*, Wege zur besseren Informiertheit – Verhaltenswissenschaftliche Ergebnisse zur Wirksamkeit des One-Pager-Ansatzes und weiterer Lösungsansätze im Datenschutz, v. 28.02.2018, S. 63 ff. (https://www.conpolicy.de/data/user_upload/Studien/Bericht_ConPolicy_2018_02_Wege_zur_besseren_Informiertheit.pdf, zuletzt abgerufen am 19.05.2022); *Efroni u. a.,* 5 European Data Protection Law Review 2019, 352; *Specht-Riemenschneider/Bienemann*, in: Specht-Riemenschneider/Werry/Werry (Hrsg.), Datenrecht in der Digitalisierung, 2019, 324 ff.

dass mit steigender Anzahl der Bildsymbole schnell die bezweckte Übersichtlichkeit und damit die Funktion als effektive Wahlhilfe eingebüßt wird. Es ist offensichtlich, dass bessere Wege der Informationsdarstellung existieren als die Entwicklung eines Kaleidoskops aus Bildsymbolen.

3. Notwendigkeit einer mehrstufigen Darstellung von Information

Seit Jahren ist weitgehend unbestritten, dass Bildsymbole (Icons), Farben oder Punktesysteme gegenüber langen Textpassagen Vorteile für die Informationswahrnehmung und -verarbeitung haben.[20] Die Schwierigkeiten bestehen jedoch darin, die richtige Anzahl und eine sinnvolle Abstufung solcher Kommunikationsmittel festzulegen. Um zu verhindern, dass Datensubjekten durch vielfältige Bildsymbole unterschiedlicher Verantwortlicher die Orientierung erschwert wird oder sie sogar in die Irre geführt werden, ist eine europaweite Standardisierung nicht nur wünschenswert, sondern notwendig.[21]

Obwohl es bereits eine Herausforderung wäre, für jede explizite Informationspflicht in der DS-GVO ein eigenständiges passendes Bildsymbol zu entwickeln, bleibt anschließend zunächst weitgehend offen, ob Datensubjekte diese Bildsymbole bewusst wahrnehmen, diese richtig einordnen und sich bei einer Entscheidung daran orientieren. Dies macht eine Auswahl auf Grundlage empirischer Studien und Tests erforderlich.[22] Zudem muss – ebenfalls auf empirischer Basis – entschieden werden, zu welchem Zeitpunkt diese Bildsymbole angezeigt werden sollen, um ihre Informationsfunktion effektiv zu erfüllen. Zugleich muss eine zu häufige Anzeige verhindert werden, weil die Bildsymbole sonst kognitiv abnutzen.[23]

---

[20] Zu „privacy nutrition labels" bereits: *Ciocchetti*, John Marshall Journal of Computer and Information Law, 2008, No. 1, 1 ff.; *Le Métayer*, in: Wright/De Hert (Hrsg.), Enforcing Privacy, 2016, 395 (415); *Efroni u. a.,* 5 European Data Protection Law Review 2019, 352 (358 ff.); *Reidenberg* u. a., 96 Washington University Law Review 2019, 1409 (1422 ff.); *Metzger*, in: Lohsse/Schulze/Staudenmayer (Hrsg.), Data as Counter-Performance: Contract Law 2.0?, 2020, S. 25 (36); mit Beispielen: *Specht-Riemenschneider/Bienemann,* in: Specht-Riemenschneider/Werry/Werry (Hrsg.), Datenrecht in der Digitalisierung, 2019, 324 ff.; sowie aus kommunikationswissenschaftlicher Perspektive: *Schröder,* in: Specht-Riemenschneider/Werry/Werry (Hrsg.), Datenrecht in der Digitalisierung, 2019, S. 345 ff.

[21] Privatrechtlich organisierte Bildsymbole dürften sich als zu vielseitig und unbestimmt erweisen. Es besteht die Gefahr eines Flickenteppich an Bildsymbolen, die deren Einordnung erschwert: Zur Einführung solcher Bildsymbole: *Chen*, What We Learned From Apple's New Privacy Labels, New York Times, 27.01.2021 (https://www.nytimes.com/2021/01/27/technology/personaltech/apple-privacy-labels.html, zuletzt abgerufen am 19.05.2022); sowie als banales Beispiel: PrivacyIcons, Mozilla Wiki, https://wiki.mozilla.org/Privacy_Icons, zuletzt abgerufen am 19.05.2022.

[22] *Artikel-29-Datenschutzgruppe*, Leitlinien für Transparenz gemäß der Verordnung 2016/679, WP 260 rev.01, 2018, S. 30; *Efroni u. a.*, 5 European Data Protection Law Review 2019, 352 (359 f.); *Hacker*, Datenprivatrecht, 2020, S. 586.

[23] *Calo*, 87 Notre Dame Law Review 2012, 1027 (1030 f.); *Efroni* u. a., 5 European Data

Sofern für alle in Art. 12–14 DS-GVO enthaltenen Informationspflichten ein eigenes Bildsymbol entwickelt werden soll, dürfte dieser Ansatz in eine komplexe datenschutzrechtliche Bildersprache münden. Obwohl jedes Bildsymbol – jedenfalls im digitalen Kontext – über ein *mouse-over* wiederum mit einer kurzen Erklärung versehen werden kann und sollte, legen Erfahrungen aus empirischen Studien nahe,[24] dass die Effektivität der Informationsvermittlung auf Grundlage von Bildsymbolen ihrerseits mit einer steigenden Anzahl von Bildsymbolen sinkt. Nur wenige Datensubjekte betreiben das „Hobby Datenschutz" und sind womöglich dazu bereit, zusätzlich die (Fremd-)Sprache der „Datenschutz-Bildsymbole" zu erlernen.

Im Ergebnis lautet die Gretchenfrage: Wie stark darf die erste Informationsstufe zugunsten der Verständlichkeit von Information reduziert werden, selbst wenn mutmaßlich 95 % der Datensubjekte ihre Informationssuche niemals über diese erste Stufe ausweiten?

Nochmals zugespitzt: Darf von einer informierten Entscheidung der Datensubjekte ausgegangen werden, obwohl diese sich regelmäßig ausschließlich an einer Kennzeichnung durch wenige Farben orientieren und die Vollständigkeit der Information allenfalls durch die Lektüre komplexer mehrstufiger Rechtstexte – und damit regelmäßig nur potentiell – erreicht werden könnte?

a) Tatsächliche Verständlichkeit und verfügbare Vollständigkeit

Nach hier vertretener Ansicht ist es sinnvoll und erforderlich, die Verständlichkeit der Information zu steigern, die Verantwortliche den Datensubjekten gemäß Art. 7 Abs. 3 S. 3, Art. 21 Abs. 4 und Art. 12 ff. DS-GVO zur Verfügung stellen müssen. Diese Entscheidung zugunsten der Verständlichkeit lässt sich mit den Studien zur Informationsverarbeitung durch Menschen begründen und geht davon aus, dass die Vollständigkeit der Information für das Datensubjekt im Einzelfall faktisch irrelevant ist. Datensubjekte können diese vollständige Information nicht unter vertretbaren Opportunitätskosten verarbeiten und wollen dies vernünftigerweise auch nicht (rationale Apathie).

Diese Erkenntnis hat zur Konsequenz, dass die *Vollständigkeit* der Information gerade nicht der individuellen Entscheidung der Datensubjekte dient, sondern die Grundlage für die *ex post*-Kontrolle durch Gerichte ist und dadurch lediglich die allgemeine Markttransparenz fördert. Zudem eröffnet die Forderung nach einer möglichst vollständigen Information Mitbewerbern, Verbrau-

---

Protection Law Review 2019, 352 (359); *Franck*, in: Gola (Hrsg.), DS-GVO, 2. Aufl. 2018, Art. 12, Rn. 46.

[24] *Conpolicy*, Wege zur besseren Informiertheit – Verhaltenswissenschaftliche Ergebnisse zur Wirksamkeit des One-Pager-Ansatzes und weiterer Lösungsansätze im Datenschutz, v. 28.02.2018, S. 57 f. (https://www.conpolicy.de/data/user_upload/Studien/Bericht_ConPolicy_2018_02_Wege_zur_besseren_Informiertheit.pdf, zuletzt abgerufen am 19.05.2022).

cherschutzverbänden und Datenschutzbehörden die Möglichkeit zur Marktbeobachtung bzw. erleichtert ihnen die Aufsicht und Kontrolle. Infolgedessen dienen die Informationspflichten tatsächlich noch nicht einmal dazu, eine kleine Gruppe von Datensubjekten als sog. informierte Minderheit hervorzubringen,[25] damit diese – stellvertretend für alle Datensubjekte – durch ihre Entscheidungen die Markttransparenz und den Wettbewerb zwischen den Anbietern fördert.[26] Vielmehr ist die Vollständigkeit der Information für die gerichtliche und behördliche Kontrolle wesentlich, nicht jedoch für das einzelne Datensubjekt. Deshalb kann die Möglichkeit zur vollständigen Erfassung und Verarbeitung der Information durch diese professionellen Leser auf die hinteren und in Textform bereitgestellten Stufen der Informationsdarstellung verlagert werden.

Aus Sicht der Datensubjekte stehen die Verständlichkeit und insbesondere die Möglichkeit zur schnellen Verarbeitung der Information ganz im Vordergrund. Es müssen Wege der *Informationsreduktion* gefunden werden, die gerade noch ausreichen, um zwei wesentliche Bedingungen zu erfüllen.

Erstens muss der jeweilige Umfang der Datenverarbeitung als potenziell relevantes Auswahlkriterium sichtbar(er) werden. *Zweitens* muss die Information genügen, um eine individuelle, den eigenen Präferenzen des Datensubjekts im Grundsatz entsprechende Entscheidung zu ermöglichen.

Sind diese beiden Bedingungen erfüllt, so kann die individuelle Entscheidung des Datensubjekts als „informiert" gewertet werden[27] und die aggregierten Entscheidungen der Datensubjekte intensivieren den Wettbewerb zwischen den Verantwortlichen um Angebote, die dieser Präferenz entsprechen. Die vereinfachte Darstellung der Information muss also einen ausreichenden und zutreffenden Differenzierungsgrad aufweisen, um Präferenzen sinnvoll abzubilden, ohne dass hieran hinsichtlich der Vollständigkeit die gleichen Ansprüche gestellt werden, wie sie für die – ebenfalls bei Interesse verfügbaren – textlichen Ausführung erwartet werden. Weil mit dieser Vereinfachung notwendigerweise eine Verkürzung einhergeht und es zu einer gewissen Unschärfe der Kategorien kommt, ist ein solches System auf regelmäßige rechtliche und empirische Überprüfung und eine anschließende Anpassung angewiesen.

---

[25] Zur theoretischen Möglichkeit, Marktversagen durch eine informierte Minderheit zu verhindern: *Schwartz/Wilde*, 127 University of Pennsylvania Law Review 1979, 630; siehe auch *Gottschalk*, AcP 206 (2006), 555 (564); kritisch dagegen: *Wagner/Eidenmüller*, 86 University of Chicago Law Review 2019, 581 (607).

[26] Dies setzt jedoch voraus, dass die Verantwortlichen nicht in der Lage sind, die Datensubjekte in informierte und weniger informierte zu segmentieren und anschließend unterschiedlich zu behandeln: Hierzu bereits: *Schwartz/Wilde*, 127 University of Pennsylvania Law Review 1979, 630 (638). Zur den verbesserten Möglichkeiten einer solchen Unterscheidung auf Grundlage eines Profiling unter Einsatz von ML: *Hacker*, Datenprivatrecht, 2020, S. 589.

[27] Solange dem Datensubjekt die Information potenziell vollständig zur Verfügung steht, gilt die Entscheidung als informiert, obwohl das Ideal einer „vollständig" informierten Entscheidung regelmäßig nicht erreicht wird, hierzu oben Kapitel 4 A.II.3.

b) Stufenweise Verbindlichkeit der Kennzeichnungskombination

Es liegt nahe, zunächst erste Erfahrungen mit einem solchen Klassifikationssystem zu machen und dessen Verbindlichkeit mit zunehmenden Erfahrungswerten zu steigern.

Dies bedeutet, dass die Verwendung einer unionsweit standardisierten Klassifizierung unterschiedlicher Datenverarbeitungen zunächst freiwillig durch die Verantwortlichen erfolgen könnte. Als Anreiz könnte die Verwendung der Klassifikation eine *Indizwirkung* dafür auslösen, dass der Verantwortliche seine Informationspflichten aus Art. 12 ff. DS-GVO erfüllt und eine auf dieser Grundlage getroffene Entscheidung der Datensubjekte in informierter Weise erfolgte. Dies setzt jedoch voraus, dass die jeweilige Klassifizierung auf denjenigen unveränderten Dokumenten (Einwilligungserklärung und Erklärung zum Datenschutz) beruht, die der Verantwortliche bei der für die Klassifizierung zuständigen Stelle hinterlegt hat.

Sobald erste Erfahrungen mit diesem Klassifizierungsmodell gemacht wurden, kann dadurch ein erhöhter Anreiz für die Teilnahme und Verwendung durch den Verantwortlichen geschaffen werden. Beispielsweise könnte die Teilnahme an diesem unionsweit einheitlichen Klassifizierungssystem nicht nur als Indiz wirken, sondern auf der nächsten Stufe eine *widerlegliche Vermutung* für die Einhaltung der Informationspflichten und die Informiertheit der auf dieser Grundlage getroffenen Entscheidung der Datensubjekte auslösen.

Es liegt nahe, dass vornehmlich solche Verantwortliche freiwillig an diesem Klassifizierungssystem teilnehmen, die eine vorteilhafte Bewertung erreichen. Dies ist jedoch nur auf den ersten Blick eine unbefriedigende Konsequenz. Selbst wenn lediglich diejenigen Verantwortlichen die Kennzeichnung verwenden, die eine besonders gute Bewertung erreicht haben, kann dies positive Folgen für den Wettbewerb haben, weil sie den Verantwortlichen eine transparente und verlässliche Kennzeichnung (*Signalling*) ihres hohen Datenschutzstandards ermöglicht und damit dabei hilft, in eine datenschonende Technik und eine datenschonende Ausgestaltung der Datenverarbeitung zu investieren und dadurch ein Marktversagen auf dem atypischen Zitronenmarkt[28] zu durchbrechen.[29]

Bevor als *ultima ratio* eine für alle Verantwortlichen zwingende Teilnahme an diesem Kennzeichnungssystem und eine Verwendung der unionsweit standardisierten Kennzeichnung erfolgt, liegt es – auch aus Gründen der verfügbaren Kapazitäten[30] – erneut nahe, zunächst in *kartellrechtsakzessorischer* Weise

---

[28] Oben Kapitel 3 C.I.2.b.

[29] Grundlegend: *Akerlof*, 84 The Quarterly Journal of Economics 1970, 488 ff.

[30] Tatsächlich könnte die Bewertung und Klassifizierung von Einwilligungserklärungen und Erklärungen zum Datenschutz ein möglicher Anwendungsfall für ML sein. In zeitlicher Hinsicht ist eine solche Möglichkeit jedoch nicht unmittelbar absehbar. Optimistischer mit Blick auf „autonome" Einwilligung auf Grundlage von ML: *Hacker*, Datenprivatrecht, 2020, S. 606 ff. (S. 618: „Die informierte Einwilligung muss von der technologischen Einwilligung

diejenigen Verantwortlichen zur Verwendung der unionsweit standardisierten Kennzeichnung zu verpflichten, die nach Ansicht der zuständigen Kartellbehörden die Position eines *Gatekeepers* bzw. eines Unternehmens mit überragender marktübergreifender Bedeutung für den Wettbewerb innehaben und aus diesem Grund auch einer (künftig) besonders strengen kartellbehördlichen Aufsicht unterliegen.

c) Erste Informationsstufe: Kennzeichen-Kombination

Welche *Informationsdarstellung* auf der ersten Stufe sinnvoll ist, um die Verständlichkeit zu optimieren und eine ausreichende Differenzierung zu bieten, ist im Ausgangspunkt keine rechtliche Frage. Hierfür sind empirische Studien erforderlich.[31] Es würde den Rahmen dieser Arbeit sprengen, wenn hier ein detailliertes Modell ausgearbeitet und empirisch getestet würde, um daraus konkrete Handlungsvorschläge für den europäischen Gesetzgeber abzuleiten.

Zudem ist nicht von der Hand zu weisen, dass jede klassifizierende Kennzeichnung erhebliche Schwierigkeiten mit sich bringt.[32] Die Komplexität bei der Auswahl der Kriterien und der anschließenden Gewichtung der Kriterien spricht dafür, dass eine zentral standardisierte Vorgehensweise – beispielsweise durch die *EU-Kommission* oder/und den *EDSA* – zwar Gefahr läuft, einen Ansatz zu wählen, den alle Beteiligten anfangs als unbefriedigend empfinden. Allerdings erscheint ein anfänglich fehleranfälliger, zugleich aber einheitlicher und standardisierter Ansatz sinnvoller, als eine Vielzahl an disparaten Kennzeichnungen, die auf freiwilliger Selbstregulierung beruhen und die bei Datensubjekten eher Verwirrung stiften, als die gewünschte Orientierung zu bieten.[33] Trotz der bestehenden Schwierigkeiten einer Klassifikation liegt es auf der Hand, eine farbliche Kennzeichnung und die Angabe eines numerischen Punktesystems (*Privacy Score*) zu kombinieren. Es ist sinnvoll, diese aus der Kennzeichnung von Lebensmitteln bekannte Möglichkeit zur Kennzeichnung von Datenverarbeitungen zu übertragen. Solche sog. *privacy nutrition labels* und

---

abgelöst werden, in deren Rahmen Techniken maschinellen Lernens den Einwilligenden unterstützen").

[31] Hierzu die Ansätze in: *Conpolicy*, Wege zur besseren Informiertheit – Verhaltenswissenschaftliche Ergebnisse zur Wirksamkeit des One-Pager-Ansatzes und weiterer Lösungsansätze im Datenschutz, v. 28.02.2018, S. 57 f. (https://www.conpolicy.de/data/user_upload/Studien/Bericht_ConPolicy_2018_02_Wege_zur_besseren_Informiertheit.pdf, zuletzt abgerufen am 19.05.2022); sowie: *Conpolicy*, Abschlussbericht: Innovatives Datenschutz-Einwilligungsmanagement, v. 07.09.2020 (https://www.bmjv.de/SharedDocs/Downloads/DE/Service/Fachpublikationen/090620_Datenschutz_Einwilligung.pdf?__blob=publicationFile&v=1, zuletzt abgerufen am 19.05.2022).

[32] Zur Schwierigkeit der Entscheidung über die relevanten Kriterien der Bewertung und den Maßstab der Bewertung ausführlich: *Reidenberg* u. a., 96 Washington University Law Review 2019, 1409 (1430 ff. bzw. 1432 ff.).

[33] *Reidenberg* u. a., 96 Washington University Law Review 2019, 1409 (1428 ff./1444).

die Möglichkeiten ihrer praktischen Umsetzung werden bereits seit mehreren Jahren diskutiert.[34]

Eine Kombination aus einer farblichen Kennzeichnung und einem Punktesystem ist deshalb sinnvoll, weil auf diesem Weg die zu bietende Information einerseits stark reduziert werden kann (Farben), dabei aber gleichzeitig durch das Punktesystem auf dieser ersten Informationsstufe ein ausreichendes Maß an Differenziertheit ermöglicht wird, so dass die Vergleichbarkeit der unterschiedlichen Angebote von Verantwortlichen verbessert und so der Wettbewerb zwischen Anbietern innerhalb einer gemeinsamen farblichen Klassifikation gefördert wird.

Eine farbliche Kennzeichnung dient insbesondere denjenigen Datensubjekten mit einer Präferenz für hohen Datenschutz dazu, ihre Entscheidungen schnell zu treffen, indem sie beispielsweise grundsätzlich nur solche, regelmäßig zahlungspflichtigen, Angebote annehmen, die über eine grüne Kennzeichnung verfügen und von farblich abweichenden Angeboten ganz Abstand nehmen, um auf Alternativen mit höherem Datenschutzniveau und – zumeist – höherem monetären Entgelt auszuweichen. Sofern jedoch eine geringe Nachfrageelastizität besteht und solche Alternativen fehlen, sind diese Datensubjekte mit hoher Datenschutzpräferenz regelmäßig bereit, ihre Informationssuche auf eine weitere Stufe auszudehnen, um auf Basis einer erweiterten Informationsgrundlage nochmals über die verfügbaren Angebote zu entscheiden.

Datensubjekte, die der Verarbeitung von personenbezogenen Daten weitgehend gleichgültig gegenüberstehen oder grundsätzlich nicht willens oder nicht fähig sind, für ein datenschonendes Angebot ein monetäres Entgelt zu bezahlen, werden solchen Kennzeichnungen hingegen eine geringe(re) Aufmerksamkeit schenken. Der infolgedessen naheliegende Einwand, dass vor allem Datensubjekte mit hoher Datenschutzpräferenz und womöglich überdurchschnittlicher monetärer Kaufkraft überproportional von solchen Kennzeichnungen profitieren, dürfte zwar zutreffend sein. Er ist aber kein Argument gegen diese Kennzeichnung.

Für eine marktwirtschaftliche Wirtschaftsordnung ist ein unterschiedlich verteiltes Konsumniveau in Abhängigkeit von einer unterschiedlichen Kaufkraft bzw. der unterschiedlichen Zahlungsbereitschaft für mannigfache Produkte keine Besonderheit. Die bei höherer Kaufkraft empirisch (wohl) nachweisbare Bereitschaft zur Zahlung einer monetären Datenschutzprämie,[35] dürfte sich damit auf die Nachfrage für (digitale) Produkte auswirken, die im

---

[34] *Ciocchetti*, John Marshall Journal of Computer and Information Law, 2008, 1ff.; *Cranor*, 10 Journal on Telecommunications & High Technology Law 2012, 273.

[35] *Grossklags/Acquisti*, Proceedings of the Sixth Workshop on Economics of Information Security 2007, 1 (12ff.); *Beresford/Kübler/Preibusch*, 117 Economics Letters 2012, 25 (26); *Hermstrüwer*, Informationelle Selbstgefährdung, 2016, S. 254ff.; *Hacker*, Datenprivatrecht, 2020, S. 629f.

Austausch gegen personenbezogene Daten und/oder monetäres Entgelt angeboten werden.[36]

Während die farbliche Kennzeichnung eine besonders leicht verständliche und schnelle Informationswahrnehmung und -verarbeitung ermöglicht, dabei aber allenfalls eine erste grobe Orientierung bietet, lässt sich der Informationsgehalt auf der ersten Informationsstufe durch die Kombination mit dem numerischen *Privacy Score* steigern. Dadurch lässt sich die Transparenz und infolgedessen der Wettbewerb zwischen den Verantwortlichen um ein hohes Datenschutzniveau innerhalb der jeweiligen farblichen Klassifikation steigern. Geht man beispielsweise von einem maximal erreichbaren *Privacy Score* von 40 Punkten aus und darf eine grüne Kennzeichnung verwendet werden, sofern das Angebot eines Verantwortlichen 31–40 Punkte erreicht, so ermöglicht die jeweilige Punktezahl nochmals eine zehnstufige Differenzierung und Auswahl zwischen allen Anbietern der grünen Klassifikation. Infolgedessen wird der Wettbewerb innerhalb der jeweiligen farblichen Klassifikation gefördert.

Als möglicher Ausgangspunkt kann eine vierfache farbliche Kennzeichnung dienen, wie sie auch im Rahmen der Kennzeichnung zur Haltung von Nutztieren verwendet wird.[37] Dieses Beispiel macht zugleich einen wichtigen Ausgangspunkt deutlich. Während die Farbe „rot" im Kontext der Nutztierhaltung für die Klassifikation „Stallhaltung" zu verwenden ist, eine Haltungsform, für die lediglich die gesetzlichen Mindeststandards an die artentypische Stallhaltung erfüllt werden müssen, beruhen alle höheren Klassifikationen auf einer Nutztierhaltung, die über das hinausgeht, was gesetzlich vorgeschrieben ist.

Hieraus lässt sich ableiten, dass die bloße Einhaltung des geltenden Rechts nicht ausreichen darf, um bereits eine grüne Klassifikation und einen *Privacy Score* von 31–40 Punkten zu erhalten. Umgekehrt gilt, dass auch eine Datenverarbeitung, die farblich mit der niedrigsten Klassifikation („rot") zu kennzeichnen ist, grundsätzlich dennoch die datenschutzrechtlichen Anforderungen an eine rechtmäßige Datenverarbeitung erfüllen muss. Allerdings ist klarzustellen, dass weder die farbliche Kennzeichnung noch der erreichte *Privacy Score* eine Aussage über die Rechtmäßigkeit der Datenverarbeitung durch den Verant-

---

[36] Ebenso: *Hacker*, Datenprivatrecht, 2020, S. 649: „Wer nicht bereit ist, entweder monetär oder datenbasiert für eine Leistung zu zahlen, kann sie nicht in Anspruch nehmen. Es gibt kein Recht auf eine völlig kostenlose Leistung – auch und gerade nicht in der digitalen Wirtschaft". So zuvor auch: *Buchner*, Die Informationelle Selbstbestimmung im Privatrecht, 2006, S. 270 („Einziger Unterschied ist in all diesen Fällen, dass der Betroffene nicht seine persönlichen Daten als Währung einsetzt, sondern das konventionelle Zahlungsmittel Geld. […] Es gibt keinen allgemeinen Anspruch auf kostenlose Produkte oder Dienstleistungen. Dies gilt auch für die Online-Welt – ungeachtet der dort weit verbreiteten Kostenlos-Mentalität.").

[37] Hierzu mit Kritik: *Verbraucherzentrale*, Haltungsform-Kennzeichnung im Handel: Die Auswahl bleibt mangelhaft, 15.12.2020 (https://www.verbraucherzentrale.de/wissen/lebensmittel/lebensmittelproduktion/haltungsformkennzeichnung-im-handel-die-auswahl-bleibt-mangelhaft-25484, zuletzt abgerufen am 19.05.2022).

wortlichen trifft. Die Teilnahme an einem solchen unionsweit standardisierten Klassifikationssystem führt nicht zu einer rechtlichen Begutachtung der Datenverarbeitung, zumal die Klassifikation auf der Beurteilung der vom Verantwortlichen eingereichten Dokumente beruht und nicht auf der durch den Verantwortlichen tatsächlich durchgeführten Datenverarbeitung.

Die Entscheidung über die Rechtmäßigkeit der Datenverarbeitung, einschließlich der Informiertheit der Datensubjekte im Zeitpunkt der Einwilligungserteilung (Art. 4 Nr. 11 DS-GVO), der tatsächlichen Erfüllung der Informationspflichten (Art. 12–14 DS-GVO) und der Einhaltung des Grundsatzes der transparenten Datenverarbeitung (Art. 5 Abs. 1 lit. a Var. 3 DS-GVO) obliegt allein den dafür zuständigen Datenschutzbehörden[38] und Gerichten.[39] Wird jedoch im Kontext einer behördlichen Überprüfung der Datenverarbeitung offenkundig, dass ein Verantwortlicher abweichend von der vorformulierten Einwilligungserteilung, der Erklärung zum Datenschutz oder den sonstigen Klauseln des Nutzungsvertrags, Daten verarbeitet, so sollte sich diese Diskrepanz zwischen den verwendeten Dokumenten und der hierauf beruhenden Kennzeichnung einerseits und der faktischen Realität der Datenverarbeitung andererseits, bei der Bemessung eines Bußgelds zulasten des Verantwortlichen auswirken.

4. Die Verarbeitungsgrundlage als zentrales Kriterium

Trotz der Notwendigkeit empirische Studien durchzuführen, wird nachfolgend ein Vorschlag für eine grobe Klassifikation aus rechtswissenschaftlicher Perspektive unterbreitet. Diese beruht auf dem hier vorgeschlagenen Stufenmodell der Erlaubnistatbestände. In Übereinstimmung mit dem in Kapitel 5 vorgeschlagenen Stufenmodell der Erlaubnistatbestände zur Gewährleistung der abgestützten informationellen Privatautonomie ist der Einwilligung grundsätzlich auch im Kennzeichnungssystem ein – positiv zu bewertender – Vorrang einzuräumen. Dennoch ist die Datenverarbeitung auf Grundlage einer Einwilligung nicht der besten Klassifikation (grüne Farbe) zugeordnet, weil diese für

[38] Allerdings ist es bei der Bemessung von Bußgeldern zulasten des Verantwortlichen zu berücksichtigen, sofern die tatsächliche Datenverarbeitung durch den Verantwortlichen systematisch von der Kennzeichnung abweicht.

[39] Hierzu gehört auch die Möglichkeit zur Klage durch Verbraucherschutzverbände auf Grundlage von § 8 Abs. 3 UWG i. V. m. § 5 UWG. Zur Beschränkung einer möglichen Klagebefugnis auf Verbraucherschutzverbände „als Datenschützer“: *Köhler*, WRP 2018, 1269 (1269); gegen eine lauterkeitsrechtliche Klagebefugnis von Mitbewerben: *LG Bochum*, K&R 2018, 737; *LG Wiesbaden*, K&R 2019, 281; *LG Magdeburg,* K&R 2019, 210; *LG Stuttgart*, WRP 2019, 1089 (Rn. 13 ff.); *Köhler*, ZD 2018, 337; *ders.*, WRP 2019, 1279; *Ohly*, GRUR 2019, 686; *Spittka*, GRUR-Prax 2019, 4. Für eine Klagebefugnis von Mitbewerbern: *OLG Hamburg*, WRP 2018, 1510 (Rn. 25); *OLG Naumburg*, GRUR 2020, 210; *Uebele,* GRUR 2019, 694 ff.

eine vertragsakzessorische und lediglich periphere Datenverarbeitungen auf Grundlage von Art. 6 Abs. 1 lit. b DS-GVO vorbehalten ist. Indem es nach hier vertretener – aber umstrittener – Ansicht möglich ist, die sog. freie Widerruflichkeit befristet auszuschließen, hat die Wahl dieser Option durch den Verantwortlichen grundsätzlich eine Klassifikation auf der letzten, roten Stufe zur Folge (zur Ausnahme sogleich).

Am anderen Ende des Spektrums kann eine Datenverarbeitung auf Grundlage von Art. 6 Abs. 1 lit. b DS-GVO der grünen Klassifikation zugeordnet werden, sofern die Vertragsakzessorietät – wie hier vertreten – lediglich eine Entlastungsfunktion für den Einwilligungstatbestand erfüllt und deshalb nicht eingreift, sofern ein Verantwortlicher versucht, die „Personalisierung und Verbesserung" von digitalen Produkten, die „Bereitstellung durchgängiger und nahtloser Erlebnisse" und die Finanzierung des Angebots durch personalisierte Werbung für Dritte als seine vertragliche Leistungspflicht zu definieren.[40]

Nach diesem Ansatz ist eine unionweit standardisierte Kennzeichnung auf der ersten Stufe sinnvoll, die eine farbliche Klassifikation und einen *Privacy Score* verbindet und die im Wesentlichen an dem zugrundeliegenden Erlaubnistatbestand der Datenverarbeitung ausgerichtet ist:

Farbe	Privacy Score	Erlaubnistatbestand
grün	36–40	**Art. 6 I lit. c** (Einhaltung von Rechtspflichten) **Art. 6 I lit. d** (Schutz lebenswichtiger Interessen)
	31–35	**Art. 6 I lit. b** (Erforderlichkeit zur Erfüllung eines Vertrags) *sofern enges Verständnis als Entlastung der Einwilligung*
gelb	26–30	**Art. 6 I lit. a** (frei widerrufliche Einwilligung)
	21–25	**Art. 9 II lit. j (i. V. m. § 27 BDSG)** (besonders sensible Daten für (öffentliche) wissenschaftliche Forschungszwecke auf Grundlage von Interessenabwägung)
orange	16–20	**Art. 6 I lit. f** (Interessenabwägung)
	11–15	**Art. 6 I lit. f i. V. m. Art. 21 II** (personalisierte Direktwerbung des Verantwortlichen innerhalb einer bestehenden Kundenbeziehung)

[40] Dies versucht beispielsweise *Facebook*. Dies als Berufungsinstanz bestätigend: *OLG Wien*, Urt. v. 07.12.2020 (nicht rechtskräftig), GZ 11 R 153/20f, 11 R 154/20b-99 S. 27 f. Zurecht mit Zweifeln an dieser Rechtsauffassung: *OLG Düsseldorf*, Vorlagebeschl. v. 24.03.2021, Kart 2/19 (V), Rn. 40. Diese Verfahren wird vom EuGH unter dem Aktenzeichen C-252/21 geführt. Sowie *ÖOGH*, Vorlagebeschl. v. 22.07.2021, 6 Ob 56/21k (Rn. 8 ff.) – *Schrems [III]*.

Farbe	Privacy Score	Erlaubnistatbestand
rot	05–10	**Art. 9 II lit. a** (besonders sensible Daten auf Grundlage einer Einwilligung für andere als Forschungszwecke)
	00–05	**Art. 6 I lit. a + teleologische Reduktion v. Art. 7 III 1** (befristeter Ausschluss der freien Widerruflichkeit)

Tabelle 2: Farbliche Klassifikation in Verbindung mit Privacy Score und Erlaubnistatbestand der Datenverarbeitung

Wie bereits erläutert, kann diese Klassifizierung allenfalls als erster grober Ausgangspunkt dienen. Zusätzlich liegt es nahe, jeweils innerhalb der farblichen Klassifikation für bestimmte Arten der Datenverarbeitung Punkte abzuziehen oder zu gewähren. Als ein solches sekundäres Kriterium könnte beispielsweise eine Datenverarbeitung unter Anwendung einer Ende-zu-Ende-Verschlüsselung der personenbezogenen Daten den *Privacy Score* ebenso erhöhen, wie eine umfangreiche Pseudonymisierung gemäß Art. 4 Nr. 5 DS-GVO.

Dagegen kann eine (rechtmäßige) Datenverarbeitung außerhalb der EU eine Reduktion des *Privacy Score* zu Folge haben, selbst wenn eine Datenverarbeitung von einem Angemessenheitsbeschluss der *EU-Kommission* gemäß Art. 45 Abs. 3 S. 1 DS-GVO, von genehmigten verbindlichen unternehmenseigenen Datenschutzregeln (engl.: corporate binding rules oder kurz: CBR) gemäß Art. 46 Abs. 2 lit. b i. V. m. Art. 47 DS-GVO oder von europäischen Standard-Vertragsklauseln (engl.: standard contract clauses oder kurz: SCC) gemäß Art. 46 Abs. 2 lit. c oder lit. d DS-GVO gedeckt ist.

Gleichwohl sollten diese sekundären Kriterien nach hier vertretener Auffassung regelmäßig nicht dazu führen, dass sich die farbliche Klassifizierung der Datenverarbeitung ändert. Anderenfalls würde die farbliche Kennzeichnung ihre Aussagekraft und Verlässlichkeit als basale Orientierungshilfe verlieren (Grundsatz der Stabilität der farblichen Klassifikation).

Infolgedessen steigt beispielsweise ein einwilligungsbasiertes Profiling auf Grundlage von besonders sensiblen personenbezogenen Daten nicht aus der roten Gruppe in eine bessere Klassifikation auf, nur weil besonders strenge Maßnahmen zur Wahrung der Sicherheit der Datenverarbeitung (Art. 32 DS-GVO) getroffen werden.

Allerdings existieren Ausnahmen von dem Grundsatz der Stabilität der farblichen Klassifikation, weil die für die Datenverarbeitung herangezogene Grundlage zwar das wichtigste Kriterium für die Klassifikation ist, es aber weitere Kriterien von so hoher Bedeutung für das Datenschutzniveau gibt, dass diese sich transparent in der Klassifikation niederschlagen müssen. Zwei solche Verschiebungen sind offensichtlich:

Erstens sind gerade im Kontext der Sicherheit der Datenverarbeitung Ausnahmen von dem Grundsatz der Stabilität der farblichen Klassifikation mög-

lich. Sofern man die Anforderungen an die Sicherheit der Datenverarbeitung gemäß Art. 32 Abs. 1 DS-GVO für dispositiv hält, so dass ein Datensubjekt in eine reduzierte Sicherheit der Datenverarbeitung einwilligen kann,[41] spricht dies dafür, dieser Risikoerhöhung für die Datensicherheit nicht nur durch eine Reduktion des *Privacy Score* in den Grenzen der bisherigen farblichen Klassifikation, sondern auch durch eine Herabstufung in eine andere farbliche Klassifizierung Rechnung zu tragen. Holt ein Verantwortlicher beispielsweise eine Einwilligung als Grundlage für die Rechtmäßigkeit der Datenverarbeitung ein und kombiniert diese mit einer Einwilligung in ein reduziertes Niveau der Anforderungen an die Sicherheit der Datenverarbeitung (Art. 32 DS-GVO), so spricht dies dafür, nicht nur den *Privacy Score*, sondern – als *negative Ausnahme* zum Grundsatz der Stabilität der farblichen Klassifikation – auch die farbliche Kennzeichnung von „gelb" auf „orange" herabzustufen.

Zweitens führt der zeitweise Ausschluss der freien Widerruflichkeit der Einwilligung unter telelogischer Reduktion des Art. 7 Abs. 3 S. 1 DS-GVO zwar grundsätzlich zu einer Einordnung in die unterste, „rote" Klassifikation. Allerdings ist die Möglichkeit zum befristeten Ausschluss der freien Widerruflichkeit gegenüber einem nicht-marktmächtigen Verantwortlichen nicht nur unionsgrundrechtlich geboten. Vielmehr ermöglicht es diese Flexibilisierung sowohl Marktzutrittsbarrieren für KMU zu vermeiden und infolgedessen den Wettbewerb zu fördern als auch die Verlässlichkeit der Rechtsbeziehung zwischen Datensubjekt und Verantwortlichem zu stabilisieren. Letzteres soll auch einen Anreiz dafür bieten, dass Verantwortliche ein Geschäftsmodelle mit höherem Datenschutzniveau wählen. Weil die Märkte für digitale Produkte sich als atypische Zitronenmärkte erwiesen haben,[42] ist die Kennzeichnung gerade ein wesentliches Instrument, um die Transparenz zu erhöhen und die datenschonende Option für Datensubjekte sichtbar zu machen (*Signalling*). Hieraus folgt notwendigerweise, dass ein Verantwortlicher, der digitale Produkte unter Wahrung eines hohen Niveau an Datenschutz (insbesondere gemäß Art. 5 Abs. 1 und Art. 25 DS-GVO) und eines hohen Niveau an Datensicherheit (Art. 32 DS-GVO) bereitstellt, zugleich aber für die Datenverarbeitung auf eine Einwilligung unter befristetem Ausschluss der freien Widerruflichkeit setzt, dennoch in der Lage sein muss, sein für Datensubjekte insgesamt positives Angebot auch positiv kennzeichnen zu können.

Kurzum: Einem Anbieter von digitalen Produkten, der die Anforderungen der DS-GVO mustergültig umsetzt, dabei aber transparent auf einen befriste-

---

[41] Hierzu: *Sattler*, in: Ebers/Steinrötter (Hrsg.), Künstliche Intelligenz und smarte Robotik im IT-Sicherheitsrecht, 2021, S. 197 (209 f.); *Hamburgische Beauftragte für Datenschutz und Informationsfreiheit*, Abdingbarkeit von technisch-organisatorischen Maßnahmen (Art. 32 DSGVO), 18.02.2021 (https://datenschutz-hamburg.de/pages/abdingbarkeit-toms/, zuletzt abgerufen am 19.05.2022).

[42] Kapitel 3 C.I.2.b.

ten Ausschluss der freien Widerruflichkeit der Einwilligung i. S. d. Art. 7 Abs. 3 S. 1 DS-GVO setzt, muss es – als *positive Ausnahme* zum Grundsatz der Stabilität der farblichen Klassifikation – jedenfalls möglich sein, die im Ausgangspunkt vorgesehene „rote" Klassifikation zu verlassen und eine Einordnung in die „orange" oder sogar „gelbe" Klassifikation zu erreichen.

III. Klassifikation als Anwendungsbereich für ML

Die Diskussion inwieweit die technologischen Innovationen von ML zur Verbesserung des Datenschutzes durch Technikgestaltung eingesetzt werden kann, wird bereits lebhaft geführt.[43] Dabei steht regelmäßig der Einsatz von ML zur Unterstützung von Datensubjekten bei Erteilung ihrer Einwilligung[44] oder eine Bewertung von Datenschutzerklärungen durch Intermediäre – insbesondere Datenschutzbehörden oder Verbraucherschutzverbände – im Zentrum der Überlegungen.[45]

Die mit ML einhergehenden technischen und professionellen Anforderungen sprechen jedoch einstweilen dafür, dass ML nicht dezentral und durch Datensubjekte eingesetzt werden wird,[46] sondern ein aussichtsreicher Anwendungsfall sich gerade in der Kombination mit standardisierten Kennzeichnungen ergeben könnte.

Letztlich geht es darum, auf der ersten Informationsstufe durch die Kombination aus farblicher Klassifikation und *Privacy Score* die Verständlichkeit von Informationen zu optimieren. Die Kennzeichnung soll die Genauigkeit und Vollständigkeit der textlichen Darstellung bestmöglich repräsentieren. Solange Einwilligungs- und Datenschutzerklärungen nicht einmal in formeller Hinsicht standardisiert sind, kommt jedes Klassifikationssystem schnell an eine Grenze. Weil ein solches unionsweites Klassifikationssystem auf ein hohes Maß an Automatisierung angewiesen ist und die Analyse von Text – neben der Bilderkennung – ein Feld ist, auf dem ML dem menschlichen Verstand weit überlegen ist, liegt es nahe, in diesem Kontext Methoden des ML einzubinden.

So können mittels ML zunächst Muster in den gängigen Einwilligungs- und Datenschutzerklärungen offengelegt werden. In einem zweiten Schritt liegt es nahe, die Analyse und anschließende Klassifikation dieser Texte mithilfe von

---

[43] *Gutachten der Datenethikkommission*, 2019, S. 153 ff. https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/it-digitalpolitik/gutachten-datenethikkommission.html, zuletzt abgerufen am 19.05.2022); zuletzt ausführlich m. w. N. *Hacker*, Datenprivatrecht, 2020, S. 570 ff.

[44] M.w.N. *Hacker*, Datenprivatrecht, 2020, S. 568.

[45] *Micklitz* u. a., 40 Journal of Consumer Policy 2017, 367 (372). *Hacker*, Datenprivatrecht, 2020, S. 570 ff.

[46] Insgesamt skeptisch gegenüber Selbsthilfemechanismen, welche die Datensubjekte selbst aktiv einbinden müssen: *Solove*, 126 Harvard Law Review (2013), 1880 (1883 ff.).

trainierten Algorithmen zu automatisieren und dadurch die Kapazitäten für diese Tätigkeit grundlegend zu erhöhen.

Eine spannende Frage bleibt, inwieweit Rechtsänderungen sich auf die Kennzeichnung auswirken können und sollten. Wie bereits ausgeführt, darf das Kennzeichnungssystem nicht dazu dienen, die Rechtmäßigkeitsprüfung der tatsächlichen Datenverarbeitung durch den Verantwortlichen (*ex ante*) und durch die Datenschutzbehörden und Gerichte (*ex post*) zu ersetzen. Dennoch liegt es auf der Hand, dass ein solches Klassifikationsverfahren auch dazu genutzt werden könnte, Verantwortliche auf mögliche Rechtsänderungen hinzuweisen. Beispielsweise hat das *OLG Düsseldorf* dem *EuGH* mit seinem Beschluss vom 24.03.2021 sowohl die Auslegung des Begriffs der besonders sensiblen personenbezogenen Daten vorgelegt[47] als auch zur Konkretisierung und Abgrenzung der Erlaubnistatbestände in Art. 6 Abs. 1 lit. b DS-GVO (vertragsakzessorische Datenverarbeitung) und Art. 6 Abs. 1 lit. f DS-GVO (Interessenabwägung) aufgefordert.[48] Auch der *ÖOGH* hat den *EuGH* zur Konkretisierung des Begriffs der besonders sensiblen personenbezogenen Daten aufgefordert und erwartetet eine klarere Abgrenzung der Erlaubnistatbestände der Einwilligung und der vertragsakzessorischen Datenverarbeitung. Obwohl in beiden Vorlageverfahren die Geschäftsmodelle von *Meta Platforms* (*Facebook*) im Zentrum stehen, müsste der *EuGH* diese Rechtsfragen grundsätzlich abstrakt beantworten.[49] Infolgedessen werden sich die Antworten des *EuGH* auf die Rechtmäßigkeit zahlreicher Einwilligungs- und Datenschutzerklärungen und Geschäftsmodelle anderer Verantwortlicher auswirken.

Sofern es gelingt, langfristig eine automatisierte Klassifikation von Einwilligungs- und Datenschutzerklärungen zu etablieren, um auf dieser Grundlage eine Kennzeichnung vorzunehmen, liegt es nahe, dass dieses automatisierte Verfahren sich leicht um Hinweise an den jeweiligen Verwender ergänzen lässt, die darüber informieren, dass möglicherweise eine Anpassung der Texte auf Grundlage einer durch eine *EuGH*-Entscheidung eingetretenen Rechtsänderung sinnvoll ist, ohne dass durch diesen generischen Hinweis bereits eine Rechtsberatung erfolgt.

---

[47] Vorlagefrage 2a des *OLG Düsseldorf*, Vorlagebeschl. v. 24.03.2021, Kart 2/19 (V), Rn. 43 ff. (*EuGH*, C-252/21).

[48] Vorlagefrage 3 und 4 des *OLG Düsseldorf*, Vorlagebeschl. v. 24.03.2021, Kart 2/19 (V), Rn. 49 bzw. Rn. 54 ff. (*EuGH*, C-252/21).

[49] Zur Tendenz des *EuGH* die Sache selbst abschließend zu entscheiden, sofern es sich beim Beklagten um ein Unternehmen aus dem Kreis von *GAFAM* handelt: *EuGH*, Urt. v. 13.05.2014, C-131/12 = NJW 2014, 2257 – *Google Spain*; hierzu oben Kapitel 1 B.V.

IV. Fazit

Aus dem Recht der AGB-Kontrolle ist seit Jahrzehnten bekannt, dass jedenfalls Verbraucher keine komplexen Rechtstexte lesen. Während diese Erkenntnis für das AGB-Recht deshalb von geringer Relevanz ist, weil das systematische Nichtlesen der AGB durch eine gerichtliche *ex post* Kontrolle kompensiert werden kann, etabliert die DS-GVO zahlreiche Informationspflichten der Verantwortlichen gegenüber den Datensubjekten, damit diese insbesondere eine informierte Einwilligung treffen oder bewusst von ihrem Widerspruchsrecht Gebrauch machen können.

Infolgedessen ist es im Datenschutzrecht von Bedeutung, dass die Datensubjekte die Information tatsächlich wahrnehmen und verarbeiten. Anders als im AGB-Recht fehlt im Datenschutzrecht zudem die Rückfallposition des dispositiven Gesetzes und der allgemeinen Handlungsfreiheit. Scheitert eine Einwilligung an der Informiertheit des Datensubjekts, so gilt grundsätzlich das Verbotsprinzip. Deshalb genügt es nicht, resigniert von einer „Fiktion der informierten Einwilligung" auszugehen und stattdessen regelmäßig den unbestimmten Auffangtatbestand der Interessenabwägung heranzuziehen. Stattdessen muss – jedenfalls vorrangig – die *Informationsdarstellung* verbessert werden.

Indem der europäische Gesetzgeber mit der DS-GVO vorrangig auf Informationspflichten und Wahlfreiheiten der Datensubjekte setzt, hat er zwar das im Vergleich zu Wahlbeschränkungen mildere Mittel gewählt und den Grundsatz der Verhältnismäßigkeit (Art. 52 Abs. 1 S. 2 GRCh) beachtet. Allerdings begründet diese Entscheidung für das Informationsmodell eine Folgenverantwortung des europäischen Gesetzgebers. Die Unionsgrundrechte aus Art. 8 GRCh, Art. 7 GRCh und Art. 16 AEUV verpflichten ihn dazu, diese Informationspflichten durch Anforderungen an die *Informationsdarstellung* zu materialisieren. Erst infolgedessen genügt der europäische Gesetzgeber seiner Pflicht zur Gewährleistung einer abgestützten informationellen Privatautonomie.

Empirische Studien haben gezeigt, dass auch die Zusammenfassung der wesentlichen Information auf einer Seite (sog. *one-pager*) allenfalls marginale Verbesserungen für die Informiertheit der Datensubjekte bringen. Dies spricht dafür, dass die Informationspflichten der DS-GVO durch weitere transparenzfördernde Maßnahmen ergänzt werden müssen.

Wie sich aus Art. 12 Abs. 7 DS-GVO ergibt, war sich der europäische Gesetzgeber von Anfang an darüber bewusst, dass die in Art. 12–14 DS-GVO vorgesehenen Informationspflichten einer Ergänzung bedürfen, die nicht auf einer textlichen, sondern einer bildlichen Darstellung beruhen. Nach hier vertretener Auffassung eröffnet Art. 12 Abs. 8 i. V. m. Art. 92 Abs. 2 DS-GVO der *EU-Kommission* nicht nur die Möglichkeit, diejenige Information zu bestimmen, die durch Bildsymbole darzustellen ist und ein Verfahren für die Bereitstellung standardisierter Bildsymbole zu erlassen. Vielmehr führt die unionsgrund-

rechtskonforme Auslegung dieser Befugnisse zu einer Verpflichtung, diese Befugnisse auch unverzüglich zu nutzen.

Allerdings ist die Verfügbarkeit von unionsweit standardisierten Bildsymbolen für die Informationspflichten aus Art. 12 ff. DS-GVO allenfalls eine notwendige, aber noch keine hinreichende Bedingung dafür, dass eine tatsächliche Ausübung von informationeller Privatautonomie ermöglicht wird. Deshalb sollten diese Bildsymbole durch eine unionsweit standardisierte Kombination aus farblicher Kennzeichnung und Angabe eines *Privacy Score* ergänzt und langfristig womöglich ersetzt werden.

Sinnvoll erscheint eine vierfache farbliche Abstufung, die mit einem numerischen *Privacy Score* kombiniert wird. Diese Kennzeichnungskombination bietet mehrfache Möglichkeiten zur Differenzierung, ohne dabei zu komplex zu sein und dadurch ihrerseits wiederum das Ziel einer übersichtlichen Informationsdarstellung zu gefährden (*information overload*). Ausgangspunkt für die Einordnung in das System ist jeweils die für die Datenverarbeitung herangezogene Rechtsgrundlage.

Auf dieser Basis können insbesondere Datensubjekte mit hoher Datenschutzpräferenz die unterschiedlichen Angebote besser vergleichen. Sofern das Produkt eines Anbieters aus Sicht eines Datensubjekts besonders wichtig ist, ermöglicht diese Kennzeichnung zumindest eine schnelle oberflächliche Bewertung und erleichtert dem Datensubjekt die Entscheidung, ob es sich lohnt, zusätzliche Information heranzuziehen, die weiterhin in textlicher Form zur Verfügung zu stellen ist.

Jedenfalls solange ein solches unionsweit standardisiertes Kennzeichnungssystem noch in der Aufbau- und Testphase ist, sollte keine allgemeine Pflicht zur Übernahme der unionsweit standardisierten Kennzeichen begründet werden. Um einen Anreiz zu schaffen, dass Verantwortliche nicht nur mit solchen Produkten an diesem Kennzeichnungssystem teilnehmen, die eine grüne Kennzeichnung mit hohem *Privacy Score* erreichen, sollte deren Verwendung jedoch als Indiz für die Erfüllung von Informationspflichten gewertet werden. Sofern dies nicht ausreicht, um eine weite Verbreitung der Kennzeichnung sicherzustellen, könnte die Nichtverwendung dieser standardisierten Kennzeichen die Vermutung auslösen, dass der Verantwortliche seine Informationspflichten nicht erfüllt und eine vom Datensubjekt auf dieser Grundlage erklärte Einwilligung nicht in informierter Weise erfolgt. Obwohl die Beweislast für die Erfüllung der Informationspflichten und die Informiertheit einer Einwilligung – jedenfalls im Zivilprozess – als für den Verantwortlichen günstige Voraussetzung ohnehin bei ihm liegt, erhöhen sich durch diese Vermutungsregel die Anforderungen an die Beweisführung.

Entscheidet sich ein Verantwortlicher für eine Verwendung der unionsweit standardisierten Kennzeichnung, so muss diese mit der – für Bildsymbole in Art. 12 Abs. 7 S. 2 DS-GVO geregelten – Pflicht einhergehen, der für die Klassifi-

zierung zuständigen Institution einen Zugang zu der jeweils aktuell verwendeten Datenschutz- und Einwilligungserklärung in maschinenlesbarer Form zur Verfügung zu stellen. Dieser Zugang ist eine Voraussetzung dafür, um langfristig eine automatisierte Klassifikation zu ermöglichen. Diese Klassifikation durch Kombination der farblichen Kennzeichnung und eines *Privacy Score* auf Grundlage der verwendeten Einwilligungs- und Datenschutzerklärungen könnte sich zudem als ein Anwendungsfall für ML erweisen. Die Klassifikation der Datenverarbeitung anhand von Texten und damit Sprache ist ein klar beschränkter Anwendungsbereich, auf dem ML besonders beeindruckende Erfolge vorzuweisen hat. Deshalb hat dieses Anwendungsszenario höhere Erfolgsaussichten als ein Einsatz von ML durch Datenschutzbehörden oder Verbraucherschutzverbände, um damit die tatsächlich durchgeführten Datenverarbeitungen zu analysieren.[50]

Als positiver Nebeneffekt setzt eine solche automatisierte oder sogar autonome Klassifizierung langfristig einen Anreiz zur Standardisierung der Einwilligungserklärungen und Datenschutzerklärungen. Zudem bietet diese Klassifizierung der zuständigen Stelle eine hilfreiche Erkenntnisquelle. Diese ist ein wertvolles Instrument in der Hand des Gesetzgebers, um die Effektivität und Effizienz des europäischen Datenschutzrecht rechtstatsächlich zu evaluieren und mögliche Reformen auch empirisch begründen zu können.

Bislang besteht keine Rechtsgrundlage, die beispielsweise der *EU-Kommission* oder einer zu beauftragenden Einrichtung einen Anspruch auf Zugang zu einer maschinenlesbaren Version der jeweiligen Einwilligungs- und Datenschutzerklärung eröffnet. Ein solcher gesetzlicher Anspruch wäre jedoch sinnvoll und eine notwendige Voraussetzung, sofern eine unionsweit standardisierte und möglichst automatisierte Kennzeichnung durch eine Kombination aus farblicher Gestaltung und *Privacy Score* langfristig implementiert werden soll.

B. Kontroll-Cockpit für datenschutzrechtliche Erklärungen

Neben der Notwendigkeit einer verbesserten Transparenz durch die Art der Informationsdarstellung wird seit geraumer Zeit auch darüber diskutiert, wie die Kontrolle der Datensubjekte über die Datenverarbeitung erhöht werden kann.[51] Anders als Instrumente, die ausschließlich der Erhöhung der Transpa-

[50] In diese Richtung: *Hacker*, Datenprivatrecht, 2020, S. 576 („Wie gesehen sind problematische Verarbeitungen jedoch [in den Texten] häufig gar nicht enthalten. Diese können lediglich durch die genannten durchsetzungsorientierten Instrumente aufgedeckt werden, welche nicht lediglich textbasierte Veröffentlichungen untersuchen, sondern auch den Code und die Wirkweise der angebotenen Anwendungen analysieren").

[51] Zu den Möglichkeiten und Grenzen des Selbstdatenschutzes, einschließlich einer Manipulation der bereitgestellten personenbezogenen Daten: *M. Wagner*, Datenökonomie und Selbstdatenschutz, 2020, S. 621 ff.

renz – beispielsweise sog. Datenschutz Dashboards – dienen, ermöglichen es *Kontroll-Cockpits* zusätzlich, die datenschutzrechtlich relevanten Erklärungen von Datensubjekten und Verantwortlichen zu bündeln und eine standardisierte Anlaufstelle für den beiderseitigen Informationsaustausch im Zusammenhang mit diesen Erklärungen zu bieten.[52] Somit ermöglichen *Kontroll-Cockpits* eine Zentralisierung und erleichtern für beide Seiten die technische Umsetzung der datenschutzrechtlichen Anforderungen an eine rechtmäßige Datenverarbeitung. Infolgedessen ist ein solches *Kontroll-Cockpit* ein möglicher Ausgangspunkt für sog. *Personal Information Management Systems* (PIMS) wie sie zunehmend gefordert werden, um die informationelle Privatautonomie von Datensubjekten abzustützen (I).

Während ein *Kontroll-Cockpit* das Datensubjekt dabei unterstützt, den Überblick und die Kontrolle über diejenigen Datenverarbeitungen zu bewahren, die sie selbst durch Erklärungen beeinflussen können, können sie im Gegenzug, also aus Sicht der Verantwortlichen, die rechtssichere Ausgestaltung der Datenverarbeitung verbessern. Allerdings erreichen freiwillige und nicht standardisierte *Kontroll-Cockpits* ihre Grenze, sofern jeder Verantwortliche ein eigenes *Kontroll-Cockpit* gestalten kann. Zudem haben solche Verantwortlichen tendenziell kein oder ein beschränktes Interesse an transparenten *Kontroll-Cockpits*, deren Geschäftsmodell gerade auf einer mehrseitigen, werbefinanzierten Plattform beruht und deren umfassende Kommerzialisierung von personenbezogenen Daten auf ihrem umfangreichen und exklusiven Zugang zu diesen beruht. Weil insbesondere *GAFAM* versuchen, ihre Produktmärkte jeweils abzuschotten oder zumindest zu kontrollieren, dürften standardisierte *Kontroll-Cockpits* – mit technischen Schnittstellen für unterschiedliche Verantwortliche – aus Sicht dieser Unternehmen unerwünscht sein.

Ausgangspunkt für eine Implementierung von *Kontroll-Cockpits* ist die Diskrepanz zwischen den durch die DS-GVO eingeräumten umfangreichen Ansprüchen der Datensubjekte und der von Datensubjekten regelmäßig bekundeten Einschätzung, dass sie die Verarbeitung von personenbezogenen Daten nur mangelhaft kontrollieren können.[53] Bereits *de lege lata* legt die DS-GVO eine Implementierung von *Kontroll-Cockpits* in mehrfacher Hinsicht nahe, ohne eine rechtliche Pflicht für deren Einführung zu enthalten (II).

---

[52] Ähnlich, allerdings mit einer engeren, auf die Einwilligung beschränkten Definition des Kontroll-Cockpits: *Conpolicy*, Abschlussbericht: Innovatives Datenschutz-Einwilligungsmanagement, v. 07.09.2020, S. 17/Fn. 9 (https://www.bmjv.de/SharedDocs/Downloads/DE/Service/Fachpublikationen/090620_Datenschutz_Einwilligung.pdf?__blob=publicationFile&v=1, zuletzt abgerufen am 19.05.2022).

[53] In einer Befragung der *EU-Kommission* aus dem Jahr 2015 und damit vor der Anwendbarkeit der DS-GVO gaben 45 % der in Deutschland befragten an, dass sie überhaupt keine Datenkontrolle besäßen, wobei hiervon 68 % berichteten, dass diese mangelnde Kontrolle sie beunruhige: Special Eurobarometer 431 (2015). Data protection (https://data.europa.eu/data/datasets/s2075_83_1_431_eng?locale=de, zuletzt abgerufen am 19.05.2022).

Die Erfüllung der Informationspflichten gemäß Art. 12 ff. DS-GVO und auch die oben vorgeschlagene Informationsdarstellung durch eine Kennzeichnungs-Kombination lassen sich sinnvoll in ein solches *Kontroll-Cockpit* integrieren. Dennoch liegt die wesentliche Funktion des *Kontroll-Cockpits* nicht nur in der Informationsvermittlung, sondern darin, die Entscheidungen und Erklärungen von Datensubjekten zu bündeln. In einer abschließenden Übersicht wird dargestellt, wie ein *Kontroll-Cockpit* insbesondere dabei helfen kann, den Widerruf der Einwilligung und den Widerspruch gegen eine Datenverarbeitung zu strukturieren und dadurch die Kontrolle der Datensubjekte zu verbessern (III).

I. Kontroll-Cockpit als Ausgangspunkt für PIMS

Seit einigen Jahren stehen *Personal Information Management Systems* (PIMS) im Zentrum der Diskussion über künftige Instrumente, die den selbstbestimmten Schutz von personenbezogenen Daten durch die Datensubjekte verbessern sollen und gleichzeitig dabei helfen, das enorme wirtschaftliche und gesellschaftliche Potential einer Verarbeitung von personenbezogenen Daten zu nutzen.[54] Mit dem *EDSB* lassen sich *PIMS* definieren als

> „neue Technologien und Ökosysteme, mit denen Menschen in die Lage versetzt werden sollen, über die Erhebung und Weitergabe ihrer personenbezogenen Daten Kontrolle auszuüben".[55]

Aus der Perspektive der Verantwortlichen könnten *PIMS* dazu dienen, ihre datenschutzrechtlichen Pflichten rechtssicher zu erfüllen und zugleich die Erklärungen der Datensubjekte, insbesondere die Einholung, die Aktualisierung und

---

[54] Hierzu jeweils m. w. N.: *EDSB*, Stellungnahme 9/2016 zu Systemen für das Personal Information Management (PIM), 2016, S. 6 (https://edps.europa.eu/sites/default/files/publication/16-10-20_pims_opinion_de.pdf, zuletzt abgerufen am 19.05.2022); *EU-Kommission*, An emerging offer of „personal information management services" (2016) (https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=40118, zuletzt abgerufen am 19.05.2022); *Stiftung Datenschutz*, Neue Wege bei der Einwilligung im Datenschutz – technische, rechtliche und ökonomische Herausforderungen, 2017, S. 20 ff. https://stiftungdatenschutz.org/fileadmin/Redaktion/Bilder/PIMS-Abschluss-Studie-30032017/stiftungdatenschutz_broschuere_20170611_01.pdf, zuletzt abgerufen am 19.05.2022); *Schweitzer/Peitz*, Datenmärkte in der digitalisierten Wirtschaft: Funktionsdefizite und Regelungsbedarf? ZWE Discussion Paper No. 17-043, 18.10.2017, S. 52 ff./88 (These 4) (http://ftp.zew.de/pub/zew-docs/dp/dp17043.pdf, zuletzt abgerufen am 19.05.2022); *Gutachten der Datenethikkommission*, 2019, 133 ff. (https://www.bmjv.de/SharedDocs/Downloads/DE/Themen/Fokusthemen/Gutachten_DEK_DE.pdf, zuletzt abgerufen am 19.05.2022); *Conpolicy*, Abschlussbericht: Innovatives Datenschutz-Einwilligungsmanagement, 07.09.2020 (https://www.bmjv.de/SharedDocs/Downloads/DE/Service/Fachpublikationen/090620_Datenschutz_Einwilligung.pdf?__blob=publicationFile&v=1, zuletzt abgerufen am 19.05.2022).

[55] *EDSB*, Stellungnahme 9/2016 zu Systemen für das Personal Information Management (PIM), S. 6.

den Widerruf der Einwilligung effizient zu organisieren. Zudem können *PIMS* vorteilhaft sein, indem sie das Vertrauen der Datensubjekte in die Datenverarbeitung stärken und infolgedessen den Zugang zu relevanten personenbezogenen Daten für möglichst viele Unternehmen offenhalten.[56]

Diese Diskussion über *PIMS* hat – soweit ersichtlich – in § 26 TTDSG[57] und Art. 10 Abs. 1 lit. b,[58] Art. 12 lit. m und lit. n sowie Art. 21 Abs. 3 DG-VO[59] und damit im Kontext der sog. Datenvermittler ihren ersten gesetzlichen Niederschlag gefunden.[60] Diese Vorschriften bzw. Vorschläge[61] greifen die bekannten Empfehlungen auf und haben – wie diese – einen wesentlichen Nachteil:

Je besser ein neutraler, wirtschaftlich unabhängiger Datenvermittler mittels *PIMS* die Kontrolle der Datenverarbeitung durch Datensubjekte sicherstellt, desto aufwendiger und teurer ist es, die hierfür erforderliche Infrastruktur zu etablieren und aufrecht zu erhalten. Umgekehrt formuliert: Nur ein Datenvermittler, der Einnahmen erzielt, kann dauerhaft die Aufgaben erfüllen, die er aus Sicht der *EU-Kommission*, der Datenschutzbehörden und der Verbraucherschutzverbände übernehmen soll. Dies spricht nicht gegen das Potential von Datenvermittlern. Zumindest dürften die zurecht hohen Anforderungen an sol-

---

[56] Es ist deshalb wichtig, den diskriminierungsfreien Datenzugang über PIMS auch rechtlich offenzuhalten, um die Aufrechterhaltung vorhandener oder Entstehung neuer marktmächtiger Unternehmen zu verhindern: Vgl. andererseits den Vorschlag des Verbands der Deutschen Automobilindustrie (*VDA*, Datensicherheit für vernetzte Mobilität, 2017, (https://www.vda.de/de/themen/innovation-und-technik/datensicherheit/was-ist.html, zuletzt abgerufen am 15.04.2020) und die Kritik hieran: *Jungbluth*, in: Roßnagel/Hornung (Hrsg.): Grundrechtsschutz im Smart Car 2019), S. 381 ff.; *vzbv*, Personal Information Management Systems (PIMS) – Chancen, Risiken und Anforderungen, 19.02.2020, S. 9.

[57] Telekommunikation-Telemedien-Datenschutz-Gesetz (TTDSG) v. 23.06.2021, BGBl. 2021 I, S. 1982). Hiernach können Dienste zur Verwaltung von Einwilligungen bei Einhaltung der in § 26 Abs. 1 Nr. 1–4 TTDSG bereits etablierten Voraussetzungen (Nutzerfreundlichkeit, Wettbewerbskonformität, kein wirtschaftliches Eigeninteresse, strenge Zweckbindung, Datensicherheit) von einer unabhängigen Stelle anerkannt werden.

[58] Gemäß Art. 10 Abs. 1 lit. b DG-VO soll die Erbringung von Vermittlungsdiensten zwischen betroffenen Personen, die ihre personenbezogenen Daten zugänglich machen wollen, und potenziellen Datennutzern, einschließlich Bereitstellung der technischen oder sonstigen Mittel als Voraussetzung solcher Dienste, in Ausübung der in der Verordnung (EU) 2016/679 verankerten Rechte einem Anmeldeverfahren unterliegen.

[59] Gemäß Art. 12 DG-VO soll die Erbringung von Vermittlungsdiensten i. S. d. Art. 10 Abs. 1 DG-VO den Bedingungen unterliegen, dass der Anbieter den Datensubjekten die Ausübung ihrer Rechte erleichtert (lit. m) und Werkzeuge zur Einholung der Einwilligung zur Verarbeitung von Datensubjekten bereitstellt (lit. n).

[60] Verordnung (EU) 2022/868 vom 30.5.2022 über europäische Daten-Governance und zur Änderung der Verordnung (EU) 2018/1724 (Daten-Governance-Rechtsakt, kurz: DG-VO), ABl. v. 3.6.2022, L 152, S. 1 ff.

[61] Mit der Forderung, eine „benutzerfreundliche Lösung (einfach und rasch zugänglich) für das Einwilligungsmanagement" in Art. 5 lit. a DMA-Vorschlag zu berücksichtigen: *EDSB*, Zusammenfassung der Stellungnahme zu dem Vorschlag für ein Gesetz über digitale Märkte, 26.04.2021, ABl. C 147, S. 4 (5).

che Datenvermittler die Chancen einer Umsetzung des in Art. 16 ff. DG-VO geregelten Konzepts eines Datenaltruismus sehr erschweren.

Datenvermittler als ein wesentlicher Anwendungsfall von *PIMS* werden nur erfolgreich sein, wenn sie ein langfristiges Geschäftsmodell etablieren können, welches das Spannungsverhältnis zwischen effektivem Datenschutz und effizienter Verwertung von personenbezogenen Daten – auch zu altruistischen Zwecken – ausgleicht. Dies setzt jedoch zunächst die Bereitschaft des Gesetzgebers voraus, zu akzeptierten, dass es Teil der informationellen Privatautonomie ist, wenn Datensubjekte die personenbezogenen Daten bewusst monetisieren. Das pauschale Argument, dass dies mit den Unionsgrundrechten nicht vereinbar sei,[62] trägt ebenso wenig, wie der Hinweis, dass einkommensschwache Datensubjekte dazu neigen könnten, ihre personenbezogenen Daten besonders stark als Gegenleistung einzusetzen.[63]

Weil kein Anspruch auf kostenlose digitale Produkte besteht, ist das individuelle Konsumniveau stets von der verfügbaren monetären Kaufkraft und der Bereitschaft zum Einsatz personenbezogener Daten zur Budgeterweiterung abhängig: Der Zugang zu digitalen Produkten im Austausch gegen eine datenschutzrechtliche Einwilligung tangiert die Menschenwürde der Datensubjekte nicht, solange diese Daten lediglich für eine personalisierte Werbeansprache verarbeitet werden.

Dagegen ist die Implementierung eines *Kontroll-Cockpits* dazu geeignet, die informationelle Privatautonomie von Datensubjekten abzustützen, sofern es als zentrale und transparente Anlaufstelle für Information, Kommunikation und die Abgabe von rechtserheblichen Erklärungen dient.

II. Gesetzliche Anknüpfungspunkte in der DS-GVO

Die Implementierung eines *Kontroll-Cockpit*s lässt sich problemlos mit den allgemeinen Grundsätzen der rechtmäßigen Datenverarbeitung begründen. Solange ein solches *Kontroll-Cockpit* vom Verantwortlichen nicht bewusst mit

---

[62] *EDSB*, Stellungnahme 4/2017 zu dem Vorschlag für eine Richtlinie über bestimmte vertragsrechtliche Aspekte der Bereitstellung digitaler Inhalte, 14.03.2017, S. 10/Nr. 17; sowie: Rede von *Giovanni Buttarelli* (EU-Datenschutz-Beauftragter), verfügbar unter https://edps.europa.eu/sites/edp/files/publication/17-01-12_digital_content_directive_sd_en.pdf, zuletzt abgerufen am 19.05.2022.

[63] So aber: *vzbv*, Personal Information Management Systems (PIMS) – Chancen, Risiken und Anforderungen, 19.02.2020, S. 10 („Eine direkte finanzielle Vergütung von Verbrauchern für die Verarbeitung ihrer Daten ist jedoch höchst problematisch. Aus einer grundrechtlichen Perspektive ist die Reduzierung von personenbezogenen Daten auf einen wirtschaftlichen Wert abzulehnen. Eine direkte finanzielle Vergütung für Verbraucher, die ihre Daten kommerzialisieren, setzt falsche Anreize, besonders für einkommensschwache Bevölkerungsgruppen."), https://www.vzbv.de/sites/default/files/downloads/2020/04/06/20-02-19_vzbv-positionspapier_pims.pdf, zuletzt abgerufen am 19.05.2022.

dem Ziel gestaltet wird, Datensubjekte zu benachteiligen und zu einer besonders umfangreichen Einwilligung in die Datenverarbeitung zu verführen, ist ein *Kontroll-Cockpit* dazu geeignet, die Verarbeitung von personenbezogenen Daten gemäß Art. 5 Abs. 1 lit. a Var. 3 DS-GVO (Grundsatz der Transparenz) in einer für das Datensubjekt nachvollziehbaren Weise transparenter zu machen.

Über die allgemeine Anforderung an eine transparente Datenverarbeitung hinaus, unterstützt ein zentrales *Kontroll-Cockpit* die Einhaltung der datenschutzrechtlichen Anforderungen an die Erteilung und die Widerruflichkeit der Einwilligung (1), erleichtert die Einführung standardisierter Prozesse für den Widerspruch gegen die Datenverarbeitung (2) und ist ein wesentliches Element zur Implementierung von Datenschutz durch Technikgestaltung gemäß Art. 25 Abs. 1 DS-GVO (3).

1. Einwilligung und Einwilligungswiderruf

Der hier vertretene Vorrang der Einwilligung nimmt die informationelle Privatautonomie ernst, setzt aber nicht nur die Möglichkeit zur Einwilligung und das Recht zum Widerruf voraus, sondern auch technische Rahmenbedingungen, welche die Einwilligungserteilung (a) und deren Widerruf (b) effektiv ermöglichen, letzteren idealerweise erleichtern und dadurch die informationelle Privatautonomie des Datensubjekts abstützen.[64]

a) Einwilligungserteilung

Die Möglichkeit zur Erteilung einer Einwilligung ist Ausdruck der gemäß Art. 8 Abs. 2 S. 1 GRCh i. V. m. Art. 16 GRCh bzw. Art. 6 Abs. 3 EUV gewährleisteten informationellen Privatautonomie. Die wirksame Erteilung einer Einwilligung setzt jedoch voraus, dass diese informiert erfolgt (aa) und differenziert ausfallen kann (bb). Ein *Kontroll-Cockpit* dient dazu, diese Voraussetzungen transparent, rechtssicher und mithilfe von Technik umzusetzen.[65] Soweit eine Einwilligung ausdrücklich erfolgen muss (cc), bietet die Einbindung in ein *Kontroll-Cockpit* aus Sicht des Verantwortlichen den Vorteil einer leichten Nachweisbarkeit.

aa) Informiertheit der Einwilligung

Gemäß Art. 4 Nr. 11 DS-GVO muss die Einwilligung in informierter Weise erfolgen. Wie bereits ausgeführt,[66] handelt es sich bei der Informiertheit um ei-

---

[64] Zur Problematik der Durchsetzung eines Einwilligungswiderrufs gegenüber einer Vielzahl von ursprünglichen Einwilligungsempfängern, oben Kapitel 5 C.III.2.c.aa.

[65] Ein solches Kontroll-Cockpit vorsehend: § 26 Abs. 2 Nr. 3a (bb) TTDSG.

[66] Hierzu bereits oben: Kapitel 4 A.II.3.

nen Zustand, der für das Datensubjekt unter zumutbarem Aufwand erreichbar sein muss. Das Datensubjekt trägt jedoch selbst das Risiko, ob es die derart zugängliche Information auch tatsächlich zur Kenntnis nimmt. Der Verantwortliche trägt dagegen die Verantwortung dafür, dass die wesentliche Information richtig, transparent und inhaltlich vollständig aufbereitet und dargestellt wird.

Unter welchen Voraussetzungen eine Einwilligung in informierter Weise erteilt wurde, wird im direkten Kontext der Einwilligung nicht eindeutig bestimmt. Immerhin geht aus ErwG 42 S. 4 DS-GVO hervor, dass

> „die betroffene Person mindestens wissen [sollte], wer der Verantwortliche ist und für welche Zwecke ihre personenbezogenen Daten verarbeitet werden sollen".

Damit stellt ErwG 42 S. 4 DS-GVO zwar einerseits klar, dass die allgemeinen Pflichten zur Information über die Identität des Verantwortlichen (Art. 13 Abs. 1 lit. a DS-GVO) und über die Zwecke der Datenverarbeitung (Art. 5 Abs. 1 lit. b DS-GVO) auch für die Einwilligung gelten. Andererseits lässt sich aus der ausdrücklichen Erwähnung dieser Information nicht in einem Umkehrschluss ableiten, dass sich die Informationspflichten des Verantwortlichen hierin bereits erschöpfen („mindestens").

Um das Risiko zu minimieren, dass die Datenverarbeitung auf Grundlage einer Einwilligung deshalb mit *ex tunc* Wirkung scheitert, weil diese nicht in informierter Weise erteilt werden konnte, liegt es nahe, dass der Verantwortliche sämtliche Informationspflichten zu erfüllen versucht, welche die DS-GVO – auch in anderem Zusammenhang – aufstellt. Obwohl die (sonstigen) Informationspflichten aus Art. 12 i. V. m. Art. 13, 14 DS-GVO unabhängig vom jeweils herangezogenen Erlaubnistatbestand sind, bieten sie zugleich einen Anknüpfungspunkt innerhalb der DS-GVO,[67] aus dem sich unionsweit einheitliche Kriterien für die Informiertheit der Einwilligung ableiten lassen.

Neben der Kategorie der zu verarbeitenden Daten (Art. 9 Abs. 1 DS-GVO) muss über die Arten der Verarbeitung, einschließlich deren Verwendung für eine automatische Entscheidungsfindung (Art. 22 Abs. 2 lit. c DS-GVO), die Empfänger der Daten (Art. 13 Abs. 1 lit. e DS-GVO), die Übermittlung in Drittländer (Art. 49 Abs. 1 S. 1 lit. a DS-GVO) und über die Widerruflichkeit der Einwilligung (Art. 7 Abs. 3 S. 3 DS-GVO) bzw. – bei zeitweisem Ausschluss der Widerruflichkeit – über das verbleibende Recht zum außerordentlichen Widerruf informiert werden.[68]

Anhand dieser allgemeinen Informationspflichten hat auch der *EDSA* seinen Katalog der Mindestanforderungen für eine informierte Einwilligung ent-

---

[67] *Heckmann/Paschke*, in: Ehmann/Selmayr/Heckmann (Hrsg.), DS-GVO, 3. Aufl., Art. 12, Rn. 6 f.

[68] Hierzu oben Kapitel 5 C.III.3.d.

wickelt.[69] Allerdings ist bei der Übertragung dieser allgemeinen Informationspflichten auf die Einwilligung zu berücksichtigen, dass die Pflichten aus Art. 12 ff. DS-GVO an die Erhebung der Daten anknüpfen und damit an den ersten Schritt der tatsächlichen Datenverarbeitung und nicht an die – regelmäßig vorher erfolgende – Erteilung der Einwilligung durch das Datensubjekt.[70]

Zudem ist der Wert eines solchen Katalogs als Orientierungshilfe sehr beschränkt, sofern er nicht regelmäßig aktualisiert wird. Die Urteile des *EuGH* in Sachen *Planet 49* und *Fashion ID* haben die Anforderungen an die informierte Einwilligung bereits weiter spezifiziert. Sofern eine Einwilligung des Datensubjekts in die Verwendung von *tracking*-Werkzeugen, insbesondere *Cookies* erfolgt, um personalisierte Werbung zu ermöglichen, muss der Verantwortliche über die Funktionsdauer der *Cookies* informieren und darüber, ob Dritte die Möglichkeit haben, auf die Daten zuzugreifen.[71] Soweit mehrere Unternehmen für die Datenverarbeitung gemeinsam verantwortlich sind, beispielsweise *Meta Platforms* (*Facebook*) als Anbieter eines sog. *social plug-ins* („Gefällt-mir-Button") und der Betreiber einer Webseite, der dieses Werkzeug in seine Webseite einbindet, ist letzterer bei Einholung der Einwilligung zur Bereitstellung detaillierter Information verpflichtet, soweit er über die Zwecke und Mittel (mit)entscheidet.[72]

Je spezifischer und umfangreicher die Informationspflichten der (gemeinsam) Verantwortlichen werden, desto wichtiger wird die Aufbereitung, Darstellung und Vermittlung dieser Information. Mit der zunehmenden Anzahl und Spezifität der Informationspflichten steigt zugleich die Gefahr, dass die Information unverständlich wird und infolgedessen die Transparenz und damit auch die potenzielle Informiertheit der Datensubjekte im Zeitpunkt der Einwilligung leidet (*information overload*).

Aus ErwG 32 S. 6 DS-GVO folgt, dass der Verantwortliche das Dilemma zwischen Vollständigkeit und Verständlichkeit nicht einseitig zugunsten der Vollständigkeit auflösen kann. Hiernach muss die Aufforderung zur Einwilligungserteilung möglichst knapp gefasst werden. Für die Informiertheit der Einwilligung genügt es gerade bei einer komplexen Datenverarbeitung nicht, wenn

---

[69] *EDSA*, Guidelines 05/2020 on consent under Regulation 2016/679, Version 1.1, 04.05.2020, No. 64 (https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_20-2005_consent_en.pdf, zuletzt abgerufen am 19.05.2022).

[70] *EDSA*, Guidelines 05/2020 on consent under Regulation 2016/679, Version 1.1, 04.05.2020, No. 72 (https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_20-2005_consent_en.pdf, zuletzt abgerufen am 19.05.2022); ebenso: *Conpolicy*, Abschlussbericht: Innovatives Datenschutz-Einwilligungsmanagement, 07.09.2020, S. 28 f. (https://www.bmjv.de/SharedDocs/Downloads/DE/Service/Fachpublikationen/090620_Datenschutz_Einwilligung.pdf?__blob=pu-blicationFile&v=1, zuletzt abgerufen am 19.05.2022).

[71] *EuGH*, Urt. v. 01.10.2019, C-673/17 = GRUR 2019, 1198 (Rn. 59 ff.) – *Planet 49*.

[72] Noch zu Art. 10 Datenschutz-RL: *EuGH*, Urt. v. 2907.2019, C-40/17 = GRUR 2019, 977 (Rn. 105) – *Fashion ID*.

ein möglichst umfassender Katalog an Informationen vorgelegt und dadurch die Informationspflichten formell eingehalten werden. Vielmehr trifft den Verantwortlichen die Pflicht, die Information mehrstufig aufzubereiten oder eine informierte Einwilligung jeweils erst dann einzuholen, wenn diese für die Nutzung eines Teilaspekts des Angebots des Verantwortlichen tatsächlich relevant wird.[73]

Je umfangreichere und spezifischere Informationspflichten die Gerichte künftig im Rahmen ihrer Auslegung von Art. 4 Nr. 11 DS-GVO entwickeln, desto wichtiger werden unionsweit standardisierte Kennzeichnungen und deren Integration in ein übersichtliches *Kontroll-Cockpit*.

bb) Differenziertheit der Einwilligung

Als Folge des Grundsatzes der Zweckkompatibilität gemäß Art. 5 Abs. 1 lit. b i. V. m. Art. 6 Abs. 4 DS-GVO muss die Einwilligung stets für einen bestimmten Zweck und bezogen auf konkrete Datenverarbeitungsvorgänge erteilt werden. Aus Sicht des Datensubjekts ist es wünschenswert, dass sowohl unterschiedliche Verarbeitungszwecke als auch unterschiedliche Verarbeitungsprozesse getrennt voneinander behandelt und nicht lediglich *en bloc* als Gegenstand einer Gesamteinwilligung angeboten werden. Allerdings führt die Verbindung mehrerer inhaltlich ähnlicher Zwecke grundsätzlich nicht dazu, dass die Einwilligung uninformiert und unfreiwillig ist.

Dem ErwG 32 S. 5 DS-GVO lässt sich keine andere Beurteilung entnehmen. Hiernach soll für alle Verarbeitungszwecke eine Einwilligung erteilt werden, wenn die Verarbeitung mehreren Zwecken dient. Daraus folgt jedoch kein Gebot zur möglichst kleinteiligen Differenzierung nach Verarbeitungszwecken.[74] Solange der europäische Gesetzgeber es sich selbst nicht zutraut, grob zwischen unterschiedlichen Verarbeitungszwecke zu differenzieren und auf diese Zwecke mit spezifischeren Erlaubnistatbeständen zu reagieren, muss auch den Verantwortlichen ein gewisses Maß an Freiheit bei der Definition ihrer Verarbeitungszwecke zugestanden werden.

Indem Art. 4 Nr. 11 DS-GVO jedoch eine Einwilligung „für den bestimmten Fall" fordert, müssen jedenfalls evident differenzierbare Verarbeitungszwecke als solche kenntlich und unterscheidbar gemacht werden. Beispielsweise hat der *EuGH* in seiner Entscheidung *Planet 49* hervorgehoben, dass die Einwilligung

---

[73] So vor der DS-GVO zu § 305 Abs. 2 BGB: *LG Frankfurt a. M.*, Urt. v. 10.06.2016, 2-03 O 364/15 Rn. 288 ff.; *Conpolicy*, Abschlussbericht: Innovatives Datenschutz-Einwilligungsmanagement, 07.09.2020, S. 28 (https://www.bmj.de/SharedDocs/Downloads/DE/Service/Fachpublikationen/090620_Datenschutz_Einwilligung.pdf?__blob=publicationFile&v=1, zuletzt abgerufen am 19.05.2022).

[74] A. A. (wohl): *EDSA*, Guidelines 05/2020 on consent under Regulation 2016/679, Version 1.1, 04.05.2020, No. 42 ff. (https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052020-consent-under-regulation-2016679_en, zuletzt abgerufen am 19.05.2022).

in die Verarbeitung personenbezogener Daten zur Durchführung eines Gewinnspiels nicht die Einwilligung in die Speicherung von *Cookies* mitumfasst.[75] Zudem stellt ErwG 43 S. 2 DS-GVO die Freiwilligkeit einer Einwilligung i. S. d. Art. 7 Abs. 4 DS-GVO in Frage,[76] sofern

„zu verschiedenen Verarbeitungsvorgängen von personenbezogenen Daten nicht gesondert eine Einwilligung erteilt werden kann, obwohl dies im Einzelfall angebracht ist".

Über die Anforderungen an die Bestimmtheit des „Verarbeitungsfalls" (Art. 4 Nr. 11 DS-GVO) und die Grenzen der Freiwilligkeit (Art. 7 Abs. 4 DS-GVO) hat der europäische Gesetzgeber dafür gesorgt, dass dem Interesse des Datensubjekts an einer Möglichkeit zur differenzierten Einwilligung spiegelbildliche Anforderungen an die Rechtmäßigkeit der Datenverarbeitung gegenüberstehen. Infolgedessen besteht zumindest ein Anreiz für den auf Rechtssicherheit bedachten Verantwortlichen, eine – soweit wie möglich – differenzierte Erteilung der Einwilligung zu ermöglichen. Dieser sog. Granularität der Einwilligung werden jedoch in zweifacher Hinsicht Grenzen gesetzt.

Erstens darf der Verantwortliche die Differenzierung nicht gezielt zulasten des Datensubjekts auf die Spitze treiben.[77] Auch insoweit ist der für Arzneimittel und Information gleichermaßen geltende Grundsatz zu beachten, dass die Dosis der Verabreichung über die heilende oder schädliche Wirkung entscheidet. Die Schwelle zum Gift hat die Ausdifferenzierung der Verarbeitungszwecke und -prozesse jedenfalls dann überschritten, wenn die Anzahl der zu aktivierenden Kästchen sehr hoch ist und der Verantwortliche dem Datensubjekt als vermeintliche Entlastung beispielsweise die Auswahl: „In alle einwilligen" anbietet und diese visuell auch noch besonders hervorhebt.

Zweitens müssen die Anforderungen an die Granularität insbesondere reduziert werden, sofern die Einwilligung gerade dazu dient, mit der Datenverarbeitung – auch privatwirtschaftlich organisierte und finanzierte – Forschungszwecke zu verfolgen. Forschung ist denknotwendig zukunftsoffen, so dass eine detaillierte Festlegung der Zwecke und Prozesse zu Beginn der Datenverarbeitung häufig weder möglich noch sinnvoll ist.[78] Dieser Gedanke ergibt sich bereits aus der Ausnahme vom Grundsatz der Zweckbindung im Fall einer Wei-

---

[75] *EuGH*, Urt. v. 01.10.2019, C-673/17 = GRUR 2019, 1198 Rn. 59 ff. – *Bundesverband/Planet49.*

[76] Ebenso: *Spindler/Dalby*, in: Spindler/Schuster (Hrsg.), Recht d. elektron. Medien, 4. Aufl. 2019, Art. 4 DS-GVO, Rn. 26.

[77] Zur Unzulässigkeit einer künstlichen Aufspaltung: *Klement*, in: Simitis/Hornung/Spiecker gen. Döhmann (Hrsg.), Datenschutzrecht, 2019, Art. 7, Rn. 6.

[78] Zur Zustimmung der DSK zum bundesweit einheitlichen Mustertext für die Patienteneinwilligung: *Ärzteblatt*, Bundesweite Patienteneinwilligung schafft Rechtssicherheit, 27.04.2020 (https://www.aerzteblatt.de/nachrichten/112355/Bundesweite-Patienteneinwilligung-schafft-Rechtssicherheit, zuletzt abgerufen am 19.05.2022); gleichwohl die Anforderungen an die Transparenz betonend: Beschluss der 97. Konferenz der DSK zur Auslegung des Begriffs „bestimmte Bereiche wissenschaftlicher Forschung" im Erwägungsgrund 33 der

terverarbeitung für wissenschaftliche Forschungszwecke gemäß Art. 5 Abs. 1 lit. b DS-GVO.

Nach Ansicht der *Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder* (DSK) folgt aus ErwG 33 S. 1 DS-GVO, dass eine breite Einwilligung (sog. *broad consent*) rechtmäßig sein kann, sofern

„das konkrete Design des Forschungsvorhabens absehbar bis zum Zeitpunkt der Datenerhebung eine vollständige Zweckbestimmung schlechthin nicht zulässt […]. Bei der einer Datenerhebung zeitlich vorgelagerten Einwilligung können dann unter engen Voraussetzungen Abstriche hinsichtlich der Bestimmtheit des Zwecks hingenommen werden".[79]

Die aufsichtsbehördliche und gerichtliche Anerkennung eines reduzierten Maßstabs an die Differenziertheit der Einwilligung im Bereich der Forschung überzeugt insbesondere deshalb, weil diese durch geeignete technische und organisatorische Maßnahmen (TOM) flankiert werden kann. Diese können die vorübergehend (zu) geringe Ausdifferenzierung der Einwilligung kompensieren und gewährleisten, dass die Interessen der Datensubjekte gewahrt bleiben.[80]

Die Kombination aus einer sog. breiten Einwilligung mit einem *Kontroll-Cockpit* bietet den zusätzlichen Vorteil, dass diese breite Einwilligung mit Hilfe des *Kontroll-Cockpits* leichter aktualisiert und konkretisiert werden kann sobald eine solche Spezifizierung der Verarbeitungszwecke möglich ist. Der Grundsatz der Datenverarbeitung nach Treu und Glauben und der Grundsatz der Transparenz gemäß Art. 5 Abs. 1 lit. a Var. 2 bzw. Var. 3 DS-GVO gebieten es, dass eine Datenverarbeitung zu Forschungszwecken nur solange auf eine sog. breite Einwilligung gestützt werden kann, bis deren Konkretisierung möglich ist. Diese Begrenzung setzt einen zusätzlichen Anreiz dafür, ein *Kontroll-Cockpit* einzurichten, das den Kontakt zwischen Verantwortlichen und Datensubjekten erleichtert und eine effektive und effiziente Anpassung der Einwilligung ermöglicht. Selbstverständlich bietet sich die Implementierung eines *Kontroll-Cockpits* auch jenseits der wissenschaftlichen Forschung an, sofern die tatsächliche Dynamik der Datenverarbeitung mit den rechtlichen Anforderungen an eine differenzierte Einwilligung synchronisiert werden soll.

cc) Ausdrücklichkeit der Einwilligung

Weil die Erteilung der Einwilligung durch das Datensubjekt eine den Verantwortlichen begünstigende Tatsache ist, trägt er hierfür die Beweislast. Zudem

---

DS-GVO, 03.04.2019 (https://www.datenschutzkonferenz-online.de/media/dskb/20190405_auslegung_bestimmte_bereiche_wiss_forschung.pdf, zuletzt abgerufen am 19.05.2022).

[79] *DSK*, Beschluss der 97. DSK zu Auslegung des Begriffs „bestimmte Bereiche wissenschaftlicher Forschung" im Erwägungsgrund 33 der DS-GVO, 03.04.2019, S. 1 (https://www.datenschutzkonferenz-online.de/media/dskb/20190405_auslegung_bestimmte_bereiche_wiss_forschung.pdf, zuletzt abgerufen am 19.05.2022).

[80] Hierzu bereits oben: Kapitel 4 A.II.2.

setzt die Informiertheit der Einwilligung voraus, dass die Einwilligung in einer für das Datensubjekt transparenten Weise eingeholt wird. Obwohl für das Erfordernis der „eindeutigen bestätigenden Handlung" auch eine konkludente Einwilligung ausreicht,[81] dürfte diese tatsächlich an Bedeutung verlieren. Jedenfalls in der virtuellen Umgebung setzen Verantwortliche regelmäßig auf eine ausdrückliche und leicht zu protokollierende Einwilligung, selbst wenn diese rechtlich nicht erforderlich ist.[82]

Die Implementierung eines standardisierten *Kontroll-Cockpits* hat aus Sicht des Verantwortlichen nicht nur den Vorteil einer einheitlichen technischen Protokollierung der Einwilligungserteilung. Vielmehr ermöglicht es dem Verantwortlichen, die Einwilligung stets ausdrücklich einzuholen und so die im Detail häufig schwierigen Abgrenzungen zu vermeiden, ob eine konkludente Einwilligung ausreicht oder eine ausdrückliche Einwilligung erforderlich ist. Diese Abgrenzungsschwierigkeiten ergeben sich insbesondere dann, wenn eine ausdrückliche Einwilligung gemäß Art. 9 Abs. 2 lit. a DS-GVO erforderlich sein könnte, weil potenziell auch besonders sensible personenbezogene Daten verarbeitet werden,[83] die Datenverarbeitung einer automatisierten Entscheidung, einschließlich Profiling, dient (Art. 22 Abs. 2 lit. c DS-GVO, Art. 20 Abs. 1 lit. a DS-GVO)[84] oder die Daten in einen Drittstaat übermittelt werden (Art. 49 Abs. 1 S. 1 lit. a DS-GVO).

Sofern der Verantwortliche es nicht (ausschließlich) selbst in der Hand hat, welche Kategorie von personenbezogenen Daten verarbeitet wird, beispielsweise weil dies von den Eingaben oder dem tatsächlichen (Online-)Verhalten des Datensubjekts abhängig ist,[85] wird er stets eine ausdrückliche Einwilligung verlangen, zumal an diese gerade keine besonders hohen Anforderungen gestellt werden. Das Aktivieren eines Einwilligungskästchens durch das Datensubjekt genügt.[86] Insbesondere ist kein sog. *Double Opt-In* Verfahren erforderlich, wenngleich dieses aus Sicht des Verantwortlichen den Nachweis erleichtert,

---

[81] Einem Schweigen des Datensubjekts kann kein Erklärungswert beigemessen werden: ErwG 32 S. 3 DS-GVO.

[82] Sofern sich ein Verantwortlicher im virtuellen Kontext auf eine konkludente Einwilligung beruft, legt das mittlerweile die intuitive – nicht rechtliche – Vermutung nahe, dass der Verantwortliche bei der Konstruktion des ursprünglichen Einwilligungsmechanismus technische Fehler gemacht hat oder die Protokollierung der Einwilligung misslungen ist.

[83] Zur bislang fehlenden klaren Abgrenzung: Vorlagefrage 2a des *OLG Düsseldorf*, Vorlagebeschl. v. 24.03.2021, Kart 2/19 (V), Rn. 43 ff.

[84] Hierzu: *Article 29-Group*, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679 (WP 251); *Gausling*, ZD 2019, 335 (338).

[85] Hierzu: Vorlagefrage 3 des *ÖOGH*, Vorlagebeschl. v. 22.07.2021, 6 Ob 56/21k – *Schrems* [*III*].

[86] ErwG 32 S. 2 DS-GVO. Insoweit vermittelt der *EDSA* einen falschen Eindruck, wenn er das „Ausfüllen eines elektronischen Formulars, Senden einer E-Mail, Hochladen eines eingescannten Dokuments, das von der betroffenen Person unterzeichnet wurde" oder das „Verwenden einer elektronischen Signatur" als Beispiele nennt: *EDSA*, Guidelines 05/2020 on consent under Regulation 2016/679, Version 1.1, 04.05.2020, No. 94 (https://edpb.europa.eu/

dass das Datensubjekt die Einwilligung erteilt hat oder sich diese jedenfalls zurechnen lassen muss, sofern es die Zugangsdaten zu der von ihm für das *Double Opt-In* Verfahren genutzten Kontaktmöglichkeit (insbesondere eMail-Zugang) weitergegeben hat.

Im Ergebnis fordert die DS-GVO zwar keinen Einsatz eines *Kontroll-Cockpits*, die Anforderungen an die Informiertheit und die Differenziertheit der Einwilligung und die Rechtsunsicherheit darüber, ob eine ausdrückliche Einwilligung erforderlich ist, setzen jedoch einen starken Anreiz für Verantwortliche, ein technisches System zu implementieren, mit dessen Hilfe die Einhaltung dieser drei Anforderungen an eine Einwilligung leicht nachgewiesen werden kann. Diese technischen Systeme lassen sich leicht in einem *Kontroll-Cockpit* umsetzen.

b) Einwilligungswiderruf

Die Einwilligung ist – nach der derzeit noch h. A. – jederzeit grundlos widerruflich und infolgedessen ein sehr instabiler Erlaubnistatbestand. Jedenfalls soweit eine Datenverarbeitung (ausschließlich) auf einer Einwilligung beruht,[87] ist es auch für den Verantwortlichen wichtig, die Anforderungen an die Widerruflichkeit konsequent umzusetzen, den Widerruf eindeutig zu protokollieren und unverzüglich die gesetzlich angeordneten Konsequenzen zu ziehen.

Mit der Implementierung eines *Kontroll-Cockpits* kann sichergestellt werden, dass der Widerruf der Einwilligung tatsächlich ebenso einfach möglich ist, wie die Erteilung der Einwilligung (aa). Darüber hinaus kann ein klar strukturiertes *Kontroll-Cockpit* – spiegelbildlich zur differenzierten Einwilligungserteilung – auch einen differenzierten Widerruf abbilden (bb). Zuletzt erleichtert es ein *Kontroll-Cockpit* dem Verantwortlichen, diejenigen Informationspflichten zu erfüllen, die durch einen Einwilligungswiderruf entstehen (cc).

aa) Einfachheit des Einwilligungswiderrufs

Gemäß Art. 7 Abs. 3 S. 4 DS-GVO muss der Widerruf der Einwilligung ebenso einfach möglich sein, wie deren ursprüngliche Erteilung. Wenn allein die Möglichkeit zum Einwilligungswiderruf ausreicht, um einen starken Anreiz zur Flucht aus der Einwilligung und in die anderen Erlaubnistatbestände zu setzen, so haben die Verantwortlichen erst recht kein Interesse daran, den Einwilligungswiderruf ebenso einfach zu ermöglichen, wie die ursprüngliche Einwilligungserteilung. Während die wirksame Einwilligung gegebenenfalls als Grundlage einer Datenverarbeitung notwendig ist und Verantwortliche sich

sites/edpb/files/files/file1/edpb_guidelines_202005_consent_en.pdf, zuletzt abgerufen am 19.05.2022).

[87] Zu den Folgen eines Einwilligungswiderrufs für den Widerspruch gemäß Art. 21 Abs. 1 DS-GVO sh. unten: 2.a.

deshalb frühzeitig um deren Erteilung durch das Datensubjekt bemühen, schwebt der freie Widerruf der Einwilligung wie ein Damoklesschwert über dem Verantwortlichen. Gerade deshalb ist es richtig, dass der europäische Gesetzgeber den Verantwortlichen gemäß Art. 7 Abs. 3 S. 4 DS-GVO dazu verpflichtet, den Einwilligungswiderruf ebenso einfach auszugestalten wie die ursprüngliche Einwilligungserteilung. Allerdings muss die Einhaltung dieser Pflicht durch Verantwortliche auch durch eine in dieser Hinsicht strengere Durchsetzung seitens der Datenschutzbehörden verbessert werden.

Viele Anbieter, die digitale Produkte im Austausch gegen eine Einwilligung in die Datenverarbeitung anbieten, setzen auf eine Gestaltung, die nicht von einer dauerhaften Einwilligung abhängig ist,[88] sondern – mittels Einwilligungsbanner – vor jeder Zugangseröffnung zu digitalen Produkten zu einer erneuten Einwilligung auffordert.[89] Infolge dieser wiederholten Aufforderung zur Einwilligungserteilung tritt das aus Art. 7 Abs. 3 S. 4 DS-GVO ableitbare Erfordernis, ein gleichermaßen ausgestaltetes Banner oder Pop-Up-Fenster mit der ausdrücklichen Option zum Widerruf vorzuhalten, in den Hintergrund.

Diese Strategie lässt sich als „eine Einwilligung für einen Inhalt" bezeichnen. Hiermit vermeiden Verantwortliche eine dauerhafte, aber widerrufliche Einwilligung und setzen stattdessen jeweils auf eine neue Einwilligung für jede erneute Bereitstellung eines digitalen Produkts oder jeden erneuten Besuch ihrer Webseite durch das Datensubjekt. Infolgedessen entstehen Ketten von Mikro-Transaktionen und diese technische Ausgestaltung verhindert, dass der Verantwortliche mit einem digitalen Produkt in Vorleistung gehen muss. Dennoch ändert diese Gestaltung nichts an der rechtlichen Pflicht, den Widerruf während der Nutzung der Webseite ebenso leicht ermöglich zu müssen, wie die ursprüngliche Erteilung. Bei einer strengen Auslegung von Art. 7 Abs. 3 S. 4 DS-GVO müsste ständig ein *Banner* oder *Pop-Up-Fenster* erscheinen, damit die hierin enthaltene Option zum Einwilligungswiderruf ebenso leicht möglich ist, wie die ursprüngliche Einwilligungserteilung, für die Anbieter von (online verfügbaren) digitalen Produkten regelmäßig diese beiden technischen Mittel verwenden.

Ein solches spiegelbildliches Vorgehen wäre auch für Datensubjekte sehr lästig. Deshalb sollte es nach hier vertretener Auffassung für eine Einhaltung von Art. 7 Abs. 3 S. 4 DS-GVO ausreichen, wenn das Angebot von digitalen Produkten – im Fall einer einwilligungsbasierten Nutzung – auf jeder Unterseite des Nutzungskontos oder der Webseite und jeweils im selben Bereich der jewei-

---

[88] Vorrangiger Grund für diese Gestaltung ist jedoch die rechtssichere Wahrung der Freiwilligkeit der Einwilligung gemäß Art. 7 Abs. 4 DS-GVO, weil der Zugang zu digitalen Inhalten regelmäßig nicht von der Einwilligung abhängig gemacht wird, durch die Notwenigkeit, diese Einwilligung jedoch ständig zu erneuern, ein Anreiz für die Datensubjekte entsteht, in die gewünschte Datenverarbeitung einzuwilligen.

[89] Diese Ausgestaltung in eine Kette von jeweils kleinen Transaktionen zwingt die Datensubjekte in Vorleistung, hierzu oben Kapitel 4 A.II.5.

ligen Unterseite eine einheitliche Schaltfläche – unter Verwendung eines europaweit standardisierten Bildsymbols i. S. d. Art. 12 Abs. 7 DS-GVO – anbietet. Über diese muss der Einwilligungswiderruf unmittelbar erreichbar sein, so dass der Widerruf der Einwilligung durch ein (weiteres) Klicken erklärt werden kann (sog. *kill switch*).[90] Diese Option lässt sich ebenfalls sinnvoll mit einem *Kontroll-Cockpit* kombinieren.

Mit dieser Option ist der Widerruf der Einwilligung zwar streng genommen nicht „ebenso einfach", wie deren ursprüngliche Erteilung. Dennoch ermöglicht diese Ausgestaltung eine einfache und praktikable Möglichkeit zum Widerruf. Auch verwirklicht ein solcher einheitlicher, leicht auffindbarer und unmittelbar zugänglicher Pfad zur Widerrufserklärung noch nicht den Anspruch, der an eine Lösung im Sinne einer *Single-Click-Privacy* befürwortet wird.[91] Dennoch ermöglicht diese Option eine sehr einfache und übersichtliche Ausübung von informationeller Privatautonomie. Zudem wäre das Angebot eines als *Single-Click-Privacy* bezeichneten Mechanismus im Zweifel seinerseits irreführend, weil ein solcher Mechanismus regelmäßig nicht dazu geeignet ist, jegliche Verarbeitung von personenbezogenen Daten zu beenden.[92]

bb) Differenziertheit des Einwilligungswiderrufs

Die Möglichkeit zu einem Widerruf der Einwilligung, der nach den Verarbeitungszwecken und Kategorien der personenbezogenen Daten differenziert, hat aus Sicht der Datensubjekte einen positiven Effekt auf ihre Wahlfreiheit und damit auf die informationelle Privatautonomie. Zudem würde der Wert von personenbezogenen Daten und ihr Verhältnis zu den im Austausch bereitgestellten Leistungen des Verantwortlichen zumindest ansatzweise transparent, sofern ein Verantwortlicher seine synallagmatische Leistung infolge eines teilweisen Widerrufs der Einwilligung seinerseits reduzieren kann oder eine Fortsetzung der bisherigen Leistungsbeziehung gegen eine gemischte Gegenleistung aus personenbezogenen Daten und monetärem Entgelt anbietet. Die Option eines differenzierten Widerrufs ermöglicht somit Preis-Signale,[93] die bei

---

[90] Mit diesem Vorschlag: *Becker*, JZ 2017, 171 (178); Aus Perspektive der Informatik: *Gray*, Future of Privacy Forum 2016, S. 9; *Zibuschka/Horsch/Kubach*, Open Identity Summit 2019, S. 119 (126).

[91] Hierzu: *Stiftung Datenschutz*, Neue Wege bei der Einwilligung im Datenschutz – technische, rechtliche und ökonomische Herausforderungen, 2017, S. 36; sowie mit dem Versuch einer Umsetzung: *PlusPrivacy*, PlusPrivacy adds management of Google privacy, v. 22.02.2018 (https://plusprivacy.com/2018/02/22/plusprivacy-adds-automatic-management-of-google-privacy-settings/, zuletzt abgerufen am 19.05.2022).

[92] Auch nach Widerruf der Einwilligung bleibt eine rechtmäßige Datenverarbeitung auf Grundlage eines anderen Erlaubnistatbestands möglich, vgl. Art. 17 Abs. 1 lit. b a. E. DS-GVO.

[93] Indem Art. 14 Abs. 4 DID-RL kein Minderungsrecht zugunsten von Verbrauchern vorsieht, sofern diese für den Zugang zu nicht vertragsgemäß bereitgestellten digitalen Produkten keinen Preis in Geld bezahlt haben, bewahrt der europäische Gesetzgeber die Gerichte

einem vollständigen Widerruf nicht entstehen, weil dieser regelmäßig die Leistungsbeziehung beendet.

Auch aus Sicht der Verantwortlichen kann die Möglichkeit zum differenzierten Widerruf sinnvoll sein, sofern die Aufrechterhaltung der Leistungsbeziehung aus Sicht des Verantwortlichen trotz einer Reduktion der Verarbeitungszwecke oder des Verarbeitungsumfangs besser ist, als die vollständige Beendigung der Datenverarbeitung. Zudem ist eine vollständige Beendigung der Austauschbeziehung infolge eines Einwilligungswiderrufs für den Verantwortlichen im B2C-Verhältnis mit erheblichen Unwägbarkeiten verbunden, weil der Verantwortliche gemäß § 327q Abs. 2 BGB[94] seine Leistungserbringung nur dann einstellen kann, wenn ihm unter Berücksichtigung des weiterhin zulässigen Umfangs der Datenverarbeitung und unter Abwägung der beiderseitigen Interessen die Fortsetzung des Vertragsverhältnisses bis zum vereinbarten Vertragsende oder bis zum Ablauf einer gesetzlichen oder vertraglichen Kündigungsfrist nicht zugemutet werden kann.

Darüber hinaus spiegelt die differenzierte Widerruflichkeit die Granularität der Einwilligungserteilung[95] und ist somit – bei mehrstufiger und übersichtlicher Ausgestaltung – ein Indiz dafür, dass der Verantwortliche sich um eine transparente Datenverarbeitung bemüht.

Weil ein differenzierter Widerruf der Einwilligung als *zusätzliche* Option zum Widerruf der gesamten Einwilligung(en) aus Sicht der Datensubjekte lediglich vorteilhaft ist, hat diese auch keinen negativen Einfluss auf die Freiwilligkeit der ursprünglichen Einwilligung. Diesen Konnex zwischen der Freiwilligkeit der Einwilligung und der Widerruflichkeit der Einwilligung stellt ErwG 42 S. 5 DS-GVO ausdrücklich her.[96]

Die Wirkung der hier vertretenen *kartellrechtsakzessorischen*, *asymmetrischen* Anwendung von Art. 7 Abs. 4 DS-GVO[97] ließe sich nochmals verstärken, sofern die Einwilligung gegenüber einem marktmächtigen Verantwortlichen nur dann freiwillig ist, wenn dieser Verantwortliche anschließend nicht nur einen vollständigen Widerruf der Einwilligung ermöglicht, sondern auch einen differenzierten Widerruf in Kombination mit einer angemessenen monetären Zahlungsoption für den Teil zulässt, der von dem Widerruf der Einwilligung umfasst ist.

---

davor, den Wert personenbezogener Daten monetär beziffern zu müssen. Hierzu bereits oben: Kapitel 3 C.II.5.

[94] Gesetz zur Umsetzung der Richtlinie über bestimmte vertragsrechtliche Aspekte der Bereitstellung digitaler Inhalte und digitaler Dienstleistungen, v. 25.06.2021, BGBl. v. 30.06.2021, Teil I Nr. 37, S. 2123 (2128).

[95] Oben: B.I.1.a.bb.

[96] Hiernach sollte nur dann davon „ausgegangen werden, dass [ein Datensubjekt seine] Einwilligung freiwillig gegeben hat, wenn [es] eine echte oder freie Wahl hat und somit in der Lage ist, die Einwilligung zu verweigern *oder zurückzuziehen*, ohne Nachteile zu erleiden" [Hervorhebung durch den Verfasser]. Hierzu oben: Kapitel 4 A.II.5.

[97] Oben Kapitel 5 C.II.1.c.cc.

Diese spiegelbildliche Berücksichtigung würde dafür sorgen, dass im Verhältnis zu einem marktmächtigen Verantwortlichen nicht nur die Wahlfreiheit bei Erteilung der Einwilligung abgestützt wird, sondern auch die Freiheit des Datensubjekts, das Austauschverhältnis zu diesem marktmächtigen Verantwortlichen zu einem späteren Zeitpunkt nicht nur vollständig zu beenden, sondern auch umgestalten zu können.

cc) Informationspflichten nach Einwilligungswiderruf

Auch im Anschluss an einen Widerruf der Einwilligung können Informationspflichten des Verantwortlichen bestehen, die sich über ein *Kontroll-Cockpit* leichter erfüllen lassen. Obwohl die DS-GVO keine ausdrücklichen Informationspflichten an den Widerruf einer Einwilligung knüpft, ist es wahrscheinlich, dass die Gerichte anhand der allgemeinen Grundsätze der rechtmäßigen Datenverarbeitung, insbesondere aus dem Grundsatz der Transparenz, weitere Informationspflichten ableiten werden.

Beispielsweise sollte über den Anspruch auf Löschung (Art. 17 DS-GVO) und auf Datenportabilität (Art. 20 DS-GVO) nach einem Einwilligungswiderruf nochmals informiert werden. Eine solche erneute Informationspflicht legt Art. 12 Abs. 2 S. 1 DS-GVO nahe, wonach der Verantwortliche dem Datensubjekt die Ausübung seiner Rechte erleichtern soll. Eine solche Informationspflicht sollte jedenfalls bestehen, sofern diese erneute Information über die Rechte des Datensubjekts aus Art. 17 und Art. 20 DS-GVO für den Verantwortlichen ohne unangemessenen Aufwand möglich ist. Insbesondere im Kontext einer Bereitstellung von digitalen Produkten ist eine solche Wiederholung anlässlich eines Einwilligungswiderrufs regelmäßig leicht möglich, weil der Kontakt zwischen Datensubjekt und Verantwortlichem zumeist ausschließlich auf Wegen der elektronischen Kommunikation stattfindet.

Eine weitere Informationspflicht trifft den Verantwortlichen nach hier vertretener Ansicht dann, wenn er eine Datenverarbeitung nach Einwilligungswiderruf auf Grundlage einer Interessenabwägung fortsetzt, obwohl diese Datenverarbeitung ursprünglich zumindest auch auf Grundlage der Einwilligung durchgeführt wurde. Obwohl ein solcher Wechsel von der Einwilligung auf einen anderen Erlaubnistatbeständen von Art. 17 Abs. 1 lit. b DS-GVO ausdrücklich vorgesehen ist, lässt die DS-GVO offen, welche Informationspflichten ein solcher Wechsel für den Verantwortlichen auslöst. Weil zudem die Abgrenzung zwischen einem Einwilligungswiderruf und einem Widerspruch gegen eine Datenverarbeitung, die bis zu diesem Zeitpunkt auf Grundlage einer Interessenabwägung erfolgte, schwierig sein kann, wird diese Thematik sogleich im Kontext des Widerspruchs nochmals,[98] nun mit Blick auf die praktische Umsetzung, vertieft.

[98] Hierzu auch bereits oben Kapitel 2 A.IV.2.

2. Widerspruch gegen die Datenverarbeitung, Art. 21 DS-GVO

Neben der Erteilung und dem Widerruf der Einwilligung ist der Widerspruch gegen eine Datenverarbeitung, die auf Grundlage einer Interessenabwägung erfolgt, die dritte wesentliche Erklärung von Datensubjekten, die in einem *Kontroll-Cockpit* sinnvoll implementiert werden kann. Abhängig vom jeweiligen Zweck der Datenverarbeitung differenziert Art. 21 DS-GVO zwischen zwei Varianten des Widerspruchs.

Sowohl aus Sicht des Datensubjekts als auch aus Perspektive des Verantwortlichen ist der Widerspruch gegen eine Datenverarbeitung zu Zwecken der Direktwerbung, einschließlich eines hiermit in Verbindung stehenden Profiling, leicht zu handhaben. Hiergegen kann das Datensubjekt gemäß Art. 21 Abs. 2 DS-GVO jederzeit und ohne Angabe von Gründen Widerspruch „einlegen".[99] Diese Variante des Art. 21 DS-GVO kann deshalb als *freier Widerspruch* bezeichnet werden.

Komplexer ist die Situation, sofern die Datenverarbeitung auf Grundlage einer Interessenabwägung zu anderen Zwecken als einer Direktwerbung erfolgt. In diesem Fall hat das Datensubjekt zwar das Recht, der Datenverarbeitung jederzeit zu widersprechen. Dieser Widerspruch muss jedoch gemäß Art. 21 Abs. 1 S. 1 DS-GVO aus Gründen erfolgen, die sich aus der besonderen Situation des Datensubjekts ergeben (*begründeter Widerspruch*).

Trotz eines begründeten Widerspruchs darf der Verantwortliche die Datenverarbeitung fortsetzen, sofern eine der gesetzlichen Gegenausnahmen greift. Dies ist gemäß Art. 21 Abs. 1 S. 2 DS-GVO der Fall, soweit der Verantwortliche zwingend schutzwürdige Gründe für die Verarbeitung nachweisen kann und diese gegenüber den Interessen, Rechten und Freiheiten des Datensubjekts überwiegen oder soweit die Datenverarbeitung der Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen dient. Gemäß Art. 21 Abs. 6 DS-GVO ist die Fortsetzung der Datenverarbeitung rechtmäßig, soweit diese wissenschaftlichen oder historischen Forschungszwecken dient oder zu statistischen Zwecken erfolgt und zur Erfüllung einer im öffentlichen Interesse liegenden Aufgabe erforderlich ist.

Obwohl aus Art. 21 DS-GVO keine Pflicht zur Implementierung eines *Kontroll-Cockpits* abgeleitet werden kann, setzt das mehrstufige Verfahren aus Widerspruchserklärung (a), Widerspruchsbegründung (b), Identifikation gegenläufiger Interessen, qualifizierter Interessenabwägung und anschließender Informationspflicht (c) über die Fortsetzung der Datenverarbeitung und die

[99] Diese Wortwahl in Art. 21 Abs. 2 DS-GVO ist unpassend, weil der Widerspruch gegenüber einem Privatrechtssubjekt erklärt wird. Ein echtes „Einlegen" eines Widerspruch kommt nicht in Betracht, weil Behörden sich bei der Datenverarbeitung nicht auf die Interessenabwägung i. S. d. Art. 6 Abs. 1 lit. f DS-GVO berufen können, Art. 6 Abs. 1 S. 2 DS-GVO.

hierfür herangezogene Rechtsgrundlage[100] einen starken Anreiz dafür, ein solches *Kontroll-Cockpit* zu implementieren.

Der Widerspruch des Datensubjekts löst eine mehrfache Kommunikation zwischen Datensubjekt und Verantwortlichem aus, die mit Hilfe eines *Kontroll-Cockpits* strukturiert und damit effizient ausgestaltet werden kann.

a) Widerspruchserklärung

Mit der Erklärung des Widerspruchs gemäß Art. 21 Abs. 1 S. 1 DS-GVO stellt das Datensubjekt seine Entscheidungszuständigkeit erstmals her, soweit personenbezogene Daten bislang auf Grundlage einer Interessenabwägung gemäß Art. 6 Abs. 1 lit. f DS-GVO verarbeitet wurden.[101] Die DS-GVO enthält mit Blick auf das Widerspruchsrecht des Datensubjekts mehrere Ansätze, die für die Implementierung eines *Kontroll-Cockpits* sprechen, ohne dass hieraus – im Grundsatz[102] – eine Implementierungspflicht des Verantwortlichen abzuleiten ist.

Gemäß Art. 21 Abs. 5 DS-GVO kann das Datensubjekt sein Widerspruchsrecht zwar mittels automatisierter Verfahren ausüben. Zudem ist der Verantwortliche gemäß Art. 12 Abs. 2 S. 1 DS-GVO immerhin dazu verpflichtet, dem Datensubjekt die Ausübung eines Widerspruchsrechts zu erleichtern. Dennoch dürfte der Anwendungsbereich von Art. 21 Abs. 5 DS-GVO vorrangig Sachverhalte betreffen, in denen ein Datensubjekt durch Auswahl der Browser-Einstellung („*do not track*“ oder „*browse in private*“) einen generellen und nicht zu begründenden Widerspruch gegen Datenverarbeitung zu Zwecken der Direktwerbung erklärt, Art. 21 Abs. 2 DS-GVO.[103] Art. 21 Abs. 5 DS-GVO eröffnet dem Datensubjekt lediglich die Möglichkeit zur Wahl eines automatisierten Verfahrens. Infolgedessen muss der Verantwortliche diese automatisierte Widerspruchserklärung jedoch allenfalls akzeptieren und einen Zugang für solche Erklärungen ermöglichen. Dagegen konstituiert Art. 21 Abs. 5 DS-GVO keine Pflicht des Verantwortlichen, seinerseits ein eigenes, automatisiertes Verfahren für Widersprüche zur Verfügung zu stellen. Dennoch setzen Art. 21 Abs. 5 DS-

---

[100] In Betracht kommen: Art. 13 Abs. 1 lit. c und lit. d DS-GVO, Art. 14 Abs. 1 lit. c und Abs. 2 lit. b DS-GVO.

[101] Oben Kapitel 2 A.IV.1.

[102] Es liegt jedoch nahe, über eine solche Pflicht zur Einführung eines *Kontroll-Cockpit* für marktmächtige Verantwortlichen bzw. einen Gatekeeper nachzudenken, sofern erste, positive Erfahrungen mit *Kontroll-Cockpit* gemacht wurden und, sofern infolgedessen Klarheit über dessen notwendige Mindestfunktionen besteht.

[103] Weil ein Widerspruch gegen eine Datenverarbeitung zu anderen Zwecken als Direktwerbung gemäß Art. 21 Abs. 1 S. 1 DS-GVO Gründe voraussetzt, die sich aus der besonderen Situation des Datensubjekts ergeben, ist zweifelhaft, ob die Auswahl eines Modus wie „do not track“ ausreicht, um diesen als (begründeten) Widerspruch gegen eine Datenverarbeitung auf Grundlage von Art. 6 Abs. 1 lit. f DS-GVO zu werten. Sofern diese Möglichkeit zum Schutz von Datensubjekten gewünscht ist, sollte sie deshalb ausdrücklich in der ePrivacy-VO geregelt werden.

GVO und Art 12 Abs. 2 S. 1 DS-GVO starke Anreize dafür, dass Verantwortliche selbst ein *Kontroll-Cockpit* anbieten, um die Modalitäten dieser erleichterten Widerspruchserklärungen selbst zu gestalten und über eigene Schnittstellen technisch an ihre IT-Systeme anzubinden.

Einen weiteren indirekten Anreiz für eine Implementierung eines *Kontroll-Cockpits* setzt Art. 21 DS-GVO indem er eine schwierige, aber zentrale Frage im Kontext der Widerspruchserklärung unbeantwortet lässt. Die für den Widerspruch erforderliche Erklärung berührt zwei wichtige Schnittstellen der DS-GVO. *Erstens* existieren Überscheidungsbereiche mit der Erklärung eines Einwilligungswiderruf. *Zweitens* bestehen Überscheidungen zwischen der Widerspruchserklärung und der Widerspruchsbegründung gemäß Art. 21 Abs. 1 S. 1 DS-GVO (unten: b). Überlässt ein Verantwortlicher den Datensubjekten die Formulierung ihrer (Beendigungs-)Erklärung, so stellt sich – unabhängig von der Auslegung dieser Erklärung – die komplexe Anschlussfrage, welche Folgen diese Erklärung hat.

Ursprung dieser Schwierigkeit ist der Wortlaut von Art. 17 Abs. 1 lit. b a. E. i. V. m. Art. 6 Abs. 1 lit. f DS-GVO. Hiernach hat der Verantwortliche die personenbezogenen Daten nur zu löschen, soweit das Datensubjekt seine Einwilligung widerruft und soweit es „an einer anderweitigen Rechtsgrundlage für die Verarbeitung [fehlt]". Diese Formulierung legt nahe, dass eine generische Beendigungserklärung, ebenso wie eine als „Einwilligungswiderruf" bezeichnete Erklärung, die Folgen für eine Datenverarbeitung auf Grundlage einer Interessenabwägung grundsätzlich unberührt lässt. Hierfür spricht zudem, dass der Widerspruch im Gegensatz zum Einwilligungswiderruf – abgesehen von Art. 21 Abs. 2 DS-GVO – nicht „frei", sondern nur qualifiziert erfolgen kann. Der Widerspruch eines Datensubjekts setzt gerade Gründe voraus, die sich aus seiner besonderen Situation ergeben, Art. 21 Abs. 1 S. 1 DS-GVO.

Allerdings ist eine solche Lösung, wonach der Einwilligungswiderruf keine Auswirkungen auf eine fortgesetzte Datenverarbeitung auf Grundlage von Art. 6 Abs. 1 lit. f DS-GVO hat, jedenfalls dann kritikwürdig, wenn der Verantwortliche ursprünglich deshalb eine Einwilligung eingeholt hatte, um dem Datensubjekt dessen Kontrolle über die Datenverarbeitung zu suggerieren oder – wahrscheinlicher – um sich selbst rechtlich gegen die Unbestimmtheit der Erlaubnistatbestände und die infolgedessen bestehende Rechtsunsicherheit einer Datenverarbeitung auf Grundlage einer Interessenabwägung i. S. d. Art. 6 Abs. 1 lit. f DS-GVO abzusichern. In diesem Fall liegt es nahe, dass jedenfalls ein bruch- und lautloses „Auswechseln" der widerrufenen Einwilligung durch den Erlaubnistatbestand der Interessenabwägung für die identische Datenverarbeitung verhindert werden sollte.

Hierfür bestehen drei Optionen. Diesen Optionen ist zunächst gemeinsam, dass eine (Beendigungs-)Erklärung des Datensubjekts nicht nur als Einwilligungswiderruf (Art. 7 Abs. 3 S. 1 DS-GVO), sondern zugleich als konkludenter

Widerspruch i. S. d. Art. 21 Abs. 1 S. 1 DS-GVO ausgelegt werden kann. Diese Auslegung ist jedenfalls überzeugend, sofern die ursprüngliche Einholung einer Einwilligung dem Datensubjekt die Kontrolle über die Datenverarbeitung suggeriert hat oder der Verantwortliche die Einwilligung als Reserve- und Sicherheits-Erlaubnistatbestand eingeholt hat. Abgesehen von dieser Auslegung einer Beendigungserklärung als konkludente Widerspruchserklärung unterscheiden sich die drei Optionen jedoch:

Erstens könnte Art. 21 Abs. 1 S. 1 DS-GVO in dieser besonderen Konstellation teleologisch reduziert werden, so dass der konkludente Widerspruch auch ohne eine Angabe von solchen Gründen wirksam ist, die sich aus der besonderen Situation des Datensubjekts ergeben.[104]

Zweitens könnte aus Art. 21 Abs. 1 S. 1 DS-GVO i. V. m. Art. 5 Abs. 1 lit. a Var. 2 DS-GVO (Grundsatz der Verarbeitung nach Treu und Glauben) eine Pflicht des Verantwortlichen abgeleitet werden, das Datensubjekt unverzüglich und ausdrücklich zur Angabe von solchen Gründen aufzufordern, die sich aus der besonderen Situation des Datensubjekts ergeben.[105] Bis zu dieser Begründung des Widerspruchs gemäß Art. 21 Abs. 1 S. 1 DS-GVO durch das Datensubjekt wäre der konkludente Widerspruch des Datensubjekts schwebend unwirksam.[106] Läuft die angemessene Frist ab, ohne dass das Datensubjekt eine Begründung des Widerspruchs nachschiebt, so entfällt auch die Wertung der Beendigungserklärung als konkludente Widerspruchserklärung.

Drittens könnte aus Art. 21 Abs. 1 S. 1 DS-GVO i. V. m. Art. 5 Abs. 1 lit. a Var. 3 DS-GVO (Grundsatz der Transparenz) lediglich eine Pflicht des Verantwortlichen abgeleitet werden, das Datensubjekt nochmals und qualifiziert über sein Recht zum Widerspruch i. S. d. Art. 21 Abs. 4 DS-GVO zu informieren.

Nach hier vertretener Ansicht erscheint die letztgenannte Lösung der erneuten Informationspflicht des Verantwortlichen angemessen. Gegen die erste Lösung einer teleologischen Reduktion des Begründungserfordernisses spricht, dass die Verantwortlichen – auch mangels klarer gesetzlicher oder gerichtlicher Abgrenzung zwischen den Erlaubnistatbeständen – in einer unüberschaubaren Anzahl oder sogar in der Mehrzahl der Datenverarbeitungen sowohl auf eine Einwilligung als auch eine Interessenabwägung setzen.[107] Infolgedessen besteht

---

[104] Tatsächlich sehen viele Anbieter digitaler Produkte die Möglichkeit vor, einer Datenverarbeitung auf Grundlage von „legitimen Interessen" einzeln oder insgesamt zu widersprechen, ohne dass dafür eine Begründung des Datensubjekts vorausgesetzt wird. Häufig handelt es sich bei diesen „legitimen Interessen" jedoch um Fälle der Direktwerbung, so dass dieser Widerspruch gemäß Art. 21 Abs. 2 DS-GVO ohnehin grundlos möglich ist.

[105] Diese Aufforderung darf allerdings nur erfolgen, soweit die Datenverarbeitung nicht der Direktwerbung dient. Gegen letztere kann „frei", also unbegründet widersprochen werden, Art. 21 Abs. 2 DS-GVO.

[106] Er wäre wirksam, soweit die Interessenabwägung einer Direktwerbung i. S. d. Art. 21 Abs. 2 DS-GVO diente, weil der Widerspruch insoweit keine Begründung voraussetzt.

[107] *Metzger*, GRUR 2019, 129 (133 f.).

die Gefahr, dass eine teleologische Reduktion des Begründungserfordernisses aus Art. 21 Abs. 1 S. 1 DS-GVO keine enge Ausnahme, sondern der Regelfall würde. Die Vorschrift liefe weitgehend leer, wenn Art. 21 Abs. 1 S. 1 DS-GVO in allen Fällen, in denen der Verantwortliche auch eine Einwilligung eingeholt hat, teleologisch reduziert wird. Diese Umkehrung des Regel-Ausnahme-Verhältnisses ist mit dem Wortlaut von Art. 21 Abs. 1 S. 1 DS-GVO nicht vereinbar. Auch der systematische Vergleich zwischen Art. 21 Abs. 1 (Begründungspflicht) und Art. 21 Abs. 2 S. 1 DS-GVO (freier Widerspruch) spricht gegen eine teleologische Reduktion von Art. 21 Abs. 1 S. 1, weil die Möglichkeit eines unbegründeten Widerspruchs nur im Fall der Direktwerbung vom Gesetzgeber gewollt war.

Gegen die zweite Option, also eine Pflicht des Verantwortlichen, das Datensubjekt aufzufordern, den (potentiellen) Widerspruch binnen einer angemessenen Frist zu begründen, spricht, dass die mit dieser Lösung einhergehende Rechtsunsicherheit über den angemessenen Zeitraum der Frist einseitig zulasten des Verantwortlichen ginge. Deshalb ist es nach hier vertretener Ansicht ausreichend, wenn der Verantwortliche, das Datensubjekt im Fall eines Einwilligungswiderrufs oder einer neutralen Beendigungserklärung nochmals und qualifiziert gemäß Art. 21 Abs. 4 DS-GVO über sein Recht zum Widerspruch informiert.

Für Verantwortliche, die einen transparenten und umfangreichen Datenschutz als positives Merkmal ihrer Produkte herausstellen wollen (sog. *competition for privacy*), setzt diese Lösung einen zweifachen Anreiz, ein *Kontroll-Cockpit* zu implementieren.

Erstens kann in einem durch den Verantwortlichen programmierten *Kontroll-Cockpit* eine eindeutige Auswahl angeboten werden, ob ein Datensubjekt den Widerruf der Einwilligung, den freien Widerspruch gemäß Art. 21 Abs. 2 DS-GVO, den zu begründenden Widerspruch gemäß Art. 21 Abs. 1 S. 1 DS-GVO oder alle drei zugleich erklären möchte. Sofern die freie Widerruflichkeit der Einwilligung zwischen Verantwortlichem und Datensubjekt befristet ausgeschlossen wurde,[108] sollte als vierte Option der außerordentliche Widerruf der Einwilligung aus wichtigem Grund vorgesehen werden,[109] wobei letzterer stets auch als Widerspruch i. S. d. Art. 21 Abs. 1 S. 1 DS-GVO auszulegen ist und regelmäßig dessen Hürde der „besonderen Situation" nehmen wird. Infolgedessen können die Erklärungen der Datensubjekte nicht nur transparent unterschieden werden. Vielmehr können, abhängig von der getroffenen Auswahl des Datensubjekts, die Gründe für diese Erklärung automatisiert abgefragt werden (dazu sogleich).

Zweitens ist die Implementierung eines *Kontroll-Cockpits* für den Verantwortlichen attraktiv, weil dadurch die Erfüllung der (nochmaligen) Informationspflicht erleichtert bzw. sogar automatisiert und zugleich protokolliert werden kann.

---

[108] Oben: Kapitel 5 C.III.2.b.
[109] Oben: Kapitel 5 C.III.3.d.

b) Begründung des Widerspruchs

Weil der begründete Widerspruch gemäß Art. 21 Abs. 1 S. 1 DS-GVO – im Gegensatz zur freien Widerruflichkeit gemäß Art. 7 Abs. 3 S. 1 DS-GVO – Gründe voraussetzt, die sich aus der besonderen Situation des Datensubjekts ergeben, hat ein *Kontroll-Cockpit* wesentliche Vorteile für Datensubjekte und für solche Verantwortlichen, denen eine effektive und rechtssichere Einhaltung datenschutzrechtlicher Anforderungen wichtig ist. Bislang ist umstritten, welche Anforderungen an die Begründung eines Widerspruchs mit der besonderen Situation des Datensubjekts zu stellen sind.

Einerseits wird vertreten, dass diese Formulierung lediglich „als eine rein prozessuale Vorgabe verstanden werden" müsse,[110] die im Ergebnis nur zur Folge habe, dass den Verantwortlichen die Argumentationslast dafür trifft, zwingend schutzwürdige Gründe für eine Fortsetzung der Datenverarbeitung darzulegen.[111] *Andererseits* wird diese Anforderung dahingehen verstanden, dass eine „atypische Konstellation besonders schutzwürdiger besonderer persönlicher Interessen" vorauszusetzen sei.[112]

Ohne dass es auf diesen Streit im Kontext einer Einführung von *Kontroll-Cockpits* ankommt, wird bereits aus dem Wortlaut deutlich, dass die Begründung des Widerspruchs nicht lediglich eine prozessuale Frage der Argumentationslast sein kann. Ginge es nur um die Erhöhung der Argumentationslast, so hätte auch ein unbegründeter Widerspruch, jedenfalls aber ein – irgendwie – begründeter Widerspruch ausgereicht und die Spezifizierung durch den Bezug auf die „besondere Situation" des Datensubjekts wäre in diesem Fall überflüssig. Eindeutig ist aber auch, dass mit der besonderen Situation des Datensubjekts nicht nur Sachverhalte gemeint sein können, die im Zusammenhang mit besonders sensiblen personenbezogenen Daten i. S. d. Art. 9 Abs. 1 DS-GVO stehen. Ein derartiges Verständnis hätte die absurde Folge, dass der Verantwortliche die Begründung des Widerspruchs des Datensubjekts möglicherweise nur überprüfen könnte, wenn das Datensubjekt zuvor einwilligt; eine Verarbeitung von besonders sensiblen personenbezogenen Daten ist *de lege lata* nur auf Grundlage einer Einwilligung (Art. 9 Abs. 2 lit. a DS-GVO) rechtmäßig oder soweit diese Verarbeitung zur Ausübung von Rechtsansprüchen gemäß Art. 9 Abs. 2 lit. f DS-GVO erforderlich ist. In beiden Fällen würde die vom Datensubjekt gewünschte Beendigung der Datenverarbeitung auf Grundlage einer Interessenabwägung nur durch eine Offenbarung besonders sensibler Daten gelingen,

---

[110] *Casper*, in: Simitis/Hornung/Spiecker gen. Döhmann (Hrsg.), Datenschutzrecht, 2019, Art. 21, Rn. 7.

[111] *Casper*, in: Simitis/Hornung/Spiecker gen. Döhmann (Hrsg.), Datenschutzrecht, 2019, Art. 21, Rn. 6.

[112] *Martini*, in: Paal/Pauly (Hrsg.), DS-GVO, 2021, Art. 21, Rn. 30; ähnlich: *Kamann/Braun*, in: Ehmann/Selmayr (Hrsg.), DS-GVO, 2018, Art. 21, Rn. 19.

die ihrerseits jedoch selbst gerade nicht auf Grundlage von Art. 6 Abs. 1 lit. f DS-GVO verarbeitet werden können.

Damit erfordert die richtige Auslegung der „besonderen Situation" in Art. 21 Abs. 1 S. 1 DS-GVO eine Begründung, die über generische Aussagen ohne jeglichen Bezug zum konkreten Datensubjekt hinausgeht. Zugleich kann es jedoch nicht erforderlich sein, dass das Datensubjekt zum Nachweis der besonderen Situation Angaben macht, die zu einer Verarbeitung von besonders sensiblen personenbezogenen Daten führt.[113]

Unabhängig von den durch die Gerichte noch zu klärenden Anforderungen an die Begründung des Widerspruchs setzt das Begründungserfordernis des Art. 21 Abs. 1 S. 1 DS-GVO einen Anreiz für die Einführung eines *Kontroll-Cockpits*. Mit dessen Hilfe lässt sich die infolge eines Widerspruchs gemäß Art. 21 Abs. 1 S. 2 DS-GVO für eine Fortsetzung der Datenverarbeitung zu treffende und zu begründende Abwägungsentscheidung erleichtern und diese kann – soweit diese zugunsten des Datensubjekts ausfällt[114] – sogar vollständig automatisiert werden. Beispielsweise kann ein *Kontroll-Cockpit* dazu genutzt werden, Begründungen vorzuformulieren und mittels *Dropdown-Menü* zur Verfügung zu stellen, so dass das Setzen eines oder mehrere Häkchen vor diesen Formulierungen für den begründeten Widerspruch ausreicht. Eine derartige Erleichterung des Widerspruchs senkt für Datensubjekte die Hürden zum Widerspruch und hilft dem Verantwortlichen dabei, seiner Pflicht aus Art. 12 Abs. 2 S. 1 DS-GVO nachzukommen.

Allerdings dürfte infolgedessen die Anzahl der Widersprüche steigen. Dies widerspricht jedenfalls den Interessen derjenigen Verantwortlichen, die umfangreich personenbezogene Daten verarbeiten. Der Anreiz, freiwillig die Möglichkeit zur Abgabe und Begründung eines Widerspruchs mit Hilfe eines *Kontroll-Cockpits* zu erleichtern, besteht deshalb erneut vorrangig für solche Verantwortlichen, die bewusst ein nutzerfreundliches, hohes Datenschutzniveau anbieten wollen oder für solche Verantwortlichen, deren Geschäftsmodell nicht maßgeblich auf eine Kommerzialisierung von personenbezogenen Daten ausgerichtet ist. Für sie bietet ein *Kontroll-Cockpit* die Möglichkeit, die datenschutzrechtliche Kommunikation mit den Datensubjekten weitgehend zu automatisieren und somit effizient zu strukturieren.

---

[113] Eine Folgefrage bleibt, welche Lösung für den Konflikt existiert, wenn ein Datensubjekt den Widerspruch mit (abstrakten) „persönlichen Gründe" begründet, aber eine konkrete Angabe dieser Gründe mit Hinweis auf die Sensibilität i. S. d. Art. 9 Abs. 1 DS-GVO verweigert. Zwar dürfte eine Verarbeitung solcher Daten gemäß Art. 9 Abs. 2 lit. f DS-GVO rechtmäßig sein. Dennoch werden Verantwortliche regelmäßig vor einer Überprüfung dieser Gründe zurückschrecken, so dass der pauschale Widerspruch mit „besonders sensiblen, persönlichen Gründen" aus Sicht der Datensubjekte regelmäßig erfolgreich sein wird.

[114] Eine automatisierte Entscheidung, die – aufgrund einer Interessenabwägung des Verantwortlichen zulasten des Datensubjekts – zu einer Fortsetzung der Datenverarbeitung führt, ist für das Datensubjekt nachteilig i. S. d. Art. 22 Abs. 1 DS-GVO und deshalb nur ausnahmsweise gemäß Art. 22 Abs. 2 DS-GVO rechtmäßig.

c) Informationspflichten

Nach hier vertretener Ansicht löst der in Art. 17 Abs. 1 lit. b a. E. DS-GVO anerkannte Wechsel der Anspruchsgrundlage von einer widerrufenen Einwilligung auf eine Interessenabwägung eine (erneute) Informationspflicht des Verantwortlichen über die Möglichkeit zum Widerspruch gemäß Art. 21 Abs. 4 DS-GVO aus.[115]

Wurde ein solcher Widerspruch vom Datensubjekt erklärt und begründet, kann der Verantwortliche seine Datenverarbeitung dennoch gemäß Art. 21 Abs. 1 S. 2 DS-GVO rechtmäßig fortsetzen, soweit er

„zwingende schutzwürdige Gründe für die Verarbeitung nachweisen [kann], die die Interessen, Rechte und Freiheiten der betroffenen Person überwiegen."

Die hiernach erforderliche Nachweisbarkeit von Gründen spricht dafür, dass der Verantwortliche auch verpflichtet ist, das Datensubjekt über diese Gründe zu informieren.

Zudem muss der Verantwortliche dem Datensubjekt gemäß Art. 12 Abs. 3 S. 1 DS-GVO unverzüglich Informationen über die infolge des Widerspruchs von ihm ergriffenen Maßnahmen zur Verfügung zu stellen. Hierunter fällt sowohl die Information über die Fortsetzung der Datenverarbeitung trotz des Widerspruchs als auch die widerspruchsgemäße (teilweise) Einstellung der Datenverarbeitung.[116]

Zuletzt folgt die Pflicht zur Information aus Art. 5 Abs. 1 lit. a Var. 3 DS-GVO (Grundsatz der Transparenz), wonach die Rechtmäßigkeit der Datenverarbeitung davon abhängt, dass die Daten in einer, für das Datensubjekt „nachvollziehbaren Weise verarbeitet werden". Auch ErwG 60 S. 2 DS-GVO unterstützt eine weite Auslegung dieser Informationspflichten. Hiernach sollte der Verantwortliche dem Datensubjekt „alle weiteren Informationen" zur Verfügung stellen, die notwendig sind, „um eine faire und transparente Verarbeitung zu gewährleisten".

d) Fazit

Die Implementierung eines *Kontroll-Cockpits* ermöglicht eine vom Verantwortlichen vorstrukturierte, standardisierte und damit eindeutige Erklärung des Widerspruchs und erlaubt die Abfrage derjenigen Gründe, die sich aus der besonderen Situation des Datensubjekts ergeben und die erforderlich sind, sofern die Datenverarbeitung nicht ausschließlich der Ermöglichung einer – nach

[115] Oben B.II.1.b.cc.

[116] Der mit Blick auf Art. 21 DS-GVO missglückte Wortlaut des Art. 12 Abs. 3 und Abs. 4 („Maßnahme") ist teleologisch dahingehend auszulegen, dass auch das künftige Unterlassen der Datenverarbeitung als „ergriffene Maßnahme" des Verantwortlichen anzusehen ist.

hier vertretener Auffassung eng auszulegenden[117] – Direktwerbung dient. Zudem erleichtert die Standardisierung und Vorformulierung von Widerspruchsgründen die anschließend gemäß Art. 21 Abs. 1 S. 2 DS-GVO erforderliche (qualifizierte) Interessenabwägung.

Die im Rahmen von Art. 21 Abs. 1 S. 2 und Abs. 6 DS-GVO erforderliche Interessenabwägung und die mit einer Weiterverarbeitung einhergehenden Informationspflichten lassen sich mit Hilfe eines *Kontroll-Cockpits* umso besser standardisieren und automatisieren, je detaillierter und eindeutiger die gerichtliche Auslegung von Art. 6 Abs. 1 lit. f und Art. 21 DS-GVO künftig ausfällt.

Implementiert der Verantwortliche ein solches *Kontroll-Cockpit* und ermöglicht infolgedessen, dass Datensubjekte ihre Widersprüche elektronisch erklären können, so soll der Verantwortliche die Datensubjekte gemäß Art. 12 Abs. 3 S. 4 DS-GVO „nach Möglichkeit auf elektronischem Weg" über die infolgedessen ergriffenen Maßnahmen unterrichten. Diese Vorschrift sollte streng ausgelegt werden, damit der Verantwortliche sich nicht – bei für ihn unliebsamen Ergebnissen – wieder in eine analoge Welt zurückzieht und dem Datensubjekt dadurch die Kenntnisnahme von Information und die Ausübung von Rechten erschwert.

3. Datenschutz durch Technikgestaltung, Art. 25 Abs. 1 DS-GVO

Ein *Kontroll-Cockpit* bietet eindeutige Vorteile, um die komplexen Anforderungen an eine wirksame Einwilligungserteilung, deren (teilweisen) Widerruf, deren Abgrenzung zum Widerspruch gemäß Art. 21 Abs. 1 DS-GVO und die zahlreichen Informationspflichten des Verantwortlichen transparent und rechtssicher zu bündeln. Dennoch folgt weder aus den Vorschriften zur Einwilligung noch aus Art. 21 DS-GVO oder den zahlreichen Informationspflichten gemäß Art. 12–14 DS-GVO eine Pflicht zur Implementierung eines *Kontroll-Cockpits*.

Soll einem solchen Mechanismus zum Durchbruch verholfen werden, ohne dabei ausschließlich auf das Eigeninteresse der Verantwortlichen zu setzen, so besteht – neben einer Lösung *de lege ferenda* – die Möglichkeit, dass Datenschutzbehörden und Gerichte einen solchen Mechanismus aus Art. 25 DS-GVO ableiten (a). Jedenfalls solange solche *Kontroll-Cockpits* unzureichend empirisch erprobt sind, liegt es jedoch nahe, die Implementierung eines transparenten *Kontroll-Cockpits* zumindest zugunsten des Verantwortlichen zu berücksichtigen, sofern es gewisse Mindestanforderungen erfüllt (b).

a) Pflicht und Anreiz für die Implementierung eines Kontroll-Cockpits

Eine rechtliche Verpflichtung des Verantwortlichen, ein *Kontroll-Cockpit* zu implementieren, lässt sich am ehesten aus dem Grundsatz eines Datenschutzes

[117] Kapitel 2 C.I.2.b.

durch Technikgestaltung ableiten. Gemäß Art. 25 Abs. 1 DS-GVO trifft der Verantwortliche vor und während der Datenverarbeitung die geeigneten technischen und organisatorischen Maßnahmen (TOM), um die Rechte der Datensubjekte zu schützen. Hierbei muss er den Stand der Technik, die Implementierungskosten und die Art, den Umfang, die Umstände und die Zwecke der Verarbeitung sowie die Risiken für die Rechte und Freiheiten der Datensubjekte berücksichtigen.

Zudem nennt ErwG 78 die Möglichkeit zur technischen Kontrolle der Datenverarbeitung durch das Datensubjekte als eine Maßnahme. Deutlicher als Art. 25 Abs. 1 DS-GVO betont ErwG 78 DS-GVO zusätzlich die Notwendigkeit zur datenschutzfreundlichen Gestaltung (*data protection by design*)[118] und bestätigt dadurch nochmals, dass sich die Pflichten des Verantwortlichen nicht in der Ausgestaltung der verwendeten Technik erschöpfen.[119]

Indem er auf die Grundsätze der Datenminimierung und der Zweckbindung verweist, wird deutlich, dass Art. 25 Abs. 1 DS-GVO den Verantwortlichen konkrete Pflichten auferlegt, die allein aus den abstrakten Grundsätzen des Art. 5 Abs. 1 DS-GVO kaum ableitbar wären. Infolgedessen kommt der Auslegung und Anwendung von Art. 25 Abs. 1 DS-GVO durch die Datenschutzbehörden und Gerichte erhebliche Relevanz für die Frage zu, ob, unter welchen Umständen und in welchem Umfang die Verantwortlichen – neben anderen TOM – ein *Kontroll-Cockpit* implementieren müssen, um den empirisch nachgewiesenen kognitiven Defiziten von Datensubjekten entgegenzusteuern und ihre rationale Apathie bei der Durchsetzung bestehender Rechte zu kompensieren.

Obwohl Art. 25 Abs. 1 DS-GVO keine konkreten Vorgaben macht, ist die Kombination aus einer standardisierten Kennzeichnung und einem *Kontroll-Cockpit* nach hier vertretener Auffassung das aussichtsreichste und mildeste Mittel,[120] um die uniongrundrechtlich zu gewährleistende informationelle Privatautonomie der Datensubjekte abzustützen.

Somit könnte aus Art. 25 Abs. 1 DS-GVO eine Pflicht zur Implementierung eines *Kontroll-Cockpits* abgeleitet werden, weil die Kosten für deren Einsatz jedenfalls für solche Verantwortliche vergleichsweise gering sind, deren Geschäftsmodell maßgeblich auf der Verarbeitung von personenbezogenen Daten

---

[118] Hierzu: *Borking*, DuD 1996, 654 f.; *AK Technik der Datenschutzbeauftragten des Bundes und der Länder*, Arbeitspapier „Datenschutzfreundliche Technologien", 1997, (http://www.datenschutz-bayern.de/technik/grundsatz/apdsft.htm, zuletzt abgerufen am 19.05.2022); *EU-Kommission*, Mitteilung der Kommission an das Europäische Parlament und den Rat über die Verbesserung des Datenschutzes durch Technologien zum Schutz der Privatsphäre, KOM(2007) 228 endgültig; *Baumgartner/Gausling*, ZD 2017, 308 (309).

[119] Hierzu m. w. N. *Sattler*, in: Ebers/Steinrötter (Hrsg.), Künstliche Intelligenz und smarte Robotik im IT-Sicherheitsrecht, 2021, S. 197, (225 f.).

[120] Ähnlich: *Roßnagel*, MMR 2005, 71 (72 ff.); *Buchner,* Die Informationelle Selbstbestimmung im Privatrecht, 2006, S. 168 f.; *Artikel-29-Datenschutzgruppe*, Stellungnahme 8/2014 zu den jüngsten Entwicklungen im Internet der Dinge, WP 223, 2014, S. 22 und S. 25.

beruht. Zudem setzt das Prinzip datenschutzfreundlicher Voreinstellungen gemäß Art. 25 Abs. 2 DS-GVO (*privacy by default*) in Kombination mit dem hier vertretenen Vorrang der Einwilligung einen zusätzlichen Anreiz dafür, die Einwilligung der Datensubjekte mit Hilfe eines transparenten *Kontroll-Cockpits* rechtswirksam einzuholen und zugleich die Informationspflichten gemäß Art. 12 ff. DS-GVO zu erfüllen.

b) Mindestanforderungen an ein Kontroll-Cockpit

Die Umsetzung von Datenschutz durch Technikgestaltung setzt voraus, dass die ergriffenen Maßnahmen die Erkenntnisse aus empirischen, verhaltensökonomischen Studien berücksichtigen. Dies hat zur Folge, dass die Möglichkeiten der Datensubjekte innerhalb eines *Kontroll-Cockpits* eigene Einstellungen vorzunehmen, jedenfalls in der gegenüber Verbrauchern verwendeten Standard-Option beschränkt werden sollten. Infolgedessen erweitert das *Kontroll-Cockpit* die Optionen und damit die Wahlfreiheit, reduziert jedoch zugleich das Risiko, dass die Übersichtlichkeit und Praktikabilität der Lösung aufgrund einer zu großen Komplexität und einer zu hohen Anzahl an Einstellungsmöglichkeiten sinkt. Sowohl eine Überforderung durch zu viel Information[121] (*information overload*) als auch eine Überlastung durch zu viele Wahlmöglichkeiten[122] (*choice overload*) muss verhindert werden.

In Anknüpfung an die hier vorgeschlagene Informationsdarstellung als Kombination aus einer farblichen Kennzeichnung und einem *Privacy Score*,[123] liegt es nahe, zunächst erste Erfahrungen mit einem solchen *Kontroll-Cockpit* abzuwarten und dann dessen Implementierung mit einer zunehmenden Verbindlichkeit zu flankieren.

Infolgedessen ist es sinnvoll, den Einsatz eines *Kontroll-Cockpits*, das die Mindestanforderungen der nachfolgenden Übersicht in transparenter Weise einhält, mit einer *Indizwirkung* auszustatten. Wird das *Kontroll-Cockpit* mit der oben vorgeschlagenen Kennzeichnung kombiniert, so könnte dies sowohl für die Einhaltung der Informationspflichten aus Art. 12 ff. DS-GVO, die Beachtung des Grundsatzes der Transparenz gemäß Art. 5 Abs. 1 Var. 3 DS-GVO als auch für die (teilweise) Beachtung des Datenschutzes durch Technikgestaltung (Art. 25 Abs. 1 DS-GVO) eine positive Indizwirkung zugunsten des Verantwortlichen entfalten. Wollen Datenschutzbehörden die Implementierung solcher Abstützungen zugunsten der informationellen Privatautonomie fördern, so könnten sie diese bei der Bemessung eines Bußgelds zugunsten der Verantwortlichen berücksichtigen und dies in der Begründung des Bußgeldbescheids transparent machen.

---

[121] *Eppler/Mengis*, 20 Information Society 2004, S. 325 ff.
[122] *Scheibehenne/Greifeneder/Todd*, (2010) Journal of Consumer Research 37, S. 409 ff.
[123] Oben A.II.3.b.

Sobald erste Erfahrungen mit solchen *Kontroll-Cockpits* vorliegen, kann ein erhöhter Anreiz für die Teilnahme und Verwendung geschaffen werden. Beispielsweise könnte die Implementierung nicht nur als Indiz wirken, sondern auf der nächsten Stufe eine *widerlegliche Vermutung* für die Einhaltung der oben genannten Anforderungen auslösen.

Bevor als *ultima ratio* eine für alle Verantwortlichen zwingende Implementierung eines *Kontroll-Cockpits* mit den nachfolgenden Mindestanforderungen erfolgt, ist es erneut sinnvoll, den mit § 19a Abs. 1 GWB und mit Art. 3 DMA-Vorschlag eingeschlagenen Weg einer strengeren Regulierung von Unternehmen mit überragender marktübergreifender Bedeutung bzw. von *Gatekeepern* fortzusetzen und diese marktmächtigen Verantwortlichen *de lege ferenda* zur Implementierung eines *Kontroll-Cockpits* zu verpflichten. Diese *kartellrechtsakzessorische*, *asymmetrische* Vorgehensweise verhindert, dass eine allgemeine Pflicht zur Implementierung eines solchen *Kontroll-Cockpits* die ohnehin für KMU bestehenden datenschutzrechtlichen Marktzutrittsbarrieren[124] nochmals erhöht.

III. Übersicht der Mindestanforderungen an ein Kontroll-Cockpit

Nachfolgend werden nicht die zahlreichen Informationspflichten aufgelistet, die sich der DS-GVO und dem BDSG entnehmen lassen und die künftig unter Rückgriff auf den Grundsatz der Transparenz (Art. 5 Abs. 1 lit. a Var. 3 DS-GVO) von Datenschutzbehörden und Gerichten vermutlich nochmals ergänzt werden. Auch diese sind selbstverständlich Mindestanforderungen, die vom Verantwortlichen und seinen Auftragsverarbeitern für eine rechtmäßige Datenverarbeitung erfüllt werden müssen.

Stattdessen werden nachfolgend die Mindestanforderungen an ein *Kontroll-Cockpit* genannt, sofern dieses dazu dienen soll, die informationelle Privatautonomie der Datensubjekte auf Grundlage des hier vorgeschlagenen Stufenmodells der Erlaubnistatbestände abzustützen.

Wie in Kapitel 3 ausgeführt, sind auf Basis von Art. 6 Abs. 1 lit. b DS-GVO nach hier vertretener Ansicht lediglich solche Datenverarbeitungen rechtmäßig, die für einen zwischen dem Datensubjekt und dem Verantwortlichen geschlossenen Vertrag nach objektivem Empfängerhorizont üblich und deshalb Teil des sachgedanklichen Mitbewusstseins des Datensubjekts bei Vertragsschluss sind.[125] Infolgedessen sind die Einwilligung und die Datenverarbeitung auf

[124] *Lianos/Motchenkova*, 9 Journal of Competition Law & Economics 2013, 419 (428); *Monopolkommission*, Wettbewerbspolitik: Herausforderung digitale Märkte, Sondergutachten 68, 2015, Rn. 302; *Rubinstein/Gal*, 59 Arizona Law Review 2017, 339 (349 ff.); *Gal/Aviv*, Journal of Competition Law and Economics 2020, 349 (351 f./386 ff.).

[125] Oben Kapitel 3 D. sowie Kapitel 5 B.I.

Grundlage einer Interessenabwägung die zentralen Ausgangspunkte für ein *Kontroll-Cockpit*. Darüber hinaus kann und sollte dieses in einem zweiten Schritt um Möglichkeiten zur Geltendmachung und technischen Abwicklung von Ansprüchen auf Auskunft,[126] auf Berichtigung und auf Ergänzung,[127] auf Beschränkung der Datenverarbeitung,[128] auf Datenportabilität[129] und auf Löschung („Recht auf Vergessenwerden")[130] ergänzt werden.

Die Besonderheiten des hier vorgeschlagenen Stufenmodells der Erlaubnistatbestände zur Gewährleistung einer abgestützten informationellen Privatautonomie sind grau unterlegt:

Erklärung	Variante	Begründung	Ausnahme	Folgen
Widerruf	**Freier Widerruf** Art. 7 III 1	nicht erforderlich		**Beendigung** der Verarbeitung
			Ausschluss des freien Widerrufs (befristet) **Voraussetzung** Teleologische Reduktion von Art. 7 III 1	**Information** über das zeitliche Ende des Ausschlusses **Information** über die Möglichkeit zum außerordentlichen Widerruf
			Wechsel fortgesetzte Verarbeitung auf anderer Grundlage	**Information** über die (neue) Grundlage der fortgesetzten Verarbeitung
	Begründeter außerordentl. Widerruf Teleologische Reduktion von Art. 7 III 1	**Auswahl** aus anerkannten, vorformulierten Gründen **Eingabe** Textfeld für eine individuelle Begründungen	**Allenfalls ausnahmsweise: Wechsel** fortgesetzte Verarbeitung auf anderer Grundlage (hohe Anforderungen: Nicht ausreichend sind zwingende Gründe i. S. d. Art. 21 I 2)	**Information** über die (neue) Grundlage der fortgesetzten Verarbeitung und Begründung der Fortsetzung

[126] Art. 15 Abs. 1 und Abs. 2 DS-GVO mit zusätzlichen Grenzen in § 34 Abs. 1 BDSG.
[127] Art. 16 DS-GVO.
[128] Art. 18 Abs. 1 DS-GVO.
[129] Art. 20 Abs. 1 DS-GVO.
[130] Art. 17 Abs. 1 DS-GVO mit zusätzlichen Grenzen in § 35 BDSG.

Erklärung	Variante	Begründung	Ausnahme	Folgen
Widerspruch	**Freier Widerspruch** (Art. 21 II) gegen Direktwerbung inkl. Profiling	nicht erforderlich	keine	**Beendigung** der Datenverarbeitung für Direktwerbung
	Begründeter Widerspruch (Art. 21 I)	Besondere Situation des Datensubjekts **Auswahl** aus anerkannten vorformulierten Gründen **Eingabe** Textfeld für eine individuelle Begründung	**Abwägung** Überwiegen von zwingenden Interessen des Verantwortlichen oder zur Durchsetzung von eigenen Ansprüchen	**Information** über die zwingenden Gründe für die Fortsetzung der Verarbeitung oder über die andere Rechtsgrundlage
	Begründeter Widerspruch (Art. 21 VI) Forschung oder statistische Zwecke	Besondere Situation des Datensubjekts **Auswahl** aus anerkannten vorformulierten Gründen **Eingabe** Textfeld für eine individuelle Begründung	Erforderlichkeit der Verarbeitung für die Erfüllung einer Aufgabe im öffentlichen Interesse (Art. 21 VI)	**Information** über die Grundlage und die Gründe für die Fortsetzung der Verarbeitung

Tabelle 3: Mindestanforderungen an ein Kontroll-Cockpit.

Zusammenfassung

Statt einer Zusammenfassung werden die gefundenen Ergebnisse in sechs Hauptthesen und 30 (Unter-)Thesen zusammengefasst.

I. Hauptthese

Das europäische Datenschutzrecht muss künftig privatrechtssensibler ausgelegt und angewendet werden.

1. These

Maßgeblich beeinflusst durch den Bericht von *Steinmüller u. a.* „Grundfragen des Datenschutzes" von 1971 litt das deutsche und leidet im Anschluss hieran auch das europäische Datenschutzrecht an einer mangelhaften Differenzierung danach, ob personenbezogene Daten in einem Vertikalverhältnis (zwischen Datensubjekten und staatlichen Verantwortlichen) oder in einem Horizontalverhältnis (zwischen Datensubjekten und unternehmerisch handelnden Verantwortlichen) verarbeitet werden.[1]

2. These

Der unionsrechtliche Grundrechtsschutz erschwert eine unionsgrundrechtskonforme Auslegung und Anwendung der DS-GVO. Bislang hat der *EuGH* die Schutz- und Gewährleistungsbereich des Art. 8 GRCh (Schutz personenbezogener Daten) und des Art. 7 GRCh (Schutz der Privatsphäre) nicht sinnvoll abgegrenzt.[2] Zudem fehlt der GRCh ein Äquivalent zur allgemeinen Handlungsfreiheit gemäß Art. 2 Abs. 1 GG.[3] Diese Lücke erschwert es, einen Interessenausgleich im Wege der praktischen Konkordanz zu erreichen.[4]

---

[1] Kapitel 1 A.I.2–3.
[2] Kapitel 1 B.II.
[3] Kapitel 1 B.IV.
[4] Kapitel 1 B.V.

3. These

Obwohl die Schwelle zur unmittelbaren Grundrechtsbindung Privater nicht vollständig überschritten wurde, kommt das Verständnis des deutschen Rechts auf informationelle Selbstbestimmung (Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG) und der europäische Schutz von personenbezogenen Daten (Art. 8 Abs. 1 GRCh/Art. 16 AEUV) und der Privatsphäre (Art. 7 GRCh) einer unmittelbaren Drittwirkung von Grundrechten sehr nahe.[5]

4. These

Das Verbot der Datenverarbeitung mit Erlaubnisvorbehalt (Art. 6 Abs. 1 und Art. 9 Abs. 1 DS-GVO) steht in einem Spannungsverhältnis zum Grundsatz der Privatautonomie.[6] Dennoch wurde dieser datenschutzrechtliche Ausgangspunkt nach einer anfänglichen Kritik durch die Privatrechtswissenschaft[7] akzeptiert. Anschließend vernachlässigte die Privatrechtswissenschaft das Recht zum Schutz natürlicher Personen vor einer Verarbeitung personenbezogener Daten (verkürzend: Datenschutzrecht) über Jahrzehnte.

5. These

Damit die DS-GVO dem Grundsatz der Verhältnismäßigkeit (Art. 52 Abs. 1 S. 2 GRCh) gerecht wird, müssen der *EuGH* und die nationalen Gerichte einen Ausgleich zwischen dem Schutz der Datensubjekte und der Ermöglichung von informationeller Privatautonomie herbeiführen, ohne dabei gegen das gemäß Art. 8 Abs. 1 GRCh (Art. 16 AEUV) grundrechtlich zu gewährleistende Untermaßverbot für den Schutz personenbezogener Daten und ohne gegen das gemäß Art. 16 GRCh und Art. 6 Abs. 3 EUV einzuhaltende Übermaßverbot einer Beeinträchtigung der (unternehmerischen) Vertragsfreiheit zu verstoßen. Dafür muss die DS-GVO künftig privatrechtssensibler ausgelegt und angewendet werden.[8]

II. Hauptthese

Wird der Erlaubnistatbestand der Interessenabwägung gemäß Art. 6 Abs. 1 lit. f DS-GVO nicht restriktiv(er) angewendet, so werden die (strengeren) Voraussetzungen der Einwilligung unterlaufen und infolgedessen die informationelle Pri-

[5] Kapitel 1 B.I.
[6] Kapitel 1 C.I–II.
[7] Kapitel 1 A.II.1–3.
[8] Kapitel 1 D.

vatautonomie der Datensubjekte beeinträchtigt. Der Erlaubnistatbestand der Interessenabwägung erfüllt eine Auffang- und Schrittmacherfunktion.

1. These

Der Erlaubnistatbestand der Interessenabwägung ist – trotz seiner Funktion als Auffangtatbestand – zu vage ausgefallen.[9] Weil das Vorlageverfahren zum *EuGH* gemäß Art. 267 AEUV systematisch nicht dafür geeignet ist, den Art. 6 Abs. 1 lit. f DS-GVO zeitnah durch Typisierungen zu konkretisieren, sollte der europäische Gesetzgeber sein Versäumnis korrigieren und den Tatbestand *de lege ferenda* beispielsweise in Form von schwarzen und grauen Listen ergänzen.[10]

2. These

Das im Kontext von Art. 6 Abs. 1 lit. f DS-GVO ausdrücklich genannte berechtigte Interesse der „Direktwerbung" (Art. 21 Abs. 2 DS-GVO) ist restriktiv auszulegen. Es umfasst ausschließlich die Datenverarbeitung für personalisierte Werbung durch den Verantwortlichen innerhalb einer bereits bestehenden Kundenbeziehung zum Datensubjekt für identische oder ähnliche Produkte des Verantwortlichen.[11]

3. These

Die Datenverarbeitung für personalisierte Werbung in Werbenetzwerken, insbesondere denjenigen von *GAFAM,* ist – auch bei bestehenden Kundenbeziehungen des Datensubjekts zu allen am Werbenetzwerk beteiligten Unternehmen – keine Direktwerbung im Sinne des Art. 21 Abs. 2 DS-GVO. Ein Profiling für personalisierte Werbung in den Werbenetzwerken von mehrseitigen Plattformen setzt jeweils eine Einwilligung gegenüber den jeweils (gemeinsam) Verantwortlichen voraus und kann nicht auf Grundlage einer Interessenabwägung erfolgen.[12]

4. These

Weil der Erlaubnistatbestand der Interessenabwägung als Generalklausel eine Schrittmacherfunktion hat, muss er künftig – anders als *de lege lata* in Art. 9 Abs. 2 DS-GVO vorgesehen – auch für eine Datenverarbeitung von besonders

[9] Kapitel 2 A.III.3.
[10] Kapitel 2 C.I.1.a.
[11] Kapitel 2 C.I.2.
[12] Kapitel 2 C.I.2.b.

sensiblen personenbezogenen Daten zur Verfügung stehen, sofern es um die kurzzeitige Erhebung und anschließende Verarbeitung von durch Gestik, Mimik und Sprache generierten Daten im Rahmen des IoT geht (z. B. Spontanäußerungen)[13] oder ausschließlich um das Trainieren von sog. künstlicher Intelligenz, insbesondere in Form des maschinellen Lernens.[14]

III. Hauptthese

Der Erlaubnistatbestand der vertragsakzessorischen Datenverarbeitung gemäß Art. 6 Abs. 1 lit. b DS-GVO ist restriktiv auszulegen. Anderenfalls werden die (strengeren) unionsrechtlichen Voraussetzungen an die Einwilligung mithilfe von Verträgen auf Grundlage des nationalen Schuldrechts unterlaufen. Infolgedessen wäre die Verwirklichung der Ziele aus Art. 1 DS-GVO gefährdet.

1. These

Je großzügiger der Erlaubnistatbestand des Art. 6 Abs. 1 lit. b DS-GVO angewendet wird, desto geringer ist die Steuerungsfunktion der DS-GVO im Privatrechtsverhältnis. Sofern der Erlaubnistatbestand der vertragsakzessorischen Datenverarbeitung weit ausgelegt wird, ermöglicht er eine Flucht aus der Einwilligung und damit eine Flucht aus der DS-GVO.[15]

2. These

Eine solche Flucht ins (nationale) Schuldrecht sollte verhindert werden, weil das nationale Schuldrecht weder einheitliche noch praktikable Kontrollmöglichkeiten bereithält.[16] Datenschutzbehörden und Gerichte sind nicht in der Lage, den vertraglichen Hauptgegenstand aus Leistung und Gegenleistung auf seine Angemessenheit zu überprüfen. Dies gilt erst recht, soweit personenbezogene Daten Teil der synallagmatischen Leistungsbeziehung sind.[17]

3. These

Dem europäischen Gesetzgeber ist es bislang nicht gelungen, die DS-GVO und die DID-RL miteinander zu synchronisieren. Dies hat zur Folge, dass eine großzügige Anwendung von Art. 6 Abs. 1 lit. b DS-GVO nicht nur zur Flucht

[13] Kapitel 2 C.I.3.b.
[14] Kapitel 2 C.I.3.c.
[15] Kapitel 3 A. und C.II.1–5.
[16] Kapitel 3 C.I.2.e. und C.II.6.
[17] Kapitel 3 C.I.1–3.

aus der DS-GVO verhilft, sondern zusätzlich erhebliche Abgrenzungsschwierigkeiten zwischen den Anwendungsbereichen von DS-GVO und DID-RL bzw. §§ 327 ff. BGB auslöst.[18]

4. These

Soweit ein Verantwortlicher eine Personalisierung von digitalen Produkten zum vertraglichen Leistungsgegenstand macht, ist die anschließende Datenverarbeitung für diese Personalisierung nicht gemäß Art. 6 Abs. 1 lit. b DS-GVO rechtmäßig. In diesem Fall sind die detaillierten und europaweit einheitlichen Anforderungen an die Einwilligung zu beachten, weil anderenfalls die Ziele der DS-GVO, also der Schutz von Datensubjekten vor der Verarbeitung von personenbezogenen Daten und der freie Verkehr von personenbezogenen Daten im Binnenmarkt gefährdet werden.[19]

IV. Hauptthese

Um die informationelle Privatautonomie der Datensubjekte zu gewährleisten, ist der Einwilligung gemäß Art. 4 Nr. 11, Art. 6 Abs. 1 lit. a, Art. 7 ff. DS-GVO im Privatrechtsverhältnis der Vorrang einzuräumen.

1. These

Der europäische Gesetzgeber hat ausschließlich die Einwilligung detailliert geregelt. Deshalb ist die Einwilligung im Verhältnis zu Art. 6 Abs. 1 lit. b und Art. 6 Abs. 1 lit. f DS-GVO *lex specialis* und damit vorrangig einzuholen.[20]

2. These

Damit ein Ausgleich zwischen dem Schutz von Datensubjekten vor der Verarbeitung von personenbezogenen Daten (Art. 8 Abs. 1 GRCh) und der Privatsphäre (Art. 7 GRCh) einerseits und der unternehmerischen Freiheit (Art. 16 GRCh) und der Vertragsfreiheit von Verantwortlichen und Datensubjekten (Art. 16 GRCh/Art. 6 Abs. 3 EUV) andererseits gelingen kann, müssen die Anforderungen an die Einwilligung im Privatrechtverhältnis flexibilisiert werden.[21]

---

[18] Kapitel 3 C.III.1–2.
[19] Kapitel 3 C.III.3.
[20] Kapitel 4 A.I.2–4. sowie Kapitel 2 C.II. und Kapitel 3 C.III.2.
[21] Kapitel 4 B.I–III.

3. These

Ohne eine unionsgrundrechtskonforme Flexibilisierung des Begriffs der Freiwilligkeit[22] und ohne die Möglichkeit zum befristeten Ausschluss der sog. freien Widerruflichkeit der Einwilligung,[23] verstoßen Art. 7 Abs. 4 bzw. Art. 7 Abs. 3 S. 1 DS-GVO gegen den Grundsatz der Verhältnismäßigkeit, Art. 52 Abs. 1 S. 2 GRCh. Dies gilt jedenfalls – aber nicht nur – soweit Datensubjekte als Unternehmer handeln.[24]

4. These

In Anlehnung an die von *Ansgar Ohly* herausgearbeitete deutsche Dogmatik der Einwilligung im Privatrecht ist auch der unionsautonome Begriff der Einwilligung nicht auf die schlichte, einseitige und jederzeit widerrufliche Einwilligung beschränkt, sondern ermöglicht eine zeitweise unwiderrufliche Einwilligung.[25] Letztere bleibt jedoch Einwilligung im Sinne des Art 6 Abs. 1 lit. a DS-GVO. Sie kann als (Gegen-)Leistung synallagmatischer Bestandteil eines Vertrags sein, ist jedoch selbst kein Vertrag i. S. d. Art. 6 Abs. 1 lit. b DS-GVO.[26]

V. Hauptthese

Bei der Verabschiedung der DS-GVO hat der europäische Gesetzgeber den seit Jahrzehnten bestehenden Märkten für eine Kommerzialisierung der vermögenswerten Bestandteile von Persönlichkeitsrechten zu wenig Rechnung getragen. Die infolgedessen mangelhafte Berücksichtigung der ökonomischen und privatrechtlichen Verhältnisse muss im Rahmen der Auslegung und Anwendung der DS-GVO nachträglich kompensiert werden. Das hier vorgeschlagene Stufenmodell der Erlaubnistatbestände ermöglicht diese nachträgliche Kompensation und gewährleistet eine abgestützte informationelle Privatautonomie der Datensubjekte.

1. These

Um die unionsgrundrechtlich garantierte Möglichkeit zur Einwilligung (Art. 8 Abs. 2 S. 1 GRCh), die informationelle Privatautonomie und den freien Verkehr personenbezogener Daten im Binnenmarkt (Art. 1 Abs. 3 DS-GVO) zu ge-

[22] Kapitel 4 B.I.1.
[23] Kapitel 4 B.II.1.
[24] Kapitel 4 B.I.2. und B.II.2.
[25] Kapitel 4 C.II.1–2.
[26] Kapitel 4 C.III.2.

währleisten,[27] kommt der Einwilligung innerhalb des Stufenmodells der Erlaubnistatbestände ein Vorrang zu. Ist eine Einwilligung der Datensubjekte nicht oder nur unter objektiv unangemessenem Aufwand erreichbar, so ist der Anwendungsbereich des ansonsten gegenüber der Einwilligung subsidiären Art. 6 Abs. 1 lit. f DS-GVO eröffnet.[28] Dies kommt insbesondere für die Verarbeitungen von Daten mit multi-relationalem Personenzug in Betracht, sofern die jeweiligen Risiken für das individuelle Datensubjekt lediglich gering sind.

2. These

Gemäß Art. 6 Abs. 1 lit. b DS-GVO ist eine Datenverarbeitung rechtmäßig, soweit sie ein notwendiger, aber lediglich untergeordneter Zwischenschritt ist, um eine andere Leistungspflicht zu erfüllen (z. B. Auslieferung und Zahlungsabwicklung im Fernabsatz). In diesem Fall können die Daten gemäß Art. 6 Abs. 1 lit. b DS-GVO in vertragsakzessorischer Weise rechtmäßig verarbeitet werden. Soweit eine solche untergeordnete Datenverarbeitung typischerweise Teil des sachgedanklichen Mitbewusstseins des Datensubjekts bei Vertragsschluss ist, erfordert diese Datenverarbeitungen keine Einwilligung. Art. 6 Abs. 1 lit. b DS-GVO hat somit die Funktion, den Einwilligungstatbestand und die Entscheidungskapazitäten des Datensubjekts zu entlasten. Infolgedessen können Datensubjekte ihre intellektuellen Entscheidungskapazitäten auf riskantere Datenverarbeitungen konzentrieren, die auf eine Einwilligung angewiesen sind.[29]

3. These

Sowohl der Vorrang der Einwilligung als auch die unionsgrundrechtlich zu gewährleistende Vertragsfreiheit von Verantwortlichen und Datensubjekten setzen voraus, dass die Freiwilligkeit der Einwilligung gemäß Art. 7 Abs. 4 DS-GVO grundsätzlich weit ausgelegt wird. Infolgedessen ist die Freiwilligkeit nicht *per se* als strenges Kopplungsverbot zu verstehen. Vielmehr etabliert die Vorschrift ein Gebot zur Berücksichtigung der jeweiligen Umstände des Einzelfalls.[30] Zu den hierbei zu berücksichtigenden Umständen zählen insbesondere die Markmacht des Verantwortlichen,[31] die Eigenschaften des Datensubjekts[32] und die situativen Umstände der Einwilligungserteilung.[33]

---

[27] Kapitel 2 C.II–III.
[28] Kapitel 5 A.I. sowie Kapitel 2 D.
[29] Kapitel 5 B.I. sowie Kapitel 3 D.
[30] Kapitel 5 C.I. und II.1.c.
[31] Kapitel 5 C.II.1.
[32] Kapitel 5 C.II.2.
[33] Kapitel 5 C.II.3.

4. These

Soweit der Verantwortliche ein marktmächtiges Unternehmen ist, also ein *Gatekeeper* im Sinne des Art. 3 DMA-Vorschlag oder ein Unternehmen mit überragender marktübergreifender Bedeutung für den Wettbewerb gemäß § 19a Abs. 1 GWB, ist die Freiwilligkeit kartellrechtsakzessorisch und damit asymmetrisch streng auszulegen. Dieses Vorgehen fördert den Wettbewerb, indem es marktmächtige Verantwortliche strengeren Regeln unterwirft. Dadurch werden zugleich Marktzutrittsbarrieren für KMU verhindert, deren Geschäftsmodelle (ebenfalls) auf dem Austausch von digitalen Produkten gegen einen Zugang zu personenbezogenen Daten beruhen.[34]

5. These

Diese kartellrechtsakzessorische, asymmetrische Auslegung und Anwendung gegenüber marktmächtigen Verantwortlichen kann insbesondere ein milderes Mittel sein, als eine kartellrechtlich initiierte Aufspaltung von marktmächtigen Verantwortlichen.[35] Um kompetenzielle Konflikte und eine Anmaßung von Wissen durch Datenschutzbehörden und nicht-spezialisierte Gerichte zu vermeiden, sollten diese die Freiwilligkeit der Einwilligung nur dann aufgrund der Marktmacht des Verantwortlichen ablehnen, sofern und soweit das zuständige *Bundeskartellamt* oder die zuständige *EU-Kommission* den Verantwortlichen in der Liste der Unternehmen mit überragender marktübergreifender Bedeutung für den Wettbewerb (GWB) bzw. der Liste der *Gatekeeper* (DMA-Vorschlag) führen.[36]

6. These

Die sog. freie Widerruflichkeit der Einwilligung steht grundsätzlich zur Disposition des Datensubjekts und kann befristet ausgeschlossen werden. Hierfür ist Art. 7 Abs. 3 S. 1 DS-GVO teleologisch zu reduzieren. Dies gilt jedenfalls – aber nicht nur – soweit Datensubjekte als Unternehmer handeln.[37]

7. These

Auch die teleologische Reduktion des Art. 7 Abs. 3 S. 1 DS-GVO ist kartellrechtsakzessorisch und damit asymmetrisch anzuwenden. Infolgedessen ist ein zeitweiser Ausschluss der Widerruflichkeit nicht gegenüber Verantwortlichen

[34] Kapitel 5 C.II.1.c.cc.
[35] Kapitel 5 C.II.4.
[36] Kapitel 5 C.II.1.c.cc.
[37] Kapitel 5 C.III.2.b.

möglich, soweit diese *Gatekeeper* (Art. 3 DMA-Vorschlag) oder ein Unternehmen mit überragender marktübergreifender Bedeutung für den Wettbewerb (§ 19a Abs. 1 GWB) sind.[38]

8. These

Die Möglichkeit zum zeitweisen Ausschluss der sog. freien Widerruflichkeit stabilisiert die Leistungsbeziehungen zwischen nicht-marktmächtigen Verantwortlichen und Datensubjekten.[39] Um die dadurch gewährleistete informationelle Privatautonomie unionsgrundrechtkonform abzustützen, ist der Ausschluss der freien Widerruflichkeit stets zu befristen (sog. *sunset clause*)[40] und eine Verlängerung des Ausschlusses bedarf einer erneuten ausdrücklichen Erklärung des Datensubjekts.[41] Der befristete Ausschluss der freien Widerruflichkeit lässt die Möglichkeit zum außerordentlichen Einwilligungswiderruf aus wichtigem Grund unberührt.[42]

VI. Hauptthese

Der Vorrang der Einwilligung als wesentliche Ausprägung der informationellen Privatautonomie sollte künftig durch zwei zusätzliche Maßnahmen abgestützt werden. Weil der europäische Gesetzgeber sich mit der DS-GVO für das Informationsmodell entschieden hat, trifft die europäischen Institutionen und vorrangig die *EU-Kommission* eine Folgenverantwortung dafür, dass dieses Informationsmodell tatsächlich ertüchtigt wird.

1. These

Um das Verständnis der Datensubjekte für die Bedeutung und für die Reichweite einer Datenverarbeitung zu erhöhen, sind die datenschutzrechtlichen Informationspflichten des Verantwortlichen mehrstufig zu erfüllen.[43] Auf der ersten Stufe sollte eine farbliche Kennzeichnung in Kombination mit einem *Privacy Score* eine erste, schnelle Beurteilung der Datenverarbeitung ermöglichen. Wesentliches Kriterium für die Einstufung ist der für die Datenverarbeitung herangezogene Erlaubnistatbestand.[44]

---

[38] Kapitel 5 C.III.2.a.
[39] Kapitel 5 C.III.3.a.
[40] Kapitel 5 C.III.3.b.
[41] Kapitel 5 C.III.3.c.
[42] Kapitel 5 C.III.3.d.
[43] Kapitel 6 A.II.3.
[44] Kapitel 6 A.II.3.c.

2. These

Die Verbindlichkeit der Einführung dieser transparenzfördernden Kennzeichnungs-Kombination durch Verantwortliche sollte nach einer Phase der empirischen Untersuchung und Erprobung sukzessive erhöht werden. Dies ist durch Anreize für eine freiwillige Einführung möglich (Vermutungswirkung für die Einhaltung datenschutzrechtlicher Informationspflichten und Berücksichtigung i.R. eines Bußgeldbescheids).[45]

3. These

Um die Informiertheit von Datensubjekten zu verbessern und um Datensubjekten die Abgabe von datenschutzrechtlichen Erklärungen und die Geltendmachung von datenschutzrechtlichen Ansprüchen zu erleichtern (Auskunft, Berichtigung, Löschung, Portabilität), ist ein transparentes *Kontroll-Cockpit* zu implementieren. Hierdurch wird es den Datensubjekten erleichtert, in transparenter Weise datenschutzrechtliche Erklärungen abzugeben und eine klare Abgrenzung zwischen dem freien Einwilligungswiderruf, dem außerordentlichen Einwilligungswiderruf, dem freien Widerspruch gegen Direktwerbung und dem begründeten Widerspruch zu erreichen.[46]

4. These

Das *Kontroll-Cockpit* ermöglicht es dem Verantwortlichen, seine Pflicht zum leichten Einwilligungswiderruf gemäß Art. 7 Abs. 3 S. 4 DS-GVO einzuhalten und die (qualifizierte) Interessenabwägung gemäß Art. 21 Abs. 1 S. 1 DS-GVO zu automatisieren.[47]

5. These

Soweit Verantwortliche ein *Kontroll-Cockpit* einführen, das den hier vorgeschlagenen Mindeststandards entspricht,[48] sollte dies zugunsten der Verantwortlichen berücksichtigt werden. Eine gesetzlich zwingende Einführung einer Kombination aus farblicher Kennzeichnung und *Privacy Score* und die zwingende Implementierung eines *Kontroll-Cockpits* setzen zunächst Erfahrungen und empirische Studien voraus. Deshalb sollte eine ausdrückliche Pflicht zur Einführung dieser Abstützungen erst nach einer Test- und Einführungsphase und dann zunächst in kartellrechtsakzessorischer, asymmetrischer Weise für

[45] Kapitel 6 A.II.3.b.
[46] Kapitel 6 B.II.2.a.
[47] Kapitel 6 B.II.2.d.
[48] Kapitel 6 B.II.3.b.

marktmächtige Verantwortliche etabliert werden.[49] Den Gerichten ist es jedoch *de lege lata* bereits möglich, aus dem Grundsatz des Datenschutzes durch Technik (Art. 25 Abs. 1 DS-GVO) eine Verpflichtung zur Implementierung eines *Kontroll-Cockpits* herzuleiten.[50]

[49] Kapitel 6 A.II.3.b. (Kennzeichen-Kombination) und B.II.3.a. (Kontroll-Cockpit).
[50] Kapitel 6 B.II.3.a.

Literaturverzeichnis

Ackermann, Thomas, Das Informationsmodell im Recht der Dienstleistungen, ZEuP 2009, 230–267.

AK Technik der Datenschutzbeauftragten des Bundes und der Länder, Arbeitspapier „Datenschutzfreundliche Technologien", Bonn 1997.

Akerlof, George A., The Market for „Lemons": Quality Uncertainty and the Market Mechanism, 84 The Quarterly Journal of Economics 1970, 488–500.

Albers, Marion, Informationelle Selbstbestimmung, Baden-Baden 2005.

–, Umgang mit personenbezogenen Informationen und Daten, in: Hoffmann-Riem, Wolfgang/Schmidt-Aßmann, Eberhard/Voßkuhle, Wolfgang (Hrsg.), Grundlagen des Verwaltungsrechts. Band II, 2. Aufl., München 2012, 127–234.

Albrecht, Jan Philipp, Das neue EU-Datenschutzrecht – von der Richtlinie zur Verordnung, CR 2016, 88–98.

Albrecht, Jan Philipp/Jotzo, Florian, Das neue Datenschutzrecht der EU, München 2016.

Alemanno, Alberto/Sibony, Anne-Lise (Hrsg.), Nudge and the Law: A European Perspective, Oxford/Portland 2015.

Alexander, Christian, Vertragsrecht und Lauterkeitsrecht unter dem Einfluss der Richtlinie 2005/29/EG über unlautere Geschäftspraktiken, WRP 2012, 515–523.

Alexy, Robert, Theorie der Grundrechte, Frankfurt a. M. 2011.

Aloisi, Antonio/Gramano, Elena, Artificial Intelligence Is Watching You at Work. Digital Surveillance, Employee Monitoring and Regulatory Issues in the EU Context, Special Issue of Comparative Labor Law & Policy Journal 2020 (https://ssrn.com/abstract=3399548).

Alpaydin, Ethem, Introduction to Machine Learning, Cambridge (MA)/London 2016.

Anweiler, Jochen, Die Auslegungsmethoden des Gerichtshofs der Europäischen Gemeinschaften, Frankfurt a. M. 1997.

Acquisti, Alessandro/John, Leslie K./Loewenstein, George, What Is Privacy Worth?, 42 The Journal of Legal Studies (2013), 249–274.

Acquisti, Alessandro/Taylor, Curtis/Wagman, Liad, The Economics of Privacy, 54 Journal of Economic Literature (2016), 442–492.

Arbeitsgruppe „Digitaler Neustart" der Konferenz der Justizministerinnen und Justizminister der Länder, Bericht vom 15.05.2017 2017.

Argenton, Cédric/Prüfer, Jens, Search engine competition with network externalities, 8 Journal of Competition Law and Economics (2012), 73–105.

Arneson, Richard, Autonomy and Preference Formation, in: Coleman, Jules/Buchanan, Allen (Hrsg.), In Harm's Way: Essays in Honor of Joel Feinberg, Cambridge, UK, 1991, 42–73.

Arning, Marian/Moos, Flemming, Big Data bei verhaltensbezogener Online-Werbung – Programmatic Buying und Real Time Advertising, ZD 2014, 242–248.

Arning, Marian/Moos, Flemming/Schefzig, Jens, Vergiss Europa!, CR 2014, 447–456.

Arnold, *René u. a.*, Any Sirious Concerns Yet? – An Empirical Analysis of Voice Assistants' Impact on Consumer Behavior and Assessment of Emerging Policy Challenges, Working Paper, 2019 (https://ssrn.com/abstract=3426809).
Arrieta-Ibarra, *Imanol u. a.*, Should We Treat Data as Labor? Moving beyond „Free", 108 AEA Papers and Proceedings (2018), 38–42.
Article 29 Data Protection Working Party, Opinion 10/2004 on More Harmonised Information Provisions, WP 100, Brüssel 2004.
–, Opinion 04/2012 on Cookie Consent Exemption, WP194, Brüssel 2012.
–, Opinion 02/2013 on apps on smart devices, WP202, Brüssel 2013.
–, Opinion 03/2013 on purpose limitation, WP203, Brüssel 2013.
–, Working Document 02/2013 providing guidance on obtaining consent for cookies, WP 208, Brüssel 2013.
–, Statement on the role of a risk-based approach in data protection legal frameworks, WP 218, Brüssel 2014.
–, Opinion 9/2014 on the application of Directive 2002/58/EC to device fingerprinting, WP 224, Brüssel 2014.
–, Opinion 03/2016 on the evaluation and review of the ePrivacy Directive (2002/58/EC), WP 240, Brüssel 2016.
–, Guidelines on the right to data portability, WP 242 rev.01, Brüssel 2017.
–, Opinion 01/2017 on the Proposed Regulation for the Privacy Regulation (2002/58/EC), WP 247, Brüssel 2017.
–, Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is „likely to result in a high risk" for the purposes of Regulation 2016/679, WP 248 rev.01, Brüssel 2017.
–, Stellungnahme 4/2007 zum Begriff „personenbezogene Daten", WP 136, Brüssel 2007.
–, Stellungnahme 1/2010 zu den Begriffen „für die Verarbeitung Verantwortlicher" und „Auftragsverarbeiter", WP 169, Brüssel 2010.
–, Stellungnahme 2/2010 zur Werbung auf Basis von Behavioural Targeting, WP 171, Brüssel 2010.
–, Stellungnahme 15/2011 zur Definition der Einwilligung, WP187, Brüssel 2011.
–, Stellungnahme16/2011zur Best-Practice-Empfehlung von EASA und IAB zu verhaltensorientierter Online-Werbung, WP 188, Brüssel 2011.
–, Stellungnahme 05/2012 zum Cloud Computing, WP 196, Brüssel 2012.
–, Stellungnahme 5/2014 zu Anonymisierungstechniken, WP 216, Brüssel 2014.
–, Stellungnahme 06/2014 zum Begriff des berechtigten Interesses des für die Verarbeitung Verantwortlichen gemäß Artikel 7 der Richtlinie 95/46/EG, WP 217, Brüssel 2014.
–, Stellungnahme 8/2014 zu den jüngsten Entwicklungen im Internet der Dinge, WP 223, Brüssel 2014.
–, Leitlinien zu automatisierten Entscheidungen im Einzelfall einschließlich Profiling für die Zwecke der Verordnung 2016/679, WP 251 rev.01, Brüssel 2018.
–, Leitlinien in Bezug auf die Einwilligung gemäß Verordnung 2016/679, WP 259 rev.01, Brüssel 2018.
–, Leitlinien für Transparenz gemäß der Verordnung 2016/679, WP260 rev.01, Brüssel 2018.
Ashley, *Kevin D.*, Artificial Intelligence and Legal Analytics. New Tools for Law Practice in the Digital Age, Cambridge 2017.

Ashkur, Daniel, Durchsetzung und Sanktionierung des Datenschutzrechts nach den Entwürfen der Datenschutzgrundverordnung, DuD 2015, 796–801.
Auer, Marietta, Materialisierung, Flexibilisierung, Richterfreiheit. Generalklauseln im Spiegel der Antinomien des Privatrechtsdenkens, Tübingen 2005.
–, Neues zu Umfang und Grenzen der richtlinienkonformen Auslegung, NJW 2007, 1106–1109.
–, Digitale Leistungen, ZfPW 2019, 130–147.
Auer-Reinsdsorff, Astrid, Noch mehr Informationspflichten, aber keine transparenten Icons in Sicht, MMR 2019, 209–210.
Ausloos, Jef, The Right to Erasure in EU Data Protection Law, Oxford 2020.
Autorité de la Concurrence/Bundeskartellamt, Competition Law and Data, Joint Report, 10.05.2016.
Ayres, Ian/Gertner, Robert, Filling Gaps in Incomplete Contracts: An Economic Theory of Default Rules, 99 Yale Law Journal (1989), 87–130.
Ayres, Ian/Schwartz, Alan, The No-Reading Problem in Consumer Contract Law, 66 Stanford Law Review (2014), 545–609.
Bach, Ivo, Neue Richtlinien zum Verbrauchsgüterkauf und zu Verbraucherverträgen über digitale Inhalte, NJW 2019, 1705–1711.
Baetge, Dietmar, Allgemeininteressen in der Inhaltskontrolle: Der Einfluss öffentlicher Interessen auf die Wirksamkeit Allgemeiner Geschäftsbedingungen, AcP 202 (2002), 972–993.
Balevi, Eren/Al Rabee, Faeik T./Gitlin, Richard D., ALOHA-NOMA for massive machine-to-machine IoT communication, IEEE International Conference on Communications (ICC) 2018, 1–5.
Balganesh, Shyamkrishna, Quasi-Property: Like, but Not Quite Property, 160 University of Pennsylvania Law Review (2012), 1889–1925.
Bamberger, Kenneth A. u. a., Can You Pay for Privacy? Consumer Expectations and the Behavior of Free and Paid Apps, 35 Berkeley Technology Law Journal (2020), 327–367 (https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3464667).
Bar-Gill, Oren, Seduction by Contract, Oxford 2012.
–, Defending (Smart) Disclosure: Comment on More than You Wanted to Know, 11 Jerusalem Review of Legal Studies (2015), 75–82.
Bartsch, Michael, Die „Vertraulichkeit und Integrität informationstechnischer Systeme" als sonstiges Recht nach § 823 Abs. 1 BGB, CR 2008, 613–617.
Basedow, Jürgen, EuGH: Über Lücken in privatrechtlichen EU-Verordnungen, ZEuP 2014, 402–409.
Bauer, Hartmut, Privatisierung von Verwaltungsaufgaben, VVDStRL 1995, 243–286.
Baumgartner, Ulrich/Gausling, Tina, Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen, ZD 2017, 308–313.
Baumann, Reinhold, Bundesdatenschutzgesetz: Plädoyer für die Beibehaltung der Gesetzeseinheit – zugleich Erwiderung auf Zöllner, RDV 1986, 1–6.
Bäcker, Matthias, Grundrechtlicher Informationsschutz gegen Private, Der Staat 51 (2012), 91–116.
–, Das Grundgesetz als Implementationsgarant der Unionsgrundrechte, EuR 2015, 389–415.
Beater, Axel, Generalklauseln und Fallgruppen, AcP 194 (1994), 82–92.
–, Deliktischer Äußerungsschutz als Rechts- und Erkenntnisquelle des Medienrechts, JZ 2004, 889–893.

Becker, Carina, Das Recht auf Vergessenwerden, Tübingen 2019.
Becker, Christoph, Die Lehre von der laesio enormis in der Sicht der heutigen Wucherproblematik, Köln 1993.
Becker, Maximilian, Ein Recht auf datenerhebungsfreie Produkte, JZ 2017, 171–181.
–, Reconciliating Data Privacy and Trade in Data – A Right to Data-avoiding Products, ZGE/IPJ 2017, 371–393.
Becker, Michael, Der unfaire Vertrag, Tübingen 2003.
BeckOK BGB, Hau, Wolfgang/Poseck, Roman (Hrsg.), 60. Edition, München 2021 (zit.: *Bearbeiter*, in: BeckOK BGB).
BeckOK DatenschutzR, Brink, Stefan/Wolff, Heinrich A. (Hrsg.), 37. Edition, München 2021 (zit.: *Bearbeiter*, in: Brink/Wolff).
Beimowski, Joachim, Zur ökonomischen Analyse Allgemeiner Geschäftsbedingungen, München 1989.
Benedikt, Kristin/Kranig, Thomas: DS-GVO und KUG – ein gespanntes Verhältnis. Ende des KUG nach 111 Jahren?, ZD 2019, 4–7.
Benndorf, Volker/Kübler, Dorothea/Normann, Hans-Theo, Privacy Concerns, Voluntary Disclosure of Information, and Unraveling: An Experiment, 75 European Economic Review 2015, 43–59.
Ben-Shahar, Omri, Data Pollution, 11 Journal of Legal Analysis (2019), 104–159.
Ben-Shahar, Omri/Chilton, Adam, Simplification of Privacy Disclosures: An Experimental Test, 45 Journal of Legal Studies (2016), 41–67.
Ben-Shahar, Omri/Schneider, Carl E., More Than You Wanted to Know, Princeton 2014.
Ben-Shahar, Omri/Strahilevitz, Lior Jacob, Contracting over Privacy: Introduction, 45 Journal of Legal Studies (2016), 1–11.
Berberich, Matthias/Steiner, Malgorzata, Blockchain Technology and the GDPR – How to Reconcile Privacy and Distributed Ledgers, 2 European Data Protection Law Review (2016), 422–426.
Beresford, Alastair R./Kübler, Dorothea/Preibusch, Sören, Unwillingness to pay for privacy: A field experiment, 117 Economics Letters (2012), 25–27.
Bergt, Matthias, Die Bestimmbarkeit als Grundproblem des Datenschutzrechts – Überblick über den Theorienstreit und Lösungsvorschlag, ZD 2015, 365–371.
–, Verhaltensregeln als Mittel zur Beseitigung der Rechtsunsicherheit in der Datenschutz-Grundverordnung, CR 2016, 670–678.
Bettman, James R./Payne, John W./Staelin, Richard, Cognitive Considerations in Designing Effective Labels for Presenting Risk Information, 5 Journal of Public Policy Marketing (1986), 1–28.
Betz, Christoph, Automatisierte Sprachanalyse zum Profiling von Stellenbewerbern, ZD 2019, 148–152.
Beverley-Smith, Huw/Ohly, Ansgar/Lucas-Schloetter, Agnes, Privacy, Property and Personality, Cambridge 2005.
Bier, Christoph/Kühne, Kay/Beyerer, Jürgen, Privacy Insight: the next generation privacy dashboard, Proceedings of the 4th Annual Privacy Forum 2016, 135–152.
Billing, Tom, Die Bedeutung von § 307 III 1 BGB im System der AGB-rechtlichen Inhaltskontrolle, München 2006.
Blendel, Karin, die Ausnahme des Hauptvertragsgegenstands und der Angemessenheit von Preis und Leistung von der Inhaltskontrolle, Jena 2014.

Blume, Peter, The Inherent Contradictions in Data Protection Law, 2 International Data Privacy Law (2012), 26–34.
Bock, *Kirsten*, Data Protection Certification: Decorative or Effective Instrument? Audit and Seals as a Way to Enforce Privacy, in: Wright, David/De Hert, Paul (Hrsg.), Enforcing Privacy. Regulatory, Legal and Technological Approaches, Schweiz 2016, 335–356.
–, Beschränkt das Datenschutzrecht die Vertragsgestaltungsfreiheit, CR 2020, 173–178.
Bock, *Kirsten/Engeler*, *Malte,* Die verfassungsrechtliche Wesensgehaltsgarantie als absolute Schranke im Datenschutzrecht, DVBl. 2016, 593–599.
Boehme-Neßler, *Volker*, Das Recht auf Vergessenwerden, NVwZ 2014, 825–830.
–, Das Ende der Anonymität, DuD, 2016, 419–423.
Bogdandy v., *Armin*, Grundrechtsgemeinschaft als Integrationsziel? Grundrechte und das Wesen der Europäischen Union, JZ 2001, 157–171.
Borking, *John*, Der Identity-Protector, DuD 1996, 654–658.
Böhm, *Franz*, Privatrechtsgesellschaft und Marktwirtschaft, 17 ORDO (1966), 75–151.
–, Demokratie und ökonomische Macht, in: Art. 16 – Freedom to Conduct a Business, in: Johann-Wolfgang-Universität Frankfurt am Main/Institute for International and Foreign Trade Law, Washington, DC (Hrsg.), Kartelle und Monopole im modernen Recht : Beiträge zum übernationalen und nationalen europäischen u. amerikanischen Recht, erstattet für die Internationale Kartellrechtskonferenz in Frankfurt am Main Juni 1960, Karlsruhe 1961.
Böhning, *Björn*, Datenschutz – Die Debatte muss geführt werden, ZD 2013, 421–422.
Borges, *Georg*, Rechtliche Rahmenbedingungen für autonome Systeme, NJW 2018, 977–982.
Botta, *Marco/Wiedemann*, *Klaus*, The interaction of EU competition, consumer, and data protection law in the digital economy: the regulatory dilemma in the Facebook odyssey, 64 The Antitrust Bulletin (2019), 428–446.
Brandimarte, *Laura/Acquisti*, *Alessandro/Loewenstein*, *George*, Misplaced confidences: Privacy and the control paradox, 4 Social Psychological and Personality Science (2013), 340–347.
Bräutigam, *Peter*, Das Nutzungsverhältnis bei sozialen Netzwerken – Zivilrechtlicher Austausch von IT-Leistung gegen personenbezogene Daten, MMR 2012, 635–641.
Bräutigam, *Peter/Klindt*, *Thomas*, Industrie 4.0, das Internet der Dinge und das Recht, NJW 2015, 1137–1142.
Brink, *Stefan/Eckhardt*, *Jens*, Wann ist ein Datum ein personenbezogenes Datum? – Anwendungsbereich des Datenschutzrechts, ZD 2015, 205–212.
Britz, *Gabriele*, Kooperativer Grundrechtsschutz in der EU, NJW 2021, 1489–1495.
–, Grundrechtsschutz durch das Bundesverfassungsgericht und den Europäischen Gerichtshof, EuGRZ 2015, 275–281.
–, Europäisierung des grundrechtlichen Datenschutzes?, EuGRZ 2009, 1–11.
Britz, *Thomas/Indenhuck*, *Moritz/Langerhans*, *Tom*, Die Verarbeitung „zufällig" sensibler Daten, ZD 2021, 559–564.
Brömmelmeyer, *Christoph*, Belohnungen für gesundheitsbewusstes Verhalten in der Lebens- und Berufsunfähigkeitsversicherung? Rechtliche Rahmenbedingungen für Vitalitäts-Tarife, r+s 2017, 225–232.
Buchner, *Benedikt*, Informationelle Selbstbestimmung im Privatrecht, Tübingen 2006.
–, Die Einwilligung im Datenschutzrecht, DuD 2010, 39–43.

–, Grundsätze und Rechtmäßigkeit der Datenverarbeitung unter der DS-GVO, DuD 2016, 155–161.
–, Die Einwilligung in Werbung, WRP 2018, 1283–1289.
–, Datenschutz und Kartellrecht, WRP 2019, 1243–1248.
–, Grundsätze des Datenschutzrechts, in: Tinnefeld, Marie-Therese u. a. (Hrsg.), Einführung in das Datenschutzrecht, 7. Aufl., Berlin 2020, 220–332.
Buchner, *Benedikt/Kühling*, *Jürgen*, DS-GVO/BDSG Kommentar, 3. Aufl., München 2020.
Bull, *Hans Peter*, Sinn und Unsinn des Datenschutzes, Tübingen 2015.
Bundeskartellamt, Fallbericht v. 15.02.2019, Az. B6–22/16 (Facebook; Konditionenmissbrauch gemäß § 19 Abs. 1 GWB wegen unangemessener Datenverarbeitung), 2019 (https://www.bundeskartellamt.de/SharedDocs/Entscheidung/DE/Fallberichte/Missbrauchsaufsicht/2019/B6-22-16.html).
Bunnenberg, *Jan Niklas*, Privates Datenschutzrecht, Baden-Baden 2020.
Busch, *Christoph*, Implementing Personalized Law, 86 The University of Chicago Law Review (2019), 309–332.
Busche, *Jan*, Privatautonomie und Kontrahierungszwang, Tübingen 1999.
Buttarelli, *Giovanni*, The EU GDPR as a clarion call for a new global digital gold standard, 6 International Data Privacy Law (2016), 77–78.
Butterworth, *Michael*, The ICO and artificial intelligence: The role of fairness in the GDPR framework, 34 Computer Law & Security Review (2018), 257–268.
Büchler, *Andrea*, Die Kommerzialisierung von Persönlichkeitsgütern. Zur Dialektik von Ich und Mein, AcP 206 (2006), 300–331.
Bydlinski, *Franz*, Privatautonomie und objektive Grundlagen des verpflichtenden Rechtsgeschäfts, Wien/New York 1967.
–, Erklärungsbewußtsein und Rechtsgeschäft, JZ 1975, 1–6.
–, Juristische Methodenlehre und Rechtsbegriff, 2. Aufl., Wien/NewYork 1991.
–, System und Prinzipien des Privatrechts, Wien 1996.
Cabinakova, *Johana/Zimmermann*, *Christian/Mueller*, *Guenter*, An Empirical Analysis of Privacy Dashboard Acceptance: The Google Case, 24th European Conference on Information Systems (ECIS) 2016, 1–18.
Cabral, Luís/Haucap, Justus/Parker, Geoffrey/Petropoulos, Georgios/Valletti, Tommaso/Van Alstyne, Marshall, The EU Digital Markets Act – A Report from a Panel of Economic Experts 2021.
Calliess, *Christian*, Konfrontation statt Kooperation zwischen BVerfG und EuGH?, NVwZ 2020, 897–904.
Calliess, *Christian/Ruffert*, *Matthias*, EUV/AEUV Kommentar, 5. Aufl., München 2016.
Calo, *Ryan*, Against Notice Skepticism in Privacy (And Elsewhere), 87 Notre Dame Law Review (2012), 1027–1072.
–, Digital Market Manipulation, 82 George Washington Law Review (2014), 995–1051.
Cámara Lapuente, Sergio, Consumer Protection and Procedural Justice, in: Terryn, Evelyne/Straetmans, Gert/Colaert, Veerle (Hrsg.), Landmark Cases of EU Consumer Law: In Honour of Jules Stuyck, Cambridge 2013, 581.
Canaris, *Claus-Wilhelm*, Die Feststellung von Lücken im Gesetz. Eine methodologische Studie über Voraussetzungen und Grenzen der richterlichen Rechtsfortbildung praeter legem, 2. Aufl., Berlin 1983.
–, Gesetzliches Verbot und Rechtsgeschäft, Heidelberg 1983.

–, Systemdenken und Systembegriff in der Jurisprudenz entwickelt am Beispiel des deutschen Privatrechts, 2. Aufl., Berlin 1983.
–, Grundrechte und Privatrecht, AcP 184 (1984), 201–246.
–, Wandlungen des Schuldvertragsrechts – Tendenzen zu seiner „Materialisierung", AcP 200 (2000), 273–364.
–, Die richtlinienkonforme Auslegung und Rechtsfortbildung im System der juristischen Methodenlehre, in: Koziol, Helmut/Rummel Peter (Hrsg.), Im Dienste Der Gerechtigkeit: Festschrift Für Franz Bydlinski, 2002, 47–103.
Caspar, *Johannes*, Klarnamenpflicht versus Recht auf pseudonyme Nutzung, ZRP 2015, 233–236.
Choi, *Jay Pil/Jeon, Doh Shin/Kim, Byung Cheol*, Privacy and personal data collection with information externalities, 173 Journal of Public Economics (2019), 113–124.
Ciacchi, *Aurelia Colombi,* Party Autonomy as a Fundamental Right in the European Union, 6 European Review of Contract Law (2010), 303–318.
Ciacchi, *Aurelia Colombi*, Egenberger and Comparative Law: A Victory of the Direct Horizontal Effect of Fundamental Rights, 5 European Journal of Comparative Law and Governance (2018), 207–211.
Ciocchetti, Corey, The Future of Privacy Policies: A Privacy Nutrition Label Filled with Fair Information Practices, 26 John Marshall Journal of Computer and Information Law (2009), 1–46.
Classen, *Claus Dieter*, Datenschutz ja – aber wie?, EuR 2014, 441–447.
–, Das kirchliche Arbeitsrecht unter europäischem Druck – Anmerkungen zu den Urteilen des EuGH (jeweils GK) vom 17.04.2018 in der C-414/16 (Egenberger) und vom 11.09.2018 in der C-68/17 (IR), EuR 2018, 752–767.
–, Zuviel des Guten? Unionsrechtliche Neuakzentuierungen beim Grundrechtsschutz, JZ 2019, 1057–1066.
Clifford, *Damian*, EU Data Protection Law and Targeted Advertising: Consent and the Cookie Monster-Tracking the Crumbs of Online User Behavior, 5 JIPITEC 2014, 194–212.
Clifford, *Damian/Ausloos*, *Jef*, Data Protection and the Role of Fairness, 37 Yearbook of European Law (2018), 130–187.
Clifford, *Damian/Graef*, *Inge/Valcke*, *Peggy*, Pre-Formulated Declarations of Data Subject Consent – Citizen-Consumer Empowerment and the Alignment of Data, Consumer and Competition Law Protections, 20 German Law Journal (2019), 679–721.
Coester, *Ulla/Fuhlert*, *Bernd*, Gesichtserkennung – eine Frage der Ethik?, DuD 2020, 48–51.
Coester-Waltjen, *Dagmar*, Die Inhaltskontrolle von Verträgen außerhalb des AGBG, AcP 190 (1990), 1–33.
Collins, *Hugh*, Regulating Contracts, Oxford 1999.
–, The impact of human rights law on contract law in Europe, 22 European Business Law Review (2011), 425–435.
Costa-Cabral, *Francisco/Lynskey*, *Orla*, Family Ties: The Intersection between Data Protection and Competition in EU Law, 54 Common Market Law Review (2017), 11–50.
Cranor, *Lorrie Faith*, Necessary but not sufficient: Standardized mechanisms for privacy notice and choice, 10 Journal on Telecommunications & High Technology Law (2012), 273–307.

Crémer, *Jacques/de Montjoye*, *Yves-Alexandre/Schweitzer*, *Heike*, Competition Policy for the Digital Era, report, Brüssel 2019.

Culik, *Nicolai/Döpke*, *Christian*, Zweckbindungsgrundsatz gegen unkontrollierten Einsatz von Big Data-Anwendungen, ZD 2017, 226–230.

Dammann, *Ulrich*, Erfolge und Defizite der EU-Datenschutzgrundverordnung – Erwarteter Fortschritt, Schwächen und überraschende Innovationen, ZD 2016, 307–314.

Danezis, *George u. a.*, Privacy and Data Protection by Design – from policy to engineering, ENISA Report, Heraklion 2014.

Danwitz von, Thomas, Die Grundrechte auf Achtung der Privatsphäre und auf Schutz personenbezogener Daten, DuD 2015, 581–585.

Dasch, Norbert, Die Einwilligung zum Eingriff in das Recht am eigenen Bild, München 1990.

Data Protection Commissioner, Report of Audit 21 December 2011 Facebook Ireland Ltd, Portarlington 2011.

Datenethikkommission, Gutachten der Datenethikkommission, Berlin 2019.

Dauner-Lieb, *Barbara*, Verbraucherschutz durch Ausbildung eines Sonderprivatrechts für Verbraucher. Systemkonforme Weiterentwicklung oder Schrittmacher der Systemveränderung?, Berlin 1983.

Di Fabio, *Udo*, Grundrechtsgeltung in digitalen Systemen. Selbstbestimmung und Wettbewerb im Netz, München 2016.

DIVSI, Daten – Ware und Währung, Hamburg 2014.

Dix, *Alexander*, Daten als Bezahlung – Zum Verhältnis zwischen Zivilrecht und Datenschutzrecht, ZEuP 2017, 1–5.

Dölemeyer, *Barbara/Klippel*, *Diethelm*, Der Beitrag der deutschen Rechtswissenschaft zur Theorie des gewerblichen Rechtsschutzes und Urheberrechts, in: Beier, Friedrich-Karl u. a. (Hrsg.), Festschrift zum 100- jährigen Bestehen der Deutschen Vereinigung für gewerblichen Rechtsschutz und Urheberrecht (GRUR), Weinheim 1991, 185–237.

Drewes, *Stefan*, Kritische Betrachtung der DSK-Orientierungshilfe zu Direktwerbung, ZD 2019, 296–301.

Drexl, *Josef*, Die wirtschaftliche Selbstbestimmung des Verbrauchers, Tübingen 1998.

–, Neue Regeln für die Europäische Datenwirtschaft? Ein Plädoyer für einen wettbewerbspolitischen Ansatz – Teil 2, NZKart 2017, 415–421.

Drexl, *Josef u. a.*, Data Ownership and Access to Data – Position Statement of the Max Planck Institute for Innovation and Competition of 16 August 2016 on the Current European Debate, Max Planck Institute for Innovation & Competition Research Paper No. 16–10, 2016.

DSK, Zur Anwendbarkeit des TMG für nicht-öffentliche Stellen ab dem 25. Mai 2018, Positionsbestimmung, Düsseldorf 2018.

–, Kurzpapier Nr. 20 – Einwilligung nach der DS-GVO, Düsseldorf 2019.

–, Orientierungshilfe der Aufsichtsbehörden für Anbieter von Telemedien, Düsseldorf 2019.

Ducato, *Rossana/Strowel*, *Alain*, Limitations to Text and Data Mining and Consumer Empowerment: Making the Case for a Right to „Machine Legibility", IIC 2019, 649–684.

de la Durantaye, *Katharina*, Wille und Erklärung, Tübingen 2020.

Ebnet, *Peter*, Der Informationsvertrag, Baden-Baden 1995.

Efroni, Zohar/Metzger, Jakob/Mischau, Lena/Schirmbeck, Marie, Privacy Icons: A Risk-Based Approach to Visualisation of Data Processing, 5 European Data Protection Law Review (2019), 352–366.

Ehmann, *Eugen/Selmayr*, *Martin* (Hrsg.), DS-GVO Kommentar, 2. Aufl., München 2018.

Ehmann, *Horst*, Informationsschutz und Informationsverkehr im Zivilrecht, AcP 188 (1988), 230–380.

Eichenhofer, *Johannes*, Privatheit im Internet als Vertrauensschutz. Eine Neukonstruktion der Europäischen Grundrechte auf Privatleben und Datenschutz, Der Staat 55 (2016), 41–67.

Eidenmüller, *Horst*, Der homo oeconomicus und das Schuldrecht: Herausforderungen durch Behavioral Law and Economics, JZ 2005, 216–224.

Eisenberg, *Malvin Aron*, The Limits of Cognition and the Limits of Contract, 47 Stanford Law Review (1995), 211–259.

Engeler, *Malte*, Das überschätzte Kopplungsverbot, ZD 2018, 55–62.

Engeler, *Malte/Felber*, *Wolfram*, Entwurf der ePrivacy-VO aus Perspektive der aufsichtsbehördlichen Praxis, ZD 2017, 251–257.

Engert, *Andreas*, Regelungen als Netzgüter: Eine Theorie der Rechtsvereinheitlichung im Vertragsrecht, AcP 213 (2013), 321–365.

–, Digitale Plattformen, AcP 218 (2018), 304–376.

–, In dubio pro libertate – zum Optionswert vertragsrechtlicher Experimente, in: Grundmann, Stefan/Möslein, Florian (Hrsg.), Innovation und Vertragsrecht, Tübingen 2020, 153–185.

Eppler, Martin J./Mengis, Jeanne, The Concept of Information Overload: A Review of Literature from Organization Science, Accounting, Marketing, MIS, and Related Disciplines, 20 Information Society (2004), 325–344.

Ernst, *Stefan*, Social Plugins: Der „Like-Button" als datenschutzrechtliches Problem, NJOZ 2010, 1917–1919.

–, Die Einwilligung nach der Datenschutzgrundverordnung, ZD 2017, 110–114.

Ertel, *Wolfgang*, Grundkurs Künstliche Intelligenz, 16. Aufl., Berlin 2016.

Ettig, *Diana*, Lizenzansprüche bei Persönlichkeitsrechtsverletzungen, NJW 2021, 1274–1277.

Europäische Kommission, Strategie für einen digitalen Binnenmarkt für Europa, COM(2015) 192 final.

–, Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über bestimmte vertragsrechtliche Aspekte der Bereitstellung digitaler Inhalte, COM(2015) 634 final.

–, Aufbau einer Europäischen Datenwirtschaft, COM(2017) 9 final.

–, Weißbuch zur Künstlichen Intelligenz, COM(2020) 65 final.

European Commission, Attitudes on Data Protection and Electronic Identity in the European Union, Special Eurobarometer 359, Brüssel 2011.

–, A Digital Single Market Strategy for Europe – Analysis and Evidence, Commission Staff Working Document, SWD (2015) 100 final.

–, Advancing the Internet of Things in Europe, Commission Staff Working Document, COM(2016) 180 final.

–, An emerging offer of „personal information management services". Current state of service offers and challenges, Report, Brüssel 2016.

–, Building a European Data Economy, COM(2017) 9 final.

Europäischer Datenschutz Ausschuss (*EDSA*), Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects, Version 2.0, Brüssel, 08.10.2019.

–, Leitlinien 05/2020 zur Einwilligung gemäß Verordnung 2016/679, Version 1.1, v. 04.05.2020.

Europäischer Datenschutz Beauftragter (*EDSB*), Privacy and competitiveness in the age of big data: The interplay between data protection, competition law and consumer protection in the Digital Economy, Preliminary Opinion, Brüssel 2014.

–, Opinion on Personal Information Management Systems: Towards more user empowerment in managing and processing personal data, Opinion 9/2016, Brüssel 2016.

–, On the coherent enforcement of fundamental rights in the age of big data, Opinion 8/2016, Brüssel 2016.

–, EDPS Opinion on the Proposal for a Regulation on Privacy and Electronic Communications (ePrivacy Regulation), Opinion 6/2017, Brüssel 2017.

–, Opinion 4/2017 on the Proposal for a Directive on certain aspects concerning contracts for the supply of digital content, Brüssel 2017.

Evans, *Dave*, The Internet of Everything. How More Relevant and Valuable Connections Will Change the World, Cisco Internet Business Solutions Group (IBSG), Report, San Jose 2012.

Evans, *David S./Schmalensee*, *Richard*, The industrial organization of markets with two-sided platforms, 3 Competition Policy International (2007), 151–179.

Everson, Michelle/Correia Gonçalves, Rui, Art. 16 – Freedom to Conduct a Business, in: Peers, Steve/Hervey, Tamara/Kenner, Jeff/Ward, Angela (Hrsg.), The EU Charter of Fundamental Rights, 2. Aufl., Oxford/München/Baden-Baden 2021, 463–488.

Ezrachi, *Ariel/Stucke*, *Maurice E.*, Is Your Digital Assistant Devious?, Oxford Legal Studies Research Paper No. 52/2016, University of Tennessee Legal Studies Research Paper No. 304, (https://ssrn.com/abstract=2828117).

Faragher, *Ramsey/Harle*, *Robert*, Location fingerprinting with bluetooth low energy beacons, 33 IEEE Journal on Selected Areas in Communications (2015), 2418–2428.

Fastrich, *Lorenz*, Richterliche Inhaltskontrolle im Privatrecht, München 1992.

Faust, *Florian*, Digitale Wirtschaft – Analoges Recht: Braucht das BGB ein Update?, Gutachten zum 71. Deutschen Juristentag, Essen 2016.

Filistrucchi, *Lapo*, Market definition in multi-sided markets, in: OECD (Hrsg.), Rethinking Antitrust Tools for Multi-Sided Platforms, Paris 2018, 37–54.

Filippi de, *Primavera/Wright*, *Aaron*, Blockchain and the Law, Cambridge (MA) 2018.

Flasiński, Mariusz, Introduction to Artificial Intelligence, Berlin 2016.

Fleischer, *Holger*, Informationsasymmetrie im Vertragsrecht, Tübingen 2001.

–, Vertragsschlußbezogene Informationspflichten im Gemeinschaftsprivatrecht, ZEuP 2000, 772–798.

–, Der Rechtsmißbrauch zwischen Gemeineuropäischem Privatrecht und Gemeinschaftsprivatrecht JZ 2003, 865–874.

Flume, *Werner*, Rechtsgeschäft und Privatautonomie, in: von Caemmerer, Ernst u. a. (Hrsg.), Hundert Jahre deutsches Rechtsleben. Festschrift zum hundertjährigen Bestehen des deutschen Juristentages 1860–1960, Karlsruhe 1960, 135–238.

–, Allgemeiner Teil des Bürgerlichen Rechts, Zweiter Band: Das Rechtsgeschäft, 4. Aufl., Heidelberg/New York 1992.

Foerster, *Max*, Automatisierung und Verantwortung im Zivilrecht, ZfPW 2019, 418–435.

Forkel, *Hans*, Zur systematischen Erfassung und Abgrenzung des Persönlichkeitsrechts auf Individualität, in: ders./Kraft, Alfons (Hrsg.), Beiträge zum Schutz der Persönlichkeit und ihrer schöpferischen Leistung, Festschrift für Heinrich Hubmann zum 70. Geburtstag, Frankfurt, 1985, 93–100.

–, Lizenzen an Persönlichkeitsrechten durch gebundene Rechtsübertragung, GRUR 1988, 491–501.

–, Zur Zulässigkeit beschränkter Übertragungen des Namensrechtes, NJW 1993, 3181–3183.

Forgó, *Nikolaus/Helfrich*, *Markus/Schneider*, *Jochen* (Hrsg.), Betrieblicher Datenschutz, 3. Aufl., München 2019.

Fornasier, *Matteo*, Freier Markt und zwingendes Vertragsrecht, Baden-Baden 2013.

de Franceschi, *Alberto*, in: Schmidt-Kessel, Martin/Kramme, Malte (Hrsg.), Geschäftsmodelle in der digitalen Welt, Jena 2017, 113–138.

Franck, *Jens-Uwe*, Eine Frage des Zusammenhangs: Marktbeherrschungsmissbrauch durch rechtswidrige Konditionen, ZWeR 2016, 137–164.

Franzen, *Martin*, Privatrechtsangleichung durch die Europäische Gemeinschaft, Berlin/New York 1999.

Franzen, Martin/Gallner, Inken/Oetker, Hartmut (Hrsg.), Kommentar zum europäischen Arbeitsrecht, 4. Aufl., München 2022.

Funke, *Michael*, Dogmatik und Voraussetzungen der datenschutzrechtlichen Einwilligung im Zivilrecht, Baden-Baden 2017.

Furrer, *Andreas*, Die Sperrwirkung des sekundären Gemeinschaftsrechts auf die nationalen Rechtsordnungen. Die Grenzen des nationalen Gestaltungsspielraums durch sekundärrechtliche Vorgaben unter besonderer Berücksichtigung des „nationalen Alleingangs", Baden-Baden 1994.

Gal, Michal S./Aviv, Oshrit, The Competitive Effects of the GDPR, 16 Journal of Competition Law & Economics (2020), 349–391.

Gal, *Michal S./Elkin-Koren*, *Niva*, Algorithmic Consumers, 30 Harvard Journal of Law and Technology (2016), 309–353.

Gambaro, *Antonio*, Abuse of rights in civil law tradition, 4 European Review of Private Law (1995), 561–570.

Gausling, *Tina*, Künstliche Intelligenz im Anwendungsbereich der Datenschutz-Grundverordnung, PinG 2019, 61–71.

Gänswein, *Olivier*, Der Grundsatz unionsrechtskonformer Auslegung nationalen Rechts, Frankfurt a. M. 2009.

Gellert, *Raphaël*, Data protection: a risk regulation? Between the risk management of everything and the precautionary alternative, 5 International Data Privacy Law (2015), 3–19.

Geminn, *Christian*, Wissenschaftliche Forschung und Datenschutz – Neuerungen durch die Datenschutz-Grundverordnung", DuD 2018, 640–646.

Gierschmann, *Sibylle*, Was „bringt" deutschen Unternehmen die DS-GVO? – Mehr Pflichten, aber die Rechtsunsicherheit bleibt, ZD 2016, 51–55.

Gierschmann, *Sibylle/Schlender*, *Katharina/Stentzel*, *Rainer/Veil*, *Winfried* (Hrsg.), Kommentar Datenschutz-Grundverordnung, Köln 2017.

Giesen, *Thomas*, Das Grundrecht auf Datenverarbeitung, JZ 2007, 918–927.

Gola, *Peter*, Neues Recht – neue Fragen: Einige aktuelle Interpretationsfragen zur DSGVO, K&R 2017, 145–149.

– (Hrsg.), DS-GVO Kommentar, 2. Aufl., München 2018.

Gola, *Peter/Piltz*, *Carlo*, Die Datenschutz-Haftung nach geltendem und zukünftigem Recht – ein vergleichender Ausblick auf Art. 77 DS-GVO, RDV 2015, 279–285.
Goldfarb, *Avi/Greenstein*, *Shane/Tucker*, *Catherine*, Introduction, in: Goldfarb, Alexander/Greenstein, Shane M./Tucker, Catherine E. (Hrsg.), Economic Analysis of the Digital Economy, Chicago/London 2015, 1–17.
Goldhammer, *Klaus/Wiegand*, *André*, Ökonomischer Wert von Verbraucherdaten für Adress- und Datenhändler, Gutachten für das BMJV, Berlin 2017.
Golland, *Alexander*, Das Kopplungsverbot in der Datenschutz-Grundverordnung, MMR 2018, 130–135.
–, Datenverarbeitung in sozialen Netzwerken, Frankfurt a. M. 2019.
Golz, *Robert/Gössling*, *Patrick*, DS-GVO und Recht am Bildnis, IPRB 2018, 68–72.
Goodfellow, *Ian/Bengio*, *Yoshua/Courville*, *Aaron*, Deep Learning, Cambridge (MA) 2016.
Gottschalk, *Eckart*, Das Transparenzgebot und allgemeine Geschäftsbedingungen, AcP 206 (2006), 555–597.
Görs, *Benjamin*, Statement, in: Lohsse, Sebastian/Schulze, Reiner/Staudenmayer, Dirk (Hrsg.), Data as Counter-Performance: Contract Law 2.0?, Oxford/Baden-Baden 2020, 265–266.
Götting, *Horst-Peter*, Persönlichkeitsrechte als Vermögensrechte, Tübingen 1995.
Götting, *Horst-Peter/Schertz*, *Christian/Seitz*, *Walter*, Handbuch Persönlichkeitsrecht, 2. Aufl., München 2019.
Grabitz, *Eberhard/Hilf*, *Meinhard*, Das Recht der Europäischen Union, 40. Aufl., München 2009.
Grabitz, *Eberhard/Hilf*, *Meinhard/Nettesheim*, *Martin*, Das Recht der Europäischen Union: EUV/AEUV, 65. EL, München, August 2018.
Graef, *Inge/Clifford*, *Damian/Valcke*, *Peggy*, Fairness and enforcement: bridging competition, data protection, and consumer law, 8 International Data Privacy Law (2018), 200–223.
Graef, *Inge/Verschakelen*, *Jeroen/Valcke*, *Peggy*, Putting the right to data portability into a competition law perspective, 4 Law: The Journal of the Higher School of Economics, Annual Review (2013), 53–63.
Grafenstein von, *Maximilian*, Das Zweckbindungsprinzip zwischen Innovationsoffenheit und Rechtssicherheit, DuD 2015, 789–795.
Gray, Stacey, Always On: Privacy Implications of Microphone-Enabled Devices, Future of Privacy Forum, 2016 (https://fpf.org/wp-content/uploads/2016/04/FPF_Always_On_WP.pdf).
Grigoleit, *Hans Christoph*, Vorvertragliche Informationshaftung, München 1997.
–, Der Verbraucheracquis und die Entwicklung des Europäischen Privatrechts, AcP 210 (2010), 354–423.
Grigoleit, *Hans Christoph/Bender*, *Philip Maximilian*, The Law between Generality and Particularity – Potentials and Limits of Personalized Law, in: Busch, Christoph/De Franceschi, Alberto (Hrsg.), Data Economy and Algorithmic Regulation, 2020, 115–136.
Grimm, *Anna*, Telematiktarife: Existierende Tarifmodelle und ihre Funktionsweisen im Kfz-Bereich, in: Schmidt-Kessel, Martin/Grimm, Anna (Hrsg.), Telematiktarife & Co. – Versichertendaten als Prämienersatz, 2018, 47–60.
Grimm, Dieter, Der Datenschutz vor einer Neuorientierung, JZ 2013, 585–592.

Grossklags, *Jens/Acquisti*, *Alessandro*, When 25 Cents is too Much: An Experiment on Willingness-to-Sell and Willingness-to-Protect Personal Information, Proceedings of the Sixth Workshop on Economics of Information Security 2007, 1–22.

Grünberger, *Michael*, Verträge über digitale Güter, AcP 218 (2018), 213–296.

–, Responsive Rechtsdogmatik – Eine Skizze, AcP 219 (2019), 924–942.

Grünberger, *Michael/Jansen*, *Nils*, Perspektiven deutscher Privatrechtstheorie, in: Grünberger, Michael/Jansen, Nils (Hrsg.), Privatrechtstheorie heute, Tübingen 2017, 1–44.

Grundmann, *Stefan*, Richtlinienkonforme Auslegung im Bereich des Privatrechts – insbesondere: der Kanon der nationalen Auslegungsmethoden als Grenze?, ZEuP 1996, 399–424.

–, Privatautonomie im Binnenmarkt, JZ 2000, 1133–1143.

–, Privatautonomie, Vertragsfunktion und „Richtigkeitschance"?, in: Grundmann, Stefan/Micklitz, Hans-W./Renner, Moritz (Hrsg.), Privatrechtstheorie, Band I, Tübingen 2015, 875–902.

–, Privatrecht und Regulierung, in: Grigoleit, Hans C./Petersen, Jens (Hrsg.), Privatrechtsdogmatik im 21. Jahrhundert: Festschrift für Claus-Wilhelm Canaris zum 80. Geburtstag, Berlin/Boston, 2017, 907–948.

Grundmann, *Stefan/Kerber*, *Wolfgang/Weatherill*, *Stephen*, Party Autonomy and the Role of Information – an Overview, in: Grundmann, Stefan u. a. (Hrsg.), Party Autonomy and the Role of Information in the Internal Market, Berlin/New York 2001, 3–38.

Gsell, *Beate*, Zivilrechtsanwendung im Europäischen Mehrebenensystem, AcP 214 (2014), 99–150.

–, Der europäische Richtlinienvorschlag zu bestimmten vertragsrechtlichen Aspekten der Bereitstellung digitaler Inhalte, ZUM 2018, 75–82.

Guckelberger, *Annette*, Veröffentlichung der Leistungsempfänger von EU-Subventionen und unionsgrundrechtlicher Datenschutz, EuZW 2011, 126–130.

Habermas, *Jürgen*, Strukturwandel der Öffentlichkeit: Untersuchung zu einer Kategorie es bürgerlichen Gesellschaft, Frankfurt a. M. 1962.

Habersack, *Mathias/Mayer*, *Christian*, Die überschießende Umsetzung von Richtlinien, in: Riesenhuber, Karl (Hrsg.), Europäische Methodenlehre, 4. Aufl., Berlin 2021, 452–491.

Hacker, *Philipp*, Verhaltensökonomik und Normativität. Die Grenzen des Informationsmodells im Privatrecht und seine Alternativen, Tübingen 2017.

–, Daten als Gegenleistung: Rechtsgeschäfte im Spannungsfeld von DS-GVO und allgemeinem Vertragsrecht, ZfPW 2019, 148–197.

–, Regulating the Economic Impact of Data as Counter-Performance: From the Illegality Doctrine to the Unfair Contract Terms Directive, in: Lohsse, Sebastian/Schulze, Reiner/Staudenmayer, Dirk (Hrsg.), Data as Counter-Performance: Contract Law 2.0?, Oxford/Baden-Baden 2020, 47–76.

–, Datenprivatrecht, Tübingen 2020.

Hanloser, *Stefan*, Anmerkung zu BGH: Opt-out durch Streichen der Einwilligungsklausel – HappyDigits, MMR 2010, 140–141.

–, Geräte-Identifier im Spannungsfeld von DS-GVO, TMG und ePrivacy-VO, ZD 2018, 213–218.

–, Anmerkung zu FashionID, ZD 2019, 458–460.

–, Keine gemeinsame Verantwortlichkeit für Datenspeicherung durch Facebook – Fashion ID, ZD 2019, 122–124.
–, Umsetzungslücken bei der ePrivacy-RL – Planet 49, ZD 2019, 264–266.
Hansen, *Marit/Berlich, Peter/Camenisch, Jan/Clauß*, *Sebastian/Pfitzmann, Andreas / Waidner*, *Michael*, Privacy-enhancing identity management, 9 Information Security Technical Report (2004), 35–44.
Hansen, *Marit/Hoepman*, *Jaap-Henk/Jensen*, *Meiko*, Readiness for the Adoption and Evolution of Privacy Enhancing Technologies, ENISA Report, Heraklion 2015.
Hansen, *Marit/Limniotis*, *Konstantinos*, Recommendations on shaping technology according to GDPR provisions. Exploring the notion of data protection by default, ENISA Report, Attiki 2018.
Härting, *Niko*, EuGH: Auslegung von „Verarbeitung personenbezogener Daten", CR 2009, 229–233.
–, Digital Goods und Datenschutz – Daten sparen oder monetarisieren?, CR 2016, 735–740.
–, DS-GVO Kommentar, Köln 2016.
Härting, *Niko/Schneider*, *Jürgen*, Datenschutz in Europa: Ein Alternativentwurf für eine Datenschutz-Grundverordnung, CRi 2013, Supplement 1, 19–38.
–, Das Ende des Datenschutzes – es lebe die Privatsphäre. Eine Rückbesinnung auf die Kern-Anliegen des Privatsphärenschutzes, CR 2015, 819–827.
Hayek, *Friedrich A.*, The Use of Knowledge in Society, 35 American Economic Review (1945), 519–530.
Heinrich, *Christian*, Formale Freiheit und materiale Gerechtigkeit, Tübingen 2000.
Heinze, *Christian*, Schadensersatz im Unionsprivatrecht. Eine Studie zu Effektivität und Durchsetzung des Europäischen Privatrechts am Beispiel des Haftungsrechts, Tübingen 2017.
Heinzke, *Philippe/Engel*, *Lennart*, Datenverarbeitung zur Vertragserfüllung – Anforderungen und Grenzen, ZD 2020, 189–194.
Helberger, *Natali*, Profiling and Targeting Consumers in the Internet of Things, in: Schulze, Reiner/Staudenmayer, Dirk (Hrsg.), Digital Revolution: Challenges for Contract Law in Practice, Baden-Baden 2016, 135–162.
Helberger, *Natali/Zuiderveen Borgesius*, *Frederik/Reyna*, *Agustin*, The Perfect Match? A Closer Look at the Relationship between EU Consumer Law and Data Protection Law, 54 Common Market Law Review (2017), 1427–1466.
Helle, *Jürgen*, Die Einwilligung beim Recht am eigenen Bild, AfP 1985, 93–101.
–, Wirtschaftliche Aspekte zivilrechtlichen Persönlichkeitsschutzes, RabelsZ 60 (1996), 448–474.
Hellgardt, *Alexander*, Regulierung und Privatrecht, Tübingen 2016.
–, Wer hat Angst vor der unmittelbaren Drittwirkung?, JZ 2018, 901–911.
Hennemann Moritz, Datenportabilität, PinG 2017, 5–8.
–, Interaktion und Partizipation – Dimensionen systemischer Bindung im Vertragsrecht, Tübingen 2020.
Herbst, *Tobias*, Was sind personenbezogene Daten?, NVwZ 2016, 902–906.
Herfurth, *Constantin*, Interessenabwägung nach Art. 6 Abs. 1 lit. f DS-GVO, ZD 2018, 514–520.
Hermstrüwer, *Yoan*, Informationelle Selbstgefährdung. Zur rechtsfunktionalen, spieltheoretischen und empirischen Rationalität der datenschutzrechtlichen Einwilligung und des Rechts auf informationelle Selbstbestimmung, Tübingen 2016.

–, Contracting Around Privacy: The (Behavioral) Law and Economics of Consent and Big Data, JIPITEC 2017, 9–26.
Herpig, *Sven/Heinemeyer*, *Max*, Maschinelles Lermen als Angriffsobjekt, in: Ebers, Martin/Steinrötter, Björn (Hrsg.), Künstliche Intelligenz und smarte Robotik im IT-Sicherheitsrecht, Baden-Baden, 2021, 65–90.
Herresthal, *Carsten*, Rechtsfortbildung im europarechtlichen Bezugsrahmen, München 2006.
–, Constitutionalisation of Freedom of Contract in EC Law, in: Huber, Peter M/Ziegler, Katja S. (Hrsg.), Current Problems in the Protection of Human Rights: Perspectives from Germany and the UK, 2013, 89–116.
–, Die Bedeutung der Charta der Grundrechte für das europäische und das nationale Privatrecht, ZEuP 2014, 238–280.
Hert De, *Paul u. a.*, The right to data portability in the GDPR: Towards user-centric interoperability of digital interoperability of digital services, Computer Law & Security Review 2018, 93–103.
Hesse, Konrad, Der Rechtsstaat im Verfassungssystem des Grundgesetzes, in: Smend, Rudolf/Hesse, Konrad/Reicke, Siegfried (Hrsg.), Staatsverfassung und Kirchenordnung : Festgabe f. Rudolf Smend zum 80. Geburtstag am 15. Jan. 1962, Freiburg 1962, 71.
Heun, *Sven-Erik/Assion*, *Simon*, Internet(recht) der Dinge, CR 2015, 812–818.
–, Smart Services: IT- und datenschutzrechtliche Herausforderungen, BB 2018, 579–584.
Heyer, *Hans Ulrich*, Anmerkung zu LG Frankfurt a. M., Urt. v. 20.12.2018 – 2/5 O 151/18: Anspruch auf vorzeitige Löschung von Insolvenzdaten in Auskunfteien nach der DSGVO, NZI 2019, 344–345.
Hinton, *Geoffrey E.*, Learning distributed representations of concepts, Proceedings of the Eighth Annual Conference of the Cognitive Science Society, 1986, 1–12.
Hinton, *Geoffrey E./Osindero*, *Simon/Teh*, *Yee-Whye*, A fast learning algorithm for deep belief nets, 18 Neural Computation (2006), 1527–1554.
von Hippel, *Fritz*, Das Problem der rechtsgeschäftlichen Privatautonomie. Beiträge zu einem Natürlichen System des privaten Verkehrsrechts und zur Erforschung der Rechtstheorie des 19. Jahrhunderts, Tübingen 1936.
Hoeren, *Thomas*, Wenn Sterne kollabieren, entsteht ein schwarzes Loch – Gedanken zum Ende des Datenschutzes, ZD 2011, 145–146.
–, Big Data und Datenqualität – ein Blick auf die DS-GVO, ZD 2016, 459–463.
–, Thesen zum Verhältnis von Big Data und Datenqualität – Erstes Raster zum Erstellen juristischer Standards, MMR 2016, 8–11.
–, Kartell- oder Datenschutzrecht: BKartA untersagt Facebook die Zusammenführung von Nutzerdaten, MMR 2019, 137–138.
Hoffmann, *Christian*, Die Verletzung der Vertraulichkeit informationstechnischer Systeme durch Google Street View, CR 2010, 514–518.
Hoffmann, *Jan Felix*, „Dateneigentum" und Insolvenz, JZ 2019, 960–968.
Hoffmann-Riem, *Wolfgang*, Informationelle Selbstbestimmung in der Informationsgesellschaft, AöR 123 (1998), 513–540.
–, Der grundrechtliche Schutz der Vertraulichkeit und Integrität eigengenutzter informationstechnischer Systeme, JZ 2008, 1009–1022.
–, Innovation und Recht – Recht und Innovation. Recht im Ensemble seiner Kontexte, Tübingen 2016.

–, Verhaltenssteuerung durch Algorithmen – Eine Herausforderung für das Recht, AöR 142 (2017), 1–42.
Hofmann, Franz, The economic part of the right to personality as an intellectual property right? A comparison between English and German Law, ZGE/IPJ 2010, 1–18.
–, Der maßgeschneiderte Preis, WRP 2016, 1074–1081.
Hoofnagle, *Chris Jay/Whittington*, *Jan*, Free: Accounting for the Costs of the Internet's Most Popular Price, 61 UCLA Law Review (2014), 606–670.
Hornung, *Gerrit*, Anmerkung zu EuGH, Urt. v. 09.11.2010, verbundene Rs. C-92/09 und C-93/09 (Schecke), MMR 2011, 127–128.
Hornung, *Gerrit/Wagner*, *Bernd*, Der schleichende Personenbezug, CR 2019, 565–574.
–, Anonymisierung als datenschutzrelevante Verarbeitung? Rechtliche Anforderungen und Grenzen für die Anonymisierung personenbezogener Daten, ZD 2020, 223–228.
Höfling, *Wolfram*, Vertragsfreiheit: Eine grundrechtsdogmatische Studie, Heidelberg 1991.
Huber, Peter M., Staat und Wissenschaft, Paderborn 2008.
–, Auslegung und Anwendung der Charta der Grundrechte, NJW 2011, 2385–2390.
–, Zur Drittwirkung von Grundrechten und Grundfreiheiten, in: Ruffert, Matthias (Hrsg.), Dynamik und Nachhaltigkeit des Öffentlichen Rechts: Festschrift für Professor Dr. Meinhard Schröder zum 70. Geburtstag, Berlin 2012, 336–342.
Hubmann, Heinrich, Das Persönlichkeitsrecht, Tübingen 1967.
Indenhuck, *Moritz/Britz*, *Thomas*, Vom Datenschutzrecht zum Datenschuldrecht – Neue Leitlinien zur Verarbeitung personenbezogener Daten bei Online-Dienstleistungen, BB 2019, 1091–1096.
Jandt, *Silke*, Spezifischer Datenschutz für Telemedien und die DS-GVO. Zwischen Rechtssetzung und Rechtsanwendung, ZD 2018, 405–408.
Jangl, *Jana*, Berichten ja, Bebildern nein? Presseberichterstattung über das nicht öffentliche Scheidungsverfahren einer prominenten deutschen Schauspielerin mit Blick auf das Verhältnis von KUG und DSGVO, ZUM 2021, 103–111.
Jarass, *Hans Dieter*, Die Bedeutung der Unionsgrundrechte unter Privaten, ZEuP 2017, 310–334.
–, Charta der Grundrechte der Europäischen Union: GRCh-Kommentar, 4. Aufl., München 2021.
Jentzsch, *Nicola,* Datenhandel und Datenmonetarisierung: Ein Überblick, in: Stiftung Datenschutz (Hrsg.), Dateneigentum und Datenhandel, 2019, 177–190.
John, *Leslie K./Acquisti*, *Alessandro/Loewenstein*, *George*, Strangers on a plane: Context-dependent willingness to divulge sensitive information, 37 Journal of Consumer Research (2011), 858–873.
Johannes, *Paul C./Roßnagel*, *Alexander*, Der Rechtsrahmen für einen Selbstschutz der Grundrechte in der Digitalen Welt, Kassel 2016.
Jolls, *Christine/Sunstein*, *Cass R.*, Debiasing through Law, 35 The Journal of Legal Studies (2006), 199–242.
Jülicher, *Tim*, Die Aussonderung von (Cloud-)Daten nach § 47 InsO, ZIP 2015, 2063–2066.
Kainer, *Friedemann*, Privatrecht zwischen Richtlinien und Grundrechten. Zu den Grenzen richtlinienkonformer Auslegung und horizontalen Richtlinienwirkungen, GPR 2016, 262–270.
Kamp, *Meike/Rost*, *Martin*, Kritik an der Einwilligung, DuD 2012, 80–84.

Kampert, *David*, Datenschutz in sozialen Online-Netzwerken de lege lata und de lege ferenda, Hamburg 2016.

Karg, *Moritz/Kühn*, *Ulrich*, Datenschutzrechtlicher Rahmen für „Device Fingerprinting" – Das klammheimliche Ende der Anonymität im Internet, ZD 2014, 285–290.

Kelley, *Patrick Gage u. a.*, Standardizing privacy notices: An online study of the nutrition label approach, Proceedings of the 28th International Conference on Human Factors in Computing Systems, 2010, 1573–1582.

Kerber, *Wolfgang*, Digital Markets, Data and Privacy: Competition Law, Consumer Law and Data Protection, GRUR Int. 2016, 639–647.

–, Data Governance in Connected Cars. The Problem of Access to In-Vehicle Data, JIPITEC 2018, 318–331.

Kernow, *Curtis E.A.*, The application of traditional tort theory to embodied machine intelligence, in: Calo, Ryan/Froomkin, Michael A./Kerr, Ian (Hrsg.), Robot Law, Oxford 2016, 51–77.

Kettner, *Sara Elisa/Thorun*, *Christian/Vetter*, *Max*, Wege zur besseren Informiertheit – Verhaltenswissenschaftliche Ergebnisse zur Wirksamkeit des One-Pager-Ansatzes und weiterer Lösungsansaätze im Datenschutz, Abschlussbericht der ConPolicy GmbH im Auftrag der Bundesanstalt für Landwirtschaft und Ernährung, 28.02.2018.

Kettner, Sara Elisa/Thorun, Christian/Spindler, *Gerald*, Innovatives Datenschutz-Einwilligungsmanagement, Abschlussbericht der ConPolicy GmbH im Auftrag des BMJV, 07.09.2020.

Kilian, *Wolfgang*, Personalinformationssysteme in deutschen Großunternehmen: Ausbaustand und Rechtsprobleme (Informationstechnik und Datenverarbeitung), Berlin 1967.

–, Juristische Entscheidung und elektronische Datenverarbeitung: Methodenorientierte Vorstudie, Darmstadt 1974.

–, Äußeres und inneres System in einem noch fragmentarischen Europäischen Schuldvertragsrecht?, in: Grundmann, Stefan (Hrsg.), Systembildung und Systemlücken in Kerngebieten des Europäischen Privatrechts, Tübingen 2000, 427–441.

–, Informationelle Selbstbestimmung und Marktprozesse. Zur Notwendigkeit der Modernisierung des Modernisierungsgutachtens zum Datenschutzrecht, CR 2002, 921–929.

–, Personal Data: The impact of Emerging Trends in the Information Society, CRi 2012, 169–175.

–, Strukturwandel der Privatheit, in: Garstka, Hansjürgen/Coy, Wolfgang (Hrsg.), Wovon – für wen – wozu? Systemdenken wider die Diktatur der Daten, Wilhelm Steinmüller zum Gedächtnis, Berlin 2014, 195–224.

Kinast, *Karsten/Kühnl*, *Christina*, Telematik und Bordelektronik – Erhebung und Nutzung von Daten zum Fahrverhalten, NJW 2014, 3057–3061.

Kingreen, Thorsten/Kühling, *Jürgen*, Weniger Schutz durch mehr Recht: Der überspannte Parlamentsvorbehalt im Datenschutzrecht – Eine Problemskizze am Beispiel des Gesundheitsdatenschutzrechts, JZ 2015, 213–221.

Kipker, *Dennis-Kenji/Kubis*, *Marcel*, Anmerkung zu Breyer, MMR 2017, 608–610.

Kipp, *Theodor*, Über Doppelwirkungen im Recht, insbesondere über die Konkurrenz von Nichtigkeit und Anfechtbarkeit, in: Kormann, Karl (Hrsg.), Festschrift der Berliner Juristischen Fakultät für Ferdinand von Martitz zum fünfzigjährigen Doktorjubiläum am 24. Juli 1911, Berlin 1911, 211–234.

Klass, *Nadine*, Die zivilrechtliche Einwilligung als Instrument zur Disposition über Persönlichkeitsrechte, AfP 2005, 507–518.
–, Das Recht auf Vergessen(-werden) und die Zeitlichkeit der Freiheit, ZUM 2020, 265–279.
Klement, *Jan Henrik*, Wettbewerbsfreiheit, Tübingen 2015.
–, Öffentliches Interesse an Privatheit, JZ 2017, 161–170.
Klimke, *Dominik*, Telematik-Tarife in der Kfz-Versicherung, r+s 2015, 217–225.
Klink-Straub, *Judith*, Do ut des data – Bezahlen mit Daten im digitalen Vertragsrecht, NJW 2021, 3217–3222.
Klippel, Diethelm, Der zivilrechtliche Schutz des Namens, Eine historische und dogmatische Untersuchung, Paderborn 1985.
–, Deliktsrechtliche Probleme des Datenschutzes, BB 1983, 407–414.
Knauff, Matthias, Auslegung oder Anwendung des Europarechts?, DÖV 2013, 375–380.
Knopp, *Michael*, Datenschutzherausforderung Webtracking, DuD 2010, 783–786.
Kohler, *Josef*, Das Autorrecht: Eine zivilistische Abhandlung, Zugleich ein Beitrag zur Lehre vom Eigenthum, vom Miteigenthum, vom Rechtsgeschäft und vom Individualrecht, Jena 1880.
–, Der Fall der Bismarckphotographie, GRUR 1900, 206–208.
Kohn, *Joachim*, Der Schadensersatzanspruch nach Art. 82 DS-GVO, ZD 2019, 498–502.
Kohte, *Wolfhard*, Die rechtfertigende Einwilligung, AcP 185 (1985), 105–161.
Köhler, *Helmut*, Wettbewerbsverstoß und Vertragsnichtigkeit, JZ 2010, 767–774.
–, Die DS-GVO – eine neue Einnahmequelle für gewerbsmäßige Abmahner?, ZD 2018, 337–338.
–, Durchsetzung der DS-GVO mittels UWG und UKlaG?, WRP 2018, 1269–1277.
Köhler, *Helmut/Bornkamm*, *Joachim/Feddersen*, *Jörn* (Hrsg.), Gesetz gegen den unlauteren Wettbewerb (UWG), 39. Aufl., München 2021.
Köndgen, *Johannes*, Grund und Grenzen des Transparenzgebots im AGB-Recht – Bemerkungen zum „Hypothekenzins-" und zum „Wertstellungs-Urteil" des BGH, NJW 1989, 943–952.
Köndgen, *Johannes/Mörsdorf*, *Oliver*, § 6 Die Rechtsquellen des Europäischen Privatrechts, in: Riesenhuber, Karl (Hrsg.), Europäische Methodenlehre, 4. Aufl., Berlin 2021, 131–180.
Körber, *Torsten*, Grundfreiheiten und Privatrecht, Tübingen 2004.
–, „Ist Wissen Marktmacht?" Überlegungen zum Verhältnis von Datenschutz, „Datenmacht" und Kartellrecht – Teil 2, NZKart 2016, 348–356.
–, Die Facebook-Entscheidung des Bundeskartellamtes – Machtmissbrauch durch Verletzung des Datenschutzrechts?, NZKart 2019, 187–195.
Korobkin, *Russell B./Ulen*, *Thomas S.*, Law and behavioral science: Removing the rationality assumption from law and economics, 88 California Law Review (2000), 1051–1144.
Korobkin, *Russell*, The Status Quo Bias and Contract Default Rules, 83 Cornell Law Review (1998), 608–687.
Krause, Peter, Die Rechtsprechung des Bundesverfassungsgerichts zum Privatrecht – Teil I, JZ 1984, 656–663.
Kring, *Markus/Marosi*, *Johannes*, Ein Elefant im Porzellanladen – Der EuGH zu Personenbezug und berechtigtem Interesse K&R 2016, 773–776.
Krohm, *Niclas/Müller-Peltzer*, *Philipp*, Auswirkungen des Kopplungsverbots auf die Praxistauglichkeit der Einwilligung, ZD 2017, 551–556.

Krönke, *Christoph*, Datenpaternalismus. Staatliche Interventionen im Online-Daten-Verkehr zwischen Privaten, dargestellt am Beispiel der Datenschutz-Grundverordnung, Der Staat 55 (2016), 319–351.
Krügel, *Tina*, Das personenbezogene Datum nach der DS-GVO, ZD 2017, 455–460.
Kubat, *Miroslav*, An introduction to machine learning, 2. Aufl., Berlin 2017.
Kurzweil, *Ray*, The Age of the Spiritual Machine, East Rutherford 1999.
Kühling, *Jürgen*, Datenschutz in einer künftigen Welt allgegenwärtiger Datenverarbeitung, Aufgabe des Rechts?, DV 2007, 153–172.
–, Die Europäisierung des Datenschutzrechts. Gefährdung deutscher Grundrechtsstandards?, Baden-Baden 2014.
–, Das „Recht auf Vergessenwerden" vor dem BVerfG – November(r)evolution für die Grundrechtsarchitektur im Mehrebenensystem, NJW 2020, 275–280.
–, Der datenschutzrechtliche Rahmen für Datentreuhänder, ZfDR 2021, 1–26.
Kühling, *Jürgen/Buchner*, *Benedikt* (Hrsg.), DS-GVO/BDSG, 2. Aufl., München 2018.
Kühling, *Jürgen/Klar*, *Manuel*, Unsicherheitsfaktor Datenschutzrecht – Das Beispiel des Personenbezugs und der Anonymität, NJW 2013, 3611–3617.
–, Anmerkung zu Breyer, ZD 2017, 27–29.
Kühling, *Jürgen/Klar*, *Manuel/Sackmann*, *Florian*, Datenschutzrecht, 4. Aufl., Heidelberg 2018.
Kühling, *Jürgen/Martini*, *Mario*, Die Datenschutz-Grundverordnung: Revolution oder Evolution im europäischen und deutschen Datenschutzrecht?, EuZW 2016, 448–454.
Kühling, *Jürgen/Sackmann*, *Florian*, Das Mehrebenensystem der Datenschutzgrundrechte im Lichte der Rechtsprechung von BVerfG und EuGH, JURA 2018, 364–377.
–, Irrweg Dateneigentum", ZD 2020, 24–30.
Labudde, *Dirk*, Künstliche Intelligenz und IT-Sicherheit – eine Bestandsaufnahme, in: Ebers, Martin/Steinrötter, Björn (Hrsg.), Künstliche Intelligenz und smarte Robotik im IT-Sicherheitsrecht 2021, 25–63.
Lang, *Sonja/Peintinger*, *Stefan*, Die wirksame Einwilligung im Datenschutzrecht, ELR 2013, 206–215.
Lanier, *Jaron,* Who Owns the Future?, New York 2013.
Langhanke, *Carmen*, Daten als Leistung, Tübingen 2018.
Langhanke, *Carmen/Schmidt-Kessel*, *Martin*, Consumer Data as Consideration, EuCML 2015, 218–223.
Larenz, *Karl/Canaris*, *Claus-Wilhelm*, Methodenlehre der Rechtswissenschaft, 3. Aufl., Berlin/Heidelberg 1995.
Lauber-Rönsberg, *Anne*: Anwendbarkeit des KUG bei journalistischen Bildnisveröffentlichungen auch nach Inkrafttreten der DSGVO – Anmerkung zu OLG Köln, Beschluss vom 18.06.2018 – 15 W 27/18, ZUM-RD 2018, 549–552.
Leistner, Matthias, Behavioral Economics und Lauterkeitsrecht, ZGE 2009, 3–58.
Leistner, Matthias/Antoine, *Lucie/Sagstetter*, *Thomas*, BIG Data, Tübingen 2021.
Lepsius, *Oliver*, Die maßstabsetzende Gewalt, in: Jestaedt, Matthias u. a. (Hrsg.), Das entgrenzte Gericht. Eine kritische Bilanz nach sechzig Jahren Bundesverfassungsgericht, Berlin 2011,159–179.
–, Der Privatrechtsdiskurs der Moderne aus der Sicht des öffentlichen Rechts, in: Grünberger, Michael/Jansen, Nils (Hrsg.), Privatrechtstheorie heute. Perspektiven deutscher Privatrechtstheorie, Tübingen 2017, 82–97.
Lerche, Peter, Zur Bindung der Tarifnormen an Grundrechte, insbesondere an das Grundrecht der Berufsfreiheit, in: Baur, Hürgen F./Hopt, Klaus J./Mailänder, K. Peter

(Hrsg.), Festschrift für Ernst Steindorff zum 70. Geburtstag am 13. März 1990, Berlin 1990, 897–910.
Lessig, *Lawrence*, Code. And Other Laws of Cyberspace, New York 1999.
Lewinski von, *Kai*, Europäisierung des Datenschutzrechts, DuD 2012, 564–570.
–, Die Matrix des Datenschutzes. Besichtigung und Ordnung eines Begriffsfeldes, Tübingen 2014.
Lewinski von, *Kai/Herrmann*, *Christoph*, Cloud vs. Cloud – Datenschutz im Binnenmarkt, ZD 2016, 467–474.
Lianos Iannis/Motchenkova, Evgenia, Market dominance and search quality in the search engine market. 9 Journal of Competition Law & Economics (2013), 419–455.
Lindacher, *Walter*, Grundsätzliches zu § 138 BGB: Zur Frage der Relevanz subjektiver Momente, AcP 173 (1973), 124–136.
Littman, *Michael L.*, Reinforcement learning improves behaviour from evaluative feedback, 521 Nature (2015), 445–451.
Lobinger, *Thomas*, Irrtumsanfechtung und Reurechtsausschluß, AcP 195 (1995), 274–282.
Loewenstein, *George u. a.*, Warning: You are about to be nudged, 1 Behavioral Science & Policy (2015), 35–42.
Lohse, *Andrea*, Facebook und die Verarbeitung der off-Facebook-Daten nach der DSGVO: Ein Fall für die kartellrechtliche Missbrauchsaufsicht?, NZKart 2020, 292–299.
Loos, *Marco/Luzak*, *Joasia*, Wanted: A Bigger Stick. On Unfair Terms in Consumer Contracts with Online Service Providers, 39 Journal of Consumer Policy (2016), 63–90.
Lorenz, *Stephan*, Der Schutz vor dem unerwünschten Vertrag, München 1997.
Luch, *Anika*, Das neue „IT-Grundrecht". Grundbedingung einer „Online-Handlungsfreiheit" MMR 2011, 75–79.
Luch, *Anika/Schulz*, *Sönke/Kuhlmann*, *Florian*, Ein Recht auf Vergessenwerden als Ausprägung einer selbstbestimmten digitalen Persönlichkeit, EuR 2014, 698–705.
Luhmann, *Niklas*, Recht und Automation in der öffentlichen Verwaltung. Eine verwaltungswissenschaftliche Untersuchung, Berlin 1966.
–, Grundrechte als Konstitution. Ein Beitrag zur politischen Soziologie, Berlin 1995.
Lüdemann, *Volker*, Connected Cars – Das vernetzte Auto nimmt Fahrt auf, der Datenschutz bleibt zurück, ZD 2015, 247–254.
Lüttringhaus, *Jan*, Vertragsfreiheit und ihre Materialisierung im Europäischen Binnenmarkt, Tübingen 2018.
Lynskey, *Orla*, The Foundations of EU Data Protection Law, Oxford 2015.
MacCarthy, Mark, New Directions in Privacy: Disclosure, Unfairness and Externalities." I/S: A Journal of Law and Policy for the Information Society 6.3 (2011), 425–512.
Mackenrodt, *Mark-Oliver/Wiedemann*, *Klaus*, Zur kartellrechtlichen Bewertung der Datenverarbeitung durch Facebook und ihrer normativen Kohärenz mit dem Datenschutzrecht und dem Datenschuldrecht. Zugleich Besprechung von BGH, Beschl. v. 23.06.2020, KVR 69/19 – *Facebook*, ZUM 2020, 89–103.
Magiera, *Siegfried*, Die Grundrechtscharta der Europäischen Union, DÖV 2000, 1017–1026.
Maier, *Natalie/Schaller*, *Fabian*, ePrivacy-VO – alle Risiken der elektronischen Kommunikation gebannt?, ZD 2017, 373–377.
Mainzer, *Klaus*, Künstliche Intelligenz – Wann übernehmen die Maschinen, Berlin 2016.

Malgieri, *Gianclaudio/Custers*, *Bart*, Pricing privacy – the right to know the value of your personal data, 34 Computer Law & Security Review (2018), 289–303.
Mallmann, *Otto*, Zielfunktionen des Datenschutzes: Schutz der Privatsphäre – korrekte Information; mit einer Studie zum Datenschutz im Bereich von Kreditinformationssystemen, Frankfurt a. M. 1977.
Mańko, *Rafał*, Contracts for the supply of digital content and digital services, Briefing EU Legislation in Progress, European Parliamentary Research Service (EPRS), 2018 (https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2018)614707).
Manning, *Christopher u. a.*, The Stanford CoreNLP natural language processing toolkit, Proceedings of 52nd Annual Meeting of the Association for Computational Linguistics: System Demonstrations 2014, 55–60.
Mansour, *Yishay/Muthukrishnan*, *S./Nisan*, *Noam*, Doubleclick Ad Exchange Auction, Working Paper, 2012 (https://arxiv.org/pdf/1204.0535).
Mantz, *Reto/Spittka*, *Jan*, Anmerkung zu Breyer, NJW 2016, 3582–3583.
Marosi, *Johannes/Matthé*, *Luisa*, Anmerkung zu Wirtschaftsakademie Schleswig-Holstein, ZD 2018, 361–363.
Marsch, *Nikolaus*, Das europäische Datenschutzgrundrecht, Tübingen 2018.
Martini, Mario/Drews, Christian/Seeliger, Paul/Weinzierl, Quirin, Dark Patterns – Phänomenologie und Antworten der Rechtsordnung", ZfDR 2021, 47–74.
Martini, *Mario/Fritzsche*, *Saskia*, Mitverantwortung in sozialen Netzwerken, NVwZ 2015, 1497–1499.
Martini, Mario/Hohmann, *Matthias*, Der gläserne Patient: Dystopie oder Zukunftsrealität?, NJW 2020, 3573–3578.
Masing, *Johannes*, Ein Abschied von den Grundrechten, SZ v. 09.01.2012, 10.
–, Herausforderungen des Datenschutzes, NJW 2012, 2305–2311.
–, Vorläufige Einschätzung der „Google-Entscheidung" des EuGH, VerfBlog 14.08.2014.
–, Einheit und Vielfalt des Europäischen Grundrechtsschutzes, JZ 2015, 477–487.
Maunz, Theodor, Dürig, Günter, Kommentar zum Grundgesetz, Stand Januar 2021, München 2021.
Mayer-Maly, *Theo*, Renaissance der laesio enormis?, in: Canaris, Claus-Wilhelm (Hrsg.), Festschrift für Karl Larenz zum 80. Geburtstag, München 1983, 395–409.
Mayer-Schönberger, *Viktor*, delete. The Virtue of Forgetting in the Digital Age, Princeton/Oxford 2009.
Mayer-Schönberger, *Viktor/Cukier*, *Kenneth*, Big Data: A revolution that will transform how we live, work, and think, Boston/New York 2013.
McCarthy, *John u. a.*, A Proposal for the Dartmouth Summer Research Project on Artificial Intelligence, Hanover (NH) 1955.
McCarthy, *J. Thomas*, The Rights of Publicity and Privacy, Band 2, S.I. 2008.
McDonald, *Aleecia M./Cranor*, *Lorrie Faith*, The Cost of Reading Privacy Policies, 4 I/O Journal of Law and Policy for the Information Society 2008, 543–568.
Meister, *Herbert*, Schutz vor Datenschutz, DuD 1986, 173–178.
Mell, *Peter/Grance*, *Timothy*, The NIST Definition of Cloud Computing – Recommendations of the National Institute of Standards and Technology, 2011, Special Publication 800–145.
Mellet, Kevin/Beauvisage, Cookie monsters. Anatomy of a digital market infrastructure, 23 Consumption Markets and Culture (2019), 1–20.
Menzel, *Hans-Joachim*, Datenschutzrechtliche Einwilligungen, DuD 2008, 400–408.

Mestmäcker, *Ernst-Joachim*, Über die normative Kraft privatrechtlicher Verträge, JZ 1964, 441–446.
Metzger, *Axel*, Rechtsgeschäfte über das Droit moral im deutschen und französischen Urheberrecht, München 2002.
–, Extra legem, intra ius. Allgemeine Rechtsgrundsätze im Europäischen Privatrecht, Tübingen 2009.
–, Dienst gegen Daten: Ein synallagmatischer Vertrag, AcP 216 (2016), 817–865.
–, Data as Counter-Performance – What Rights and Duties do Parties Have?, JIPITEC 2017, 2–8.
–, Mehr Freiheit wagen auf dem Markt der Daten, in: Dutta, Anatol/Heinze, Christian (Hrsg.), „Mehr Freiheit wagen". Beiträge zur Emeritierung von Jürgen Basedow, Tübingen 2018, 131–152.
–, Digitale Mobilität – Verträge über Nutzerdaten, GRUR 2019, 129–136.
–, Verträge über digitale Inhalte und digitale Dienstleistungen: Neuer BGB-Vertragstypus oder punktuelle Reform? JZ 2019, 577–586.
–, A Market Model for Personal Data: State of the Play under the New Directive on Digital Content and Digital Services, in: Lohsse, Sebastian/Schulze, Reiner/Staudenmayer, Dirk (Hrsg.), Data as Counter-Performance: Contract Law 2.0?, Oxford/Baden-Baden 2020, 25–45.
Metzger, *Axel/Efroni*, *Zohar/Mischau*, *Lena/Metzger*, *Jakob*, Data-Related Aspects of the Digital Content Directive, JIPITEC 2018, 90–109.
Meyer, *Jürgen/Hölscheidt*, *Sven* (Hrsg.), Charta der Grundrechte der Europäischen Union, 5. Aufl., Baden-Baden 2019.
Michl, *Walther*, Das Verhältnis zwischen Art. 7 und Art. 8 GRCh – zur Bestimmung der Grundlage des Datenschutzgrundrechts im EU-Recht, DuD 2017, 349–353.
Micklitz, *Hans*, Ungeheuerliche Neuigkeiten?, VuR 2017, 43–47.
Micklitz, *Hans/Pałka*, Przemysław/*Panagis*, *Yannis*, The Empire Strikes Back: Digital Control of Unfair Terms of Online Services, 40 Journal of Consumer Policy (2017), 367–388.
Mischau, *Lena*, Daten als „Gegenleistung" im neuen Verbrauchervertragsrecht, ZEuP 2020, 335–365.
Mitchell, *Tom M.*, Machine Learning, New York 1997.
Monopolkommission, Wettbewerbspolitik: Herausforderung digitale Märkte, Sondergutachten 68, Bonn 2015.
Monreal, *Manfred*, Weiterverarbeitung nach einer Zweckänderung in der DS-GVO, ZD 2016, 507–512.
Moos, *Flemming/Rothkegel*, *Tobias*, Anmerkung zu Breyer, MMR 2016, 845–847.
–, Anmerkung zu Wirtschaftsakademie Schleswig-Holstein, MMR 2018, 596–600.
–, Anmerkung zu Fashion ID, MMR 2019, 584–587.
–, Anmerkung zu Planet 49, MMR 2019, 736–740.
Möslein, *Florian*, Dispositives Recht. Zwecke, Strukturen und Methoden, Tübingen 2011.
Mundt, *Andreas*, Die Facebook-Entscheidung des Bundeskartellamtes, NZKart 2019, 117–118.
Mugdan, *Benno*, Die gesammten Materialien zum Bürgerlichen Gesetzbuch für das Deutsche Reich, Band 2, Berlin 1899.
Münchener Kommentar zum BGB, Säcker, Franz J. u. a. (Hrsg.), (zit.: *Bearbeiter*, in: MüKo, BGB).

–, *Wendehorst, Christiane*, BGB § 312g Widerrufsrecht, Band 3 Schuldrecht – Allgemeiner Teil II, 7. Aufl., München 2016.
–, *Roth, Herbert*, BGB § 656 Heiratsvermittlung, Band 6 Schuldrecht – Besonderer Teil III, 8. Aufl., München 2020.
–, *Habersack, Mathias*, BGB § 762 Spiel, Wette, Band 7 Schuldrecht – Besonderer Teil IV, 8. Aufl., München 2020.
Nationale Akademie der Wissenschaften Leopoldina/acatech – Deutsche Akademie der Technikwissenschaften/Union der deutschen Akademien der Wissenschaften, Individualisierte Medizin – Voraussetzungen und Konsequenzen, Halle (Saale) 2014.
Neighbour, Kerstin, Arbeitsrecht – Realität und Herausforderungen, in: Sassenberg, Thomas/Faber, Tobias (Hrsg.), Industrie 4.0 und Internet of Things, 2. Aufl., München 2020, 277–314.
Nettesheim, Martin, Privatleben und Privatsphäre, in: Grabenwarter, Christoph (Hrsg.), Enzyklopädie Europarecht, Band II, 2014, § 9, Baden-Baden 2014, 385–414.
Neuner, Jörg, Die Einwilligung im Deliktsrecht, JuS 2021, 617– 626.
–, Die Rechtsfortbildung, in: Riesenhuber, Karl (Hrsg.), Europäische Methodenlehre, 4. Aufl., Berlin 2021, 351–376.
Ng, Annalyn/Soo, Kenneth, Data Sicience – Was ist das eigentlich, Berlin 2018.
Nietsch, Thomas, Zur Überprüfung der Einhaltung des Datenschutzrechts durch Verbraucherverbände, CR 2014, 272–278.
Nipperdey, Hans Carl, Grundrechte und Privatrecht, in: ders. (Hrsg.), Festschrift für Erich Molitor zum 75. Geburtstag, 1962, 17–33.
Nissenbaum, Helen, Privacy as Contextual Integrity, 79 Journal Washington Law Review (2004), 119–157.
Norberg, Patricia A./Horne, Daniel R./Horne, David A., The privacy paradox: Personal information disclosure intentions versus behaviors, 41 Journal of Consumer Affairs (2007), 100–126.
Obar, Jonathan/Oeldorf-Hirsch, Anne, The biggest lie on the Internet, 21 Information, Communication & Society (2018), 1–20.
Obergfell, Eva Inés, Verträge über digitale Inhalte als Lizenzverträge, in: Verhandlungen des 71. Deutschen Juristentages, Band II/1, München 2017, K 53-K 72.
–, Big Data und Urheberrecht, in: Ahrens, Hans-Jürgen u. a. (Hrsg.), Festschrift für Wolfgang Büscher, Köln 2018, 223–232.
OECD, Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value, Paris 2013.
Oechsler, Jürgen, Gerechtigkeit im modernen Austauschvertrag. Die theoretischen Grundlagen der Vertragsgerechtigkeit und ihr praktischer Einfluß auf Auslegung, Ergänzung und Inhaltskontrolle des Vertrages, Tübingen 1997.
Ohly, Ansgar, Richterrecht und Generalklausel im Recht des unlauteren Wettbewerbs, Köln 1997.
–, „Volenti non fit iniuria" – Die Einwilligung im Privatrecht, Tübingen 2002.
–, Verändert das Internet unsere Vorstellung von Persönlichkeit und Persönlichkeitsrecht?, AfP 2011, 428–438.
–, UWG-Rechtsschutz bei Verstößen gegen die Datenschutz-Grundverordnung?, GRUR 2019, 686–693.
Paal, Boris, Schadensersatzansprüche bei Datenschutzverstößen, MMR 2020, 14–19.
Paal, Boris/Pauly, Daniel A. (Hrsg.), DS-GVO BDSG Kommentar, 3. Aufl., München 2021.

Paulus, *David*, Die automatisierte Willenserklärung, JuS 2019, 960–965.
Paulus, *David/Matzke*, *Robin*, Smart Contracts und das BGB – Viel Lärm um nichts?, ZfPW 2018, 431–465.
Pechstein, *Matthias/Nowak*, *Carsten/Häde*, *Ulrich*, Frankfurter Kommentar zu EUV, GRC und AEUV, 1. Aufl., Tübingen 2017.
Peifer, *Karl-Nikolaus*, Individualität im Zivilrecht, Tübingen 2001.
–, Das Recht auf Vergessenwerden – ein neuer Klassiker vom Karlsruher Schlossplatz, GRUR 2020, 34–37.
Peifer, *Karl-Nikolaus/Kamp*, *Johannes*, Datenschutz und Persönlichkeitsrecht, ZUM 2009, 185–190.
Peppet, *Scott R.*, Unraveling Privacy: The Personal Prospectus and the Threat of a Full Disclosure Future, 105 Northwestern University Law Review (2011), 1153–1203.
–, Regulating the internet of things: first steps toward managing discrimination, privacy, security and consent, 93 Texas Law Review (2014), 85–178.
Perlich, Claudia/Dalessandro, Brian/Raeder, Ori/Stitelman, Troy/Provost, Foster, Machine learning for targeted display advertising: transfer learning in action, in: 95 Mach Learn (2014), 103–127.
Pernice, Ingolf, Machtspruch aus Karlsruhe: „Nicht verhältnismäßig? – Nicht verbindlich? – Nicht zu fassen…", EuZW 2020, 508–519.
Pertot, *Tereza*, Die Auslegung des datenschutzrechtlichen Koppelungsverbots – Lockerung durch den Corte di Cassazione, GPR 2019, 54–57.
– (Hrsg.), Rechte an Daten, Tübingen 2020.
Petri, *Thomas*, Datenschutzrechtliche Verantwortlichkeit im Internet – Überblick und Bewertung der aktuellen Rechtsprechung, ZD 2015, 103–106.
–, Datenschutzrechtliche Verantwortlichkeit im Internet – Überblick und Bewertung der aktuellen Rechtsprechung, ZD 2015, 103–106.
–, Anmerkung zu Wirtschaftsakademie Schleswig-Holstein, EuZW 2018, 540–541.
Piltz, *Carlo*, Die Datenschutz-Grundverordnung, K&R 2016, 557–567.
Plath, *Kai-Uwe* (Hrsg.), Kommentar zu DSGVO, BDSG und den Datenschutzbestimmungen des TMG und TKG, 3. Aufl., Köln 2018.
Podszun, Rupprecht, Der Verbraucher als Marktakteur: Kartellrecht und Datenschutz in der „Facebook"-Entscheidung des BGH, GRUR 2020, 1268–1276.
Polański, *Paul Przemysław*, Some thoughts on data portability in the aftermath of the Cambridge Analytica scandal, EuCML 2018, 141–147.
Pollmann, *Maren/Kipker*, *Dennis-Kenji*, Informierte Einwilligung in der Online-Welt, DuD, 2016, 378–381.
Posner, *Eric A./Weyl*, *Glen*, Radical Markets: Uprooting Capitalism and Democracy for a Just Society 2018.
Posner, *Richard A.*, Privacy, in: Newman, Peter (Hrsg.), The New Palgrave Dictionary of Economics and the Law, Band 3, London 1998, 103–107.
Preibusch, *Sören/Kübler*, *Dorothea/Beresford*, *Alastair R.*, Price versus Privacy. An Experiment into the competitive advantage of collecting less personal information, Electronic Commerce Research 2013.
Preis, *Ulrich*, Verbot der Altersdiskriminierung als Gemeinschaftsgrundrecht. Der Fall „Mangold" und die Folgen, NZA 2006, 401–410.
Prosser, *William L.*, Privacy, 48 California Law Review (1960), 383–423.
Purtova, *Nadezhda*, The law of everything. Broad concept of personal data and future of EU data protection law, 10 Law, Innovation and Technology (2018), 40–81.

Quelle, *Claudia*, The ‚Risk Revolution' in EU Data Protection Law: We can't Have our Cake and Eat it, Too, in: Leenes, Ronald u. a. (eds.), Data Protection and Privacy: The Age of Intelligent Machines, 33–62.
Radlanski, *Philip*, Das Konzept der Einwilligung in der datenschutzrechtlichen Realität, Tübingen 2016.
Raschke, *Philip u. a.*, Designing a GDPR-Compliant and Usable Privacy Dashboard, Proceedings of the IFIP International Summer School on Privacy and Identity Management 2017, 221–236.
Raue, *Benjamin*, Meinungsfreiheit in sozialen Netzwerken, JZ 2018, 961–970.
–, Rechtssicherheit für datengestützte Forschung, ZUM 2019, 684–693.
–, Die Rechte des Sacheigentümers bei der Erhebung von Daten, NJW 2019, 2425–2430.
Rauer, *Nils/Ettig*, *Diana*, Aktuelle Entwicklungen zum rechtskonformen Einsatz von Cookies – Die Rechtslage auf dem Prüfstand von Kommission und Gerichten, ZD 2016, 323–327.
Reidenberg, Joel R./Russell, N. Cameron/Herta, Vlad/Sierra-Rocafort, William/Norton, Thomas B, Trustworthy Privacy Indicators: Grades, Labels, Certifications, and Dashboard, 96 Washington University Law Review (2019), 1409–1460.
Reifert, *Natascha*, Codes of Conduct nach der DS-GVO, ZD 2019, 305–310.
Reiners, *Wilfried*, Datenschutz in der Personal Data Economy – Eine Chance für Europa, ZD 2015, 51–55.
Reinhardt, *Jörn*, Konturen des europäischen Datenschutzgrundrechts Zu Gehalt und horizontaler Wirkung von Art. 8 GRCh, AöR 142 (2017), 544–665.
Renz, *Hartmut T./Frankenberger*, *Melanie*, Compliance und Datenschutz – Ein Vergleich der Funktionen unter Berücksichtigung eines risikobasierten Ansatzes, ZD 2015, 158–161.
Richards, *Neil M./Smart*, *William D.*, How should the law think about robots?, in: Calo, Ryan /Froomkin, Michael A./Kerr, Ian (Hrsg.), Robot Law, Cheltenham, 2016, 3–22.
Richter, *Heiko*, Anmerkung zu Breyer, EuZW 2016, 912–914.
Riechert, *Anne*, Dateneigentum – ein unauflösbarer Interessenkonflikt?, DuD 2019, 353–360.
Riehm, Thomas, Freie Widerruflichkeit der Einwilligung und Struktur der Obligation. Date als Gegenleistung?, in: Pertot, Tereza (Hrsg.), Rechte an Daten, Tübingen 2020, 175–206.
Riehm, *Thomas/Meier*, *Stanislaus*, Die rechtliche Durchsetzung von Anforderungen an die IT-Sicherheit, in: Ebers, Martin/Steinrötter, Björn (Hrsg.), Künstliche Intelligenz und smarte Robotik im IT-Sicherheitsrecht, Baden-Baden, 2021, 241–262.
Riesenhuber, *Karl*, System und Prinzipien des Europäischen Vertragsrechts, Berlin 2003.
–, Die Einwilligung des Arbeitnehmers im Datenschutzrecht, RdA 2011, 257–265.
–, EU-Vertragsrecht, Tübingen 2013.
–, Die Auslegung, in: Riesenhuber, Karl (Hrsg.), Europäische Methodenlehre, 4. Aufl., Berlin 2021, 285–321.
–, Privatautonomie–Rechtsprinzip oder „mystifizierendes Leuchtfeuer", ZfPW 2018, 352–368.
–, Neue Methode und Dogmatik eines Rechts der Digitalisierung?, AcP 219 (2019), 892–923.
Ritter, *Franziska/Schwichtenberg*, *Simon*, Die Reform des UKlaG zur Eliminierung des datenschutzrechtlichen Vollzugsdefizits – neuer Weg, neue Chancen?, VuR 2016, 95–102.

Robrahn, *Rasmus/Bremert*, *Benjamin*, Interessenskonflikte im Datenschutzrecht, ZD 2018, 291–297.
Rocher, *Luc/Hendrickx*, *Julien M./de Montjoye*, *Yves-Alexandre*, Estimating the success of re-identifications in incomplete datasets using generative models, 10 Nature Communications (2019), Article 3069, 1–9.
Rogosch, *Patricia Maria*, Die Einwilligung im Datenschutzrecht, Baden-Baden 2013.
Romanowski, Sasha/Acquisti, Alessandro, Privacy Costs and Personal Data Protection: Economic and Legal Perspectives, 24 Berkeley Technology Law Journal (2009), 1061–1102.
Rosenkranz, *Frank*, Spezifische Vorschriften zu Verträgen über die Bereitstellung digitaler Produkte im BGB, ZUM 2021, 195–210.
Roßnagel, *Alexander*, Anmerkung zu *Lindqvist*, MMR 2004, 95–100.
–, EuGH: Personenbezogene Daten im Internet. Anmerkung, MMR 2004, 95–100.
–, Modernisierung des Datenschutzrechts für eine Welt allgegenwärtiger Datenverarbeitung, MMR 2005, 71–75.
–, Big Data – Small Privacy? – Konzeptionelle Herausforderungen für das Datenschutzrecht, ZD 2013, 562–567.
–, Wie zukunftsfähig ist die Datenschutz-Grundverordnung?, DuD 2016, 561–565.
–, Datenschutzgrundsätze – unverbindliches Programm oder verbindliches Recht?, ZD 2018, 339–344.
–, Pseudonymisierung personenbezogener Daten, ZD 2018, 243–247.
–, Kein „Verbotsprinzip" und kein „Verbot mit Erlaubnisvorbehalt" im Datenschutzrecht, NJW 2019, 1–5.
–, Datenschutz in der Forschung. Die neuen Datenschutzregelungen in der Forschungspraxis von Hochschulen, ZD 2019, 157–164.
Roßnagel, Alexander/Müller, *Jürgen*, Ubiquitous Computing – neue Herausforderungen für den Datenschutz, CR 2004, 625–631.
Roßnagel, *Alexander/Nebel*, *Maxi/Richter*, *Philipp*, Was bleibt vom Europäischen Datenschutzrecht? Überlegungen zum Ratsentwurf der DS-GVO, ZD 2015, 455–460.
Roßnagel, *Alexander u. a.*, Datensparsamkeit oder Datenreichtum? Zur neuen politischen Diskussion über den datenschutzrechtlichen Grundsatz der Datensparsamkeit, Policy Paper des Forums „Privatheit und selbstbestimmtes Leben in der digitalen Welt", Karlsruhe 2017.
Roßnagel, *Alexander/Pfitzmann*, *Andreas/Garstka*, *Hansjürgen*, Modernisierung des Datenschutzrechts, Gutachten im Auftrag des Bundesministeriums des Innern, Berlin 2001.
Roßnagel, *Alexander/Schnabel*, *Christoph*, Das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme und sein Einfluss auf das Privatrecht, NJW 2008, 3534–3538.
Roth, *Wulf-Henning/Jopen*, *Christian*, Die richtlinienkonforme Auslegung, in: Riesenhuber, Karl (Hrsg.), Europäische Methodenlehre, 4. Aufl., Berlin 2021, 357–452.
Rothmann, *Robert/Buchner*, *Benedikt*, Der typische Facebook-Nutzer zwischen Recht und Realität, DuD 2018, 342–346.
Röthel, *Anne*, Privatautonomie im Spiegel der Privatrechtsentwicklung: ein mystifizierendes Leuchtfeuer, in: Bumke, Christian/Röthel, Anna (Hrsg.), Autonomie im Recht, Tübingen 2017, 91–115.
Rott, *Peter*, Unfair Contract Terms, in: Twigg-Flesner, Christian (Hrsg.), Research Handbook on EU Consumer and Contract Law, Cheltenham 2016, 287–313.

Rubinstein, *Daniel L./Gal*, *Michal S.*, Access Barriers to Big Data, 59 Arizona Law Review (2017), 339–381.
Rubinstein, *Ira S.*, Regulating Privacy by Design, 26 Berkeley Technology Law Journal (2011), 1409–1456.
Rubinstein, *Ira/Petkova*, *Bilyana*, The International Impact of the General Data Protection Regulation, in: Cole, Mark/Boehm, Franziska (Hrsg.), Commentary on the General Data Protection Regulation, Cheltenham, (https://ssrn.com/abstract=3167389).
Rudkowski, *Lena*, Vertragsrechtliche Anforderungen an die Gestaltung von „Self-Tracking"-Tarifen in der Privatversicherung, 106 ZVersWiss (2017), 453–502.
Ruffert, Matthias, Vorrang der Verfassung und Eigenständigkeit des Privatrechts, Tübingen 2001.
–, Privatrechtswirkung der Grundrechte, JuS 2020, 1–6.
Russell, Stuart J./Norvig, Peter, Artificial Intelligence. A Modern Approach, 3. Aufl., Upper Saddle River 2010.
Sack, *Rolf*, Sittenwidrigkeit, Sozialwidrigkeit und Interessenabwägung, GRUR 1970, 493–503.
–, Das Anstandsgefühl aller billig und gerecht Denkenden und die Moral als Bestimmungsfaktoren der guten Sitten, NJW 1985, 761–769.
Samuelson, Pamela, Privacy as Intellectual Property, 52 Stanford Law Review (1999), 1125–1173.
Sandfuchs, Barbara, Privatheit wider Willen?, Tübingen 2015.
Sandrock, *Otto*, Subjektive und objektive Gestaltungskräfte bei der Teilnichtigkeit von Rechtsgeschäften: Ein Beitrag zur Auslegung von § 139 BGB, AcP 159 (1960), 481–546.
Sasse, *Thorsten*, Die Grundrechtsberechtigung juristischer Personen durch die unternehmerische Freiheit gemäß Art. 16 der Europäischen Grundrechtecharta, EuR 2012, 628–653.
Sattler, *Andreas*, Personenbezogene Daten als Leistungsgegenstand, JZ 2017, 1036–1046.
–, Personenbezogene Daten als Leistungsgegenstand, in: Schmidt-Kessel, Martin/Grimm, Anna (Hrsg.), Telematiktarife & Co. – Versichertendaten als Prämienersatz, 2018, 1–46.
–, Rezension: Carmen Langhanke, Daten als Leistung, JZ 2018, 760–770.
–, From Personality to Property?, in: Bakhoum, Mor/Conde Gallego, Beatriz/Mackenrodt, Mark-Oliver/Surblytė-Namavičienė, Gintare (Hrsg.), Personal Data in Competition, Consumer Protection and Intellectual Property Law – Towards a Holistic Approach? Berlin 2018, 27–54.
–, Der Einfluss der Digitalisierung auf das Gesellschaftsrecht, BB 2018, 2243–2253.
–, Gemeinsame Verantwortlichkeit – getrennte Pflichten GRUR 2019, 1023–1026.
–, Privatautonomie oder Determinismus – Welchen Weg geht das Datenschuldrecht?, in: Ochs, Carsten/Friedewald, Michael/Hess, Thomas/Lamla, Jörn (Hrsg.), Die Zukunft der Datenökonomie, Wiesbaden 2019, 215–247.
–, Autonomy or Heteronomy – Proposal for a Two-Tier Interpretation of Art. 6 GDPR, in: Lohsse, Sebastian/Schulze, Reiner/Staudenmayer, Dirk (Hrsg.), Data as Counter-Performance: Contract Law 2.0?, Oxford/Baden-Baden 2020, 225–251.
–, Vorgaben der DSGVO für die IT-Sicherheit, in: Ebers, Martin/Steinrötter, Björn (Hrsg.), Künstliche Intelligenz und smarte Robotik im IT-Sicherheitsrecht, Baden-Baden 2021, 197–239.

Savigny von, *Friedrich Carl*, System des heutigen Römischen Rechts, Band III, Berlin 1840.

Schack, Haimo, Anmerkung zu BGH 01.12.1999 – I ZR 49/97 – *Marlene Dietrich* (vermögenswerte Bestandteile des postmortalen Persönlichkeitsrechts), JZ 2000, 1060–1062.

Schäfer, *Hans-Bernd/Ott*, *Claus*, Lehrbuch der ökonomischen Analyse des Zivilrechts, 5. Aufl., Berlin/Heidelberg 2012.

Schantz, *Peter*, Die Datenschutz-Grundverordnung – Beginn einer neuen Zeitrechnung im Datenschutzrecht, NJW 2016, 1841–1847.

Schantz, *Peter/Wolff*, *Heinrich Amadeus*, Das neue Datenschutzrecht, München 2017.

Scheibehenne, B., Greifeneder, R., & Todd, P. M. (2010). Can there ever be too many options? A meta-analytic review of choice overload. 37 Journal of Consumer Research (2010), 409–425.

Schemmel, *Frank*, Anmerkung zu OLG Frankfurt a. M.: Unwirksamkeit des Verkaufs von Adressdaten wegen fehlender Einwilligung der Adressinhaber, BB 2018, 723–724.

Scherer, Inge, Abschied vom „psychischen Kaufzwang" – Paradigmenwechsel im neuen Lauterkeitsrecht, WRP 2005, 672–676.

Schiedermair, *Stephanie*, Der Schutz des Privaten als internationales Grundrecht, Tübingen 2012.

Schild, *Hans-Hermann/Tinnefeld*, *Marie-Theres*, Datenschutz in der Union — Gelungene oder missglückte Gesetzentwürfe? DuD 2012, 312–317.

Schmidt, *Kirsten-Johanna*, Datenschutz als Vermögensrecht – Datenschutzrecht als Instrument des Datenhandels, Berlin 2020.

Schmidt-Kessel, *Martin*, Rechtsmißbrauch im Gemeinschaftsrecht – Folgerungen aus den Rechtssachen Kefalas und Diamanti, in: Jud, Britta/Bachner, Thomas/Bollenberger, Raimund/Halbwachs, Verena/Kalss, Susanne/Meissel, Franz-Stefan/Ofner, Helmut/Rabl, Christian (Hrsg.), Prinzipien des Privatrechts und Rechtsvereinheitlichung, 2001, 61–83.

Schmidt-Kessel, *Martin/Grimm*, *Anna*, Unentgeltlich oder entgeltlich? – Der vertragliche Austausch von digitalen Inhalten gegen personenbezogene Daten, ZfPW 2017, 84–108.

– (Hrsg.), Telematiktarife & Co. – Versichertendaten als Prämienersatz, Karlsruhe 2018.

Schmidt-Kessel, *Martin/Erler*, *Katharina/Grimm*, *Anna/Kramme*, *Malte*, Die Richtlinienvorschläge der Kommission zu Digitalen Inhalten und Online-Handel – Teil 2, GPR 2016, 54–71.

Schmidt-Rimpler, *Walter*, Grundfragen einer Erneuerung des Vertragsrechts, AcP 147 (1941), 130–197.

–, Zum Vertragsproblem, in: Baur, Fritz u. a. (Hrsg.), Funktionswandel der Privatrechtsinstitutionen: Festschrift Für Ludwig Raiser Zum 70. Geburtstag, Tübingen 1974, 3–26.

Schmitz, *Thomas*, Die EU-Grundrechtecharta aus grundrechtsdogmatischer und grundrechtstheoretischer Sicht, JZ 2001, 837–843.

Schmolke, *Klaus Ulrich*, Grenzen der Selbstbindung im Privatrecht. Rechtspaternalismus und Verhaltensökonomik im Familien-, Gesellschafts- und Verbraucherrecht, Tübingen 2014.

Schneider, *Jochen*, Schließt Art. 9 DS-GVO die Zulässigkeit der Verarbeitung bei Big Data aus?, ZD 2017, 303–308.

–, Datenschutz nach der EU-Datenschutz-Grundverordnung, 2. Aufl., München 2019.

Schöbener, Burkhard/Stork, Florian, Anti-Diskriminierungsregelungen der Europäischen Union im Zivilrecht – zur Bedeutung der Vertragsfreiheit und des Rechts auf Privatleben, ZEuS 2004, 43–82.

Schricker, Gerhard/Loewenheim, Ulrich, in: Loewenheim, Ulrich/Leistner, Matthias/Ohly, Ansgar (Hrsg.), Urheberrecht Kommentar, 6. Aufl., München 2020.

Schröder, Michael/Taeger, Jürgen (Hrsg.), Scoring im Fokus: Ökonomische Bedeutung und rechtliche Rahmenbedingungen im internationalen Vergleich, Neuss 2014.

Schulze, Reiner, Die Digitale-Inhalte-Richtlinie – Innovation und Kontinuität im europäischen Vertragsrecht, ZEuP 2019, 695–721.

Schur, Nico, Die Lizensierung von Daten, Tübingen 2020.

Schwamberger, Sebastian, Anmerkung zu OGH 6 Ob 104/18h: Reichweite des datenschutzrechtlichen Koppelungsverbots nach alter und neuer Rechtslage, GPR 2019, 57–59.

Schwartmann, Rolf/Hentsch, Christian-Henner, Eigentum an Daten – Das Urheberrecht als Pate für ein Datenverwertungsrecht, RDV 2015, 221–230.

Schwartz, Paul M., Privacy and Democracy in Cyberspace, 52 Vanderbilt Law Review (1999), 1609–1702.

–, Property, Privacy, and Personal Data, 117 Harvard Law Review (2004), 2055–2128.

–, Global Data Privacy: The EU Way, 94 NYU Law Review 2019, 771–818.

Schwartz, Paul M./Solove, Daniel J, The PII problem: Privacy and a new concept of personally identifiable information, 86 NYU Law Review (2011), 1814–1894.

Schwartz, Alan/Wilde, Louis L., Intervening in Markets on the Basis of Imperfect Information: A Legal and Economic Analysis, 127 University of Pennsylvania Law Review (1979), 630–682.

Schwarze, Jürgen, in: Schwarze, Jürgen/Becker, Ulrich/Hatje, Armin/Schoo, Johann (Hrsg.), EU-Kommentar, 4. Aufl., Baden-Baden 2019.

Schweitzer, Heike, Neue Machtlagen in der digitalen Welt? Das Beispiel unentgeltlicher Leistungen, in: Körber, Torsten/Kühling, Jürgen (Hrsg.), Regulierung-Wettbewerb-Innovation, Baden-Baden 2017, 269–305.

–, Datenzugang in der Datenökonomie: Eckpfeiler einer neuen Informationsordnung, GRUR 2019, 569–580.

–, *Schweitzer, Heike/Fetzer, Thomas/Peitz, Martin*, Digitale Plattformen: Bausteine für einen künftigen Ordnungsrahmen, ZEW Discussion Paper No. 16–042, 2016 (http://ftp.zew.de/pub/zew-docs/dp/dp16042.pdf).

Schweitzer, Heike/Peitz, Martin, Datenmärkte in der digitalisierten Wirtschaft: Funktionsdefizite und Regelungsbedarf, ZEW Discussion Paper No. 17–043, 2017 (http://ftp.zew.de/pub/zew-docs/dp/dp17043.pdf).

Schweitzer, Heike/Haucap, Justus/Kerber, Wolfgang/Welker, Robert, Modernisierung der Missbrauchsaufsicht für marktmächtige Unternehmen, Gutachten für das Bundesministerium für Wirtschaft und Energie, Berlin 2018.

Schwenke, Matthias Christoph, Individualisierung und Datenschutz, Wiesbaden 2006.

Shalev-Shwartz, Shai/Ben-David, Shai, Understanding Machine Learning, New York 2014.

Shils, Edward, Privacy: Its Constitution and Vicissitudes, 31 Law and Contemporary Problems (1966), 281–306.

Simitis, Spiros, Datenschutz: Von der legislativen Entscheidung zur richterlichen Interpretation, NJW 1981, 1697–1701.

–, Die informationelle Selbstbestimmung – Grundbedingung einer verfassungskonformen Informationsordnung, NJW 1984, 398–405.
– (Hrsg.), Bundesdatenschutzgesetz, 7. Aufl., Baden-Baden 2011.
Simitis, *Spiros/Hornung*, *Gerrit/Spiecker gen. Döhmann*, *Indra* (Hrsg.), Datenschutzrecht, Baden-Baden 2019.
Solmecke, *Christian/Vondrlik*, *Simon-Elias*, Rechtliche Probleme bei Produkten mit serverbasierten Zusatzdiensten – Was passiert, „wenn der Kühlschrank keine Einkaufsliste mehr schreibt …", MMR 2013, 755–760.
Solove, *Daniel J.*, I've Got Nothing to Hide and Other Misunderstandings of Privacy, 44 San Diego Law Review (2007), 745–772.
–, Understanding Privacy, Cambridge (MA) 2008.
–, Introduction: Privacy self-management and the consent dilemma, 126 Harvard Law Review (2013), 1880–1903.
Sosnitza, *Olaf*, Die Verkehrsauffassung im Markenrecht, WRP 2014, 1136–1142.
–, Das Internet der Dinge – Herausforderung oder gewohntes Terrain für das Zivilrecht? CR 2016, 764–772.
Specht, *Louisa*, Konsequenzen der Ökonomisierung informationeller Selbstbestimmung, Köln 2012.
–, Das Verhältnis möglicher Datenrechte zum Datenschutzrecht, GRUR Int. 2017, 1040–1047.
–, Daten als Gegenleistung – Verlangt die Digitalisierung nach einem neuen Vertragstypus?, JZ 2017, 763–770.
Specht, *Louisa/Herold*, *Sophie*, Roboter als Vertragspartner, MMR 2018, 40–44.
Specht-Riemenschneider, *Louisa*, Diktat der Technik. Regulierungskonzepte technischer Vertragsinhaltsgestaltung am Beispiel von Bürgerlichem Recht und Urheberrecht, Baden-Baden 2019.
Specht-Riemenschneider, *Louisa/Schneider*, *Ruben*, Die gemeinsame Verantwortlichkeit im Datenschutzrecht, MMR 2019, 503–509.
Specht-Riemenschneider, *Louisa/Bienemann, Linda*, Informationsvermittlung durch standardisierte Bildsymbole, in Specht-Riemenschneider, Louisa/Werry, Nikola/Werry, Susanne (Hrsg.), Daten in der Digitalisierung, 2018, 324–344.
Spelge, Karin, Der Beschäftigtendatenschutz nach Wirksamwerden der Datenschutz-Grundverordnung, DuD 2016, 775–781.
Spiecker gen. Döhmann, *Indra*, Teil-Verfassungsordnung Datenschutz, in: Vesting, Thomas/Korioth, Stefan (Hrsg.), Der Eigenwert des Verfassungsrechts, Tübingen, 2011, 263–287.
Spindler, *Gerald*, Datenschutz- und Persönlichkeitsrechte im Internet – der Rahmen für Forschungsaufgaben und Reformbedarf, GRUR 2013, 996–1003.
–, Datenschutz- und Persönlichkeitsrechte im Internet, GRUR-Beilage 2014, 101–108.
–, Selbstregulierung und Zertifizierungsverfahren nach der DS-GVO, ZD 2016, 407–414.
–, Die neue EU-Datenschutz-Grundverordnung, DB 2016, 937–947.
–, Text und Data Mining – urheber- und datenschutzrechtliche Fragen, GRUR 2016, 1112–1120.
–, Ausgewählte Rechtsfragen der Umsetzung der digitalen Inhalte-Richtlinie in das BGB, MMR 2021, 451–454 (Teil 1) und 528–533 (Teil 2).
Spindler, *Gerald/Schmitz*, *Peter/Liesching*, *Marc* (Hrsg.), TMG, 2. Aufl., München 2018.

Spindler, *Gerald/Schuster*, *Fabian*, Recht der elektronischen Medien, 4. Aufl., München 2019.
Spindler, *Gerald/Sein*, *Karin*, Die endgültige Richtlinie über Verträge über digitale Inhalte und Dienstleistungen, MMR 2019, 415–420.
–, Die Richtlinie über Verträge über digitale Inhalte, MMR 2019, 488–493.
Spittka, *Jan*, Können Wettbewerber wegen DS-GVO-Verstößen abmahnen? GRUR-Prax 2019, 4–6.
Srinivasan, *Dina*, Why Google Dominates Advertising Markets, 24 Stanford Technology Law Review (2020), 55–175.
Stach, *Christoph u. a.*, Privacy-avare: An approach to manage and distribute privacy settings, 3rd IEEE International Conference on Computer and Communications (ICCC) Chengdu 2017, 1460–1468.
Starke, *Max*, EU-Grundrechte und Vertragsrecht, Tübingen 2016.
Staudenmayer, *Dirk*, Auf dem Weg zum digitalen Privatrecht – Verträge über digitale Inhalte, NJW 2019, 2497–2501.
–, Die Richtlinien zu den digitalen Verträgen, ZEuP 2019, 663–694.
Steege, *Hans*, Ist die DS-GVO zeitgemäß für das autonome Fahren?, MMR 2019, 509–513.
Steinbeck, *Anja*, Die Zukunft der aggressiven Geschäftspraktiken, WRP 2008, 865–870.
Steindorff, *Ernst*, Wirtschaftsordnung und -steuerung durch Privatrecht, in: Baur, Fritz u. a. (Hrsg.), Funktionswandel der Privatrechtsinstitutionen: Festschrift Für Ludwig Raiser Zum 70. Geburtstag, Tübingen 1974, 621–644.
–, EG-Vertrag und Privatrecht, Baden-Baden 1996.
Steinmetz, *Wenzel*, Die Kontrollsperre des § 307 Abs. 3 BGB bei Verträgen über immaterielle Gegenstände, Tübingen 2022.
Steinmüller, *Wilhelm*, EDV und Recht: Einführung in die Rechtsinformatik, Berlin 1970.
Steinmüller, *Wilhelm u. a.*, Grundfragen des Datenschutzes, Gutachten im Auftrag des Bundesministeriums des Innern, 1971, BT-Drs. VI/3826, 5–224.
Stelljes, *Harald*, Stärkung des Beschäftigtendatenschutzes durch die Datenschutz-Grundverordnung, DuD 2016, 787–791.
Stempel, *Christian*, Die „Grundsätze des bürgerlichen Rechts", das sekundäre Unionsrecht und der nationale Richter, ZEuP 2010, 925–944.
–, Treu und Glauben im Unionsprivatrecht, Tübingen 2016.
Stiftung Datenschutz, Neue Wege bei der Einwilligung im Datenschutz – technische, rechtliche und ökonomische Herausforderungen, Leipzig 2017.
Stigler, *George J.*, The Economics of Information, 69 Journal of Political Economy (1961), 213–225.
–, The Theory of Price, 4. Aufl., NewYork/London 1987.
Stoffels, *Markus*, Schranken der Inhaltskontrolle, JZ 2001, 843–849.
Streinz, *Rudolf*, EUV/AEUV-Kommentar, 3. Aufl., München 2018.
Streinz, *Rudolf/Michl*, *Walther*, Die Drittwirkung des europäischen Datenschutzgrundrechts (Art. 8 GRCh) im deutschen Privatrecht, EuZW 2011, 384–388.
Suhr, *Jan*, Richtlinienkonforme Auslegung im Privatrecht und nationale Auslegungsmethodik, Baden-Baden 2011.
Sunstein, *Cass R.*, Memorandum for the Heads of Executive Departments and Agencies: Informing Consumers through Smart Disclosure, Washington D.C. 2011.

Sydow, *Gernot* (Hrsg.), Europäische Datenschutzgrundverordnung. Handkommentar, 2. Aufl., Baden-Baden 2018.
Taeger, *Jürgen*, Scoring in Deutschland nach der EU-Datenschutzgrundverordnung, ZRP 2016, 72–75.
Taeger, *Jürgen*, Verbot des Profiling nach Art. 22 DS-GVO und die Regulierung des Scoring ab Mai 2018, RDV 2017, 3–9.
Taeger, *Jürgen/Gabel*, *Detlev* (Hrsg.), DSGVO BDSG Kommentar, 3. Aufl., Frankfurt a. M. 2019.
Taeger, *Jürgen/Schweda*, *Sebastian*, Die gemeinsam mit anderen Erklärungen erteilte Einwilligung, ZD 2020, 124–129.
Tavanti, *Pascal*, Datenverarbeitung zu Werbezwecken nach der Datenschutz-Grundverordnung (Teil 1), RDV 2016, 231–240.
–, Datenverarbeitung zu Werbezwecken nach der Datenschutz-Grundverordnung (Teil 2), RDV 2016, 295–306.
Tene, *Omer/Polonetsky*, *Jules*, Big data for all: Privacy and user control in the age of analytics, 11 Northwestern Journal of Technology and Intellectual Property (2012), 239–273.
Thaler, *Richard/Sunstein*, *Cass R.*, Nudge: Improving Decisions About Health, Wealth, and Happiness, New Haven/London 2008.
Thomas, *Stefan*, Wettbewerb in der digital economy: Verbraucherschutz durch AGB-Kontrolle im Kartellrecht? NZKart 2017, 92–98.
Thon, *Marian*, Transnationaler Datenschutz: Das Internationale Datenprivatrecht der DS-GVO, RabelsZ 84 (2020), 24–61.
Thouvenin, *Florent*, Wem gehören meine Daten? Zu Sinn und Nutzen einer Erweiterung des Eigentumsbegriffs, Schweizerische Juristen-Zeitung 113/2017, 21–32.
Thym, *Daniel*, Vereinigt die Grundrechte!, JZ 2015, 53–63.
Tinnefeld, *Marie-Therese/Conrad*, *Isabell*, Die selbstbestimmte Einwilligung im europäischen Recht, ZD 2018, 391–398.
Trute, *Hans-Heinrich*, Der Schutz personenbezogener Informationen in der Informationsgesellschaft, JZ 1998, 822–831.
Tsai, *Janice Y. u. a.*, The effect of online privacy information on purchasing behavior: An experimental study, 22 Information Systems Research (2011), 254–268.
Turing, *Alan M.*, Computing Machinery and Intelligence, 59 Mind 1950, 433–460.
Turing, *Alan M.*, Intelligent Machinery, Report, 1948, zunächst unpubliziert, posthum abgedruckt, in: Copeland, Jack (Hrsg.), The Essential Turing, Oxford 2004, 410–432.
Tversky, *Amos/Kahneman*, *Daniel*, Availability: A heuristic for judging frequency and probability, 5 Cognitive Psychology (1973), 207–232.
Uebele, *Fabian*, Datenschutzrecht vor Zivilgerichten, GRUR 2019, 694–703.
Uecker, *Philip*, Die Einwilligung im Datenschutzrecht und ihre Alternativen, ZD 2019, 248–251.
–, Extraterritorialer Anwendungsbereich der DS-GVO, ZD 2019, 67–71.
Ungern von-Sternberg, *Joachim*, Schlichte einseitige Einwilligung und treuwidrig widersprüchliches Verhalten des Urheberberechtigten bei Internetnutzungen, GRUR 2009, 369–375.
Unseld, *Christopher*, Zur Bedeutung der Horizontalwirkung von EU-Grundrechten, Tübingen 2019.
Unseld, *Florian*, Die Übertragbarkeit von Persönlichkeitsrechten, GRUR 2011, 982–988.

Urbach, *Nils*, Betriebswirtschaftliche Besonderheiten digitaler Güter, in: Schmidt-Kessel, Martin/Kramme, Malte (Hrsg.), Geschäftsmodelle in der digitalen Welt, Jena 2017, 39–62.

Varian, *Hal*, Intermediate Micro-Economics, 8. Aufl., New York/London 2010.

Veil, *Winfried*, DS-GVO: Risikobasierter Ansatz statt rigides Verbotsprinzip – Eine erste Bestandsaufnahme, ZD 2015, 347–352.

–, Die Datenschutz-Grundverordnung: des Kaisers neue Kleider, NVwZ 2018, 686–696.

–, Einwilligung oder berechtigtes Interesse? – Datenverarbeitung zwischen Skylla und Charybdis, NJW 2018, 3337–3344.

Verbraucherzentrale Bundesverband (vzbv), Neue Datenintermediäre – Anforderungen des vzbv an „Personal Information Management Systems" (PIMS) und Datentreuhänder, 15.09.2020.

Vogelgesang, *Klaus*, Grundrecht auf informationelle Selbstbestimmung?, Baden-Baden 1987.

Wagner, *Gerhard*, Geldersatz für Persönlichkeitsverletzungen, ZEuP 2000, 200–228.

–, Materialisierung des Schuldrechts unter dem Einfluss von Verfassungsrecht und Europarecht, in: Blaurock, Uwe/Hager, Günter (Hrsg.), Obligationenrecht im 21. Jahrhundert, Baden-Baden 2010, 13–84.

–, Anmerkung, JZ 2017, 522–525.

Wagner, *Gerhard/Eidenmüller*, *Horst*, Down by Algorithms: Siphoning Rents, Exploiting Biases, and Shaping Preferences: Regulating the Dark Side of Personalized Transactions, 86 University of Chicago Law Review (2019), 581–609.

Wagner, *Manuela*, Datenökonomie und Datenselbstschutz – Grenzen der Kommerzialisierung personenbezogener Daten, Köln 2020.

Wandtke, *Artur*, Die Kommerzialisierung der Kunst und die Entwicklung des Urheberrechts im Lichte der Immaterialgüterrechtslehre von Josef Kohler, GRUR 1995, 385–392.

Warren, *Samuel D./Brandeis Louis D.*, The right to privacy, 4 Harvard Law Review (1890), 193–220.

Weber, *Rolf H.*, Internet of Things – New security and privacy challenges, 26 Computer Law & Security Review (2010), 23–30.

Weichert, *Thilo*, Big Dada im Gesundheitsbereich, Studie im Rahmen von Assessing Big Data (ABIDA), 2018 (https://www.abida.de/sites/default/files/ABIDA%20Gutachten-Gesundheitsbereich.pdf).

–, Informationstechnische Arbeitsteilung und datenschutzrechtliche Verantwortung – Plädoyer für eine Mitverantwortlichkeit bei der Verarbeitung von Nutzungsdaten, ZD 2014, 605–610.

–, „Sensitive Daten" revisited, DuD 2017, 538–543.

Weidert, *Stefan/Klar*, *Manuel*, Datenschutz und Werbung – gegenwärtige Rechtslage und Änderungen durch die Datenschutz-Grundverordnung, BB 2017, 1858–1864.

Wendehorst, *Christiane*, Consumer Contracts and the Internet of Things, in: Schulze, Reiner/Staudenmayer, Dirk (Hrsg.), Digital Revolution. Challenges for Contract Law in Practice, Baden-Baden 2016, 189–223.

–, Die Digitalisierung und das BGB, NJW 2016, 2609–2613.

–, Hybride Produkte und hybrider Vertrieb. Sind die Richtlinienentwürfe vom 9. Dezember 2015 fit für den digitalen Binnenmarkt?, in: Wendehorst, Christiane/Zöchling-Jud, Brigitta (Hrsg.), Ein neues Vertragsrecht für den digitalen Binnenmarkt?, Wien 2016, 45–89.

–, Verbraucherrelevante Problemstellungen zu Besitz- und Eigentumsverhältnissen beim Internet der Dinge, Rechtsgutachten für Sachverständigenrat für Verbraucherfragen beim Bundesministerium der Justiz und für Verbraucherschutz, Berlin 2016.
–, Personal Data in Data Value Chains – Is Data Protection Law Fit for the Data Economy?, in: Lohsse, Sebastian/Schulze, Reiner/Staudenmayer, Dirk (Hrsg.), Data as Counter-Performance: Contract Law 2.0?, Oxford/Baden-Baden 2020, 193–223.
–, Die neuen kaufrechtlichen Gewährleistungsregelungen – ein Schritt in Richtung unserer digitalen Realität, JZ 2021, 974–984.
Wendehorst, *Christiane/Graf von Westphalen*, *Friedrich*, Das Verhältnis zwischen Datenschutz-Grundverordnung und AGB-Recht, NJW 2016, 3745–3750.
Wendehorst, *Christiane/Schwamberger*, *Sebastian/Grinzinger*, *Julia*, Datentreuhand – Wie hilfreich sind sachenrechtliche Konzepte?, in: Pertot, Tereza (Hrsg.), Rechte an Daten, 2020, 103–121.
Wendland, *Matthias*, Sonderprivatrecht für Digitale Güter, ZvglRWiss 2019, 191–230.
Wente, *Jürgen*, Informationelles Selbstbestimmungsrecht und absolute Drittwirkung der Grundrechte, NJW 1984, 1446–1447.
Werkmeister, *Christoph/Schwaab*, *Michael*, Auswirkungen und Reichweite des datenschutzrechtlichen Forschungsprivilegs, CR 2019, 85–90.
Wesel, *Uwe*, Geschichte des Rechts, München 2006.
Westin, *Alan F.*, Privacy and Freedom, New York 1967.
Westphalen Graf von, *Friedrich*, Unionsrechtliche Folgen des AGB-Missgriffs, NJW 2012, 1770–1773.
–, Richtlinienentwurf der Kommission betreffend die Bereitstellung digitaler Inhalte und das Recht des Verbrauchers auf Schadensersatz, BB 2016, 1411–1418.
–, Nutzungsbedingungen von Facebook–Kollision mit europäischem und deutschem AGB-Recht, VuR 2017, 323–332.
–, Ersetzung einer missbräuchlichen Klausel durch dispositives nationales Recht? – Spannungsverhältnis zwischen EuGH- und BGH-Judikatur, BB 2019, 67–74.
Westphalen Graf von, *Friedrich/Wendehorst*, *Christiane*, Hergabe personenbezogener Daten für digitale Inhalte, BB 2016, 2179–2187.
Whittington, *Jan/Hoofnagle*, *Chris Jay*, Unpacking Privacy's Price, 90 North Carolina Law Review (2011), 1327–1370.
Wiebe, *Andreas*, Information als Schutzgegenstand im System des geistigen Eigentums, in: Fiedler, Herbert/Ullrich, Hans (Hrsg.), Information als Wirtschaftsgut, Köln 1997, 93–152.
Wiegand, *Wolfgang*, Die Entwicklung des Sachenrechts im Verhältnis zum Schuldecht, AcP 190 (1990), 112–138.
Willis, *Lauren E.*, Why Not Privacy by Default?, 29 Berkeley Technology Law Journal (2014), 61–133.
Wind, *Irene*, Haftung bei Verarbeitung personenbezogener Daten, RDV 1991, 16–24.
Windel, *Peter A.*, Unsinnige, rechtlich unmögliche und verbotswidrige Leistungsversprechen, ZGS 2003, 466–472.
Winston, *Patrick Henry*, Artificial Intelligence, 3. Aufl., Reading (MA) 1992.
Winter, *Christian/Battis*, *Verena/Halvani*, *Oren*, Herausforderungen für die Anonymisierung von Daten, ZD 2019, 489–493.
Wintermeier, *Martin*, Inanspruchnahme sozialer Netzwerke durch Minderjährige – Datenschutz aus dem Blickwinkel des Vertragsrechts, ZD 2012, 210–214.
Wischmeyer, *Thomas*, Regulierung intelligenter Systeme, AöR 143 (2018), 1–66.

Wismer, *Sebastian/Rasek*, *Arno*, Market definition in multi-sided markets, in: OECD (Hrsg.), Rethinking Antitrust Tools for Multi-Sided Platforms, Paris 2018, 55–67.

Wissenschaftliche Dienste – Deutscher Bundestag, Zulässigkeit der Transkribierung und Auswertung von Mitschnitten der Sprachsoftware „Alexa" durch Amazon, WD 10 – 3000 – 032/19, Sachstand, Berlin 2019.

Wolf, *Manfred*, Rechtsgeschäftliche Entscheidungsfreiheit und vertraglicher Interessenausgleich, Tübingen 1970.

Wolff, *Heinrich Amadeus*, Die datenschutzrechtlich Rechtfertigungsbedürftigkeit der Verweise auf Webseiten durch Betreiber von Suchmaschinen – Anmerkung zum Google Urteil des EuGH, BayVBl 2015, 9–16.

Wright, *David/De Hert*, *Paul*, Introduction to Privacy Impact Assessment, in: Wright, David/De Hert, Paul (Hrsg.), Privacy Impact Assessment, Dordrecht 2012, 3–32.

Yuan, *Tianyu*, Lernende Roboter und Fahrlässigkeitsdelikt, RW 2018, 477–504.

Zech, *Herbert*, Information als Schutzgegenstand, Tübingen 2012.

–, Daten als Wirtschaftsgut – Überlegungen zu einem „Recht des Datenerzeugers", CR 2015, 137–146.

–, „Industrie 4.0" – Rechtsrahmen für eine Datenwirtschaft im digitalen Binnenmarkt, GRUR 2015, 1151–1160.

–, Künstliche Intelligenz und Haftungsfragen, ZfPW 2019, 198–219.

–, Entscheidungen digitaler autonomer Systeme: Empfehlen sich Regelungen zu Verantwortung und Haftung?, Gutachten für den 73. Deutschen Juristentag 2020.

Zibuschka, *Jan/Nofer*, *Michael/Hinz*, *Oliver*, Zahlungsbereitschaft für Datenschutzfunktionen intelligenter Assistenten, Multikonferenz Wirtschaftsinformatik (MKWI) 2016, 1391–1402.

Zibuschka, *Jan/Horsch, Moritz/Kubach, Michael*, The ENTOURAGE Privacy and Security Reference Architecture for Internet of Things Ecosystems, Open Identity Summit 2019, 119–130.

Ziebarth, *Wolfgang*, Google als Geheimnishüter? – Verantwortlichkeit der Suchmaschinenbetreiber nach dem EuGH-Urteil, ZD 2014, 394–399.

Ziegenhorn, *Gero/von Heckel*, *Katharina*, Datenverarbeitung durch Private nach der europäischen Datenschutzreform, NVwZ 2016, 1585–1591.

Zimmermann, *Christian/Accorsi*, *Rafael/Müller*, *Günter*, Privacy dashboards: reconciling data-driven business models and privacy, Ninth International Conference on Availability, Reliability and Security, 2014, 152–157.

Zimmermann, *Reinhard*, The Law of Obligations, Capetown 1990.

Zöllner, *Wolfgang*, Zivilrechtswissenschaft und Zivilrecht im ausgehenden 20. Jahrhundert, AcP 188 (1988), 85–100.

–, Informationsordnung und Recht, Berlin 1990.

–, Regelungsspielräume im Schuldvertragsrecht: Bemerkungen zur Grundrechtsanwendung im Privatrecht und zu den sogenannten Ungleichgewichtslagen, AcP 196 (1996), 1–36.

–, Die gesetzgeberische Trennung des Datenschutzes für öffentliche und private Datenverarbeitung, RDV 1985, 3–16.

Zscherpe, *Kerstin*, Anforderungen an die datenschutzrechtliche Einwilligung im Internet, MMR 2004, 723–727.

Zuiderveen Borgesius, *Frederik J.*, Improving Privacy Protection in the Area of Behavioural Targeting, Alphen aan den Rijn 2015.

–, Personal data processing for behavioural targeting: which legal basis?, 5 International Data Privacy Law (2015), 163–176.
–, Singling out People without Knowing Their Names – Behavioural Targeting, Pseudonymous Data, and the New Data Protection Regulation, 32 Computer Law & Security Review (2016), 256–271.
Zuiderveen Borgesius, *Frederik J./Kruikemeier, Sanne/Boerman, Sophie C./Helberger*, *Natali*, Tracking Walls, Take-It-Or-Leave-It Choices, the GDPR, and the ePrivacy Regulation, 3 European Data Protection Law Review (2017), 1–16.

Alle Online-Quellen wurden zuletzt am 19.05.2022 aufgerufen.

Stichwortverzeichnis