Benedikt Buchner, Jürgen Kühling

Die Einwilligung in der Datenschutzordnung 2018

Volenti non fit inuria – „Dem Einwilligenden geschieht kein Unrecht". Dieses Grundprinzip des Rechts liegt auch dem Datenschutzrecht zugrunde. Wie dieses Prinzip unter der DS-GVO im Einzelnen umgesetzt und gewährleistet werden soll, ist Gegenstand der folgenden Ausführungen.

Mit der Verabschiedung, Ausfertigung und Veröffentlichung des „Datenschutzanpassungsgesetzes" (DSAnpG)[1] im Juni 2017 hat die Datenschutzgrundverordnung der EU (DS-GVO)[2] nunmehr auch ihr Pendant im nationalen Datenschutzrecht bekommen. Beide Regelwerke werden ab dem 25. Mai 2018 gelten und bilden die beiden zentralen Säulen der neuen Datenschutzordnung 2018. Der Beitrag skizziert am Beispiel der Einwilligung das komplexe Zusammenspiel von DS-GVO und nationalem Recht, um sodann auf wesentliche Neuerungen und zentrale Fragestellungen der Datenschutzordnung 2018 für den Erlaubnistatbestand der Einwilligung einzugehen.

1 Das Zusammenspiel von DS-GVO, BDSG-neu und bereichsspezifischen Regeln

Dadurch, dass die Kommission mit ihrem ursprünglichen, kohärenten Vorschlag einer europäischen Datenschutzverordnung mit zahlreichen Konkretisierungsmöglichkeiten auf supranationaler Ebene – in Form von Durchführungsrechtsakten und delegierten Rechtsakten – gescheitert ist, und in den Trilog-Verhandlungen auf Betreiben der Mitgliedstaaten stattdessen eine Vielzahl von obligatorischen und fakultativen Öffnungsklauseln Eingang in die Verordnung gefunden haben, wird die Struktur der Datenschutzordnung ab 2018 nochmals komplizierter ausfallen.

1.1 Regelungen der DS-GVO

Die wesentlichen Vorgaben für den Erlaubnistatbestand der Einwilligung finden sich künftig in der DS-GVO. Das gilt zunächst für die verbindliche Definition der Einwilligung in Art. 4 Nr. 11 DS-GVO. Von zentraler Bedeutung ist sodann Art. 7 DS-GVO, der ausweislich seiner Überschrift die „Bedingungen für die Einwilligung" normiert. Ergänzend hierzu sind die Erwägungsgründe zu berücksichtigen, insbesondere EG 32 f. DS-GVO sowie 42 f. DS-GVO. Für die Einwilligung eines Kindes gilt zudem Art. 8 DS-GVO. In ihrer Funktion als Erlaubnistatbestand für die Verarbeitung personenbezogener Daten ist die Einwilligung in Art. 6 DS-GVO normiert, darüber hinaus auch noch in Art. 9 DS-GVO (Verarbeitung besonderer Kategorien personenbezogener Daten), in Art. 22 DS-GVO (automatisierte Entscheidungen) sowie in Art. 49 DS-GVO (Datenübermittlung an Drittländer). Ferner ist Art. 88 DS-GVO zu beachten, der den Mitgliedstaaten im Arbeitnehmerdatenschutz Gestaltungsmöglichkeiten u.a. auch für die Einwilligung einräumt. Ergänzend ist auf Art. 83 DS-GVO zu verweisen, der insbesondere in Abs. 5 lit. a DS-GVO ein Bußgeld bei Nichtbeachtung der Einwilligungsbedingungen nach den Art. 5, 7 und 9 DS-GVO vorsieht. EG 171 DS-GVO normiert schließlich eine Übergangsregelung für Datenverarbeitungen auf der Basis von Einwilligungen, die noch auf der Grundlage der Richtlinie 95/46/EG erteilt wurden.

1.2 Nationales Recht

Sowohl Art. 8 DS-GVO als auch Art. 9 DS-GVO und Art. 88 DS-GVO enthalten Öffnungsklauseln für die Modifikation der Regelungen der DS-GVO durch mitgliedstaatliches Recht. Hier-

1 Gesetz zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 (Datenschutz-Anpassungs- und -Umsetzungsgesetz EU – DSAnpUG-EU), BGBl. (im Erscheinen).

2 Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), ABl.EU 2016 L 119/1.

Prof. Dr. Benedikt Buchner, LL.M. (UCLA)

Institut für Informations-, Gesundheits- und Medizinrecht (IGMR)
Universität Bremen

E-Mail: bbuchner@uni-bremen.de

Professor Dr. Jürgen Kühling, LL.M.

Inhaber des Lehrstuhls für Öffentliches Recht, Immobilienrecht, Infrastrukturrecht und Informationsrecht, Universität Regensburg, Mitglied der Monopolkommission

E-Mail: Juergen.Kuehling@jura.uni-regensburg.de

zulande hat der Bundesgesetzgeber von diesen Öffnungsklauseln bislang nur für den Fall des Beschäftigtendatenschutzes (Art. 88 DS-GVO) Gebrauch gemacht. So muss für die Bedeutung der Einwilligung im Arbeitnehmerdatenschutzrecht künftig auch der Blick in die Vorschrift des § 26 BDSG-neu wandern, die in ihrem Abs. 2 ausführlich die Wirksamkeit einer Einwilligung im Rahmen von Beschäftigungsverhältnissen regelt. Der Fokus der Regelung liegt hierbei auf der Frage der Freiwilligkeit einer Einwilligung.

Soweit es um die Verarbeitung sogenannter besonderer Kategorien personenbezogener Daten im Sinne des Art. 9 DS-GVO geht, steht es dem nationalen Gesetzgeber nach Art. 9 Abs. 2 lit. a DS-GVO frei, den Erlaubnistatbestand der Einwilligung als Legitimationsgrundlage auch für eine Verarbeitung solcher besonders sensibler Daten auszuschließen. Im Zuge der Novellierung des Sozialdatenschutzrechts hat der deutsche Gesetzgeber – trotz vielfach erhobener Forderungen – von dieser Öffnungsklausel jedoch keinen Gebrauch gemacht. Ausgangspunkt der §§ 67a ff. SGB X-E ist vielmehr, dass auch Sozialdaten grundsätzlich auf Grundlage einer Einwilligung der betroffenen Person erhoben werden und sonst nicht verarbeitet werden dürfen.[3]

Hingewiesen sei schließlich auch darauf, dass der Bundesgesetzgeber im Rahmen des DSAnpUG-EU zugleich die Richtlinie 2016/680/EU zum Datenschutz im Strafrechtsbereich umgesetzt hat. Hier findet sich für diesen spezifischen Sektor eine eigenständige Regelung der Einwilligung in § 51 BDSG-neu, die jedoch nur für die Datenverarbeitung zu Zwecken der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit gilt (vgl. Art. 1 Abs. 1 RL 2016/680).[4]

1.3 Zweistufiges Regelungssystem

Insgesamt entsteht künftig im Anwendungsbereich der DS-GVO abweichend vom bisherigen Recht auch für die Einwilligung ein zweistufiges Regelungssystem mit gleichermaßen unmittelbar geltenden Normen auf beiden Ebenen.[5] Primär relevant sind die Vorgaben der vorrangigen Regelungen insbesondere in den Art. 7 und 8 DS-GVO. Für Teilbereiche ist – ergänzend – die zweite Stufe der nationalen Bestimmungen zu beachten. Hier greift weiter die Zweiteilung in das allgemeine BDSG (dann in der neuen Fassung) und die allgemeinen Landesdatenschutzgesetze einerseits und die Vielzahl bereichsspezifischer Regelungen auf Bundes- und Landesebene andererseits. Dabei müssen die Landesdatenschutzgesetze erst noch angepasst werden – hoffentlich auf der Linie des BDSG-neu. Im Übrigen muss aber vor allem das gesamte sektorspezifische Datenschutzrecht auf Bundes- und Landesebene noch bis zur Geltung der DS-GVO am 25. Mai 2018 auf seine Vereinbarkeit mit den europäischen Vorgaben geprüft und gegebenenfalls aufgehoben, ergänzt oder modifiziert werden. Das gilt mit Blick auf die Einwilligung etwa für die kaum überschaubare Vielzahl an Regelungen im Gesundheitsbereich, die teils eigenständige Bestimmungen zur Einwilligung haben.

3 Siehe Beschlussempfehlung und Bericht des Ausschusses für Arbeit und Soziales vom 31.5.2017, BT-Drs. 18/12611.

4 Ausführlicher zur Rolle der Einwilligung als Erlaubnistatbestand für eine Datenverarbeitung unter der RL 2016/680 s. Schwichtenberg, DuD 2016, 605, 606 f. sowie Stief, StV 2017, 470.

5 Siehe dazu und zum Folgenden bereits Kühling, NJW 2017, 1985 f.

2 Bedeutung und Wirksamkeit der Einwilligung unter der DS-GVO

An der Bedeutung der Einwilligung als zentralem Erlaubnistatbestand für eine Verarbeitung personenbezogener Daten wird sich auch unter der DS-GVO nichts ändern.[6]

2.1 Einwilligung als tatsächliche Selbstbestimmung

Soweit die Tragfähigkeit der Einwilligung als Erlaubnistatbestand für die DS-GVO in Frage gestellt wird, wird als Begründung hierfür in erster Linie darauf verwiesen, dass die Hürden, die für die Einholung einer wirksamen Einwilligung zu überwinden sind, künftig teils höher angesetzt sind und es daher entsprechend schwierig bzw. unmöglich sein soll, eine rechtswirksame Einwilligung einzuholen.[7] Fragwürdig ist diese Einschätzung allerdings schon mit Blick darauf, dass bislang die rechtlichen bzw. die tatsächlichen Hürden für die Einholung einer Einwilligung oftmals viel zu niedrig angesetzt waren und sich die Einwilligung in einem bloßen Formalismus erschöpft hatte, der mit einer wirklichen Ausübung informationeller Selbstbestimmung nur wenig zu tun hatte. Daher mag es durchaus so sein, dass die Einwilligung künftig in Konstellationen, in denen sie bislang als Erlaubnistatbestand bzw. als Feigenblatt instrumentalisiert werden konnte, obwohl sie mit einer Ausübung informationeller Selbstbestimmung tatsächlich nichts zu tun hatte, künftig nicht mehr praktikabel sein wird. Im Sinne eines effektiven Datenschutzes ist dies aber ohne Einschränkung zu begrüßen.

2.2 Ausdrücklichkeit und Freiwilligkeit

Neuerungen bringt die DS-GVO hinsichtlich der Wirksamkeit einer Einwilligung vor allem für die Freiwilligkeit und Ausdrücklichkeit einer solchen Einwilligung. Ist bislang immer wieder vertreten worden, dass die Einwilligung auch im Wege eines sogenannten Opt-out eingeholt werden kann,[8] stellt künftig die DS-GVO klar, dass allein eine aktive und unmissverständliche Willensbetätigung seitens der betroffenen Person in Form des Opt-in als wirksame Einwilligung eingeordnet werden kann.[9]

Was wiederum die Freiwilligkeit einer Einwilligung angeht, gibt die DS-GVO einen ausdifferenzierten Katalog von Kriterien an die Hand, um zu beurteilen, ob eine Einwilligung im Einzelfall als freiwillig und damit wirksam einzuordnen ist. Dabei sind die Voraussetzungen, die an eine freiwillige Einwilligung gestellt werden, durch die DS-GVO nicht unbedingt strenger als bislang normiert, sondern in erster Linie präziser und auch praxisnaher. Vor allem tragen die Vorgaben der DS-GVO dem Umstand Rech-

6 Ebenso Albers in Beck OK Datenschutzrecht DS-GVO Art. 6 Rn. 19 (das „zentrale Scharnier des privaten Datenschutzrechts"); Ernst, ZD 2017, 110; Stemmer in Beck OK Datenschutzrecht DS-GVO Art. 7 Rn. 1; Wendehorst/v. Westphalen, NJW 2016, 3745 („wichtigster Rechtfertigungsgrund"). Siehe zum Ganzen auch schon Buchner, DuD 2016, 155, 158, sowie ausführlich Buchner/Kühling in Kühling/Buchner, DS-GVO, 2017, Art. 7 Rn. 10 ff.

7 So Schneider/Härting, ZD 2012, 199, 201; ähnlich auch Härting, DSGVO, 2016, Rn. 401. Frenzel in Paal/Pauly DS-GVO, 2016, Art. 7 Rn. 26, spricht gar von einer möglichen „Flucht vor der Einwilligung".

8 S. insb. die beiden Entscheidungen des BGH zu den Kundenbindungssystemen Payback und HappyDigits, BGH, DuD 2008, 818, 820 (Payback) und DuD 2010, 493, 495 (Happy Digits).

9 S. Art. 4 Nr. 11 DS-GVO („unmissverständlich abgegebene Willensbekundung") und insb. auch EG 32: „Stillschweigen, bereits angekreuzte Kästchen oder Untätigkeit der betroffenen Person sollten daher keine Einwilligung darstellen."

nung, dass es durchaus auch Konstellationen gibt, in denen eine Einwilligung nicht auf einem uneingeschränkt freien Willen der betroffenen Person beruht, insbesondere dann, wenn diese Einwilligung vom Gegenüber zur Vorbedingung für den Abschluss eines Schuldverhältnisses gemacht wird („take it or leave it"). Ob in solcherlei Konstellationen eine Einwilligung als unfreiwillig und mithin unwirksam einzustufen ist, hängt entscheidend auch davon ab, ob dadurch eine Datenverarbeitung legitimiert werden soll, die über das hinausgeht, was für eine Vertragserfüllung an sich erforderlich ist.[10] Damit wendet sich die DS-GVO zwar von einer „lupenreinen" Freiwilligkeitsmaxime ab, verleiht aber gerade dadurch der Einwilligung als Erlaubnistatbestand mehr Praxisnähe und damit auch mehr Legitimation.

2.3 Form

Was die Formwirksamkeit der Einwilligung anbelangt, präsentieren sich die Anforderungen der DS-GVO im Vergleich zum bisherigen BDSG zunächst einmal als weniger streng, weil die DS-GVO kein grundsätzliches Schriftformerfordernis bei der Einwilligung kennt. Mit Blick auf die umfangreichen Nachweiserfordernisse, wie sie die DS-GVO nicht nur speziell für die Einwilligung, sondern ganz allgemein für die Rechtmäßigkeit einer Datenverarbeitung dem Verantwortlichen auferlegt, wird jedoch in der Praxis auch künftig der Regelfall die Einholung einer schriftlichen Einwilligung sein bzw. einer elektronischen Einwilligung, die entsprechend protokolliert wird.

2.4 Nationales Recht

Schließlich ist bei der Einwilligung als Erlaubnistatbestand noch das oben angesprochene Zusammenspiel zwischen DS-GVO und nationalem Recht zu beachten. So hat der nationale Gesetzgeber in Ausführung des Regelspielraums nach Art. 88 DS-GVO für die Einwilligung im Rahmen eines Beschäftigungsverhältnisses nach § 26 Abs. 2 Satz 3 BDSG-neu die Schriftform vorgesehen. Für den Sozialdatenschutz sieht § 67b Abs. 2 Satz 1 SGB X-E vor, dass die Einwilligung schriftlich oder elektronisch erfolgen soll.

Zugleich sind die nationalen Regelungen zum Beschäftigten- und zum Sozialdatenschutz auch ein Beleg dafür, dass der Einwilligung als Rechtfertigung für eine Datenverarbeitung in Zukunft noch mehr Bedeutung beigemessen wird, weil ihr trotz aller potenziellen Freiwilligkeitsdefizite zumindest nicht grundsätzlich die Legitimation als Erlaubnistatbestand abgesprochen wird. Von Bedeutung ist dies in erster Linie für den Sozialdatenschutz, da seit der Entscheidung des BSG vom Dezember 2008 der Einwilligung eine Bedeutung als eigenständiger Erlaubnistatbestand abgesprochen wird.[11] Nach weit verbreiteter Ansicht – und unter Verweis auf die Argumentation des BSG – soll hier das Angewiesensein auf Sozialleistungen und das Ungleichgewicht zwischen Betroffenen und Behörde generell eine Freiwilligkeit und damit eine Wirksamkeit der Einwilligung ausschließen. Im Beschäftigtendatenschutz sind hingegen bislang die Maßstäbe – zumindest vom Bundesarbeitsgericht – tendenziell großzügiger angesetzt worden. Die Möglichkeit einer Einwilligung in die Datenverarbeitung ist hier auch schon bislang nicht grundsätzlich ausgeschlossen worden.[12]

3 Die Einwilligung von Kindern

Für die neueren Herausforderungen der Dienste der Informationsgesellschaft hat die DS-GVO in Art. 8 immerhin für die Einwilligung von Kindern eine explizite Anpassung an das Internet-Zeitalter vorgenommen und eine neue Regelung geschaffen. Hintergrund ist die besondere Schutzbedürftigkeit von Minderjährigen, die regelmäßig überdurchschnittlich internetaffin sind und oftmals eine breite Datenspur im Internet hinterlassen, ohne sich über die Folgen im Klaren zu sein. Das gilt insbesondere für die Nutzung scheinbar kostenloser Dienste wie Facebook oder WhatsApp, bei denen die Nutzer mit ihren Daten zahlen. Die Norm wirft jedoch mindestens ebenso viele Fragen auf, wie sie beantwortet.

Im Grundansatz verwirft die Norm das bislang in Deutschland greifende Modell der Einzelfallbewertung im Rahmen der Prüfung der Einsichtsfähigkeit des Minderjährigen. Diese kann bei manchem Heranwachsenden mit 16 noch nicht gegeben sein, bei anderen hingegen bereits mit 15. An die Stelle tritt ein typisierendes, *abgestuftes Alterskonzept* für die Rechtmäßigkeit der Datenverarbeitung.[13] Wenn der Minderjährige bereits das 16. Lebensjahr vollendet hat, ist die Verarbeitung auf der Basis dessen Einwilligung rechtmäßig, falls die weiteren Voraussetzungen des Art. 6 Abs. 1 lit. a und Art. 7 DS-GVO vorliegen. Ist die Altersgrenze des 16. Lebensjahres noch nicht erreicht, bedarf es zusätzlich der Einwilligung der Erziehungsberechtigten bzw. deren Zustimmung zur Einwilligung. Diese strenge Altersgrenze kann von den Mitgliedstaaten abgesenkt werden bis auf das Alter von 13 Jahren. Eine Rückkehr zum flexiblen Modell ist jedoch nicht vorgesehen. Auch hier zeigt sich damit der Hybrid-Charakter der Verordnung, die keine Vollharmonisierung wird erreichen können.

Der deutsche Gesetzgeber hat nun im BDSG-neu von dieser Öffnungsklausel jedoch keinen Gebrauch gemacht. Damit schlägt der Modellwandel samt hoch angesetzter Altersgrenze im deutschen Recht voll durch. Die Änderungen sind gleichwohl überschaubar, hat der BGH doch im Jahr 2014 geurteilt, dass die Einsichtsfähigkeit bei Jugendlichen im Alter von 15 bis 17 Jahren grundsätzlich noch nicht gegeben ist.[14] Ein Hinweis auf die Vorzugswürdigkeit des differenzierenden Modells gegenüber einer *starren Altersgrenze*[15] kann daher nur de lege ferenda an den Unionsgesetzgeber adressiert werden. Interpretatorische Konsequenzen für Personen unter 16 Jahren hat dies nicht. Gerade bei Diensten der Informationsgesellschaft, die regelmäßig keinen persönlichen Kontakt zu dem Betroffenen implizieren, gibt es jedoch gute Gründe für ein einfach zu handhabendes Modell der starren Altersgrenze. Umgekehrt gilt im Übrigen sehr wohl, dass die Schutzbedürftigkeit von Personen mit dem Erreichen des 16. Lebensjahrs nicht endet. Diese kann aber nur über die übrigen Einwilligungsvoraussetzungen des Art. 7 DS-GVO erreicht

10 Vgl. Buchner/Kühling in Kühling/Buchner, Art. 7 Rn. 46 ff.

11 BSG, MedR 2009, 685 (Weitergabe von Patientendaten durch Leistungserbringer).

12 Siehe BAG, DuD 2015, 553 (Einwilligung in die Online-Veröffentlichung von Video-Aufnahmen im Rahmen der Öffentlichkeitsarbeit eines Unternehmens).

13 Siehe dazu schon Buchner/Kühling in Kühling/Buchner, Art. 8 Rn. 3.

14 BGH, NJW 2014, 2282; siehe ferner Jandt/Roßnagel, MMR 2011, 673 (639); Möhrke-Sobolewski/Klas, K&R 2016, 373 (374).

15 So Schulz in Gola, DS-GVO, 2017, Art. 8 Rn. 10.

werden. Denn Art. 8 Abs. 1 S. 1 DS-GVO normiert eine unwiderlegbare Annahme der Einsichtsfähigkeit für Personen jenseits des 16. Lebensjahres. Sie substituiert die zuvor im Rahmen der Einwilligung zu prüfende Wirksamkeitsvoraussetzung der Einsichtsfähigkeit und stellt vielmehr selbst eine solche dar.[16] Flankierenden Schutz bietet im Übrigen die Widerrufbarkeit der Einwilligung.

Es überrascht wenig, dass eine Kontroverse darüber entfacht ist, wann denn ein Angebot „*einem Kind direkt gemacht wird*". Eindeutig ist dies sicherlich, wenn schon durch die Aufmachung des Dienstes klar ist, dass sich dieser unmittelbar an die Kinder selbst als Betroffene der Datenverarbeitung wendet. Das hängt selbstverständlich von der Aufmachung des Angebots ab und nicht vom Produkt. Relevant ist das Gepräge im Rahmen der Erfassung der Daten. Ist der Dienst etwa so ausgelegt, dass eine kindgerechte Sprache bei der Dateneingabe gepflegt wird, liegt die Einordnung auf der Hand. Auf diesen offensichtlichen Fall ist der Anwendungsbereich aber keineswegs beschränkt. Ebenso unzweifelhaft erfasst werden vielmehr auch Dienste, die sowohl an Erwachsene als auch an Kinder adressiert sind („dual use"). Dies ist vom Wortlaut gedeckt und rechtfertigt sich vor dem Hintergrund der Schutzbedürftigkeit auch in teleologischer Hinsicht[17]. Der Anwendungsbereich geht jedoch noch einen Schritt weiter und erfasst auch Dienste, die sich spezifisch an Erwachsene richten. Zwar scheint auf den ersten Blick der Wortlaut dagegen zu sprechen. Das ist grammatikalisch jedoch keineswegs zwingend,[18] ja nicht einmal naheliegend. So kann das Wort „direkt" auch als „unmittelbar" im Sinne eines Verzichts auf die Einschaltung einer weiteren Person, namentlich des Erziehungsberechtigten, verstanden werden.[19] In systematischer Hinsicht sei insofern auf EG 38 S. 3 DS-GVO verwiesen, der in Bezug auf Präventions- und Beratungsdienste jene Unmittelbarkeit formuliert. In teleologischer Hinsicht ist teilweise gerade hier Schutz notwendig, wenn man etwa an das Angebot eines digitalen Datingdienstes für – vermeintlich – Volljährige denkt.[20] Soll es wirklich ausreichen, dass der jugendliche Nutzer ohne nähere Altersverifikation anklickt, dass er bereits 18 Jahre alt ist?[21] Das ist auch in systematischer Perspektive wenig überzeugend, verpflichtet Art. 8 Abs. 2 DS-GVO doch gerade den Anbieter zu entsprechenden Maßnahmen, um das tatsächliche Vorliegen der Einwilligung der Eltern sicherzustellen.

Eben diese Verpflichtung steht in ihrer Reichweite jedoch ebenfalls in Streit und ist von großer praktischer Bedeutung. Was nicht reicht, ist klar: das bloße Anklicken einer Box, dass die Eltern einverstanden sind. Was ist aber positiv verlangt? Weitgehende Einigkeit besteht, dass das sogenannte „*Double-Opt-in-Verfahren*" (DOI-Verfahren) einen sinnvollen Mechanismus darstellt.[22] Die Missbrauchsrisiken dieses Verfahrens liegen zwar auf der Hand, kann der Heranwachsende doch durch eine „gefakte" E-Mail-Adresse der Eltern oder durch den unmittelbaren Missbrauch des elterlichen E-Mail-Accounts eine zweite bestätigende E-Mail der Eltern vortäuschen. Dieser Missbrauch wird aber grundsätzlich hingenommen werden müssen.[23] Im Übrigen ist ein Rechtsvergleich erkenntnisstiftend: So hat die US-amerikanische Federal Trade Commission in Anwendung vergleichbarer Vorgaben im US-amerikanischen Recht neben dem DOI-Verfahren eine Reihe erwägenswerter Mechanismen angeführt und zwar u.a. ein von den Eltern unterschriebenes Dokument (per Post, Fax oder elektronischem Scan), den Rückgriff auf Kreditkarten der Eltern zur Legitimation von Transaktionen und ein Telefongespräch oder eine Videokonferenz mit den Eltern von geschultem Personal unter einer kostenfreien Telefonnummer. Derartige verschärfte Anforderungen werden je nach Schutzbedürftigkeit der Daten bis hin zum Postident-Verfahren bei besonders sensiblen Daten zu verlangen sein. Es werden also differenzierende Ansätze zur Auflösung des Spannungsverhältnisses von Datensparsamkeit und Praktikabilität einerseits und Minderjährigenschutz anderseits zu entwickeln sein.[24]

Die Konsequenz des Art. 8 DS-GVO ist einfach und nachvollziehbar: Erster Ansprechpartner der Diensteanbieter bei Personen, die das 16. Lebensjahr noch nicht vollendet haben, wird weiterhin – oder künftig wohl eher verstärkt – der Träger elterlicher Verantwortung sein.[25]

Groteske Lösungen, wie sie etwa der Instant-Messenger-Diensteanbieter WhatsApp seit Jahren praktiziert, der allseits bekannt flächendeckend Dienste an Personen unter 16 Jahren anbot, obwohl laut den eigenen Nutzungsbedingungen 16 Jahre das Mindestalter darstellte, und später das Mindestalter auf 13 Jahre absenkte bzw. auf das Alter, das „[…] erforderlich ist, […] [um die] Dienste ohne elterliche Zustimmung zu nutzen"[26], gehören jedenfalls der Vergangenheit an. Ein bisschen Mehr werden sich die hoch innovativen Dienste der Informationsgesellschaft des 21. Jahrhunderts schon einfallen lassen müssen.

4 Last but not least: Einwilligung bei einer Datenverarbeitung im Mehrpersonenverhältnis

Nochmals komplexer gestaltet sich der Erlaubnistatbestand der Einwilligung, wenn Daten in Mehrpersonenverhältnissen verarbeitet werden, wie es etwa bei sozialen Netzwerken oder Instant-Messenger-Diensten der Fall ist. Denn hier ist sowohl das Verhältnis des Diensteanbieters – etwa WhatsApp – zu den Nutzern, als auch das der Nutzer untereinander zu betrachten.[27] Geht es dann noch um die Einwilligung von Minderjährigen, steigert sich die Komplexität abermals. Zuletzt wurde das in zwei Entscheidungen des Amtsgerichts Bad Hersfeld vom März und Mai

16 Siehe dazu schon Buchner/Kühling in Kühling/Buchner, Art. 8 Rn. 19; ebenso im Ergebnis Frenzel in Paal/Pauly, Art 8 Rn. 10; Plath in Plath, BDSG/DV-GVO, 2016, Art 8 Rn. 1.

17 Buchner/Kühling in Kühling/Buchner, Art. 8 Rn. 15; ebenso Heckmann/Pascke in Ehmann/Selmayr, DS-GVO, 2017, Art. 8 Rn. 20 f.

18 Anders aber Frenzel in Paal/Pauly, Art 8 Rn. 7.

19 Buchner/Kühling in Kühling/Buchner, Art. 8 Rn. 16.

20 So das Beispiel bei Frenzel in Paal/Pauly, Art 8 Rn. 7.

21 So aber wohl im Ergebnis Frenzel in Paal/Pauly, Art 8 Rn. 7.

22 Dazu Gola/Schulz, ZD 2013, 475 (479); Möhrke-Sobolewski/Klas, K&R 2016, 373 (377 f.).

23 So zutreffend Möhrke-Sobolewski/Klas, K&R 2016, 373 (378).

24 Näher dazu Buchner/Kühling in Kühling/Buchner, Art. 8 Rn. 24 ff.

25 Möhrke-Sobolewski/Klas, K&R 2016, 373 (375).

26 Vgl. *WhatsApp Inc.*, WhatsApp Nutzungsbedingungen, abrufbar im WWW unter der URL https://www.whatsapp.com/legal/?l=de#key-updates.

27 Dazu umfassend Heberlein, Datenschutz im Social Web, Materiell-rechtliche Aspekte der Verarbeitung personenbezogener Daten durch Private in sozialen Netzwerken (in Vorbereitung), Kapitel 3, A.

2017 deutlich,[28] die aktuell für viel Diskussionsstoff sorgen.[29] Hier hat das Gericht jeweils in einem sorgerechtlichen Verfahren der Mutter des Kindes auferlegt, hinsichtlich sämtlicher im Adressbuch ihres Kindes eingetragenen Personen eine Zustimmungserklärung zur Übermittlung der Daten an WhatsApp einzuholen. Sollte das tatsächlich im Nutzer-Nutzer-Verhältnis erforderlich sein, dürfte das Ende von WhatsApp in der jetzigen Nutzungsform besiegelt sein.

So überraschend die Entscheidungen des Gerichts auf den ersten Blick anmuten mögen, so konsequent und folgerichtig sind sie doch auf den zweiten Blick. Das Datenschutzrecht kennt keine Einwilligung zulasten Dritter.[30] Daher reicht es auch nicht aus, wenn sich ein Anbieter bei der Verarbeitung von Daten, die sich nicht auf den Nutzer selbst, sondern auf dritte Personen beziehen, allein auf die Einwilligung des unmittelbar betroffenen Nutzers stützt. Konsequenterweise hatte daher das LG Berlin bereits 2013 eine Klausel von Apple für unwirksam erklärt, mittels derer Nutzer sich damit einverstanden erklären sollten, dass Apple Daten über die Familie oder Freunde erhebt, wenn der Nutzer die Daten über diese Person „zur Verfügung stellt" (z.B. „Name, Adresse, E-Mail und Telefonnummer").[31]

Ebenso nicht ausreichend – und daher vom AG Bad Hersfeld zu Recht verworfen – ist aber auch der Ansatz von WhatsApp, sich von der eigenen datenschutzrechtlichen Verantwortlichkeit einfach dadurch freizuzeichnen, dass man sich qua AGB eine Art von Rechtmäßigkeits-Bestätigung seitens der Nutzer ausstellen lässt.[32] Es kann nicht angehen, dass sich ein Anbieter als der datenschutzrechtlich Verantwortliche seiner Pflicht zum rechtmäßigen Umgang mit personenbezogenen Daten dadurch entledigt, dass er auf dem Papier seine Nutzer dazu verpflichtet, sich um eine „Autorisierung" der Datenverarbeitung zu kümmern – noch dazu, ohne dann in irgendeiner Weise Anstalten zu treffen, diese unterstellte Autorisierung zumindest zu überprüfen.

Nicht zuletzt zeugt es auch von einem ebenso selektiven wie fragwürdigen Rechtsbewusstsein von Facebook, wenn einerseits – wie ganz aktuell im vom KG Berlin entschiedenen Fall zum digitalen Nachlass – der Mutterkonzern Facebook in eher fragwürdiger Vehemenz auf den Schutz der Vertraulichkeit zugunsten dritter Kommunikationspartner in einer Eltern-Kind-Beziehung pocht, andererseits aber die Unternehmenstochter WhatsApp dieser Vertraulichkeit offensichtlich keine Bedeutung beimisst. In dem Verfahren vor dem KG Berlin, in dem es um die Frage ging, ob Eltern ein Einsichtsrecht in den Facebook-Account ihrer verstorbenen Tochter zusteht,[33] wurde Facebook nicht müde zu betonen, dass es mit dem Fernmeldegeheimnis und Datenschutz anderer Kommunikationspartner nicht vereinbar sei, den Eltern eine solche Einsicht zu gewähren. Seiner Tochter WhatsApp hat Facebook diese datenschutzrechtliche Sensibilität offensichtlich noch nicht vermitteln können. Der Umstand, dass auch die Information, wer in wessen Adressbuch als Kommunikationspartner steht, ein – mitunter sogar äußerst sensibles – personenbezogenes Datum ist, scheint für WhatsApp nicht weiter von Belang zu sein. WhatsApp unternimmt hier noch nicht einmal einen ernsthaften Versuch, durch Einholung einer Einwilligung bei den (Dritt-)Betroffenen dem datenschutzrechtlichen Rechtmäßigkeitsprinzip zu genügen.

5 Fazit

Dass es aktuell an einem Familienrichter des Amtsgerichts Bad Hersfeld ist, einem milliardenschweren Internetkonzern zum wiederholten Male erklären zu müssen, dass und warum dieser noch immer nicht einmal die elementarsten Grundzüge des deutschen und europäischen Datenschutzrechts (keine Datenverarbeitung ohne Erlaubnistatbestand) beherzigt, sagt viel darüber aus, wie es derzeit um die Durchsetzungskraft des Datenschutzrechts bestellt ist. Gerade in der Online-Welt beschränkt sich die Einwilligung oftmals auf einen bloßen Formalismus – wenn sie denn überhaupt eingeholt wird. Umso mehr ist es zu begrüßen, dass ab Mai 2018 mit der DS-GVO die Vorgaben für eine wirksame Einwilligung präzisiert werden und zugleich deren Durchsetzung effektiver ausgestaltet ist.[34] Vor allem mit ihren Bußgeldtatbeständen spricht die DS-GVO eine Sprache, die auch Facebook & Co. verstehen, nämlich dass es in Zukunft mehr Rendite verspricht, Datenschutz zu beachten als diesen weiter zu ignorieren.

28 AG Bad Hersfeld Beschl. v. 20.03.2017, Az.: F 111/17 EASO sowie Beschl. v. 15.05.2017, Az.: F 120/17 EASO (März-Entscheidung in diesem Heft).

29 S. statt aller FAZ v. 3.7.2017 („Datenweitergabe durch Whatsapp – Meine Kontakte, deine Kontakte"); abrufbar unter http://www.faz.net/aktuell/feuilleton/medien/weitergabe-von-kontakten-durch-whatsapp-vor-gericht-15085153.html (letzter Abruf 5.7.2017).

30 Zur Unwirksamkeit einer „Einwilligung zulasten Dritter" s. schon LG Berlin, DuD 2013, 598, 600 (Datenschutzklauseln von Apple).

31 LG Berlin, DuD 2013, 598, 600.

32 S. die sog. Datenschutzrichtlinie von WhatsApp (Fn. 26), in der es u.a. heißt: „Du stellst uns regelmäßig die Telefonnummern in deinem Mobiltelefon-Adressbuch zur Verfügung, darunter sowohl die Nummern von Nutzern unserer Dienste als auch die von deinen sonstigen Kontakten. Du bestätigst, dass du autorisiert bist, uns solche Nummern zur Verfügung zu stellen."

33 S. dazu KG Berlin, DuD 2017, 510 – Digitaler Nachlass.

34 Siehe ausführlich zur künftigen Durchsetzung des Datenschutzrechts unter der DS-GVO den Beitrag von Bergt in diesem Heft.