

DATENSCHUTZ FÜR MINDERJÄHRIGE NACH DER EUROPÄISCHEN DATENSCHUTZ- GRUNDVERORDNUNG (DSGVO) VOM 27. APRIL 2016

Jochen Krüger / Stephanie Vogelgesang / Michael Weller

Vizepräsident des Amtsgerichts Saarbrücken a.D. und wissenschaftlicher Mitarbeiter, juris-Stiftungsprofessur für Rechtsinformatik und CISPA an der Universität des Saarlandes

66123 Saarbrücken, DE
jochen.krueger@uni-saarland.de

Wissenschaftliche Mitarbeiterin, juris-Stiftungsprofessur für Rechtsinformatik und CISPA an der Universität des Saarlandes

66123 Saarbrücken, DE
stephanie.vogelgesang@uni-saarland.de

Rechtsanwalt, Geschäftsführer der Europäischen EDV-Akademie des Rechts gGmbH

Science Park 2, 66123 Saarbrücken, DE
weller@ear.eu

Schlagnote: *Europäische Datenschutz-Grundverordnung, DSGVO, Minderjähriger, Kind, Jugendlicher, Datenerhebung, Datenverarbeitung, Datenschutz, informationelle Selbstbestimmung, Einwilligungsfähigkeit, Dienste der Informationsgesellschaft*

Abstract: *Die Wahl des Themas beruht auf zwei Überlegungen: 1. In Zeiten der digitalen Aufrüstung der Gesellschaft erhält das Recht der Minderjährigen auf informationelle Selbstbestimmung eine neue praktische und theoretische Dimension. 2. Dies wird auch in der neuen Europäischen Datenschutz-Grundverordnung (DSGVO) deutlich. Im Erwägungsgrund 38 wird das spezifische Gefährdungspotential für personenbezogene Daten von Kindern betont. Der Beitrag befasst sich mit den rechtlich relevanten Regelungen für Minderjährige in der DSGVO und thematisiert allgemeine Probleme des Datenschutzes bei Minderjährigen.*

1. Allgemeine Problemstellung

Die digitale Aufrüstung der Gesellschaft ist unumkehrbar und lässt auch das Recht nicht unberührt. Dies soll im Zusammenhang mit dem Datenschutz für Minderjährige nach der Europäischen Datenschutz-Grundverordnung (DSGVO)¹ näher erörtert werden. Im Mittelpunkt steht dabei Art. 8 DSGVO.

1.1. Zur Aktualität des Themas

Kinder und Jugendliche fühlen sich von den neuen Medien und Techniken besonders angezogen und nutzen auch das Internet.² Dies kann zu einer Vielzahl von rechtlichen Fragestellungen führen und zwar gerade auch mit Blick auf zentrale rechtliche Gestaltungsprinzipien. So ist ausweislich § 4 Bundesdatenschutzgesetz (BDSG) die Einwilligung des Betroffenen in die Datenerhebung und -verarbeitung ein tragender Systembaustein. § 4a BDSG enthält insoweit auch weitere Einzelheiten zu Fragen der Einwilligung. Für die sich bei Minderjährigen aufdrängende Frage, ob bzw. ab welcher Altersstufe diese rechtlich wirksam in eine sie betreffende Datenerhebung und -verarbeitung einwilligen können, gibt jedoch auch § 4a BDSG keine klare Antwort.

¹ 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).

² JIM-Studie 2015, S. 29 ff. (http://www.mpfs.de/fileadmin/files/Studien/JIM/2015/JIM_Studie_2015.pdf, alle Internetquellen zuletzt abgerufen am 3. Januar 2017) bzw. KIM-Studie 2014, S. 31 ff. (http://www.mpfs.de/fileadmin/files/Studien/KIM/2014/KIM_Studie_2014.pdf).

Insbesondere fehlt eine standardisierte Altersgrenze. Abgestellt wird im Ergebnis auf eine Einsichtsfähigkeit des minderjährigen Nutzers im Einzelfall.³ Unklar bleibt dabei weitestgehend, welche Kriterien dafür herangezogen werden sollen und wie diese gegebenenfalls im Streitfall festgestellt werden können. Schon mit Blick auf diesen spezifisch inhaltlichen Gesichtspunkt ist von Interesse, ob und inwieweit die neue DSGVO Regelungen zum Datenschutz von Minderjährigen enthält.

1.2. Zur rechtlichen Relevanz des Themas

Daneben ist die Einbeziehung der DSGVO auch aus allgemeinen rechtstheoretischen Überlegungen erforderlich. Die DSGVO gilt ab dem 25. Mai 2018⁴ unmittelbar⁵ in allen Mitgliedstaaten und wird Teil der jeweiligen Rechtsordnung.⁶ Der inhaltliche Anwendungsbereich der Verordnung wird insbesondere konkretisiert durch Art. 1 DSGVO in Verbindung mit Erwägungsgrund (EG) 1 und 2. In der Sache geht es um den Schutz personenbezogener Daten und den freien Verkehr mit diesen Daten. Allerdings kann die Europäische Union deutsche Gesetze nicht direkt verändern oder außer Kraft setzen.⁷ Im Konfliktfall muss daher die Frage des Anwendungsvorrangs erörtert werden. Diese Problematik wird jedoch gegenstandslos, soweit die DSGVO den Nationalstaaten Regelungskompetenzen einräumt. Insoweit ist das hier gewählte Thema auch geeignet, die zuvor skizzierten rechtstheoretischen Bezugspunkte zwischen DSGVO und nationalem Recht exemplarisch an einer abgegrenzten Sachproblematik zu verdeutlichen.

2. Zur systematischen Bedeutung des Art. 8 DSGVO

Im vorliegenden Beitrag werden schwerpunktmäßig Fragen des Art. 8 DSGVO erörtert. Dieser befasst sich mit der Einwilligung von Kindern bei Diensten der Informationsgesellschaft. In der Sache geht es damit um rechtliche Möglichkeiten, aber auch den Schutz Minderjähriger in Zeiten der Digitalisierung.

2.1. Rechte und Schutz Minderjähriger in Zeiten der Digitalisierung

Auch Minderjährige haben grds. ein Recht auf informationelle Selbstbestimmung. Dieses Recht wird in Deutschland auf nationaler Ebene aus Art. 2 Abs. 1 i.V. mit Art. 1 Abs. 1 GG hergeleitet⁸ und ergibt sich auf Unionsebene aus Art. 8 der Charta der Grundrechte der Europäischen Union.

In Zeiten der verstärkten Digitalisierung des Alltags erhält dieses Recht der Minderjährigen eine neue praktische und theoretische Dimension. Dies kommt auch in der DSGVO selbst zum Ausdruck.⁹ Von besonderem inhaltlichem Interesse ist dabei EG 38. Darin heißt es unter anderem:

Kinder verdienen bei ihren personenbezogenen Daten besonderen Schutz, da Kinder sich der betreffenden Risiken, Folgen und Garantien und ihrer Rechte bei der Verarbeitung personenbezogener Daten möglicherweise weniger bewusst sind. Ein solcher besonderer Schutz sollte insbesondere die Verwendung personenbezogener Daten von Kindern für Werbezwecke oder für die Erstellung von Persönlichkeits- oder Nutzerprofilen und die Erhebung von personenbezogenen Daten von Kindern bei der Nutzung von Diensten, die Kindern direkt angeboten werden, betreffen.

Damit wird das spezifische Gefährdungspotential für Kinder im Zusammenhang mit persönlichen Daten formuliert und in der Sache anerkannt. Zudem werden in EG 38 relativ konkrete Sachverhalte erwähnt, bei denen

³ GOLLA/SCHOMERUS, BDSG Kommentar, 12. Aufl. 2015, § 4a, Rn. 2a.

⁴ Vgl. Art. 99 Abs. 2 DSGVO.

⁵ Vgl. Art. 288 Abs. 2 S. 1 AEUV.

⁶ Vgl. ROSSNAGEL, in: Roßnagel (Hrsg.), Europäische Datenschutz-Grundverordnung, 1. Aufl. 2017, § 1, Rn. 1.

⁷ Vgl. ROSSNAGEL (Fn. 6), § 1, Rn. 31.

⁸ Vgl. dazu auch JANDT/ROSSNAGEL, Social Networks für Kinder und Jugendliche – Besteht ein ausreichender Datenschutz?, MMR 2011, 638.

⁹ Vgl. zu entsprechenden Datenschutzregelungen auch MÖHRKE-SOBOLEWSKI/KLAS, Zur Gestaltung des Minderjährigendatenschutzes in digitalen Informationsdiensten, K&R 2016, 375.

nach Vorstellung des Ordnungsgebers die Schutzbedürftigkeit von Minderjährigen besonders ausgeprägt ist. Dazu zählen die Themen «personenbezogene Daten für Werbezwecke», «Erstellung von Nutzerprofilen» und «Erhebung personenbezogener Daten von Kindern bei der Nutzung von Diensten, die Kindern direkt angeboten werden». Allgemein ist die besondere Schutzbedürftigkeit von Kindern in der digitalen Welt erkennbar ein zentrales Anliegen der DSGVO. Dies kommt auch in weiteren Erwägungsgründen und Regelungen der DSGVO zum Ausdruck. So befasst sich EG 58 mit Grundfragen der Transparenz. Danach sollen die Informationen allgemein präzise, leicht zugänglich und verständlich sowie in klarer und einfacher Sprache abgefasst sein. Bei Kindern wird zusätzlich gefordert, dass Informationen und Hinweise in einer dergestalt klaren und einfachen Sprache erfolgen, dass ein Kind sie verstehen kann. Dieses Anliegen wird materiell in Art. 12 Abs. 1 S. 1 DSGVO – dieser betrifft Fragen der transparenten Information und Kommunikation – mit Bezug auf Kinder auch so umgesetzt. Die Gruppe der Kinder wird auch ausdrücklich bei den Aufgaben der Aufsichtsbehörden (vgl. Art. 57 Abs. 1 lit. b) bzw. bei Verhaltensregeln (vgl. Art. 40 Abs. 2 lit. g) erwähnt.

2.2. Zur Tatbestandsstruktur des Art. 8 DSGVO

Art. 8 DSGVO ist überschrieben mit «Bedingungen für die Einwilligung eines Kindes in Bezug auf Dienste der Informationsgesellschaft». Die tatbestandliche Struktur des Art. 8 DSGVO enthält einige dogmatische Feinheiten, aber auch Problembereiche, die auf den ersten Blick nicht immer gleich sichtbar werden.

2.2.1. Anmerkungen zu einzelnen Tatbestandsmerkmalen

Nicht eindeutig geklärt ist bereits der Begriff des Kindes. Anders als im Vorentwurf¹⁰ fehlt in der nunmehr beschlossenen DSGVO eine formale Definition. Art. 8 DSGVO erwähnt die Altersstufe der 16jährigen und bezieht diese damit erkennbar in die Gruppe der Kinder ein. Dies steht im Gegensatz etwa zum deutschen Jugendschutzgesetz (JuSchG). Gemäß § 1 Abs. 1 Nr. 1 JuSchG sind Kinder Personen, die noch nicht 14 Jahre alt sind. Im vorliegenden Zusammenhang wird daher grds. auch von Minderjährigen oder Jugendlichen gesprochen.

Art. 8 DSGVO gilt nur für die Verarbeitung von personenbezogenen Daten. Damit knüpft Art. 8 an die für das Datenschutzrecht zentrale Begriffsbestimmung in Art. 4 Nr. 1 DSGVO an.¹¹ Personenbezogene Daten sind dabei im Einzelfall von den anonymen Daten abzugrenzen. Diese sind, wie sich aus EG 26 ergibt, nicht Teil des Datenschutzkonzepts der DSGVO.¹² Besonders beachtet werden muss, dass Art. 8 sich ausschließlich auf die Einwilligung nach Art. 6 Abs. 1 UAbs. 1 lit. a DSGVO bezieht. Diese Regelung erfasst daher nicht die übrigen in Art. 6 Abs. 1 UAbs. 1 lit. b – f DSGVO aufgeführten Fallgruppen, die zur Rechtmäßigkeit der Verarbeitung personenbezogener Daten führen. Insbesondere betrifft Art. 8 nicht die Verarbeitungsvorgänge, die zur Erfüllung vorvertraglicher oder vertraglicher Pflichten des Diensteanbieters erforderlich sind (Art. 6 Abs. 1 UAbs. 1 lit. b DSGVO). Dies folgt systematisch auch aus Art. 8 Abs. 3 DSGVO. Danach lässt die Regelung in Art. 8 Abs. 1 das allgemeine Vertragsrecht der Mitgliedstaaten ausdrücklich unberührt.

2.2.2. Dienste der Informationsgesellschaft im Sinne des Art. 8 DSGVO

Wesentliche Bedeutung im Rahmen des Art. 8 DSGVO hat insbesondere das Tatbestandsmerkmal «Dienste der Informationsgesellschaft». Die Begrifflichkeit «Dienst der Informationsgesellschaft» wird ausdrücklich in Art. 4 Nr. 25 DSGVO definiert. Danach handelt es sich um eine Dienstleistung im Sinne des Artikels 1 Nummer 1 Buchstabe b der Richtlinie (EU) 2015/1535 des Europäischen Parlaments und des Rates vom 9. September 2015. Rechtstheoretisch auffallend ist dabei, dass Art. 8 als Norm einer Verordnung durch eine Richtlinie präzisiert wird, die selbst nicht unmittelbar gilt.¹³

¹⁰ Dort wurde gemäß Art. 4 Nr. 18 das Kind als jede Person bis zur Vollendung des 18. Lebensjahres definiert.

¹¹ Vgl. dazu näher ERNST, in: Paal/Pauly (Hrsg.), DS-GVO, Kommentar, 2017, Art. 4, Rn. 3 ff.

¹² Vgl. RICHTER (Fn. 6), § 4, Rn. 101.

¹³ So zu Recht FRENZEL, in: Paal/Pauly (Fn. 11), Art. 8, Rn. 6.

Aus Art. 1 Nr. 1 lit. b der Richtlinie (RL) ergibt sich, dass eine Dienstleistung der Informationsgesellschaft jede in der Regel gegen Entgelt elektronisch im Fernabsatz und auf individuellen Abruf eines Empfängers erbrachte Dienstleistung ist. Anschließend werden in der RL die Ausdrücke «im Fernabsatz erbrachte Dienstleistung», «elektronisch erbrachte Dienstleistung» sowie «auf individuellen Abruf eines Empfängers erbrachte Dienstleistung» näher beschrieben. Sodann enthält Art. 1 den Hinweis auf eine Beispielliste der nicht unter diese Definition fallenden Dienste in Anhang I. Ausweislich Anhang I gilt z.B. die Buchung eines Flugtickets über ein Computernetz, wenn sie in einem Reisebüro in Anwesenheit eines Kunden vorgenommen wird, nicht als ein im Fernabsatz erbrachter Dienst. Nicht elektronisch erbrachte Dienste sind nach der Negativliste in Anhang I etwa eine medizinische oder anwaltliche Beratung per Telefon/Telefax. Fernsehdienste oder Hörfunkdienste werden ausdrücklich nicht als Dienste eingestuft, die auf individuellen Abruf eines Empfängers erbracht werden.

Deutlich wird dabei, dass – wie bisher auch – für einen Dienst der Informationsgesellschaft wesentlich ist, dass der wirtschaftlich tätige Erbringer und der Empfänger der Dienstleistung nicht gleichzeitig physisch an einem Ort sind und dass der Dienst in der Regel gegen Entgelt erbracht wird.¹⁴ Jedenfalls unterfallen der Definition typische Suchmaschinenangebote (z.B. von «Google») oder Content-Angebote (z.B. von «wetter.de»).

2.2.3. Weitere tatbestandliche Probleme

Gem. Art. 8 muss das Angebot «einem Kind direkt» gemacht werden. Dabei ist nicht davon auszugehen, dass sich das Angebot speziell i.S.v. ausschließlich an Minderjährige richtet.¹⁵ Es genügt, dass der Dienst jedenfalls auch einem Kind angeboten wird, sodass es von diesem ohne weiteres genutzt werden kann. Für diese Auslegung sprechen insbesondere auch Schutzzwecküberlegungen. Würde man das Einwilligungserfordernis nach Art. 8 auf gezielte Sonderangebote für Jugendliche beschränken, würde dies den Anwendungsbereich von Art. 8 deutlich reduzieren.

Tatbestandliche Probleme können sich insbesondere auch i.R.d. Art. 8 Abs. 2 DSGVO ergeben. Danach muss der Verantwortliche sich unter Berücksichtigung der verfügbaren Technik vergewissern, dass die Eltern auch tatsächlich zugestimmt haben. Die Grundproblematik ist in der Ausgangslage angelegt. Bei Diensten der Informationsgesellschaft geht es typischerweise um Kommunikationsvorgänge unter Abwesenden.¹⁶ Nicht unrealistisch ist dabei die Gefahr, dass der Jugendliche eine Zustimmung der Eltern nur vorspiegelt.¹⁷ Erforderlich wird daher eine ausdrückliche Kontaktaufnahme mit den Eltern sein. Als Mittel zur Einholung der Einwilligung des Erziehungsberechtigten wird dabei das Double-Opt-In-Verfahren (DOI-Verfahren) genannt.¹⁸ An die vom Jugendlichen bekannt gemachte E-Mail-Adresse der Eltern wird eine E-Mail mit Bestätigungslink gesendet. Dadurch erhalten diese die Möglichkeit, ihre Einwilligung zu erklären. Die erkennbare Schwäche dieses Konzepts ist es, dass nicht sichergestellt werden kann, dass es sich auch tatsächlich um die E-Mail-Adresse der Eltern handelt. Will der Anbieter Sicherheit haben, muss er auf eine andere Art und Weise – z.B. mittels Postident-Verfahren – Kontakt mit den Eltern aufnehmen. Dies würde jedoch in der Sache einen Medienbruch darstellen.¹⁹ Jedenfalls enthält die Regelung des Art. 8 Abs. 2 DSGVO ein erhebliches Risikopotential für die jeweiligen Anbieter von Diensten der Informationsgesellschaft.

¹⁴ Vgl. zum Begriff Dienst der Informationsgesellschaft i.S.d. Art. 12 Abs. 1 der RL 2000/31/EG z.B. EuGH, Urteil vom 15. September 2016, Rs. C-484/14, ECLI:EU:C:2016:689 (McFadden) – NJW 2016, 3503.

¹⁵ Vgl. dazu FRENZEL, in: Paal/Pauly (Fn. 11), Art. 8, Rn. 7.

¹⁶ Dies wird zu Recht von FRENZEL, in: Paal/Pauly (Fn. 11), Art. 8, Rn. 13 betont.

¹⁷ Vgl. zur Gefahr unwahrer Angaben durch den Minderjährigen auch JANDT/ROSSNAGEL (Fn. 8), MMR 2011, 641.

¹⁸ Vgl. dazu im Einzelnen MÖHRKE-SOBOLEWSKI/KLAS (Fn. 9), K&R 2016, 377 bzw. GOLA/SCHULZ, DS-GVO – Neue Vorgaben für den Datenschutz bei Kindern?, ZD 2013, 479.

¹⁹ Dies betonen MÖHRKE-SOBOLEWSKI/KLAS (Fn. 9), K&R 2016, 377.

3. Fragen der Einwilligungsfähigkeit im Rahmen des Art. 8 DSGVO

3.1. Zur Diskussion um die Einwilligungsfähigkeit von Minderjährigen

In den zuvor skizzierten Grenzen des Tatbestandes geht Art. 8 DSGVO davon aus, dass Kinder ab dem vollendeten 16. Lebensjahr eigenständig eine rechtlich wirksame Einwilligung erklären können. Diese Altersgrenze ist in der Sachdiskussion teilweise als realitätsfremd kritisiert worden. Sie werde der typischen Medienkompetenz von Jugendlichen nicht gerecht. Im Zweifel würden 15-Jährige die Eltern nicht erst um Zustimmung bitten, wenn sie sich bei einem Dienst wie Facebook oder Snapchat anmelden wollen. Dass hier Diskussionsbedarf entsteht, ist schon deshalb naheliegend, weil der Vorentwurf dafür noch das vollendete 13. Lebensjahr vorgesehen hatte. Nach Art. 8 Abs. 1 UAbs. 2 DSGVO können die Mitgliedsstaaten auch eine niedrigere Altersgrenze vorsehen, die jedoch nicht unter dem vollendeten 13. Lebensjahr liegen darf. Daher wird hier auch die Frage erörtert, inwieweit die in der Verordnung vorgesehene Altersgrenze von 16 Jahren mit anderen Altersgrenzen im deutschen Rechtssystem wertungsmäßig vereinbar ist und ob die Altersgrenze für eine wirksame Einwilligung herabgesetzt werden sollte. Dabei geht es letztlich auch um Fragen der typisierten Grundrechtsmündigkeit von Minderjährigen und zwar im digitalen Bereich. Dass allgemein auch niedrigere Altersstufen als 16 Jahre bei Grundrechten von Minderjährigen in Betracht kommen können, zeigt z.B. das Gesetz über die religiöse Kindererziehung (KERzG). Gemäß § 5 KERzG kann das Kind bereits ab dem vollendeten 14. Lebensjahr allein über das religiöse Bekenntnis entscheiden.

3.2. Zu den rechtlichen Vorgaben des Art. 8 DSGVO

Ausgangspunkt der weiteren Überlegungen sind zunächst die rechtlichen Vorgaben des Art. 8 DSGVO. Art. 8 geht davon aus, dass Jugendliche unter 16 Jahren der Einwilligung der Eltern bedürfen, also Jugendliche nach dem vollendeten 16. Lebensjahr selbst entscheiden können.

Inhaltlich knüpft Art. 8 an Art. 6 Abs. 1 UAbs. 1 lit. a DSGVO an.²⁰ Die Einwilligung ist dabei eine zentrale Fallgruppe, die neben den übrigen Alternativen des Art. 6 DSGVO (zum Beispiel Vertragserfüllung)²¹ die Verarbeitung personenbezogener Daten rechtfertigt. In der Sache bleibt die Einwilligung ein entscheidender Grundpfeiler des Datenschutzes.²² Konkrete Anforderungen an die Einwilligung lassen sich aus der Begriffsdefinition gemäß Art. 4 Nr. 11 DSGVO sowie aus Art. 7 DSGVO (Bedingungen für die Einwilligung) ableiten.²³ Aus dem festgeschriebenen Gestaltungskorridor in Art. 8 DSGVO (zwischen vollendetem 16. und vollendetem 13. Lebensjahr) ergibt sich zudem die Verpflichtung zu einer typisierten Altersregelung.²⁴ Nach deutschem Recht wurde bei der Frage der Einwilligung nicht auf die Geschäftsfähigkeit abgestellt, sondern auf die individuelle Fähigkeit, die Konsequenzen einer Einwilligung richtig einzuschätzen.²⁵

3.3. Altersgrenzen bei Jugendlichen im deutschen Recht

In Beiträgen, die sich mit Art. 8 DSGVO befassen, wird bereits die Vielfalt von Altersgrenzen bei Jugendlichen im deutschen Recht angesprochen.²⁶ Hingewiesen wurde unter anderem auf § 19 StGB oder § 5 KERzG. Dabei wird für die Frage der Strafmündigkeit bzw. für die freie Entscheidung über das religiöse Bekenntnis an die Altersstufe ab 14 Jahre angeknüpft. Erwähnt wird auch § 36 SGB I. Danach kann ein 15-jähriger eigenverantwortlich Anträge auf Sozialleistungen stellen. Bezug genommen wird teilweise auch auf das zivilrechtliche Deliktsrecht. Wer nicht das 7. Lebensjahr vollendet hat, ist gemäß § 828 Abs. 1 BGB deliktsrechtlich nicht

²⁰ Vgl. dazu auch FRENZEL, in: Paal/Pauly (Fn. 11), Art. 8, Rn. 9.

²¹ Vgl. dazu näher NEBEL, in: Roßnagel (Fn. 6), § 3, Rn. 72.

²² So ALBRECHT, Das neue EU-Datenschutzrecht – von der Richtlinie zur Verordnung, CR 2016, 91.

²³ Vgl. zu den damit verbundenen Fragen PILTZ, Die Datenschutz-Grundverordnung, K&R 2016, 564.

²⁴ So im Ergebnis auch NEBEL, in: Roßnagel (Fn. 6), § 3, Rn. 98.

²⁵ Vgl. MÖHRKE-SOBOLEWSKI/KLAS (Fn. 9), K&R 2016, 374.

²⁶ Vgl. dazu MÖHRKE-SOBOLEWSKI/KLAS (Fn. 9), K&R 2016, 376 bzw. GOLA/SCHULZ (Fn. 18), ZD 2013, 475/476.

verantwortlich. Bei Unfällen mit Kraftfahrzeugen wird die Haftungsgrenze gemäß § 828 Abs. 2 BGB auf 10 Jahre erhöht.

Bereits diese wenigen Beispiele zeigen, dass auf nationaler Ebene²⁷ eine durchgängige Verantwortlichkeitsstufe für Minderjährige nicht erkennbar ist. Sachlich hilfreich erscheint es, insbesondere auch das JuSchG mit einzubeziehen. Dieses enthält eine Reihe von Normen für ein abgestuftes Schutzkonzept für Kinder und Jugendliche. So wird deutlich, dass Kinder für eine Vielzahl von Aktivitäten die Zustimmung der Eltern benötigen. Dabei sind Kinder Personen, die noch nicht 14 Jahre alt sind. Ab dem Alter von 16 Jahren haben Jugendliche dagegen (z.B. bei Gaststättenbesuchen oder Tanzveranstaltungen) deutlich größeren Freiraum. Dies spricht unter allgemeinen Systemgesichtspunkten zunächst dafür, im Rahmen des Art. 8 DSGVO die Gruppe der 14jährigen und die Gruppe der 16jährigen als realistische Alternative in die engere Wahl zu ziehen.

3.4. Mögliche Entscheidungskriterien im Rahmen des Art. 8 DSGVO

Für die endgültige Festlegung der angemessenen Altersstufe sollen im Folgenden weitere potentielle Entscheidungskriterien näher erörtert werden.

3.4.1. Tendenzaussagen durch die DSGVO selbst?

Der Vorentwurf der DSGVO hatte noch eine Altersstufe von 13 Jahren im Rahmen des Art. 8 festgeschrieben. Nunmehr sieht Art. 8 Abs. 1 die Altersstufe ab 16 Jahren als Regelfall vor. Dies könnte für eine Tendenz des Verordnungsgebers sprechen, die Altersstufe möglichst hoch anzusetzen. Aus den Hinweisen von Albrecht zum neuen EU-Datenschutz ergibt sich jedoch eher das Gegenteil.²⁸ Die jetzige Ausgestaltung des Art. 8 DSGVO hat einen ausgeprägten Kompromisscharakter. EU-Parlament und EU-Kommission auf der einen und Mitgliedsstaaten auf der anderen Seite konnten sich in der Sache nicht einigen. Mit der jetzigen Regelung sollte im Ergebnis verhindert werden, dass es – so Albrecht – auf nationaler Ebene «vollkommen unrealistische Altersgrenzen» zwischen 16 und 18 Jahren geben würde. Aus der Erhöhung der Altersstufe im Rahmen des Art. 8 DSGVO lassen sich daher keine Tendenzaussagen ableiten.

3.4.2. Zur Anknüpfung an Gesichtspunkte der Geschäftsfähigkeit

Nahe liegt ein Bezug zu Fragen der Geschäftsfähigkeit nach dem BGB. Zwar wurde im deutschen Recht viel Wert auf den Unterschied zwischen «Grundrechtsfähigkeit des Minderjährigen» und Geschäftsfähigkeit gelegt.²⁹ Zu Recht wird aber betont, dass die Öffnungsklausel des Art. 8 Abs. 1 UAbs. 2 DSGVO gerade auch dazu dient, einen Gleichlauf mit den nationalen Regelungen über die Geschäftsfähigkeit herstellen zu können. Zudem hat die Ausgangssituation bei Art. 8 – Inanspruchnahme eines Dienstes gegen Einwilligung und Zugang zu persönlichen Daten – jedenfalls rechtsgeschäftsähnlichen Charakter.³⁰

Teilweise wird in diesem Zusammenhang betont, dass die gesetzliche Wertung zur Geschäftsfähigkeit im BGB an das 7. Lebensjahr anknüpft, während die DSGVO den Schutz bis mindestens zum 13. Lebensjahr ausdehnt.³¹ Dies ist formal richtig, kann aber eine Tendenzaussage für eine möglichst niedrige Altersstufe im Rahmen des Art. 8 DSGVO nicht begründen. Zwar beginnt die Geschäftsfähigkeit mit dem 7. Lebensjahr.³² Bei Art. 8 DSGVO geht es aber darum, ab wann Minderjährige eigenständig, also ohne Mitwirkung der Eltern, entscheiden können. Ein eigenständiges rechtsgeschäftliches Handeln ist Minderjährigen aber z.B. gemäß § 107 BGB nur dann erlaubt, wenn das Geschäft lediglich rechtliche Vorteile bietet oder es sich zumindest nur

²⁷ Dies gilt für Deutschland.

²⁸ Vgl. dazu und zum Folgenden ALBRECHT (Fn. 22), CR 2016, 97.

²⁹ Vgl. zum Beispiel GOLA/SCHOMERUS (Fn. 3), § 4a, Rn. 25 m.w.N.

³⁰ So zu Recht FRENZEL, in: Paal/Pauly (Fn. 11), Art. 8, Rn. 12.

³¹ So MÖHRKE-SOBOLEWSKI/KLAS (Fn. 9), K&R 2016, 376.

³² Umkehrschluss aus § 104 Nr. 1 BGB und § 106 BGB.

um ein neutrales Geschäft handelt.³³ Bei Art. 8 DSGVO «bezahlt» aber der Minderjährige mit seinen persönlichen Daten. Auch eine Regelung wie § 110 BGB (Taschengeldparagraph) lässt sich argumentativ nicht auf Art. 8 DSGVO übertragen. Bei § 110 BGB handelt es sich um einen Fall konkludenter Einwilligung des gesetzlichen Vertreters.³⁴ Danach kann ein Minderjähriger eigenständig einen Vertrag abschließen, wenn er die vertraglichen Leistungen mit Mitteln bewirkt, die ihm ausdrücklich zur freien Verfügung überlassen wurden. Diese Begrenzung der Risiken auf den Umfang der überlassenen Mittel hat im Rahmen des Art. 8 DSGVO keine Entsprechung. Normen wie §§ 112, 113 BGB, die die Erweiterung der Geschäftsfähigkeit bei Erwerbsgeschäften oder Arbeitsverhältnissen betreffen, sind nicht verallgemeinerungsfähige Sonderregelungen.

3.4.3. Zur gewachsenen digitalen Erfahrung von Jugendlichen

Für Jugendliche ist Technik und Internet heutzutage eine Selbstverständlichkeit. In diesem Zusammenhang kann auf die JIM-Studie von 2015³⁵ zum Medienumgang 12- bis 19-Jähriger verwiesen werden. Danach besitzen 92% der Jugendlichen ein Smartphone. Schon bei den 12- und 13-Jährigen sind es 86%. Dies ist zunächst ein starkes Argument für eine möglichst niedrige Eingangsstufe. Kinder sollen in der digitalen Welt geschützt werden. Es ist aber auch ihre Teilhabe an dieser Welt zu fördern.³⁶ Andererseits hat gerade die DSGVO den Grundsatz betont, dass Jugendliche sich der Risiken bei der Verarbeitung personenbezogener Daten möglicherweise weniger bewusst sind (EG 38 DSGVO).

3.4.4. Zur Bedeutung des Elternrechts

Insbesondere ist auch zu berücksichtigen, dass eine selbstständige Einwilligungsmöglichkeit im Rahmen des Art. 8 DSGVO gleichzeitig bedeutet, dass die Eltern damit zwangsweise aus der jeweiligen rechtlichen Verantwortung ausgeschlossen werden. Dies zeigt, dass die Grundrechtsmündigkeit eines Minderjährigen mit Blick auf die elterlichen Verpflichtungen gemäß Art. 6 Abs. 2 GG eingeordnet werden muss.³⁷ Danach sind Pflege und Erziehung der Kinder das natürliche Recht der Eltern und die zuvörderst ihnen obliegende Pflicht. Im Rahmen des Art 6 Abs. 2 GG ist anerkannt, dass mit wachsendem Alter und damit wachsender Grundrechtsmündigkeit die Eltern nicht grundlos eine Einwilligung verweigern dürfen. Die hier bevorzugte späte Entlassung in die digitale Selbstständigkeit (ab dem 16. Lebensjahr) hat den Vorteil, dass damit der potentielle Zugriff und die Verantwortlichkeit der Eltern vorher bestehen bleibt. Dies erscheint gerade bei Unternehmensstrategien, die sich um junge Menschen als Kunden von morgen verstärkt bemühen,³⁸ nicht unwesentlich.

3.4.5. Zum Aspekt der Ausweispflicht

Dieses Konzept – selbstständige Einwilligung erst ab dem 16. Lebensjahr – hat zudem einen nicht zu unterschätzenden Vorteil für die beteiligten Unternehmen. Verstöße gegen die Pflichten aus Art. 8 sind in Art. 83 Abs. 4 lit. a DSGVO sanktioniert³⁹ und können zu hohen Geldbußen führen. Ab 16 Jahre ist aber jeder Deutsche grds. gem. § 1 des Gesetzes über Personalausweise und den elektronischen Identitätsnachweis (Personalausweisgesetz – PAuswG) verpflichtet, einen Personalausweis zu besitzen. Die Einbeziehung des Personalausweises bei der Altersverifikation könnte daher die Risiken für die Wirtschaft bei der Feststellung der notwendigen Einwilligung mildern.⁴⁰ Im Anwenderhandbuch des Bundesministeriums des Innern zum Ein-

³³ Vgl. dazu ELLENBERGER, in: Palandt (Hrsg.), Kommentar BGB, 76. Aufl. 2017, § 107, Rn. 7.

³⁴ ELLENBERGER, in: Palandt (Fn. 33), § 110, Rn. 1.

³⁵ Vgl. dazu und zum Folgenden JIM-Studie 2015 (Fn. 2), S. 46.

³⁶ Vgl. Art. 19 der Charta der digitalen Grundrechte der Europäischen Union, ausgearbeitet von einer Gruppe von Bürgern, <https://digitalcharta.eu/> zuletzt abgerufen am 03.01.2017.

³⁷ Zu diesem Aspekt auch FRENZEL, in: Paal/Pauly (Fn. 11), Art. 8, Rn. 2.

³⁸ Vgl. dazu näher MÖHRKE-SOBOLEWSKI/KLAS (Fn. 9), K&R 2016, 373.

³⁹ Die allgemeinen Verstöße gegen die Bedingungen der Einwilligung werden dagegen in Art. 83 Abs. 5 lit. a sanktioniert – vgl. dazu FRENZEL, in: Paal/Pauly (Fn. 11), Art. 83, Rn. 22.

⁴⁰ Vgl. auch JANDT/ROSSNAGEL (Fn. 8), MMR 2011, 642, dort Fn. 47 zur Bedeutung eines Personalausweises bei der Altersverifikation.

satz des neuen Bundespersonalausweises wird ausdrücklich auf den Einsatz des Personalausweises bei Fragen der Altersüberprüfung hingewiesen.⁴¹

3.4.6. Die gewählte Altersstufe im Lichte der bisherigen bundesdeutschen Rechtsprechung

Die für Art. 8 DSGVO vorgeschlagene Altersstufe würde sich auch im Rahmen der bisherigen Wertung der nationalen Gerichte halten. Insbesondere im sogenannten Lauterkeitsrecht⁴², etwa bei der Ausnutzung geschäftlicher Unerfahrenheit gemäß § 4 Nr. 2 Gesetz gegen den unlauteren Wettbewerb (UWG) in der Fassung ab dem 4. August 2009,⁴³ hatte sich die Rechtsprechung mit Fragen der Einwilligungsfähigkeit von Minderjährigen befassen müssen. So hat der BGH in seiner Entscheidung vom 22. Januar 2014 (Nordjob-Messe) ausgeführt, dass auch für Jugendliche zwischen 15 und 17 Jahren die mit der Preisgabe persönlicher Daten und der Einwilligungserklärung verbundenen Nachteile nur schwer erkennbar sind.⁴⁴ Auch aus der zunehmenden Erfahrung mit digitalen Medien – so der BGH – lassen sich nicht ohne weiteres Rückschlüsse auf die Erkennbarkeit der Folgen einer Preisgabe von personenbezogenen Daten ziehen.

4. Zusammenfassung und Ausblick

Nach dem hiesigen Vorschlag soll die Altersgrenze für die Einwilligungsfähigkeit gemäß Art. 8 DSGVO für das deutsche Recht auf 16 Jahre festgesetzt werden. In der Sache bedeutet dies, dass der nationale Gesetzgeber nicht tätig werden muss. Die nationale Regelungsmöglichkeit im Rahmen des Art. 8 DSGVO hat zwei strukturelle Nachteile. Zum einen gilt die hier vorgeschlagene Altersstufe nur im Rahmen des Art. 8 DSGVO, also nur bei Diensten der Informationsgesellschaft. Bei nicht digitalen Angeboten bleibt es bei der bisherigen Regelung der Einwilligungsfähigkeit im Einzelfall. Zum anderen bedeutet die Möglichkeit nationaler Regelungen allgemein, dass die Normen in den einzelnen Ländern unterschiedlich ausfallen können. Damit wird das Ziel eines einheitlichen europäischen Datenschutzkonzeptes nicht erreicht. Insbesondere müssen grenzüberschreitend arbeitende Unternehmen sich im Rahmen des Art. 8 DSGVO auf unterschiedliche nationale Regelungen einstellen.

Jedenfalls ist der Umstand, dass Art. 8 DSGVO überhaupt eine feste Altersgrenze bei Minderjährigen vorsieht, als ein deutlicher methodischer und inhaltlicher Vorteil gegenüber der bisherigen bundesdeutschen Regelung einzustufen. Die bloße Orientierung an der Einsichtsfähigkeit im Einzelfall erscheint gerade bei Massenphänomenen wie der Internetnutzung vom System her wenig praktikabel.

⁴¹ BUNDESMINISTERIUM DES INNERN, Der Personalausweis – Anwenderhandbuch für Wirtschaft und Verwaltung, Stand: Dezember 2010, S. 33/34.

⁴² Vgl. dazu KLUTE, Die aktuellen Entwicklungen im Lauterkeitsrecht, NJW 2015, 450 ff.

⁴³ Vgl. nunmehr § 4a Abs. 2 S. 2 UWG in der Fassung vom 2. Dezember 2015.

⁴⁴ Vgl. dazu und zum Folgenden BGH, Urteil vom 22. Januar 2014, I ZR 218/12, Rn. 35, 37.