forum <privatheit>
selbstbestimmtes_leben_in_der_digitalen_welt

FORUM PRIVATHEIT UND SELBSTBESTIMMTES LEBEN IN DER DIGITALEN WELT

White Paper

EINWILLIGUNG

Möglichkeiten und Fallstricke aus der Konsumentenperspektive

White Paper

EINWILLIGUNG

Möglichkeiten und Fallstricke aus der Konsumentenperspektive

Autorinnen und Autoren:
Alexander Roßnagel[1], Tamer Bile[1], Maxi Nebel[1], Christian Geminn[1], Murat Karaboga[2], Frank Ebbers[2], Benjamin Bremert[3], Ingrid Stapf[4], Mena Teebken[5], Verena Thürmel[5], Carsten Ochs[6], Markus Uhlmann[6], Nicole Krämer[7], Yannic Meier[7], Michael Kreutzer[8], Linda Schreiber[8], Hervais Simo[8]

(1) Universität Kassel, Projektgruppe verfassungsverträgliche Technikgestaltung (provet)
(2) Fraunhofer-Institut für System- und Innovationsforschung ISI, Karlsruhe
(3) Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein (ULD), Kiel
(4) Universität Tübingen, Internationales Zentrum für Ethik in den Wissenschaften (IZEW)
(5) Universität München, Institut für Wirtschaftsinformatik und Neue Medien (WIM)
(6) Universität Kassel, Fachgebiet Soziologische Theorie
(7) Universität Duisburg-Essen, Sozialpsychologie
(8) Fraunhofer-Institut für Sichere Informationstechnologie SIT, Darmstadt

Herausgeber:
Michael Friedewald, Regina Ammicht Quinn, Marit Hansen, Jessica Heesen, Thomas Hess, Nicole Krämer, Jörn Lamla, Christian Matt, Alexander Roßnagel, Michael Waidner

Inhalt

1
Einleitung

Ein verbreiteter Mythos in der Einführungsphase der Datenschutz-Grundverordnung war die Annahme, dass nun für jede Datenverarbeitung eine Einwilligung eingeholt werden müsse. Sehr viele datenverarbeitende Stellen sahen sich dazu veranlasst, von jeder betroffenen Person eine Einwilligung einzuholen, da sie glaubten, nur auf diese Weise rechtssicher personenbezogene Daten verarbeiten zu können. Alternative Verarbeitungsgrundlagen und auch bereits bestehende Einwilligungserklärungen schienen nicht genügend Sicherheit zu bieten – es drohten vermeintlich exorbitante Sanktionen durch die neuen Bußgeldbestimmungen der Datenschutz-Grundverordnung. Resultat war eine regelrechte Schwemme an Aufforderungen, in Datenverarbeitungen einzuwilligen. Dies führte nicht nur zu einer Einwilligungsmüdigkeit bei den Adressaten, sondern erwies sich auch als tiefgreifendes Ärgernis bei allen Beteiligten, wodurch das öffentliche Ansehen der Datenschutz-Grundverordnung und allgemein des Datenschutzes mitunter nachhaltig beschädigt wurde. Diese massenhafte Belästigung wurde nicht der Unwissenheit oder Unsicherheit der datenverarbeitenden Stellen zugerechnet, die zwischen dem Inkrafttreten der Verordnung und ihrem Geltungsbeginn zwei Jahre Zeit hatten, sich in die Vorgaben einzuarbeiten, sondern als überflüssige bürokratische Anforderung der Datenschutz-Grundverordnung angesehen.

Die Einwilligung ist zwar der vornehmste Ausdruck der informationellen Selbstbestimmung, aber nicht die einzige Möglichkeit, die Verarbeitung personenbezogener Daten zu legitimieren. Die Datenschutz-Grundverordnung regelt die Einwilligung in Art. 6 Abs. 1 UAbs. 1 lit. a DSGVO als eine von sechs möglichen Grundlagen für eine rechtmäßige Verarbeitung von personenbezogenen Daten. Nach Art. 6 Abs. 1 UAbs. 1 lit. a DSGVO ist eine Verarbeitung rechtmäßig, wenn die betroffene Person ihre Einwilligung zu der Verarbeitung der sie betreffenden personenbezogenen Daten für einen oder mehrere bestimmte Zwecke gegeben hat. Als Einwilligung gilt nach Art. 4 Nr. 11 DSGVO „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“. Die Einwilligung führt in der Praxis jedoch zu strukturellen Nachteilen. Aus Sicht der datenverarbeitenden Stelle verspricht die Einwilligung durch ihre jederzeitige Widerrufbarkeit und den (zumindest auf dem Papier) strengen Wirksamkeitsvoraussetzungen im Vergleich zu anderen Tatbeständen verhältnismäßig wenig Planungssicherheit. Hier kommen vor allem für private datenverarbeitende Stellen die Erfüllung eines Vertrags gemäß Art. 6 Abs. 1 UAbs. 1 lit. b DSGVO oder überwiegende berechtigte Interessen gemäß Art. 6 Abs. 1 UAbs. 1 lit. f DSGVO oder für öffentliche Stellen die Wahrnehmung einer Aufgabe im öffentlichen Interesse oder die Ausübung öffentlicher Gewalt gemäß Art. 6 Abs. 1 UAbs. 1 lit. e DSGVO in Betracht. Aus Sicht der betroffenen Person ist die Einwilligung anfällig für Machtungleichgewichte. Schon lange vor dem Inkrafttreten der Datenschutz-Grundverordnung haben überlange, komplizierte und häufig unverständliche Einwilligungserklärungen die ursprüngliche Funktion der Einwilligung als Instrument einer selbstbestimmten Entscheidung ad absurdum geführt.[1] Die Folge war und ist, dass vorformulierte Einwilligungserklärungen ungelesen bestätigt werden und Einwilligungen als Rechtfertigungstatbestand damit letztlich zur Farce werden.

Der Unionsgesetzgeber hat die Schwächen der Einwilligung in der Praxis erkannt. Er hat an der Erkenntnis festgehalten, dass jede Verarbeitung personenbezogener Daten ein Eingriff in das Grundrecht auf Datenschutz ist und nach dem Vorbehalt des Gesetzes für solche Eingriffe einer gesetzlichen Legitimation bedarf.[2] Daher hat er die

Zulässigkeitstatbestände aus der Datenschutz-Richtlinie in Art. 6 Abs. 1 DSGVO beibehalten und die Einwilligung an die erste Stelle gesetzt. Er hat sich dabei zum Ziel gesetzt, die Einwilligung durch die Datenschutz-Grundverordnung zu stärken. Aus diesem Grund enthält sie im Vergleich zur Datenschutz-Richtlinie eine deutlich schärfere Definition, weil sie eine eindeutige bestätigende Handlung fordert und eine beiläufige oder implizite Handlung ausschließt (Erwägungsgrund 32 DSGVO). Außerdem werden die Informiertheit und Freiwilligkeit als Voraussetzungen stärker betont. Die Datenschutz-Richtlinie war an dieser Stelle keineswegs so eindeutig.

Ob dieses Ziel der Selbstbestimmung durch Einwilligung in der Praxis erreicht werden kann, untersucht das vorliegende White Paper in einer interdisziplinären Zusammenschau. Zunächst werden das Konzept der Einwilligung sowie die gesetzlichen Regelungen zur datenschutzrechtlichen Einwilligung beleuchtet. Im Anschluss daran wird dargestellt, welche Bedeutung die Einwilligung in der Praxis tatsächlich hat. Anschließend stellt das White Paper die Defizite der Einwilligung in der Praxis dar und schließt mit regulatorischen und technischen Handlungsempfehlungen, um sie als Instrument der Selbstbestimmung weiter zu stärken.

2
Konzept der Einwilligung

Im deutschen und im europäischen Datenschutzrecht wurde die Einwilligung von Anfang an als eine mögliche Erlaubnis der betroffenen Person neben den gesetzlichen Erlaubnissen gesehen. So sah das erste Bundesdatenschutzgesetz von 1977 die Einwilligung als eine Möglichkeit der zulässigen Verarbeitung personenbezogener Daten vor: „Die Verarbeitung personenbezogener Daten, die von diesem Gesetz geschützt werden, ist in jeder ihrer § 1 Abs. 1 genannten Phasen nur zulässig, wenn dieses Gesetz oder eine andere Rechtsvorschrift sie erlaubt oder der Betroffene eingewilligt hat" (§ 3 BDSG 1977). Inhaltlich erlaubte Art. 7 lit. a EG-DSRL 95/46 in gleicher Weise die Datenverarbeitung auf der Grundlage einer Einwilligung. Das Konzept der Einwilligung diente bereits zu Beginn ihrer Karriere als eine Art „Auffangbecken", um Datenverarbeitungen rechtlich abzusichern, die über die gesetzlichen Erlaubnistatbestände nicht legitimiert werden konnten. Bereits damals wurde das Konzept dafür kritisiert, den gesetzlich zulässigen Rahmen für die Verarbeitung personenbezogener Daten zu weit auszudehnen.

Durch die Möglichkeit der Einwilligung ist das Datenschutzrecht stark individualistisch ausgerichtet. Es vertraut darauf, dass Transparenz und Eigenverantwortung für den Schutz der Grundrechte ausreichend sind: Der Datenverarbeiter muss die betroffene Person über die Datenverarbeitung informieren und diese kann dann entscheiden, ob sie in die Datenverarbeitung einwilligt. Für die Einwilligung unterstellt das Datenschutzrecht, dass die Grundrechte auf Datenschutz (Art. 7 und 8 GRCh) und informationelle Selbstbestimmung (Art. 2 Abs. 1 und Art. 1 Abs. 1 GG) gewahrt werden können, indem gleichberechtigte Partner die Zwecke und Bedingungen der Datenverarbeitung aushandeln.

Für die Einwilligung setzt das Recht die Entscheidungsautonomie der betroffenen Person voraus, die als freies verantwortliches Individuum unter der Bedingung der Entscheidungsfreiheit und voller Information für sich entscheiden kann, ob es einer Datenverarbeitung zustimmt. Dem Konzept der Einwilligung liegt die sozialhistorisch gewachsene Vorstellung zugrunde, dass soziale Akteure jedenfalls prinzipiell bei ausreichender Informiertheit und Abwesenheit externer Zwänge in der Lage und der Pflicht seien, autonom über die Umstände ihres eigenen Lebens zu entscheiden. „Autonom" sind die Entscheidungen dann, wenn das eigene Handeln mit dem eigenen Wollen und Wünschen in Übereinstimmung ist, und wenn es möglich ist, sich mit eigenem Wollen und Wünschen zu identifizieren.[3] Dies kann dann erfolgen, wenn Personen Gründe und Motive ihres Handelns zumindest bei Bedarf offenlegen und in Übereinstimmung mit ihrer Entscheidung bringen können. In Bezug auf die Einwilligung hieße das: Person A willigt in die vorgenommenen Datenverarbeitungen aus den Gründen X, Y, und Z bewusst und selbstbestimmt ein.

Aus rechtlicher Sicht stellt eine Datenverarbeitung, die auf Grundlage einer informierten Einwilligung erfolgt, keinen Eingriff in die Grundrechte der betroffenen Personen dar, weil die informationelle Selbstbestimmung nicht beeinträchtigt sein kann, wenn die betroffene Person über die Datenverarbeitung selbst bestimmt hat. Das Konzept der Einwilligung steht für die (wirtschaftliche) Handlungsfreiheit und schließt damit das Recht - und die Verantwortung - ein, selbst über die Verwendung der eigenen Daten zu bestimmen. Insbesondere in Folge des Volkszählungsurteils des Bundesverfassungsgerichts aus dem Jahr 1983,[4] mit dem das Grundrecht auf „informationelle Selbstbestimmung" Eingang in das Datenschutzrecht fand, avancierte die Einwilligung zum genuinen Ausdruck eben jener informationellen Selbstbestimmung, die überdies auch die Gewährleistung der Handlungs- und Mitwirkungsfähigkeit des Einzelnen zum Ziel hatte. Die Einwilligung soll als

ausreichende Grundlage der Verarbeitung auch sehr umfangreicher und sehr persönlichkeitsbezogener Daten gelten.

Dieses Konzept einer die Datenverarbeitung rechtfertigenden Einwilligung hat vielfältige Voraussetzungen, deren Vorliegen nicht einfach unterstellt werden kann, und sie verursacht Wirkungen, für die eine Rechtfertigungswirkung hinterfragt werden muss. Daher erfährt dieses Konzept in Auseinandersetzung mit den Bedingungen der sozialen Wirklichkeit vielfache Modifikationen.

Aus vielen Gründen können ausreichende Informationen über die Datenverarbeitung und notwendiges Wissen über die Folgen einer Datenverarbeitung nicht unterstellt werden. Aus psychologischer Sicht ist zu berücksichtigen, dass Personen in den seltensten Fällen über alle nötigen Informationen verfügen, um Vor- und Nachteile einer Einwilligung in ein angemessenes Verhältnis zu setzen. Forschung im Rahmen zum Beispiel des Privacy Calculus[5] zeigen, dass viele Personen zwar eine Balance zwischen den Vor- und Nachteilen der Preisgabe von Daten herzustellen versuchen, dass aber oft der unmittelbare Belohnungswert, der auf die Einwilligung folgt (im Sinne des Zugangs zu gewünschten Online-Services) salienter ist als die potenziellen Risiken. Somit stellt die Einwilligung psychologisch nur ein Hindernis auf dem Weg zur Gratifikation dar und es besteht kein wirkliches Interesse, die Zielsetzungen der Datenverarbeitung zu verstehen. Allerdings zeigen Studien, dass höheres Wissen über potenzielle negative Folgen mit einer umsichtigeren Datenpreisgabe einhergeht. Bei mangelnder Informiertheit scheinen dagegen fast ausschließlich Gratifikationen das Verhalten zu beeinflussen.[6]

Eine weitere Grenze des Einwilligungskonzeptes bildet die ungleiche Verteilung von digitalen Fähigkeiten und digitalem Wissen, auch Medienkompetenz genannt. Hier konnten empirische Untersuchungen[7] zeigen, dass sozioökonomische Faktoren wie Bildung oder Alter mit dem Ausmaß an Medienkompetenz einhergehen. Personen aus sozioökonomisch schlechter gestellten Gesellschaftsschichten haben häufig einen geringeren Zugang zu Informations- und Kommunikationstechnologien und somit meist auch eine geringere Medienkompetenz. Noch zentraler ist die generell anzunehmende Wissenskluft, die sich darauf bezieht, dass sozioökonomisch schlechter gestellte sowie weniger formal gebildete Gruppen bei steigender Verfügbarkeit von Informationen überproportional weniger Wissenszuwachs zu verzeichnen haben als gebildetere und sozioökonomisch besser gestellte Gruppen. Dies gilt auch für Wissen im Zusammenhang mit Datenschutz und Datenökonomie. Für das Konzept der Einwilligung bedeutet dies, dass nicht alle Personen dieselben Voraussetzungen haben, wenn sie vor die Entscheidung gestellt werden, in die Verarbeitung der eigenen Daten einzuwilligen. Manche Personen(gruppen) können bestimmte Risiken oder Vorteile besser abschätzen, wohingegen andere Personen(gruppen) selbst mit hohem Aufwand, sich zu informieren, bestimmte Vorgänge nicht nachvollziehen können, da ihnen beispielsweise nötiges Vorwissen fehlt. Weitere relevante Faktoren könnten darüber hinaus fehlende kognitive Fähigkeiten oder Sprachbarrieren sein. Vor diesem Hintergrund werden durch das Einwilligungskonzept manche Personen von vornherein benachteiligt, da das Konzept der Einwilligung nicht zwischen unterschiedlichen Personengruppen unterscheidet.

Ähnlich kann es aus vielen Gründen auch an den Voraussetzungen einer ausreichenden Entscheidungsautonomie fehlen. So ist es auf Grund der in den vergangenen Jahrzehnten exponentiell angestiegenen Verarbeitung personenbezogener Daten und des hieraus resultierenden gewachsenen Macht- und Wissensgefälles zwischen Anbietern und Nutzern von digitalen Kommunikationsdiensten und sozialen Zwängen zur Nutzung bestimmter Dienste höchst fragwürdig, ob bei vielen betroffenen Personen überhaupt von einer Entscheidungsautonomie die Rede sein kann.

Insbesondere mit Blick auf Heranwachsende stellt sich die Frage, was die Entscheidungsautonomie von Personen jeweils voraussetzt sowie wie diese im Altersverlauf einzuordnen ist und auch ermöglicht werden kann.[8] Gleichzeitig legt der

Blick auf vulnerablere gesellschaftliche Gruppen (wie Kinder, Menschen mit Behinderungen oder auch ältere Menschen) nahe, dass ein alleiniger Rückgriff auf Autonomie der betroffenen Personen problematisiert werden kann. Vielmehr sollte die Verständlichkeit und Nachvollziehbarkeit des Umgangs personenbezogener Daten gewährleistet sein, welche dann eine informierte Entscheidung zugrunde legen kann. Folglich kommt es auf eine Art „Barrierefreiheit" der gesetzlichen Instrumente zum Datenschutz an.

Weiter stellt sich grundsätzlich die Frage, inwieweit die idealtypische Vorstellung autonomen Entscheidens dem alltäglichen Vollzug praktischen Handelns wenigstens prinzipiell entspricht. Tagtägliche Handlungsvollzüge verlaufen typischerweise durch halbbewusstes Abspulen von Routinen. Die Einwilligung in digitale Angebote kann durchaus Teil solcher Routinen werden, so etwa beim Akzeptieren von Cookies oder anderen Tracking-Techniken,[9] bei sehr regelmäßigem App-Download oder stark von der Peer Group forcierter Nutzung von Social Networks.

Grenzen müssen dem Konzept der Einwilligung auch hinsichtlich ihrer Folgen gezogen werden: Ihr müssen Grenzen gesetzt werden, wenn sie die Selbstbestimmung selbst in Frage stellt. § 6 BDSG a. F. sah zum Beispiel vor, dass eine Einwilligung in den Ausschluss oder die Beschränkung bestimmter Betroffenenrechte unwirksam war. Die Datenschutz-Grundverordnung enthält keine entsprechende explizite Regel, allerdings sind die Betroffenenrechte der Verordnung gemeinhin als nicht abdingbar formuliert.[10] Zudem sieht sie Einschränkungen und Abweichungen von den Betroffenenrechten nur im Rahmen von Rechtsvorschriften nach Art. 23 DSGVO vor. Dieser erwähnt die Einwilligung nicht, sodass zugunsten des Schutzes der betroffenen Person davon auszugehen ist, dass hier auf diese Rechte nicht verzichtet werden kann.[11]

Berücksichtigt man diese empirischen Einwände gegen eine Einwilligung und ihre Wirkung, kann die dem Konzept der Einwilligung zugrunde gelegte Vorstellung von Handlungsautonomie immer noch im Sinne einer wünschenswerten, normativen Idealfigur verstanden werden: Akteure sollen zumindest im Prinzip in die Lage versetzt werden, Entscheidungen an bewussten und formulierbaren Gründen auszurichten, selbst wenn ihnen in der Praxis des Entscheidungsvollzugs nicht ständig solche Gründe bewusst sind oder sie diese nicht jedes Mal explizit machen. Die Einwilligung soll so gestaltet sein, dass sie möglichst darauf hinwirkt, informierte, bewusste Handlungsträger hervorzubringen, die selbstbestimmt Gründe für ihre Entscheidungen angeben und so Verantwortung für ihre Lebensumstände übernehmen können. Autonome Akteure werden nach dieser Modifikation nicht als ontologische Voraussetzung, sondern normatives Idealziel verstanden. Gewährleistet werden soll die grundsätzliche Möglichkeit, sich ausreichend zu informieren und autonom und bewusst zu entscheiden. Die Grenzen der Einwilligung liegen dann dort, wo Akteure aus prinzipiellen Gründen nicht hinreichend informiert sein können (kognitive Grenzen), nicht selbstbestimmt agieren können (äußere Zwänge) oder denen – aus welchen Gründen auch immer – nicht die Verantwortung für ihre Lebensumstände zugemutet werden kann. Die Grenzen der Einwilligung werden immer dann sichtbar, wenn das Konzept als nicht-intendierte Nebenfolge der Praxis in eine andere Richtung, als in die Hervorbringung des normativ angestrebten Akteurstyps wirkt. Grenzen sind also auch dann erreicht, wenn die (Nicht-)Einwilligung nicht folgenlos bleibt, beispielweise wenn Informationen über Akteure per Inferenz gewonnen werden können oder wenn die Datenverarbeitung auch dann stattfindet, wenn die geforderte Einwilligung bewusst verweigert wird.[12] Hier zeigt sich, dass auch dann, wenn Rahmenbindungen für autonome Entscheidungen idealtypisch unterstellt werden können, die Autonomie von Personen angesichts von inferenzbasierten Daten-Analysen gefährdet sein kann.

3
Regelungen zur datenschutzrechtlichen Einwilligung

Im Gegensatz zur Datenschutz-Richtlinie ist die Einwilligung in der Datenschutz-Grundverordnung vergleichsweise umfangreich geregelt:

3.1 Voraussetzungen einer wirksamen Einwilligung

Art. 4 Nr. 11 DSGVO enthält nicht nur eine Definition der Einwilligung, sondern auch eine Auflistung der Anforderungen an eine wirksame Einwilligung. Danach muss die Einwilligung nicht nur eine Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung sein, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist. Sie muss daneben auch:

- auf einer ausreichenden Informationsgrundlage über die Datenverarbeitung und
- freiwillig erteilt worden sein sowie
- die Datenverarbeitung, auf die sie sich bezieht, ausreichend bestimmt beschreiben.

Sie erfordert keine bestimmte Form wie zuvor in Deutschland die Schriftform, sondern muss lediglich unmissverständlich den bestimmten Datenverarbeitungsvorgang erlauben. Es ist unzulässig anzunehmen, dass eine Einwilligung stillschweigend oder mutmaßlich erfolgt sei.[13] Eine konkludente Einwilligung durch schlüssiges Verhalten darf nur dann angenommen werden, wenn eine einwilligende Erklärung unmissverständlich und ausreichend bestimmt erfolgt ist. Ob diese Voraussetzungen erfüllt sind, muss der Verantwortliche nach Art. 7 Abs. 1 DSGVO nachweisen. Im Folgenden werden die rechtlichen Voraussetzungen einer wirksamen Einwilligung näher untersucht.

3.2 Gewährleistung einer wirksamen Einwilligung

Um die Einhaltung der Voraussetzungen einer Einwilligung zu gewährleisten, enthält die Datenschutz-Grundverordnung einige Bedingungen, die bei der Aufforderung zur Abgabe einer Einwilligung zu beachten sind. So muss nach Art. 7 Abs. 2 Satz 1 DSGVO das Einwilligungsersuchen in den Fällen, in denen die Einwilligung der betroffenen Person durch eine schriftliche Erklärung erfolgt, die noch andere Sachverhalte betrifft (wie zum Beispiel AGB), „in verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache erfolgen, dass es von anderen Sachverhalten zu unterscheiden ist". Darüber hinaus fordert Art. 7 Abs. 2 Satz 1 DSGVO aber nicht nur gestalterische, sondern auch eine inhaltliche Transparenz, wobei die Übergänge fließend sind. Nach dieser Vorschrift muss eine schriftliche Einwilligungsklausel so platziert sein, dass sie die betroffene Person nicht übersehen kann. Dies kann etwa durch eine Einrahmung und Hervorhebung mittels Fettdruck gewährleistet werden.[14]

Die Information vor der Einwilligung muss mindestens die Themen der Art. 13 und 14 DSGVO umfassen. Nach Art. 7 Abs. 3 Satz 3 DSGVO muss der Verantwortliche die betroffene Person vor Abgabe der Einwilligung über ihr Recht auf Widerruf der Einwilligung und die Rechtsfolgen des Wiederrufs in Kenntnis setzen.

Freiwillig ist die Einwilligung, wenn sie ohne Zwang und aus freier, autonomer Entscheidung der betroffenen Person erteilt wird.[15] Zum Schutz der Freiwilligkeit der

Einwilligung thematisiert Art. 7 Abs. 4 DSGVO mögliche Kopplungen des Einwilligungsverlangens mit anderen Willenserklärungen: „Bei der Beurteilung, ob die Einwilligung freiwillig erteilt wurde, muss dem Umstand in größtmöglichem Umfang Rechnung getragen werden, 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". Die Vorschrift statuiert somit kein Kopplungsverbot, sondern enthält nur eine „Berücksichtigungspflicht". Sie lässt somit Kopplungen zu, wenn diese gerechtfertigt erscheint. Sie soll im Ergebnis z.B. nicht bei den Social Networks greifen, wenn die Einwilligung wirtschaftlich die Gegenleistung für die geldfreien Leistungen der Plattform ist.[16]

Freiwilligkeit fehlt, wenn die erklärende Person nicht fähig ist, den Gegenstand der Einwilligung, ihre Bedeutung und ihre Folgen kognitiv zu erfassen und seinen Willen selbstbestimmt zu bilden und zu betätigen. Dies gilt vor allem für ein Kind, das nicht einwilligungsfähig ist, weil es zu dieser Einsicht und Handlung noch nicht in der Lage ist. Dies gilt aber auch für alle Personen, die auf Grund von Krankheiten und Behinderungen hierzu ebenfalls nicht in der Lage sind. Ob diese Einsicht vorliegt, ist im Einzelfall je nach Umfang und Bedeutung der Datenverarbeitung, dem Inhalt der Einwilligung und den geistigen Fähigkeiten der Person zu beurteilen.

Die Einwilligung muss ausreichend bestimmt sein, um aus ihr erkennen zu können, welche Daten für welchen Zweck in welcher Form wie lange verarbeitet werden dürfen. Für bestimmte Datenverarbeitungen hat die Einwilligung aber nur einen rechtfertigenden Charakter, wenn sie ausdrücklich die bestimmte Form der Datenverarbeitung zum Gegenstand hat. Ausdrücklich muss dies nach Art. 9 Abs. 2 lit. a DSGVO für die Einwilligung in die Verarbeitung besonderer Kategorien personenbezogener Daten und nach Art. 22 Abs. 2 lit. c DSGVO für die Einwilligung in automatisierte Einzelfallentscheidungen einschließlich Profiling erfolgen.

3.3 Rechtsfolgen einer wirksamen Einwilligung

Die informierte und freiwillige Einwilligung legitimiert nach Art. 6 Abs. 1 UAbs. 1 lit. a DSGVO die ausreichend bestimmt beschriebene Datenverarbeitung. Sie stellt keinen Verstoß dar, der Aufsichtsmaßnahmen nach Art. 58 DSGVO oder Sanktionen nach Art. 83 DSGVO nach sich ziehen kann.

Auswirkungen hat die Verarbeitungsgrundlage auch auf die Betroffenenrechte. Nach einer Einwilligung in die Datenverarbeitung kann die betroffene Person das Recht auf Datenübertragung nach Art. 20 DSGVO geltend machen. Dieses Recht kommt nur zur Anwendung bei personenbezogenen Daten, die aufgrund einer Einwilligung nach Art. 6 Abs. 1 UAbs. 1 lit. a oder Art. 9 Abs. 2 lit. a DSGVO oder aufgrund eines Vertrags nach Art. 6 Abs. 1 UAbs. 1 lit. b DSGVO verarbeitet werden. Dagegen kann die betroffene Person für personenbezogene Daten, die z.B. aufgrund berechtigter Interessen nach Art. 6 Abs. 1 UAbs. 1 lit. f DSGVO verarbeitet werden, dieses Recht nicht geltend machen. Umgekehrt kann eine betroffene Person keinen Widerspruch gegen eine Datenverarbeitung nach Art. 21 DSGVO einlegen, wenn sie in die Datenverarbeitung eingewilligt hat.

3.4 Widerruf einer Einwilligung

Der Widerruf einer Verarbeitung ist nach Art. 7 Abs. 3 DSGVO jederzeit ohne Angabe von Gründen möglich. Der Widerruf der Einwilligung muss so einfach wie die Erteilung der Einwilligung sein. Mit dem Wirksamwerden des Widerrufs entfällt die legitimierende Wirkung der Einwilligung ex nunc. Die betroffene Person kann nach Art. 17 Abs. 1 lit. b DSGVO eine Löschung ihrer Daten verlangen. Durch den Widerruf der Einwilligung wird aber die Rechtmäßigkeit der aufgrund der Einwilligung bis zum Widerruf erfolgten Verarbeitung nicht berührt.

3.5 Einwilligung eines Kindes

Willigen Kinder in die Verarbeitung ihrer Daten ein, gelten auch für sie die allgemeinen Regelungen zur Definition einer *wirksamen* Einwilligung in Art. 4 Nr. 11 DSGVO, zur grundsätzlichen Erlaubniswirkung der Einwilligung in Art. 6 Abs. 1 UAbs. 1 lit. a DSGVO, zur ausdrücklichen Einwilligung in die Verarbeitung besonderer Kategorien personenbezogener Daten in Art 9 Abs. 2 lit. a DSGVO und in automatisierte Entscheidungen nach Art. 22 Abs. 2 lit. c sowie zu weiteren Voraussetzungen jeder Einwilligung in Art. 7 DSGVO.

Für die Wirksamkeit der Einwilligung ist die Einsichtsfähigkeit in den Gegenstand der Einwilligung, ihre Bedeutung und ihre Folgen erforderlich. Diese Einsicht ist grundsätzlich im Einzelfall zu beurteilen. Die Verordnung regelt keine Altersgrenze, von der an das Kind als einsichtsfähig gilt. Nach Art. 8 Abs. 1 UAbs. 1 Satz 1 DSGVO gilt jedoch die Einwilligung eines Kindes bei einem Angebot von Diensten der Informationsgesellschaft, das einem Kind direkt unterbreitet wird, als rechtmäßig, wenn das Kind das sechzehnte Lebensjahr vollendet hat. Mit dieser starren Altersgrenze, die einen Kompromiss zwischen sehr unterschiedlichen Vorstellungen im Gesetzgebungsprozess unter Berücksichtigung der mitgliedstaatlichen Rechtstraditionen darstellt, soll im Internet, in dem die Einsichtsfähigkeit nicht durch Augenschein festgestellt werden kann, Rechtssicherheit für alle Beteiligte gewährleistet werden. Von dieser typisierenden Festlegung der Einwilligungsfähigkeit kann im Einzelfall weder nach unten noch nach oben abgewichen werden.

Nach der Öffnungsklausel des Art. 8 Abs. 1 UAbs. 2 DSGVO dürfen jedoch Mitgliedstaaten durch gesetzliche Regelung diese Grenze bis zur Vollendung des dreizehnten Lebensjahres senken. Diese Grenze richtet sich wohl nach den Nutzungsbedingungen der großen amerikanischen Plattformen wie Facebook, WhatsApp, Twitter und YouTube, die die Nutzung ab 13 Jahren zulassen. Von dieser Öffnungsklausel haben die Mitgliedstaaten sehr unterschiedlich Gebrauch gemacht. Die Altersgrenze auf 13 Jahre festgesetzt haben Belgien, Dänemark, Estland, Finnland, Lettland, Malta, Portugal, Schweden und das Vereinigte Königreich. Ab 14 Jahren dürfen Kinder in Bulgarien, Italien, Litauen, Österreich, Spanien und Zypern ohne Zustimmung ihrer Eltern in die Datenverarbeitung von Diensten der Informationsgesellschaft einwilligen. Eine Grenze mit 15 Jahren sehen Frankreich, Griechenland, Slowenien und Tschechien vor. Die Altersgrenze der Datenschutz-Grundverordnung haben nur Deutschland, Irland, Kroatien, Luxemburg, Niederlande, Polen, Rumänien, Slowakei und Ungarn beibehalten.

Im Gegensatz zu dieser Regelungsabsicht zeigen allerdings aktuelle Studien,[17] dass Kinder in Deutschland vorranging Angebote wie Facebook, YouTube oder WhatsApp selbständig nutzen – auch und gerade, wenn sie unter 16 Jahren alt sind. In der Praxis wird häufig eine falsche Altersangabe durch Kinder gemacht, um das Angebot nutzen zu können. Dadurch, dass die Social Media dies ermöglichen, verhindern sie, dass Eltern ihrer Fürsorgepflicht angemessen nachkommen können. Diese müssen jedoch für ihre Kinder einstehen, auch wenn ihnen die Wahrnehmung ihrer eigenen

Verantwortung im Rahmen einer mediengerechten Erziehung durch die gelebte Praxis deutlich erschwert wird. Diese Diskrepanz der Regelung zur tatsächlichen Nutzungsrealität beruht neben einer unzureichenden Altersverifikation der Social Media unter anderem auf der Unwissenheit und der fehlenden Informiertheit der Kinder wie der Eltern.

Die starre Altersgrenze gilt jedoch nur für die Datenverarbeitung für „Dienste der Informationsgesellschaft" – also die Internetnutzung. Für alle anderen Datenverarbeitungen muss anhand der Einsichts- und Handlungsfähigkeit des Kindes individuell festgestellt werden, ob die Einwilligung freiwillig ist. Auf diese Feststellung übt allerdings die gesetzliche Festlegung der Einwilligungsfähigkeit bei 16 Jahren für Dienste der Informationsgesellschaft einen indirekten Einfluss auf. Es wird vertreten, dass unterhalb dieser Altersgrenze im Streitfall der Verantwortliche die Einwilligungsfähigkeit und oberhalb der Altersgrenze die betroffene Person die fehlende Einwilligungsfähigkeit nachweisen muss.

Hat das Kind die festgesetzte Altersgrenze oder die individuelle Einwilligungsfähigkeit noch nicht erreicht, so ist die Datenverarbeitung nach Art. 8 Abs. 1 UAbs. 1 Satz 2 DSGVO „nur rechtmäßig, sofern und soweit diese Einwilligung durch den Träger der elterlichen Verantwortung für das Kind oder mit dessen Zustimmung erteilt wird". Art. 8 Abs. 2 DSGVO verpflichtet den verantwortlichen Datenverarbeiter, unter Berücksichtigung der verfügbaren Technik angemessene Anstrengungen zu unternehmen, um sich in solchen Fällen zu vergewissern, dass die Einwilligung durch den Träger der elterlichen Verantwortung für das Kind oder mit dessen Zustimmung erteilt wurde". Die derzeit praktizierten Verfahren, die sich auf die Selbstbehauptung der Benutzer über ihr Alter verlassen und der Kontaktierung der Sorgeberechtigten bei Angabe der Minderjährigkeit dienen, sind einfach anzuwenden, jedoch ebenso leicht zu umgehen. Nutzende können bei der Abfrage falsche Altersangaben machen oder personenbezogene Daten verwenden, die ihnen nicht gehören, oder die Alterskontrolle umgehen, indem sie Änderungen am Endgerät vornehmen.

Eine einfache technische Umsetzung hinsichtlich der Altersverifikation ergibt sich aus dem COPPA-Kontext. Diese Ansätze sind allerdings erheblicher Kritik ausgesetzt, vor allem hinsichtlich ihrer Effektivität, der Einhaltung von Datenschutzvorgaben (z.B. Datenminimierung) und der Benutzerfreundlichkeit. Nutzende können bei der Abfrage falsche Altersangaben machen bzw. personenbezogene Daten verwenden, die ihnen möglicherweise nicht gehören, oder die Alterskontrolle umgehen, indem sie Änderungen am Endgerät vornehmen - beispielsweise Cookies im Browser löschen. Weitere gängige Verfahren zur Online Altersüberprüfung sind i. d. R. Konzepte aus dem Europäischen Kontext. Diese stellen wirksame Alternativen zu der inzwischen als unwirksam eingestuften Methode aus denen COPPA dar. Beispiele hierfür reichen von Altersverifikationsmethoden über Ident-Services (z. B. Foto-/Video-Ident-Verfahren), Methoden über elektronische Funktionen des Personalausweises inklusive der Pseudonym-Funktion und der Online-Ausweisfunktion (eID-Funktion),[18] Altersverifikationsmethoden über Micropayment Services (z. B. Giropay-ID) bis hin zu Altersverifikationsmethoden über Single-Sign-on-Dienste (z. B. Verimi)[19] und Vertrauensdienste (z.B. Schufa).[20]

Alternative Altersverifikationssysteme, die hinsichtlich dieser Kritikpunkte geeigneter sind, nutzen sog. Attribute-based Credentials.[21] Bei der Nutzung der Attribute-based Credentials (unverkettbare Berechtigungsnachweise) muss keine Übermittlung eines Ausweisdokuments zur Altersüberprüfung oder ein Einschalten eines Vertrauensdienstes bei jedem Überprüfungsvorgang stattfinden. Mit Attribute-based Credentials wird eine Umsetzung des Prinzips der Datenminimierung angestrebt und lediglich ein Nachweis erbracht, dass die Nutzenden eine bestimmte Altersgrenze (z. B. 13 oder 16) nicht überschritten haben. Das genaue Alter sowie weitere Identitätsattribute die i. d. R. in Ausweisdokumenten vorhanden und für die

Regelungen zur datenschutzrechtlichen Einwilligung

Altersüberprüfung nicht relevant sind, werden den Dienstanbietern nicht offengelegt / vorgelegt.

Zur Einholung des Elternconsent können Dienstanbieter und Plattformbetreiber auf vielfältige Mechanismen zurückgreifen. Diese setzen i. d. R. auf eine Kontaktaufnahme mit Sorgeberechtigten und deren Identitätsprüfung nach Feststellung der Minderjährigkeit der Nutzenden an. Beispiele hierfür sind Mechanismen, die auf ein bereits bestehendes Nutzerkonto beim Verantwortlichen ruhen und eine Einwilligungseinholung mit Hilfe eines per SMS an die jeweiligen Sorgeberechtigten gesendeten Bestätigungs- bzw. Sicherheitscodes, z. B. im Zusammenhang mit einer Bezahltransaktion, ermöglicht. Ein alternativer Ansatz setzt auf Photo- bzw. Video-Ident-Identifizierung als Teil der verifizierten Einwilligung der Eltern. Dabei legt der jeweilige Erziehungsberechtigte der Minderjährigen im Rahmen eines Videochats einen amtlichen Lichtbildausweis vor und willigt nach erfolgreicher Legitimationsüberprüfung in die vorangegangene Datenverarbeitung ein. Weitere Mechanismen umfassen u. a. eine Bereitstellung eines vom Elternteil zu unterzeichnenden Einverständnisformulars, welches per Post, Fax oder elektronischem Scan zurückgesandt werden soll. Die Erklärung enthält Sicherheitsfragen, die nur von den Erziehungsberechtigten richtig beantwortet werden können.

Mit Blick auf die in Deutschland geltende UN-Kinderrechtskonvention und die geplante Aufnahme der Kinderrechte ins Grundgesetz stellt sich über den Aspekt der Freiwilligkeit hinaus die Frage, ob eine zu starke Altersbegrenzung dann problematisch sein kann, wenn Kinder beispielsweise Hilfsangebote suchen (z.B. bei Gewalt in der Familie), bei denen sie unabhängig agieren wollen. Auch kann ein zu stark reglementierter Schutz den ebenfalls verbrieften Ansprüchen von Kindern auf Partizipation, Informationsfreiheit oder dem Recht auf Bildung und Spiel entgegenwirken.

4
Bedeutung der Einwilligung in der Praxis

Trotz zahlreicher Debatten rund um die Bedeutung der Einwilligung und ihr Verhältnis zu den übrigen Erlaubnistatbeständen, liegen keine systematischen wissenschaftlichen Untersuchungen zu der Bedeutung der Einwilligung in der Praxis vor.[22] Um den Wissensstand auf diesem Gebiet auszubauen, führte das Forum Privatheit eine empirische Untersuchung zu der Frage durch, auf welche Erlaubnistatbestände die 50 von Deutschland aus meistbesuchten Webseiten ihre Datenverarbeitung in der Praxis stützen.

4.1 Ergebnisse einer empirischen Untersuchung

Die Ergebnisse der Auswertung aller 50 Webseiten sind in drei Tabellen dargestellt. In Tabelle 0-1 sind Anzahl und prozentualer Anteil der insgesamt 1115 Nennungen pro Erlaubnistatbestand zu sehen. Detaillierter zeigt *Tabelle 4-2*, für wie viele unterschiedliche Zwecke sich die untersuchten Webseiten auf welche Rechtsgrundlage stützen. Dieser Tabelle kann somit entnommen werden, wie häufig sich jede der untersuchten Webseiten auf welche Rechtsgrundlage stützte. Erwähnenswert in diesem Zusammenhang ist, dass einige Datenschutzerklärungen deutlich spezifischere Zweckangaben enthielten als andere. Entsprechend ergibt die Summe der von beispielsweise Google aufgeführten Verarbeitungszwecke insgesamt nur 12 unterschiedliche Zwecke, während gmx.de auf 44 Zwecke kommt. *Tabelle 4-3* zeigt, welche Zweck-Kategorien am häufigsten auf welche Rechtsgrundlagen gestützt werden. Verschiedene Webseiten führen für dieselbe Zweck-Kategorie teilweise unterschiedliche Rechtsgrundlagen an - für den Zweck der Bereitstellung und Weiterentwicklung eines Dienstes werden sogar fünf unterschiedliche Rechtsgrundlagen angeführt.

Die Ergebnisse zeigen, dass ein berechtigtes Interesse die am häufigsten angeführte Rechtsgrundlage ist. Auf sie wird für 47% aller (524 von 1115) Nennungen zurückgegriffen.

Die Vertragserfüllung ist der am zweithäufigsten genannte Erlaubnistatbestand. Für 29% (320 von 1115) aller Nennungen wurde diese als Rechtsgrundlage angegeben (vgl. *Tabelle 4-3*). Sie spielt insbesondere für die Verarbeitungszwecke der Bereitstellung und Weiterentwicklung eines Dienstes (32), die Durchführung von Kaufverträgen (31) und die nicht-werbliche Kommunikation zu technischen, sicherheits- und vertragsrelevanten Belangen (24) eine Rolle. Allerdings werden auch diese Verarbeitungszwecke häufig auf das berechtigte Interesse des Verantwortlichen gestützt. Die Durchführung von Kaufverträgen hat immerhin 9 Nennungen, die nicht-werbliche Kommunikation 16 und die Bereitstellung und Weiterentwicklung eines Dienstes sogar 42 (vgl. *Tabelle 4-3*). Darüber hinaus erfolgte die Datenverarbeitung auf Grundlage des berechtigten Interesses ansonsten insbesondere zur Gewährleistung der Sicherheit und Betriebsfähigkeit des Dienstes oder der Webseite (37), zur Personalisierung von Werbung (34 Mal), zu statistischen Zwecken bzw. zur Auswertung und Analyse (33) und zur Personalisierung eines Dienstes in EU (31).Die Einwilligung spielt hingegen nur eine geringe Rolle. Nur für 13% (146 von 1115) der Nennungen wurde die Einwilligung als Rechtsgrundlage genannt. Lediglich für den Zweck des Newsletter-Versands (16) und der Zustellung personalisierter Werbung (19) spielt die Einwilligung eine größere Rolle. Allerdings wurde in vielen Fällen für beide Verarbeitungszwecke auch die Rechtsgrundlage der Vertragserfüllung (12 für den Newsletter-Versand und 9 für personalisierte Werbung) sowie des berechtigten Interesses (11 für den Newsletter-Versand und 34 für personalisierte Werbung) angeführt (vgl. *Tabelle 4-3*).

Bedeutung der Einwilligung in der Praxis

Seltener als auf die Einwilligung stützen sich die Verantwortlichen nur auf die Erlaubnistatbestände der Erfüllung einer rechtlichen Verpflichtung (11% bzw. 120), des Schutzes lebenswichtiger Interessen des Betroffenen (0% bzw. 3) und die Wahrnehmung einer Aufgabe im öffentlichen Interesse (0% bzw. 2). Auf die Rechtsgrundlage der Erfüllung einer rechtlichen Verpflichtung, der Verantwortliche unterliegen, stützen sich die Verantwortlichen zum Zwecke der Erfüllung rechtlicher Pflichten in 32 Fällen und zum Zwecke der Einhaltung und Durchsetzung rechtlicher Forderungen in 15 Fällen. Für beide Verarbeitungszwecke wurde allerdings auch mehrfach auf das berechtigte Interesse zurückgegriffen (in 19 Fällen zur Einhaltung und Durchsetzung rechtlicher Forderungen sowie in 16 Fällen Erfüllung rechtlicher Pflichten).

Rechts-grundlage	Einwilligung (Art. 6 Abs. 1 lit. a)	Vertragser-füllung (Art. 6 Abs. 1 lit. b	Erfüllung rechtl. Pflichten (Art. 6 Abs. 1 lit. c)	Schutz le-benswichtiger Interessen (Art. 6 Abs. 1 lit. d)	Aufgabe im öffentl. Interesse (Art. 6 Abs. 1 lit. e)	Berechtigte Interessen (Art. 6 Abs. 1 lit. f)	Summe
Zweck-Kategorien	146	320	120	3	2	524	1115
Prozent aller Zweck-Kategorien	13%	29%	11%	0%	0%	47%	100%

Tabelle 4-1: Ergebnisse der Auswertung: Anzahl und prozentualer Anteil der Nennungen pro Erlaubnistatbestand (eigene Auswertung und Darstellung)

# im Ranking	**Webseite**	Einwilli-gung (Art. 6 Abs. 1 lit. a)	Vertrags-erfüllung (Art. 6 Abs. 1 lit. b	Erfüllung rechtl. Pflichten (Art. 6 Abs. 1 lit. c)	Schutz lebens-wichtiger Interes-sen (Art. 6 Abs. 1 lit. d)	Aufgabe im öffentl. Interesse (Art. 6 Abs. 1 lit. e)	Berech-tigte Interes-sen (Art. 6 Abs. 1 lit. f)
1	google.com	2	1	1			8
2	youtube.com	2	1	1			8
3	google.de	2	1	1			8
4	facebook.com	5					8
5	amazon.de		4	5			9
6	wikipedia.org	2		4			4
7	ebay.de	7	9	5	2		21
8	bild.de	1	9	4			15
9	t-online.de	3	2	4			6
10	ebay-kleinanzeigen.de	3	11	1			8
11	web.de	12	13	1			18
12	instagram.com	5					8
13	gmx.net	12	13	1			18
14	spiegel.de		1				2
15	pornhub.com		3	5			5
16	xhamster.com	1	5	3			6
17	twitter.com	7	8	1			6
18	google.com.br	2	1	1			8
19	netflix.com		5				4
20	focus.de	4	16	2		1	16
21	paypal.com	4	10	2			7
22	dhl.de	3	5	2			11
23	otto.de	3	7	2			12
24	welt.de	5	9	2			16
25	samsung.com	2	4	3			6
26	chip.de		14				12
27	spacetoday.xyz						
28	yahoo.com		6	3			8
29	idealo.de	1	11	6			11
30	merkur.de	5	7				9

31	live.com	2	13	5			21
32	derwesten.de	5	9				16
33	twitch.tv		3				
34	outbrain.com		9	4			11
35	chefkoch.de	4	7	3			12
36	taboola.com		3	1			17
37	whatsapp.com		9	6			14
38	xnxx.com		7	4			16
39	reddit.com		11	4			15
40	immobilienscout24.de	4	7	3			12
41	n-tv.de		1	2			8
42	mobile.de	6	10	7			9
43	tagesschau.de	7	3	2	1	1	4
44	bing.com	2	13	5			21
45	tz.de	1	3				11
46	wetter.com	3	6	2			12
47	telekom.com	6	6	3			7
48	mydealz.de	4	4	2			9
49	mediamarkt.de	6	9	3			13
50	livejasmin.com	3	11	4			18
SUMME		**146**	**320**	**120**	**3**	**2**	**524**

Tabelle 4-2: Für wie viele unterschiedliche Zwecke setzten die untersuchten Webseiten auf welche Rechtsgrundlage (eigene Auswertung und Darstellung)

Zweck-Kategorien	Einwilligung (Art. 6 Abs. 1 lit. a)	Vertragserfüllung (Art. 6 Abs. 1 lit. b	Erfüllung rechtl. Pflichten (Art. 6 Abs. 1 lit. c)	Schutz lebens-wichtiger Inte-ressen (Art. 6 Abs. 1 lit. d)	Aufgabe im öffentl. Interesse (Art. 6 Abs. 1 lit. e)	Berechtigte Interessen (Art. 6 Abs. 1 lit. f)
Newsletter-Versand	16	12	1	0	0	11
Newsletter-Analyse	1	1	0	0	0	4
Befragungen und Marktforschung	5	4	1	0	0	9
Nicht-Personalisierte Werbung	3	2	0	0	0	11
Werbung per Post, Telefon, Email, SMS	2	0	0	0	0	2
Personalisierte Werbung	19	9	0	0	0	34
Sensible Daten	2	1	0	0	0	1
Spracherkennung	4	2	0	0	0	3
Hotline Gespräche	4	3	0	0	0	1
Hotline Gespräche Analyse	0	1	0	0	0	2
Daten an Dritte oder Nicht EU-Land	7	12	10	0	0	28
Identifizierung und Authentifizierung	1	9	3	0	0	13
Bonitätsprüfung	0	6	1	0	0	10
Kontaktaufnahme seitens des Nutzers	7	18	1	0	0	17
Bereitstellung und Weiterentwicklung eines Dienstes	8	32	1	0	1	42
Lokale Services, GPS-Standort	6	7	0	0	0	8
Durchführung von Kaufverträgen	5	31	1	0	0	9
Bereitstellung von Nachrichten, Meldungen, Tweets	3	8	2	0	0	15
Gewährleistung der Sicherheit Betriebsfähigkeit	3	7	9	0	0	37
Kommunikation zu Themen denen Nutzer folgt	3	6	0	0	0	0
Nicht-werbliche Kommunikation zu technischen, sicherheits- und vertragsrelevanten Belangen (Betrugswarnungen, Konto-Sperrung oder Vertragsänderungen)	1	24	0	0	0	16
Filterung von Nachrichten zum Schutz vor Betrug	0	0	0	0	0	1
Vermittlung von Verträgen	0	8	0	0	0	3
Gutscheine, Rabatte und Sonderaktionen	2	2	0	0	0	4

Aktionen und Gewinnspiele	6	14	0	0	0	3
Shopping-Personalisierung	0	2	0	0	0	2
Wissenschaftliche Forschungszwecke	1	0	1	0	0	10
Betrugsprävention	1	7	10	0	0	21
Erbringung von Zahlungsdiensten	2	12	0	0	0	6
Steuerrechtliche Pflichten, Geldwäscheprüfung	0	0	8	0	0	3
Personalisierung eines Dienstes in der EU	7	10	0	0	0	31
Personalisierung eines Dienstes außerhalb der EU	0	0	0	0	0	1
Marketing allgemein	3	7	0	0	0	26
Einhaltung von Verpflichtungen gegenüber Entwicklern	0	0	5	0	0	11
Einhaltung und Durchsetzung rechtlicher Forderungen	0	6	15	0	0	19
Ausübung und Verteidigung von Rechtsansprüchen	0	2	4	0	0	4
Erfüllung rechtlicher Verpflichtungen	0	2	32	1	0	16
Mitwirkung an Gerichtsverfahren	0	0	1	0	0	2
Web-Tracking durch Dritte	3	2	0	0	0	8
Verhinderung von Tod usw.	0	1	6	2	0	4
Zustellung von Produkten	0	6	0	0	0	0
Bonusprogramme, Co-Branding-Kreditkarten	0	2	0	0	0	2
Unternehmenskauf	0	1	1	0	0	1
Automatisierte Entscheidungsfindung, Profiling	2	1	2	0	0	1
Verknüpfung von Diensten	1	0	0	0	0	2
Widerspruch	0	0	2	0	1	3
Statistische Zwecke, Auswertung und Analyse	5	8	0	0	0	33
Anbieten intelligenter Services	0	0	0	0	0	2
Interaktion mit Webseite Kommentarfunktion usw.	5	2	0	0	0	4
Kundenrückgewinnung	2	0	0	0	0	0
Geolokalisierung veröffentlichter Nutzerinhalte	0	1	0	0	0	0
Altersverifikation	0	1	0	0	0	1
Bug-Bounty	1	0	0	0	0	1
Forderungsverkauf, Inkassodienste	0	0	0	0	0	1
Fehlerdiagnose	0	3	0	0	0	6
Veröffentlichung von Nutzerinhalten	3	6	1	0	0	5
Kontaktaufnahme seitens Unternehmen	1	12	1	0	0	6
Bewerberauswahl	0	1	0	0	0	0
Push-Benachrichtigungen	1	2	0	0	0	3
Sonstige betriebliche und geschäftliche Zwecke	0	1	1	0	0	2
Kommunikation mit anderen Nutzern	0	1	0	0	0	1
Zutritt zu physischem Grundstück	0	1	0	0	0	0
Einheitliches Schriftbild	0	0	0	0	0	1
Vorlesefunktion	0	0	0	0	0	1
Schulungszwecke für Mitarbeiter	0	1	0	0	0	0
Summe	**146**	**320**	**120**	**3**	**2**	**524**

Tabelle 4-3: Rechtgrundlagen die für verschiedene Zwecke einer Webseite genannt wurden (eigene Auswertung und Darstellung)

4.2 Funktion der Einwilligung

Die Einwilligung hat in der Praxis vor allem Bedeutung als Ersatzrechtsgrundlage, die datenverarbeitenden Organisationen Datenverarbeitungen ermöglicht, die ansonsten rechtlich illegitim wären. Sie ermöglicht eine Verantwortungsverschiebung von den datenverarbeitenden Organisationen auf die Nutzenden, denen formal die Entscheidung übertragen wird, über die Legitimität der Datenverarbeitung zu urteilen.

Von den Verantwortlichen wird die Einwilligung in der Praxis als wichtigstes Instrument zur rechtlichen Absicherung ihrer Datenverarbeitung verstanden. Seit der Anwendbarkeit der Datenschutz-Grundverordnung (25. Mai 2018) greifen viele Verantwortliche, insbesondere die für den Versand von Newslettern Verantwortlichen,

aber auch Dienstebetreiber, auf die Einholung der Einwilligung der Empfänger oder Kunden zurück, auch wenn für die jeweilige Datenverarbeitung die Erlaubnistatbestände der Vertragserfüllung nach Art. 6 Abs. 1 UAbs. 2 lit. b DSGVO oder der berechtigten Interessen nach Art. 6 Abs. 1 UAbs. 1 lit. b DSGVO gelten können.

Bedeutung der Einwilligung in der Praxis

Inzwischen scheint sich dagegen herumgesprochen zu haben, dass eine systematische Verarbeitung personenbezogener Daten – insbesondere, wenn sie Infrastrukturcharakter hat – auf einer rechtlich unsicheren Grundlage steht, wenn sie auf Einwilligungen setzt. Denn bei jeder Verweigerung oder bei jedem Widerruf der Einwilligung verliert der Verantwortliche einen Kunden oder ein Mitglied oder muss für diese eine systemwidrige Sonderregelung vorsehen. Daher versuchen zumindest große Verantwortliche und Infrastrukturanbieter ihre Datenverarbeitung auf die genannten Erlaubnistatbestände der Vertragserfüllung oder der berechtigten Interessen zu stützen. Ihre Interessen setzen sie dabei mit Hilfe von allgemeinen Geschäftsbedingungen und in diese integrierte Datenschutzerklärungen durch. Die Einwilligung wird in diesen Fällen eher zur zusätzlichen Absicherung genutzt, auf die verzichtet werden kann, wenn bei einem Widerruf nachträglich der datenschutzrechtliche Erlaubnistatbestand gewechselt werden soll.[23]

5
Defizite der Einwilligung in der Praxis

In der Praxis zeigt sich, dass die Wirksamkeitsvoraussetzungen für eine Einwilligung vielfach nicht erfüllt sind oder sogar nicht erreicht werden können.[24] Der folgende Abschnitt untersucht einige der größten Defizite, die Verantwortlichen und betroffenen Personen in der Praxis begegnen und eine wirksame Einwilligung verhindern (können).

5.1 Freiwilligkeit

Die Datenschutz-Grundverordnung setzt voraus, dass die Einwilligung zur Datenverarbeitung freiwillig erteilt wird. Eine Einwilligung ist freiwillig, wenn sie auf der freien Entscheidung der betroffenen Person beruht und ohne Zwang gegeben wurde. Wenn Akteure sich auch anders entscheiden können, und zwar ohne dass ihnen daraus Nachteile entstehen, handeln sie nicht aus Zwang. In der Praxis finden sich betroffene Personen oft in Situationen wieder, in denen diese Maßgabe in Frage gestellt ist. Dies gilt beispielsweise bei Einwilligungen in Infrastrukturen, auf die man angewiesen ist. Aufgrund der zunehmenden Integration digitaler Dienste in den Alltag wird dies auf immer mehr Datenverarbeitungsvorgänge zutreffen. Dies gilt vor allem für Suchmaschinen oder Social Networks, wenn aus beruflichen oder sozialen Gründen ein Nutzungszwang besteht und man sich diesem mangels alternativer Angebote nur schwer entziehen kann. Können Jugendliche auf die Teilnahme an Instagram verzichten? Können Berufstätige auf die Teilnahme an Xing verzichten? Können Wissenschaftlerinnen auf die Teilnahme an Research Gate verzichten? Will eine betroffene Person diese Infrastrukturen nutzen, ist dies nur zu den Bedingungen und Vorgaben möglich, die der Infrastrukturbetreiber vorgibt („take it or leave it"). Eine Wahlmöglichkeit besteht nicht. Ob dieser Zwang durch den Verantwortlichen oder die Faktizität der Technik selbst erzeugt wird, spielt keine Rolle. Er sorgt jedenfalls dafür, dass eine betroffene Person faktisch keine freiwillige Einwilligung erteilen kann.

Aus psychologischer Perspektive ist die Frage nach der Freiwilligkeit bei der Einwilligung nicht eindeutig zu beantworten – je nach Theorie gibt es Unterschiede, was als freiwillig angesehen wird und was nicht. Von Freiwilligkeit im psychologischen Sinn wird gemeinhin gesprochen, wenn es keine externen Zwänge gibt, die stark genug sind (zum Beispiel im Rahmen dissonanztheoretischer Überlegungen), ein Handeln zu erzwingen. Was stark genug ist, ist aber fraglich. Aus psychologischer Sicht würde man hinsichtlich der Nutzung technischer Systeme (anders als bei lebensbedrohlichen Lagen) wahrscheinlich aber letztlich eher zu dem Schluss kommen, dass man das technische System ja nicht nutzen MUSS, man KANN sich dagegen entscheiden. Greift man andererseits auf die Selbstbestimmungstheorie[25] nach Ryan und Deci zurück, stößt man auf den Begriff der Autonomie. Das Gegenteil der Autonomie bildet die Heteronomie, die Fremdbestimmtheit. Autonomes Verhalten ist solches, das beispielsweise durch intrinsische Motivation gekennzeichnet ist. Fremdbestimmung liegt hingegen vor, wenn externe Reize wie Belohnung oder Bestrafung das Verhalten beeinflussen. Da es bei der Einwilligung zur Datenverarbeitung i.d.R. nur die Möglichkeit zur Zustimmung gibt, wenn man eine Website besuchen, oder einen Service nutzen möchte, kann nicht oder nur eingeschränkt von einer autonomen Entscheidung gesprochen werden. Es besteht zumeist noch die Option, eine Website oder einen Service nicht zu nutzen. Würde Individuen die Wahlmöglichkeit gelassen, der Datenverarbeitung entweder zuzustimmen oder diese abzulehnen, könnte schon eher von autonomen oder freiwilligen Entscheidungen die Rede sein. Die Selbstbestimmungstheorie ist hier allerdings nur eingeschränkt anwendbar, da die Einwilligung nicht das Ziel einer Handlung und somit kein motiviertes Verhalten – sondern vielmehr Nebenprodukt einer anderen Handlung – ist.

Defizite der Einwilligung in der Praxis

Die für Freiwilligkeit notwendige Abwägung der Vor- und Nachteile einer Entscheidung kann aber auch – nach den Annahmen des privacy calculus[26] in Verbindung mit der Construal-Level-Theorie[27] – eingeschränkt oder unmöglich sein. Oftmals wird das Entscheidungsverhalten im Internet offenbar in erster Linie von erwarteten unmittelbaren Gratifikationen beeinflusst und weniger von antizipierten negativen Konsequenzen. Menschen erschaffen sich abstrakte mentale Modelle über die Auswirkungen zukünftiger Entscheidungen. Der Grad der Abstraktion hängt dabei mit der zeitlichen Distanz zusammen; unmittelbare Auswirkungen werden konkreter antizipiert, wohingegen Konsequenzen in der entfernteren Zukunft zu abstrakteren Vorstellungen führen. Konkretere Antizipationen haben allerdings einen stärkeren Einfluss auf das Verhalten als solche, die abstrakt bleiben. Diese empirisch gut bestätigte Theorie kann als Erklärung für oben angeführtes Muster dienen. Menschen haben ein bestimmtes Ziel vor Augen (bspw. einen Produktkauf über eine Website), dessen Erreichung sie mit einer Gratifikation assoziieren. Selbst wenn Privatheitsrisiken in dieser Situation salient sind, liegen sie weiter in der Zukunft als die Gratifikation und sind zudem mit Unsicherheit verbunden, wohingegen das Eintreten der Gratifikation sehr wahrscheinlich ist. Somit lässt sich erklären, weshalb antizipierte positive Konsequenzen, die man „direkt vor Augen" hat und die nur einen Klick entfernt sind, einen stärkeren Einfluss auf das Verhalten haben als potenzielle negative Konsequenzen. Darüber hinaus würde das Eintreten der antizipierten Gratifikation oder das Erreichen eines bestimmten Ziels durch den Akt des Informierens verzögert. Aus der psychologischen Forschung weiß man allerdings, dass Menschen unmittelbare Gratifikationen verzögerten vorziehen. Daher bleiben Datenschutzerklärungen meist ungelesen oder Cookie-Banner werden schlicht weggeklickt, ohne sich ausreichend zu informieren.

Daher stellt sich die Frage, ob in Konstellationen, in denen marktmächtige Infrastrukturbetreiber wesentliche Infrastrukturen für die öffentliche Kommunikation zur Verfügung stellen, der Gesetzgeber die Grundrechte der Betroffenen stärker schützen sollte. Zwar gelten die Grundrechte unmittelbar nur gegenüber dem Staat, aufgrund der objektivrechtlichen Funktion der Grundrechte mittelbar aber auch gegenüber den Bürgern (auch z.B. privatwirtschaftlichen Unternehmen und Vereinen) Nach der jüngeren Rechtsprechung des Bundesverfassungsgerichts kann diese Grundrechtsbindung für Infrastrukturbetreiber verstärkt sein, da sie eine öffentliche Verantwortung haben. Wenn Grundrechte Freiheit schützen, indem sie Macht begrenzen, und wenn Macht stärker von Infrastrukturbetreibern ausgeübt wird als vom Staat, können sich die Grundrechte nicht nur gegen den Staat richten. Sie müssen auch diejenigen verpflichten, die durch ihre technischen Infrastrukturen diese Macht ausüben. Als privatwirtschaftliche Konglomerate können sie sich zwar grundsätzlich auf Berufs- und Eigentumsfreiheit berufen. Wie das Bundesverfassungsgericht z.B. 2016 in seinem Urteil zum Atomausstieg festgestellt hat, wird dieser Grundrechtsschutz jedoch immer schwächer, je weiter er sich vom Zweck dieser Grundrechte entfernt, den Erwerb der Lebensgrundlagen und die persönliche Freiheit zu sichern.[28] Wenn die Ausübung dieser Grundrechte zur Akkumulation von enormer gesellschaftlicher Macht führt, die die Freiheit anderer Menschen gefährdet, dann muss diese Macht – nach den Entscheidungen des Bundesverfassungsgerichts zu Fraport,[29] zum Bierdosen-Flashmob,[30] zum Fußballstadionverbot[31] und zu Social Networks[32] – durch die Grundrechte anderer begrenzt werden. „Je nach Gewährleistungsinhalt und Fallgestaltung kann […] die mittelbare Grundrechtsbindung Privater einer Grundrechtsbindung des Staates […] nahe oder auch gleich kommen".[33] Dies kommt für den „Schutz der Kommunikation" insbesondere dann in Betracht, „wenn private Unternehmen die Bereitstellung schon der Rahmenbedingungen öffentlicher Kommunikation selbst übernehmen und damit in Funktionen eintreten, die – wie die Sicherstellung der Post- und Telekommunikationsdienstleistungen – früher dem Staat als Aufgabe der Daseinsvorsorge zugewiesen waren".[34] Diese Überlegung dürfte vor allem für private Anbieter relevant werden, die Infrastrukturen der digitalen Gesellschaft betreiben: Je abhängiger die Gesellschaft von ihren Infrastrukturleistungen ist und je tiefgreifender ihre Leistungserbringung die Ver-

Defizite der Einwilligung in der Praxis

wirklichung von Grundrechten, insbesondere der informationellen Selbstbestimmung und der gesellschaftlichen Kommunikation, beeinflusst, desto eher unterliegen sie einer staatsgleichen Grundrechtsbindung. Diese Grundrechtsbindung ermöglicht dem Gesetzgeber die Bedingungen der Datenverarbeitung so festzulegen, dass der Schutz der Grundrechte der betroffenen Person gewahrt ist und die Datenverarbeitung zu fairen Konditionen erfolgt.

An der Voraussetzung der Freiwilligkeit der Einwilligung fehlt es auch, wenn die Erfüllung eines Vertrags einschließlich der Erbringung einer Dienstleistung von der Einwilligung zu einer Verarbeitung personenbezogener Daten abhängig gemacht wird, die für die Erfüllung des Vertrags nicht erforderlich sind. Nicht erforderlich für die Erfüllung des Vertrags ist die Datenverarbeitung für Zwecke der Werbung, zur Profilbildung oder zum Weiterverkauf an Dritte. Art. 7 Abs. 4 DSGVO enthält allerdings kein striktes Kopplungsverbot, sondern nur eine Pflicht zu prüfen, ob eine Kopplung die Freiwilligkeit einer Einwilligung einschränkt.

In Fällen, in denen die Diensterbringung (etwa in sozialen Netzwerken) nicht an eine monetäre Vergütung geknüpft ist, sondern der Diensteanbieter die Nutzungsdaten zur Profilbildung und zur Generierung von Werbeeinnahmen verwendet, ist umstritten, ob nach Art. 7 Abs. 4 DSGVO die Freiwilligkeit zu verneinen ist.[35]

Im Ergebnis spricht viel dafür, die Freiwilligkeit bei einer Kopplung zwischen der Dienstenutzung und einer obligatorischen Einwilligung in die zur Finanzierung des Dienstes notwendigen Datenverarbeitung in vielen Fällen zu verneinen, soweit Nutzende faktisch keine andere Wahl haben.[36] Anders kann es freilich zu bewerten sein, wenn dem Nutzer nicht nur die Option der „Dienste gegen Datennutzung" angeboten wird, sondern auch eine kostenpflichtige Variante ohne die Möglichkeit des Diensteanbieters zur Verwertung von personenbezogenen Daten des Nutzers. In diesen Fällen wurde in der Vergangenheit bereits angenommen, dass eine in diesem Kontext abgegebene Einwilligungserklärung jedenfalls nicht an der Freiwilligkeit scheitert, da dem Nutzer auch die Option einer kostenpflichtigen Dienstenutzung zur Verfügung gestanden hätte. An den übrigen spezifischen Problemen der Einwilligung als Rechtsgrundlage vermag diese Ansicht allerdings nichts zu ändern.

5.2 Informiertheit

Die Datenschutz-Grundverordnung setzt voraus, dass die betroffene Person, die in eine Datenverarbeitung einwilligt, ausreichend über die Tätigkeit, in die sie einwilligt, informiert ist. Das in Art. 5 Abs. 1 lit. a DSGVO formulierte Transparenzgebot gilt somit auch für die Einwilligung. Die Abgabe einer informierten Entscheidung erfordert, dass die betroffene Person die zumutbare Möglichkeit hat, die Konsequenzen ihrer Entscheidung zu erkennen. Nur wenn die betroffene Person Kenntnis über alle entscheidungsrelevanten Informationen verfügt, kann sie Risiken und Vorteile abschätzen und auf dieser Grundlage über die Datenverarbeitung entscheiden.

Der betroffenen Person sind zumindest Informationen über die Identität des Verantwortlichen, den Zweck der Verarbeitung, die verarbeiteten Daten sowie die Absicht einer ausschließlich automatisierten Entscheidung nach Art. 22 Abs. 2 lit. c DSGVO oder einer Datenübermittlung in Drittländer nach Art. 49 Abs. 1 Satz 1 lit. a DSGVO mitzuteilen, bevor sie in die entsprechende Datenverarbeitung einwilligt. Zudem ist die betroffene Person nach Art. 7 Abs. 3 Satz 3 DSGVO über die Möglichkeit eines Widerrufs in Kenntnis zu setzen.

Die notwenigen Informationen sind nach Art. 12 Abs. 1 Satz 1 DSGVO „in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache zu übermitteln; dies gilt insbesondere für Informationen, die sich speziell an Kinder richten."

Informationen, die sprachlich bewusst so gestaltet sind, dass sie verschleiernd oder unangemessen beschwichtigend auf Nutzende wirken sind unzureichend. Vielfach ist die Datenverarbeitung derart komplex, dass es dem Verantwortlichen sehr schwerfallen dürfte, diese präzise, transparent und verständlich in einer klaren und einfachen Sprache darzustellen.

Damit der Zweck des Grundrechtsschutzes durch Information sichergestellt werden kann, ergibt sich aus Art. 12 Abs. 1 DSGVO, dass die Informationen so angeboten werden müssen, dass sie einerseits dem jeweiligen Interesse und andererseits der jeweiligen Aufnahmekapazität der betroffenen Person entsprechen. Die Informationen müssten daher in unterschiedlichem Umfang und unterschiedlichen Konkretisierungsstufen (wie etwa als Icon, Informationen auf einer einzigen Seite oder umfangreiche Darstellung) präsentiert werden, die die betroffene Person auswählen kann.

Zudem muss die Übermittlung der Informationen praktikabel sein. Sie muss daher grundsätzlich im gleichen Medium übermittelt werden, wie die Datenerhebung erfolgt. Ausnahmefälle, in denen eine Übermittlung mit dem gleichen Medium nicht möglich sind, sollten zulässig sein.[37] Dies kann etwa der Fall sein, wenn auf einem analogen Datenträger nicht alle notwendigen Informationen Platz haben und daher ergänzend ein Weblink auf die fehlenden Informationen verweist. Allerdings darf die Übermittlung der Information durch ein alternatives Medium nicht dazu führen, dass die Erlangung der Informationen für betroffene Personen erschwert wird.

Schließlich müssen die Informationen situationsadäquat gegeben werden. Hierzu fordert Art. 13 Abs. 1 DSGVO für die Erhebung von personenbezogenen Daten, dass die Informationen „zum Zeitpunkt der Erhebung" mitzuteilen sind. Für eine Einwilligung heißt das, dass sie unmittelbar vor der Erhebung, in die eingewilligt werden soll, erfolgt und alle im Hinblick auf die fragliche Verarbeitung relevanten Informationen umfasst. In der Praxis wird der betroffenen Person allerdings häufig schon beim ersten Kontakt eine Einwilligungserklärung vorgelegt, die unter Einbezug von Datenschutzerklärungen auch alle denkbaren Möglichkeiten weit in der Zukunft liegender Datenverarbeitungen umfasst. Selbst im unwahrscheinlichen Fall, dass eine betroffene Person die ihr bereitgestellten Informationen tatsächlich gelesen hat, wird sie sich wohl in den seltensten Fällen an die umfassenden Inhalte dieser Information und die Inhalte ihrer Einwilligung erinnern, sobald die Daten dann (irgendwann) tatsächlich erhoben werden. Dies ist in dieser Weise unzureichend.[38]

Aus psychologischer Sicht ist es fragwürdig, ob Menschen überhaupt jemals über „alle" relevanten Informationen verfügen, wenn sie Entscheidungen treffen oder ob dies überhaupt sinnvoll wäre. Entscheidungstheorien zufolge ist es nur bis zu einem bestimmten Zeitpunkt effizient, Informationen zu einer Entscheidung zu sammeln. Danach übersteigen die Kosten den zu erwartenden Nutzen (wenn zum Beispiel zwei Stunden lang Datenschutzbestimmungen von sieben verschiedenen Anbietern gelesen werden müssten). Ein weiteres Problem, das verhindert, dass Personen „alle entscheidungsrelevanten Informationen" einbeziehen können, ist die Tatsache, dass Menschen über begrenzte Rationalität verfügen und limitierte kognitive Ressourcen haben, die die Güte von informationsbasierten Entscheidungen einschränken.

Weiter kann auf Seite der Akteure die Frage gestellt werden, ob sie über hinreichend kognitive Kapazitäten verfügen (können), die Komplexität der Datenverarbeitung angemessen einzuschätzen. Dies gilt erst recht für Kinder aufgrund ihrer noch in der Entwicklung befindlicher kognitiver Fertigkeiten.[39] Aufgrund der grundsätzlichen Unmöglichkeit, die Komplexität der digitalen Infrastruktur zu überschauen, gilt dies auch für alle Laien und sogar für viele Experten. Hinzu kommt, dass oft nur über sehr weite Zwecke oder Zweckänderungen informiert wird. In eine ähnliche, weil zeitlich gelagerte Richtung, weist die Problematik der „Verwitterung" der Einwilligung.[40] Dazu kommt das Problem der Inferenz, d.h. das Problem, dass über Akteure auch dann Informationen gewonnen werden können, die mit hinreichender Wahrscheinlichkeit

Defizite der Einwilligung in der Praxis

korrekt sind, wenn sie selbst gar keine Daten freigeben haben, die die Informationsgewinnung zulassen (Inferenzproblem). Auch hier droht Informiertheit leer zu laufen.

Die aktuelle technische Umsetzung der Anforderung einer Einwilligung der betroffenen Person durch eine informierte Willensbekundung umfasst in der Regel drei Klassen von Mechanismen: Privacy-Policies, Cookie-Policies und bis zu einem gewissen Grad (Default) Privacy Settings- und Permission-Listen. Privacy-Policies und Cookie-Policies (auch Cookie Banner, Cookie Warnung bzw. Cookie Pop Up) werden als Transparenz-Instrumente zum Nachweis der Identität und Datenpraktiken des Verantwortlichen vor dem Verarbeitungsvorgang eingesetzt. (Default) Privacy Settings- und Permission-Listen werden ergänzend zu Privacy-Policies und Cookie-Policies eingesetzt. Beide zielen primär auf eine bewusste und informierte Zustimmung der Datenpreisgabe und einer nachträglichen Zugriffskontrolle ab. Leider stoßen diese Mechanismen in der Praxis immer öfter an ihre Grenzen.

Jüngste Forschungsergebnisse und Beobachtungen belegen, dass Privacy-Policies und Cookie-Policies vier Jahre nach Inkrafttreten der Datenschutz-Grundverordnung für Laien weiterhin schwer verständlich formuliert werden[41] und zum Teil widersprüchliche Klauseln und Formulierungen beinhalten.

Cookie-Policies weisen ähnliche Schwächen auf: Nutzende bekommen bei (erstmaligem) Aufruf einer Seite oder eines Dienstes oft ellenlange, verklausulierte und unübersichtlich dargestellte Informationen über das Verwenden von Cookies und entsprechenden Zwecke und Widerspruchsoptionen. Ähnlich wie im Fall der Privacy-Policies, müssen die Nutzenden häufig bei Cookie-Policies die Cookie-Praktiken der Verantwortlichen nicht aktiv durch ein Klicken bestätigen. Ausnahmefälle sind Praktiken, die auf Tracking- und Werbe-Cookies von Drittanbietern beruhen: Hier werden im Cookie Banner entsprechende Default-Einstellungen vorgeschaltet und Entscheidungsboxen eingebaut. Allerdings sind diese vorgeschalteten Default-Einstellungen und Entscheidungsboxen nicht immer im Sinne des in der Datenschutz-Grundverordnung vorgesehenen Privacy-by-Default Prinzips umgesetzt. Darüber hinaus ist, aufgrund der eingeschränkten Benutzbarkeit und Funktionalität dieser Mechanismen (z.B. kein Enforcement ohne Zustimmung des Drittanbieters)[42] davon auszugehen, dass Internetnutzende die Cookie-Warnungen ohne weitere Überlegungen systematisch „bestätigen", wegklicken oder gar ignorieren.

(Default) Privacy Settings etwa im Kontext von sozialen Netzwerken und Permission-Listen für mobile Apps zielen zwar darauf ab, Nutzenden wichtige und entscheidungsrelevante Informationen über den zu erwartenden Umgang mit personenbezogenen Informationen zu liefern, ignorieren in der Praxis aber sehr oft wichtige Hürden auf dem Weg zu einem informierten Willensbekundungsprozess. So informieren (Default) Privacy Settings- und Permission-Liste kaum über Inferenz-Risiken einer Einwilligungsentscheidung.

Auch Alternativvorschläge, wie etwa mehrschichtige Kurzrichtlinien (multi-layered short policies),[43] Datenschutzetiketten (engl. Privacy nutrition labels),[44] Datenschutzsymbole und -bilder[45] sowie Comic-basierte Schnittstellen zur Übermittlung von wichtigen Details über Datenpraktiken[46] adressieren die Probleme der traditionellen Instrumente der Einverständniserklärungen nur zum Teil.

Darüber hinaus greifen heutige Mechanismen zur Förderung informierter Willensbekundungen in zunehmend populären Szenarien der allgegenwärtigen Datenverarbeitung und rechnenden Räumen nur bedingt ein. Schnittstellen, über die den Betroffenen entscheidungsrelevante Informationen zur Verfügung gestellt werden können, sind in der Regel entweder kaum vorhanden oder eine Informationsübermittlung im Sinne der Datenschutz-Grundverordnung aufgrund physikalischer Einschränkungen (z.B. kleine oder fehlende Displayfläche) grundsätzlich nicht praktikabel/möglich.

5.3 Bestimmtheit

Nach Art. 6 Abs. 1 lit. a DSGVO ist die Einwilligung für einen oder mehrere bestimmte Zwecke zu geben. Eine wirksame Einwilligung muss demnach ausreichend klar bestimmt sein. In der Vorschrift manifestiert sich der Zweckbindungsgrundsatz aus Art. 5 Abs. 1 lit. b DSGVO. Nach diesem muss jede Datenerhebung für festgelegte, eindeutige und legitime Zwecke erfolgen. Für die Einwilligung heißt dies, dass der Verantwortliche den Zweck der Datenverarbeitung zum Zeitpunkt der Einwilligung so präzise festlegen muss, dass die betroffene Person in der Lage ist zu beurteilen, zu welchem Zweck der Verantwortliche welche bestimmten personenbezogenen Daten verarbeiten und möglicherweise an Dritte weiterleiten möchte.

In der Praxis umschreibt der Verantwortliche diese Angaben jedoch sehr oft durch unbestimmte Formulierungen (z.B. „für Geschäftszwecke", „Weitergabe an befreundete Unternehmen", „Verbesserung der Dienstleistung", „sämtliche Nutzungsdaten" oder „für berechtigte Interessen") und führt auch alle möglichen zukünftigen Zwecke auf, von denen er noch gar nicht weiß, ob er sie verfolgen will. Durch derartige Formulierungen riskiert der Verantwortliche allerdings die Wirksamkeit der Einwilligungserklärung. Die Einwilligung ist nur dann bestimmt genug, wenn die betroffene Person vor dem konkreten Einzelfall der Datenverarbeitung abschätzen (und auch nur so rechtfertigend einwilligen) kann, von wem unter welchen Umständen welche Datenverarbeitung zu welchen Zwecken vorgenommen wird. Diese Voraussetzungen erfüllen die genannten Fälle jedenfalls nicht.

Bedenklich ist auch die in der Datenschutz-Grundverordnung allerdings ausdrücklich vorgesehene Möglichkeit eines „Broad Consent" im Bereich der wissenschaftlichen Forschung. Zur Förderung der Forschung ermöglicht dies, Einwilligungen zu Forschungszwecken einzuholen, auch wenn diese Zwecke bei der Erhebung der Daten im Einzelnen noch nicht detailliert bekannt sein können. Dies ist allerdings nur zulässig, wenn die Zwecke so konkret wie möglich und nur so abstrakt wie nötig sind.

In der Praxis gängige und implementierte technische Umsetzungsmöglichkeiten beschränken sich oft auf die zuvor erwähnten Privacy Policies und AGB. Mit diesen Instrumenten sind allerdings differenzierte Mitbestimmungsoptionen für Betroffene nicht vorgesehen: Der Zweck der Datenverarbeitung zum Zeitpunkt der Einwilligung wird ausschließlich durch den oder die jeweils Verantwortlichen festgelegt; Betroffene können dies entweder unverändert akzeptieren oder auf die Dienstnutzung verzichten.

In der Forschung sind über die Jahre verschiedene Abhilfevorschläge konzipiert worden, darunter "Platform for Privacy Preferences" (P3P),[47] Just-In-Time Click-Through Agreements (JITCTAs),[48] "Enterprise Policy Authorization Language" (EPAL),[49] und „An Accountability Policy Language" (A-PPL),[50] „Data Handling Policy (DHP) language"[51] und das Konzept des „dynamic consent".[52]

"Platform for Privacy Preferences" (P3P), der den ältesten dieser Vorschläge bildet, ermächtigt die Betroffenen, Präferenzen im Hinblick auf Zweck, Aufbewahrungszeit und Bedingungen auszudrücken.[53] P3P ist allerdings als Lösung für Websites konzipiert worden. Andere Rahmenwerke, in der Regel P3P-Erweiterungen, die darauf abzielen Besonderheiten bestehender organisationsinterner Datenverarbeitungslösungen zu berücksichtigen, wurden ebenfalls vorgeschlagen. Beispiele sind oben genannt. Das Konzept von JITC-TA basiert auf der Unterteilung der großen, vollständigen Datenschutzhinweise bzw. Servicebedingungen in kleinere Teile, die zu situativ angemessenen Zeiten den Betroffenen präsentiert werden. Die Zustimmung der betroffenen Personen wird erst dann eingeholt, wenn Bedingungen nach denen personenbezogene Daten auf eine bestimmte Weise verarbeitet werden müssen gelten und vom Betroffenen mitbestimmt werden. Durch die Konfrontation von Benutzern mit kleinen kontextsensitiven Informationen soll die erforderliche kognitive Belastung seitens des Betroffenen verringert werden, während Kontextrelevanz und Grad der

Defizite der Einwilligung in der Praxis

Spezifität zunimmt. Umgekehrt geht die dynamische Zustimmung davon aus, dass sich die Notwendigkeit der Verarbeitung personenbezogener Daten im Laufe der Zeit ändert, möglicherweise auf eine Weise, die zum Zeitpunkt der Veröffentlichung der vorhergehenden Version der Richtlinie nicht vorhersehbar gewesen wäre.

Diese Ansätze haben jedoch in der Praxis bislang versagt und sind für neu entstehende kontextsensitive smarte Umgebungen vor dem Hintergrund der oben beschriebenen Einschränkungen nur bedingt geeignet. Bestehende technische Ansätze für smarte Umgebungen sind vor allem im Kontext von offline Tracking Szenarien und IoT entstanden. Zwei davon sind: Fahrzeugtracking über Videoüberwachung (z.B. im Fall von Automatic Number Plate Recognition) und Mobile Location Analytics (z. B. Video/Wi-Fi/Bluetooth Tracking in Gebäuden).

Um Nutzern die Kontrolle über ihre privaten Informationen in kontextsensitiven IT-Umgebungen zu geben, wird eine agentenbasierte Architektur vorgeschlagen, um Interaktionen zwischen Agent und Datensammler zu spezifizieren, darunter auch ob und unter welchen Modalitäten Nutzerdaten genutzt werden sollten.[54] Jüngste Vorschläge setzen auf Register,[55] in denen Richtlinien und Präferenzen zur Datenerfassung für IoT-Geräte gesammelt und eingetragen, und von Privacy Assistant Apps[56] auf mobile Endgeräte bei Bedarf abgerufen werden.

All diese Vorschläge haben einen starken prototypischen Charakter. Weitere notwendige Schritte hin zu einem breiten Einsatz in vielfältigen Real-World-Szenarien müssen noch unternommen werden. Hier könnte beispielsweise die Handhabbarkeit derartiger Technologien mittels Usability-Studien erprobt und weiterentwickelt werden.

5.4 Nachweispflicht

Verarbeitet ein Verantwortlicher personenbezogene Daten auf Grundlage einer Einwilligung, so muss er gemäß Art. 7 Abs. 1 DSGVO im Streitfall nachweisen, dass die betroffene Person in die Verarbeitung eingewilligt hat. Die Datenschutz-Grundverordnung legt die Form für den Nachweis nicht fest, erfordert aber eine Einwilligungsform, die einen solchen Nachweis ermöglicht. Es ist davon auszugehen, dass Verantwortliche in der Praxis – nicht zuletzt auch, um sich vor zivilrechtlicher Haftung oder ordnungsrechtlichen Sanktionen zu schützen – die schriftliche Form präferieren werden, da diese die am besten dokumentierbare Einwilligungserklärung darstellt.

Gerade wenn es um elektronisch erteilte Einwilligungserklärungen geht, stellt sich das Problem des konkreten Nachweises. Wenn eine elektronische Protokollierung implementiert wird, dann werden in der Regel nur Metadaten gespeichert, die eigentliche Einwilligungserklärung ist bei einer elektronischen Einwilligung nicht körperlich und kann daher nicht Gegenstand einer Protokollierung sein. So müsste nicht nur der Umstand gespeichert werden, dass ein Nutzer zu einem bestimmten Zeitpunkt auf eine bestimmte Schaltfläche geklickt hat, sondern diese Interaktion auch in den Kontext der jeweils konkreten Seitendarstellung gesetzt werden. Es zeigt sich, dass in der Praxis lediglich Verfahren geschaffen werden können, in denen unter Berücksichtigung aller Umstände der Datenverarbeitung die Vermutung für die Erteilung einer Einwilligung spricht, da der Vorgang der Einwilligungserteilung praktisch nicht nachgewiesen werden kann. So spricht ein vom Verantwortlichen implementiertes Double-Opt-In-Verfahren und der protokollierte Zeitstempel für die Erteilung einer Einwilligung, ein bösgläubiger Verantwortlicher kann den Zeitstempel allerdings auch „von Hand“ im Protokoll gespeichert haben. Im Kern muss man also davon ausgehen, dass der Verantwortliche Verfahren, in denen es auf die Erteilung einer Einwilligung durch die betroffenen Personen ankommt, so zu implementieren hat, dass eine spätere Datenverarbeitung technisch und tatsächlich jedenfalls

unwahrscheinlich ist, wenn die betroffene Person nicht zuvor den Prozess der Einwilligungserteilung durchlaufen und die Einwilligung dabei erteilt hat.

5.5 Einwilligung von Kindern

Kindheit ist heute mediatisiert. Digitale Medien haben Einzug in das Leben von Kindern gehalten, wie aktuelle empirische Daten offenlegen. Sie zeigen eine stärkere Verfügbarkeit und wachsende Nutzungszahlen von Medien bei immer jüngeren Kindern. So stellt die aktuelle *KIM-Studie* fest, dass fast alle Kinder zwischen sechs und 13 Jahren (98 %) zuhause das Internet nutzen können. Gut zwei Drittel von ihnen zählen sich zu den Internetnutzern.[57] Täglich oder zumindest mehrmals wöchentlich überwiegende Tätigkeiten sind die Recherche über Suchmaschinen (65 %), das Verschicken von *WhatsApp*-Nachrichten (62 %) oder das Schauen von *YouTube*-Videos (56 %)[58]. Beliebteste soziale Medien der 14-24-Jährigen sind, laut *DIVSI-Studie*, *WhatsApp, YouTube* und *Instagram*.[59]

Die Zahlen belegen, dass Kinder weitläufig Zugang zu digitalen Medien haben und umfassender Datenverarbeitung unterliegen. Zu den typischen digitalen Medien, die bereits von Kindern genutzt werden, gehören verschiedenste Social-Media-Plattformen, aber auch andere onlinebasierte Dienstleistungen wie Cloud-Gaming Services, Multiplayerspiele, die Inanspruchnahme von Mikrotransaktionsdiensten sowie diverse Smartphone-Apps, zu denen eine Einwilligung erforderlich ist. Da Kinder aufgrund ihrer besonderen Verletzlichkeit und vor allem in der früheren Kindheit aufgrund der sich erst noch entwickelnden kognitiven Fähigkeiten, die für eine informierte Einwilligung notwendig sind, besonders schutzbedürftig sind, ist die Verarbeitung von personenbezogenen Daten von Kindern mit besonderen Anforderungen verbunden. Dies ist in Artikel 16 der UN-Kinderrechtskonvention[60] als ein „Recht auf Privatsphäre" und damit als expliziter Anspruch von Kindern allen Alters formuliert. Nach der Grundrechtecharta der Europäischen Union können Kinder sich sogar verfassungsrechtlich garantiert auf den Schutz ihres Privatlebens nach Art. 7 und den Schutz ihrer Daten nach Art. 8 GRCh sowie auf besonderen Schutz und Fürsorge nach Art. 24 GRCh berufen. Die Datenschutz-Grundverordnung regelt den Schutz von Kindern nur punktuell.[61] Für die Einwilligung durch Kinder legt Art. 8 DSGVO nur eine Altersgrenze bei einem Angebot von Diensten der Informationsgesellschaft fest.[62] Für alle übrigen Bereiche bedarf es der – individuell zu bestimmenden – Einsichtsfähigkeit des Kindes. Eine Einschränkung der Einwilligungsfähigkeit von Kindern fehlt in der Datenschutz-Grundverordnung, obwohl dies gerade bei besonderen Kategorien von Daten oder bei automatisierten Entscheidungen im Einzelfall zum Schutz der Kinder geboten wäre.[63]

Für die Internetnutzung durch Kinder ist zu beachten, dass Kinder – abseits der gesetzlichen Regelungen – verschiedenste Angebote, voran Social Media Angebote (wie WhatsApp, Instagram, Snapchat) nutzen, obwohl sie unter 16 Jahre sind, indem sie beispielsweise in der Praxis entweder ein höheres Alter angeben und gleichzeitig die betroffenen Eltern nicht notwendigerweise von dieser Praxis und ihren möglichen Folgen wissen müssen. Es wäre also nach Lösungen zu suchen, die diese Regulierungs-Praxis-Kluft sinnvoll aufgreifen und Formen des Schutzes von Kindern ermöglichen, die ihnen dennoch gesellschaftliche Partizipation auch in digitalen Umfeldern gewährleisten. Dies wird auch im schulischen Bereich relevant, wenn im Klassenverbund beispielsweise WhatsApp-Klassenchats genutzt werden und Kinder zur Nutzung dieser Plattformen eingeladen werden, ohne die sie wichtige Informationen für den Schulalltag nicht erhalten würden. Dabei wird zu leicht eine freiwillige Entscheidung im Sinne einer Kontrolle über ihre personenbezogenen Daten stückweise auch über institutionelle Sachzwänge und fehlende Informiertheit der betroffenen Schulen aufgegeben.

Defizite der Einwilligung in der Praxis

Als unerwünschte Nebenfolge kann an dieser Stelle noch ein drohender negativer Sozialisationseffekt angeführt werden: Die heute noch kindlichen und jugendlichen Nutzenden prägen die Nutzungskultur von morgen. Eine Gewöhnung an Schutzmechanismen, die praktisch wirkungslos bleiben, wäre geeignet, Gleichgültigkeit oder Fatalismus als Basismentalität der Nutzung digitaler Infrastrukturen anzuerziehen. Aus diesem Grunde sollte mit Einwilligungsverfahren bei Kindern und Jugendlichen ganz besonders sorgfältig umgegangen werden.

Kinder gehören zu einer besonders vulnerablen Personengruppe, da sie, wie oben beschrieben, je nach Alter nur bedingt Handlungsfolgen abschätzen können. Gerade hinsichtlich der Nutzung digitaler Medien bedarf es eines pädagogisch angemessenen Schutzhandelns der Eltern. Dieses ist unter anderem durch Art. 24 GRCh und die UN-Kinderrechtskonvention verbrieft, in denen etwa vorgesehen wird, dass kein Kind willkürlichen Eingriffen in seine Privatsphäre ausgesetzt werden darf und dass Kinder einen rechtlichen Schutz gegen derartige Eingriffe haben. Als besonders problematisch ist dabei zu erachten, dass Kinder neben möglichen Eingriffen in ihre Privatsphäre durch unüberlegte Einwilligungen in Datenverarbeitungsprozesse ferner Technologien ausgesetzt sind, die durch gezielte Designentscheidungen so gestaltet sind, dass Abhängigkeit erzeugt wird oder biologische Belohnungssysteme auf eine Art ausgenutzt werden, so dass einem suchtartigen Mediennutzungsverhalten Vorschub geleistet wird. Vor solchen Technologien, bei deren Gestaltung Anleihen aus der Captology – also jener Disziplin, welche sich mit computerbasierten Verhaltenssteuerungen beschäftigt – genommen werden, ist bei Kindern dringend abzuraten. Erforderlich wäre ferner die Anbringung deutlicherer Hinweise auf potenzielle Suchtrisiken.

5.6 Verhältnis der Einwilligung zu anderen Erlaubnistatbeständen

Die DSGVO enthält keine Aussage über das Verhältnis der Erlaubnistatbestände zueinander. Art. 6 Abs. 1 UAbs. 1 DSGVO vermittelt durch die Formulierung „mindestens“ den Eindruck, dass zur Rechtfertigung einer Datenverarbeitung auch mehrere Erlaubnistatbestände nebeneinander erfüllt sein können. Nach dieser Auslegung könnte der Verantwortliche sich mehrere Erlaubnistatbestände offenhalten und die Datenverarbeitung erst im Nachhinein etwa auf eine Interessenabwägung stützen, wenn die betroffene Person ihre Einwilligung in die Datenverarbeitung widerrufen hat. Dadurch würde aber das Widerrufsrecht der betroffenen Person ausgehöhlt werden, da trotz erfolgtem Widerruf der Einwilligung die Datenverarbeitung fortgesetzt würde.

Zudem würde sich eine solche Interpretation von Art. 6 Abs. 1 DSGVO auch auf das Recht auf Datenübertragung nach Art. 20 DSGVO auswirken. Dieses Recht setzt voraus, dass die Daten aufgrund einer Einwilligung nach Art. 6 Abs. 1 UAbs. 1 lit. a oder Art. 9 Abs. 2 lit. a DSGVO verarbeitet werden. Für die betroffene Person kann es unter Umständen bei der Einwilligung von zentraler Bedeutung gewesen sein, dieses Recht zu haben. Wenn der Verantwortliche aber nachträglich seine Datenverarbeitung auf eine Interessenabwägung stützt, nimmt er der betroffenen Person dieses Recht. Außerdem hat er in diesem Fall bei Erhebung der Daten der betroffenen Person nicht die notwendigen Informationen erteilt, die bei einer Berufung auf überwiegende berechtigte Interessen gegeben werden müssen. Obwohl er sie nach Art. 7 Abs. 3 Satz 3 DSGVO auf ihr Widerrufsrecht hingewiesen hat, führt er nach einem Widerruf die weitere Datenverarbeitung auf der Grundlage des gesetzlichen Erlaubnistatbestands fort.

Ein nachträglicher Wechsel des Erlaubnistatbestands würde einen Verstoß gegen den Grundsatz von Treu und Glauben nach Art. 5 Abs. 1 lit. a DSGVO darstellen. Danach

hat die Rechtsausübung des Verantwortlichen im Sinne der englischen Sprachfassung „fair" zu sein und darf keine der betroffenen Personen benachteiligen. Eine faire Datenverarbeitung muss daher zumindest umfassen, dass sich die betroffene Person sicher sein kann, dass ein Ausüben ihrer Rechte auch die gewünschten Rechtsfolgen hat, dass also eine Einwilligung das Recht zur Datenübertragung begründet und ein Widerruf der Einwilligung tatsächlich die zukünftige Datenverarbeitung unzulässig macht. Andernfalls würde der betroffenen Person Entscheidungsmacht suggeriert und diese später umgangen. Wenn ein Verantwortlicher seine Datenverarbeitung bereits auf die Erlaubnistatbestände der Art. 6 Abs. 1 UAbs. 1 lit. b oder f DSGVO stützen kann, missbraucht er daher das Vertrauen der betroffenen Person, wenn er zusätzlich eine Einwilligung verlangt.[64]

Nach alledem kann das Verhältnis zwischen Einwilligung und allen anderen Erlaubnistatbeständen nur so bestimmt werden, dass ein Verantwortlicher sich neben einer Einwilligung nicht zusätzlich auf einen gesetzlichen Erlaubnistatbestand berufen kann. Wenn er von der betroffenen Person eine Einwilligung einfordert, muss er sich auch auf die Regeln zu einer Einwilligung einlassen. Er muss dann vor allem einen Widerruf der Einwilligung gegen sich gelten lassen und kann nicht trotz des Widerrufs die Datenverarbeitung unter Berufung auf einen anderen gesetzlichen Erlaubnistatbestand fortsetzen.[65]

6 Handlungsempfehlungen

Sowohl die Regelungen als auch die Praktiken der datenschutzrechtlichen Einwilligung führen dazu, dass die Einwilligung ein Instrument ist, das die Umsetzung der Grundrechte auf Datenschutz und informationelle Selbstbestimmung nicht stärkt, sondern in vielen Fällen sogar gefährdet. Auf der Grundlage der bisherigen Erwägungen werden im Folgenden eine Reihe von Regelungs- und Gestaltungsvorschlägen aufgezeigt, die zum einen die notwendigen Voraussetzungen einer Einwilligung gewährleisten und zu weitgehende Folgen einer Einwilligung beschränken soll. Die Vorschläge beschränken sich auf die datenschutzrechtliche Einwilligung als solche und beziehen sich nicht auf sonstige Aspekte des Datenschutzes.[66]

6.1 Regelungsvorschläge

Hinsichtlich der Konkurrenz zu anderen Erlaubnistatbeständen sollte in der Datenschutz-Grundverordnung klargestellt werden, dass ein Verantwortlicher sich neben einer Einwilligung nicht zusätzlich auf einen gesetzlichen Erlaubnistatbestand berufen kann. Wenn er von der betroffenen Person eine Einwilligung einfordert, muss er sich auch auf die Regeln zu einer Einwilligung einlassen. Er muss dann vor allem einen Widerruf der Einwilligung gegen sich gelten lassen und kann nicht trotz des Widerrufs die Datenverarbeitung unter Berufung auf einen anderen gesetzlichen Erlaubnistatbestand fortsetzen; zudem muss er der betroffenen Person eine Übertragung ihrer Daten ermöglichen.[67]

Die Einwilligung sollte in mehreren Gründen beschränkt werden, um Missbrauch vorzubeugen: Die Datenschutz-Grundverordnung sollte ausdrücklich regeln, dass eine betroffene Person nicht wirksam in eine Datenverarbeitung einwilligen kann, die Rechte der betroffenen Person nach der Datenschutz-Grundverordnung beschränkt.

Das Risiko von Einwilligungen (Wahrscheinlichkeit des unzureichenden Verstehens möglicher Folgen und der umfassenden und langfristigen Datenverarbeitung und das Schadenspotential) von Kindern nach Art. 9 Abs. 2 lit. a DSGVO in die Verarbeitung von personenbezogenen Daten besonderer Kategorien ist bei Kindern unvertretbar hoch. Sie dürften im Regelfall die Bedeutung der Einwilligung nicht überblicken. So können Kinder noch zu wenig die künftigen Folgen einer Einwilligung gerade in die Verarbeitung solcher, besonders schützenwerter Daten erkennen und darüber frei und informiert entscheiden. Die Schwierigkeiten, nach einer positiven Einschätzung der Einwilligungsfähigkeit durch den Verantwortlichen die Datenverarbeitung in der Praxis wieder rückgängig zu machen und alle Daten bei allen Verantwortlichen löschen zu lassen, sind ebenfalls beträchtlich. Angesichts dieser Risiken sollte die wirksame Einwilligung eines Kindes in die Verarbeitung von personenbezogenen Daten besonderer Kategorien ausgeschlossen werden.[68]

Auch das Risiko von Einwilligungen von Kindern in ausschließlich auf einer automatisierten Verarbeitung — einschließlich Profiling — beruhenden Entscheidung nach Art. 22 Abs. 2 lit. c DSGVO ist immens. Die Wahrscheinlichkeit, dass ein Kind die Wirkungsweise, die Bedeutung, die Folgen und den möglichen Nachteil einer ausschließlich auf einer automatisierten Verarbeitung beruhenden Entscheidung nicht ausreichend erkennt und bewertet, und das Schadenspotential, das für das Kind aus dieser Datenverarbeitung erwachsen kann, sind besonders hoch. Um den Risiken für Kinder zu begegnen, sollte eine Einwilligung eines Kindes für eine auf einer automatisierten Verarbeitung – einschließlich Profiling – beruhenden Entscheidung

nach Art. 22 Abs. 2 lit. c DSGVO unterworfen zu werden, explizit ausgenommen werden.[69]

Eine Einwilligung sollte nach einer angemessenen Frist, die vom Risiko der Datenverarbeitung und den üblichen Verwendungsbedingungen der Einwilligung im Anwendungsbereich der Datenverarbeitung abhängig sein soll, ihre rechtliche Wirkung verlieren – und eventuell erneuert werden müssen.

Um eine Information der betroffenen Person sicherzustellen, die eine informationelle Selbstbestimmung durch Einwilligung sicherstellt, sollte die Datenschutz-Grundverordnung ausdrücklich bestimmen, dass

- diese Information sich auf die unmittelbar bevorstehende Datenerhebung bezieht und beschränkt,[70]
- die Information in verschiedenen Konkretisierungsgraden zur Kenntnis genommen werden kann (Symbol, Einseiter, ausführliche Erläuterung),
- in der Information ausdrücklich die Maßnahmen zur datenschutzgerechten Systemgestaltung nach Art. 25 Abs. 1 DSGVO und zu datenschutzfreundlichen Voreinstellungen erläutert werden,
- die Informationen und der Informationsprozess Teil der Datenschutz-Folgenabschätzung nach Art. 35 DSGVO sein muss.

Ein Verstoß gegen die Regelungen zur Einwilligung sollte ausdrücklich auch als Verstoß gegen den unlauteren Wettbewerb und als ungerechtfertigter Wettbewerbsvorteil gewertet werden.

6.2 Gestaltungsvorschläge

Jenseits von rechtlichen Regelungen sollte auf Defizite der datenschutzrechtlichen Einwilligung durch Änderungen in der Datenschutzpraxis der Verantwortlichen, der betroffenen Personen und sonstigen Stellen reagiert werden:

In allen Bildungsstätten sollte Kompetenz im Erkennen und im Umgang mit Datenschutzrisiken als Teil der Medienbildung erlernt und eingeübt werden. Dies gilt nicht nur für Schulen, sondern auch für Hochschulen und alle Institutionen der Bildung von Lehrenden. Für alle Bildungsstätten sollten Angebote gefördert werden, die sich explizit an Schüler und Studierende richten und die gezielt datenschutzgerecht gestaltet sind. Ein Zwang zur Einwilligung in kommerzielle Angebote, die Daten der Schüler und Studierenden zur Refinanzierung nutzen, muss ausgeschlossen werden.

Verantwortliche sollten nicht die Einwilligung in mehrere Zwecke gleichzeitig fordern. Die betroffene Person sollte die Möglichkeit haben, in bestimmte Datenverarbeitungen nicht einzuwilligen. Verantwortliche sollten das Instrument der Zertifizierung nutzen, so dass die betroffene Person „guten Gewissens“ in eine zertifizierte Datenverarbeitung einwilligen kann. Ohne kognitive Grenzen zu strapazieren, könnte eine betroffene Person gerade bei komplexen Datenverarbeitungsvorgängen auf die Prüfung von unabhängigen Instanzen vertrauen. Mit der Zertifizierung rückt entsprechend die Informierung von Nutzenden über die Vertrauenswürdigkeit von Organisationen in den Vordergrund. Staatliche Stellen sollten daher das Instrument der Zertifizierung stärker fördern und fordern.

Die Einwilligungspraxis ist bisher so gestaltet, dass die Einwilligung eine Hürde auf dem Weg zu den Gratifikationen der Nutzung eines Dienstes ist. Für die betroffene Person besteht kein wirkliches Interesse, die Datenschutzerklärungen zu lesen und die Datenschutz-Politik des Verantwortlichen zu verstehen. Diese negative Konstellation könnte der Verantwortliche schon dadurch aufheben, dass er mehrere Nutzungsmöglichkeiten zur Auswahl stellt, die auch andere psychologische Alternativen als „möchte nutzen“,

„möchte nicht nutzen“ enthalten. Denkbar wären etwa folgende Optionen, die den Nutzenden eine höhere Freiwilligkeit verschaffen würden: „ich willige ein und kann nutzen“, „ich lehne ab und kann nicht nutzen“, „ich möchte mich nicht informieren, möchte den Service aber dennoch nutzen“, „ich möchte zunächst über die wichtigsten Risiken informiert werden und dann entscheiden“, „ich fühle mich bereits ausreichend informiert“ und ähnliche Alternativen. Denkbar wäre auch eine generell zweistufige Abfrage, bei der die betroffene Person zuerst Angaben zum eigenen Informationsstand und Informationswunsch macht, dann entsprechende Informationen adaptiert präsentiert bekommt und dann einwilligen oder ablehnen kann.

7
Anhang

#	Webseite	Untersucht	Gültigkeits-datum der DS-Erklärung	Webseiten-Links
1	google.com	JA	15.10.2019	https://policies.google.com/privacy?hl=de#infodelete
2	youtu-be.com	identisch mit 1 Goog-le.com	15.10.2019	https://policies.google.com/privacy?hl=de#infodelete
3	google.de	identisch mit 1 Goog-le.com	15.10.2019	https://policies.google.com/privacy?hl=de#infodelete
4	face-book.com	JA	19.04.2018	https://de-de.facebook.com/about/privacy/legal_bases https://policies.google.com/privacy?hl=de#infodelete
5	amazon.de	JA	01.10.2019	https://www.amazon.de/gp/help/customer/display.html?ie=UTF8&nodeId=201909010&ref_=footer_privacy
6	wikipedia.org	JA	17.05.2018	https://foundation.wikimedia.org/wiki/Privacy_policy
7	ebay.de	JA	30.07.2019	https://www.ebay.de/help/policies/member-behavior-policies/datenschutzerklrung?id=4260#section12
8	bild.de	JA	06.01.2020	https://www.bild.de/corporate-site/datenschutz/datenschutz/artikel-datenschutz-54485502.bild.html###wt_ref=https%3A%2F%2Fm.bild.de%2Fcorporate-site%2Fdatenschutz%2Fdatenschutz%2Fartikel-datenschutz-54485502.bildMobile.html&wt_t=1578933822933
9	t-online.de	JA	"jeweils aktuell"	https://www.stroeerdigitalpublishing.de/index.html%3Fp=2614.html
10	ebay-kleinanzei-gen.de	JA	25.05.2018	https://themen.ebay-kleinanzeigen.de/datenschutzerklaerung/
11	web.de	identisch mit 13 gmx	13.01.2020	https://agb-server.web.de/datenschutz
12	instagram.com	identisch mit 4 face-book	19.04.2018	https://help.instagram.com/519522125107875
13	gmx.net	JA	13.01.2020	https://agb-server.gmx.net/datenschutz
14	spiegel.de	JA	22.05.2018	https://www.spiegel.de/extra/datenschutzerklaerung-so-gehen-wir-mit-ihren-daten-um-a-1207780.html
15	pornhub.com	JA	01.01.2020	https://www.pornhub.com/information#privacy
16	xhamster.com	JA	25.03.2019	https://xhamster.com/info/privacy
17	twitter.com	JA	01.01.2020	https://help.twitter.com/de/rules-and-policies/data-processing-legal-bases
18	goog-le.com.br	identisch mit 1 Goog-le.com	15.10.2019	https://policies.google.com/privacy?hl=de#infodelete
19	netflix.com	JA	24.04.2019	https://help.netflix.com/de/legal/privacyhttps://help.netflix.com/legal/privacy
20	focus.de	JA	22.01.2020	https://www.focus.de/intern/datenschutzerklaerung-datenschutzerklaerung-fuer-die-webseite-www-focus-de_id_6846331.html
21	paypal.com	JA	19.08.2019	https://www.paypal.com/de/webapps/mpp/ua/privacy-full?locale.x=de_DE
22	dhl.de	JA	03.02.2020	https://www.dhl.de/de/toolbar/footer/datenschutz.html
23	otto.de	JA	25.05.2018	https://www.otto.de/shoppages/service/datenschutz
24	welt.de	JA	06.09.2018	https://www.welt.de/services/article157550705/Datenschutzerklaerung-WELT-DIGITAL.html
25	sam-sung.com	JA	04.06.2019	https://www.samsung.com/de/info/privacy/

26	chip.de	JA	09.12.2019	https://www.chip.de/s_specials/Datenschutz-CHIP-Online_45829526.html#glossary-services
27	spacetoday.xyz	JA	nicht angegeben	https://spacetoday.xyz/privacy-policy
28	yahoo.com	JA	01.10.2019	https://www.verizonmedia.com/policies/ie/de/verizonmedia/privacy/index.html
29	idealo.de	JA	27.02.2019	https://www.idealo.de/preisvergleich/Datenschutz.html
30	merkur.de	JA	01.08.2019	https://www.merkur.de/ueber-uns/datenschutz/
31	live.com	JA	01.01.2020	https://privacy.microsoft.com/de-de/privacystatement
32	derwesten.de	JA	nicht angegeben	https://www.derwesten.de/datenschutz/
33	twitch.tv	JA	12.09.2019	https://www.twitch.tv/p/de-de/legal/privacy-notice/
34	outbrain.com	JA	23.05.2018	https://www.outbrain.com/legal/privacy#privacy-policy
35	chefkoch.de	JA	01.12.2019	https://www.chefkoch.de/magazin/datenschutz.html
36	taboola.com	JA	01.01.2020	https://www.taboola.com/privacy-policy
37	whatsapp.com	JA	24.04.2018	https://www.whatsapp.com/legal/#privacy-policy-information-we-collect
38	xnxx.com	JA	25.05.2018	https://info.xnxx.com/privacy_policy
39	reddit.com	JA	10.01.2020	https://www.redditinc.com/policies/privacy-policy-january-10-2020
40	immobilienscout24.de	JA	29.05.2018	https://www.immobilienscout24.de/agb/datenschutz.html
41	n-tv.de	JA	01.05.2018	https://www.n-tv.de/ntvintern/Datenschutzerklaerung-article15745191.html
42	mobile.de	JA	25.05.2018	https://www.mobile.de/service/privacyPolicy?lang=de
43	tagesschau.de	JA	03.12.2019	https://www.tagesschau.de/kontakt_und_hilfe/datenschutz/index.html
44	bing.com	identisch mit 31 live.com bzw. Microsoft	01.01.2020	https://privacy.microsoft.com/de-de/privacystatement
45	tz.de	JA	01.08.2019	https://www.tz.de/ueber-uns/datenschutz/
46	wetter.com	JA	23.01.2020	https://www.wetter.com/datenschutz/adsb/
47	telekom.com	JA	22.11.2019	https://www.telekom.com/de/telekom/datenschutzhinweis-1808
48	mydealz.de	JA	12.09.2019	https://www.mydealz.de/datenschutz
49	mediamarkt.de	JA	01.05.2018	https://www.mediamarkt.de/de/shop/datenschutzhinweis_shop.html#DSOnlineshop
50	livejasmin.com	JA	09.10.2019	https://www.livejasmin.com/de/privacy-policy#point3.7

Tabelle 7-1: Vollständige Liste aller Webseiten, deren Datenschutzerklärungen untersucht wurden (Quelle der Liste: https://www.similarweb.com/top-websites/germany/ - Zugriff: Dezember 2019)

Anmerkungen

[1] Gluck, J. et al. (2016): "How Short is Too Short? Implications of Length and Framing on the Effectiveness of Privacy Notices", Symposium on Usable Privacy and Security (SOUPS '16).

[2] Roßnagel, A. (2019): Kein „Verbotsprinzip“ und kein „Verbot mit Erlaubnisvorbehalt“ im Datenschutzrecht – Zur Dogmatik der Datenverarbeitung als Grundrechtseingriff. In: NJW – Neue Juristische Wochenschrift, Nr. 1-2, S. 1.

[3] Rössler, B. (2001): Der Wert des Privaten, Frankfurt a. M: Suhrkamp., S. 104.

[4] BVerfGE 65, 1 (42 ff.).

[5] z.B. Culnan, M. J., Armstrong, P. K. (1999): Information privacy concerns, procedural fairness, and impersonal trust: An empirical investigation. Organization science, 10(1), 104-115.

[6] z.B. Bol, N., Dienlin, T., Kruikemeier, S., Sax, M., Boerman, S. C., Strycharz, J., Helberger, N., De Vreese, C. H. (2018): Understanding the effects of personalization as a privacy calculus: analyzing self-disclosure across health, news, and commerce contexts. Journal of Computer-Mediated Communication, 23(6), 370-388.; Dienlin, T., Metzger, M. J. (2016): An extended privacy calculus model for SNSs: Analyzing self-disclosure and self-withdrawal in a representative US sample. Journal of Computer-Mediated Communication, 21(5), 368-383.

[7] z.B. Livingstone, S., Stoilova, M., Nandagiri, R. (2019): Children's data and privacy online: growing up in a digital age: an evidence review.; Taddicken, M. (2011): Selbstoffenbarung im Social Web. Ergebnisse einer Internet-repräsentativen Studie des Nutzerverhaltens in Deutschland. *Publizistik*, *56*, 281-303.

[8] S. hierzu 3.5.

[9] S. Forum Privatheit (2018): White Paper „Tracking“, Beschreibung und Bewertung neuer Methoden. Hrsg.: Friedewald, M. et al., Karlsruhe: Fraunhofer ISI, https://www.forum-privatheit.de/download/tracking/.

[10] Dix, in: Simitis/Hornung/Spiecker 2019, Art. 12 Rn. 6.

[11] a.A. Franck, L., in: Gola, P. (2018): Datenschutz-Grundverordnung-Kommentar. München: C.H. Beck. 2. Auflage, Art. 12 Rn. 30.

[12] Mantelero, Alessandro (2014): The future of consumer data protection in the E.U. Re-thinking the “notice and consent” paradigm in the new era of predictive analytics. In: Computer Law and Security Review 30 (6), 643-660.

[13] Erwägungsgrund 32 Satz 3 DSGVO.

[14] Taeger, J., in: Taeger, J., Gabel, D. (2019): DSGVO/BDSG-Kommentar. Frankfurt a.M.: dfv. 3. Aufl., Art. 7 Rn. 63.

[15] Schulz, S., in: Gola, P. (2018): Datenschutz-Grundverordnung-Kommentar. München: C. H. Beck. 2. Aufl., Art. 7 Rn. 21.

[16] S. z.B. Klement, J. H., in: Simitis, S., Hornung, G., Spiecker gen. Döhmann, I. (2019): Datenschutzrecht-Kommentar. Baden-Baden: Nomos, Art. 7 Rn. 58 ff.; Buchner, B., Kühling, J., in: Kühling, J., Buchner, B. (2018): DSGVO/BDSG-Kommentar. München: C. H. Beck. 2. Aufl., Art. 7 Rn. 48.

[17] S. z.B. KIM-Studie (2018): Kindheit, Internet, Medien, Basisuntersuchung zum Medienumgang 6- bis 13-Jähriger, https://www.mpfs.de/fileadmin/files/Studien/KIM/2018/KIM-Studie_2018_web.pdf.

[18] Poller, A., Waldmann, U., Vowé, S., Türpe, S. (2012): Electronic identity cards for user authentication—promise and practice. IEEE Security & Privacy, (1), 46-54.; Bender, J., Dagdelen, Ö., Fischlin, M., Kügler, D. (2012): Domain-specific pseudon-

ymous signatures for the German identity card. In International Conference on Information Security (pp. 104-119). Springer, Berlin, Heidelberg.

[19] Monika Ermert (2018): SINGLE SIGN-ON MADE IN GERMANY. Verimi, NetID oder ID4me? Welche der deutschen Single-Sign-on-Lösungen ist am vielversprechendsten? Golem.de erläutert die Unterschiede zwischen Verimi, NetID und ID4me. Golem, 11. September 2018. https://www.golem.de/news/single-sign-on-made-in-germany-wettstreit-zwischen-verimi-netid-oder-id4me-1809-136504.html.

[20] https://www.schufa.de/loesungen-unternehmen/fraudprevention/geschaeft-privatkunden/schufa-identitaetscheck-jugendschutz/.

[21] Rannenberg, K., Camenisch, J., Sabouri, A. (2015): Attribute-based Credentials for Trust. Identity in the Information Society, Springer.

[22] Bestehende empirische Untersuchungen fokussieren beispielsweise insb. auf die Lesbarkeit von Datenschutzerklärungen: Litman-Navarro, K. (2019): We Read 150 Privacy Policies. They Were an Incomprehensible Disaster., https://www.nytimes.com/interactive/2019/06/12/opinion/facebook-google-privacy-policies.html.

[23] S. hierzu kritisch Kap. 5.6.

[24] S. hierzu bereits Kap. 2.

[25] S. z.B. Deci, E. L., Ryan, R. M. (2008): Self-determination theory: A macrotheory of human motivation, development, and health. Canadian psychology/Psychologie canadienne, 49(3), 182.

[26] S. Kap. 2.

[27] Trope, Y., Liberman, N. (2010): Construal-level theory of psychological distance. Psychological review, 117(2), 440-463.

[28] *BVerfGE* 143, 246, Rn. 218f.

[29] *BVerfGE* 128, 226 (253).

[30] *BVerfG*, NJW 2015, 2485.

[31] *BVerfGE* 148, 267 (283f.).

[32] *BVerfG* (2. Kammer), NVwZ 2019, 959 (Rn. 15).

[33] *BVerfGE* 128, 226 (248).

[34] *BVerfGE* 128, 226 (249f.); verstärkt durch *BVerfG*, NJW 2015, 2485 (2486).

[35] Für Freiwilligkeit z.B. Klement, in: Simitis, S., Hornung, G., Spiecker gen. Döhmann, I. (2019): Datenschutzrecht-Kommentar. Baden-Baden: Nomos, Art. 7 Rn. 58 ff.; Buchner, B., Kühling, J., in: Kühling, J., Buchner, B. (2018): DSGVO/BDSG-Kommentar. München: C. H. Beck. 2. Aufl., Art. 7 Rn. 48. Gegen Freiwilligkeit z.B. Kühling, J., Martini, M. (2016): Die Datenschutz-Grundverordnung: Revolution oder

[36] Kühling, J., Buchner, B. (2016): Evolution im europäischen und deutschen Datenschutzrecht? In: EuZW – Europäische Zeitschrift für Wirtschaftsrecht, Nr. 12, 451; Buchner, B. (2016): Grundsätze und Rechtmäßigkeit der Datenverarbeitung unter der DS-GVO. In: DuD – Datenschutz und Datensicherheit, Nr. 40, S. 155.

[37] So Forderungen in Kontext der Evaluation der DSGVO – s. Roßnagel, A. (2020): Evaluation der Datenschutz-Grundverordnung, Verfahren – Stellungnahmen – Vorschläge. In: DuD – Datenschutz und Datensicherheit, Nr. 44, 291. Ob dies derzeit schon zulässig ist, ist umstritten, s. z.B. Paal, B., Hennemann, M. (2018): Datenschutz-Grundverordnung/Bundesdatenschutzgesetz-Kommentar. München: C. H. Beck. 2. Aufl., Art. 12 Rn. 38 ff.

[38] Roßnagel, A. (2019): Evaluation der Datenschutz-Grundverordnung aus Verbrauchersicht, Gutachten im Auftrag des Verbraucherzentrale Bundesverbands e.V.

(vzbv), S. 34. https://www.vzbv.de/sites/default/files/downloads/2019/12/04/19-11-26_gutachten_evaluation_dsgvo.pdf.

[39] S. Kap. 5.5.

[40] Custers, Bart (2016): Click here for consent forever: Expiry dates for informed consent. In: Big Data & Society 3 (1), 1-6.

[41] Litman-Navarro, K., We Read 150 Privacy Policies. They Were an Incomprehensible Disaster, https://www.nytimes.com/interactive/2019/06/12/opinion/facebook-google-privacy-policies.html; Linden, T., Khandelwal, Hamza, H., Fawaz K. (2019): The Privacy Policy Landscape After the GDPR, v3.

[42] We value your privacy ... now take some cookies:Measuring. the gdpr's impact on web privacy," in 26th Annual Network and Distributed System Security Symposium, NDSS 2019, San Diego, California, USA, February 24-27. The Internet Society.

[43] Artikel 29-Datenschutzgruppe (2018): Leitlinien für Transparenz gemäß der VO 2016/679. WP 260 rev. 01. Brüssel. S. 22 ff., https://www.ldi.nrw.de/mainmenu_Service/submenu_Links/Inhalt2/Artikel-29-Gruppe/wp260rev01_de.pdf

[44] Kelley, P.G., Cesca, L., Bresee, J., Cranor, L.F. (2010): Standardizing privacy notices: an online study of the nutrition label approach. In: Proceedings of the CHI, pp. 1573–1582. ACM.

[45] Cranor, L. F. (2012): Necessary but not sufficient: Standardized mechanisms for privacy notice and choice. J. on Telecomm. & High Tech. L., 10, 273.Clarke, N., Furnell, S., Angulo, J., Fischer-Hübner, S., Wästlund, E., Pulls, T. (2012): Towards usable privacy policy display and management. Information Management & Computer Security; Hansen, M. (2009): Putting Privacy Pictograms into Practice-a European Perspective. GI Jahrestagung, 154, 1-703.

[46] Tabassum, M., Alqhatani, A., Aldossari, M., Richter Lipford, H. (2018): Increasing user attention with a comic-based policy. In Proceedings of the CHI. ACM.

[47] World Wide Web Consortium. (2002): The platform for privacy preferences 1.0 (P3P1. 0) specification.

[48] Patrick, A.S., Kenny, S. (2003): From privacy legislation to interface design: implementing information privacy in human-computer interactions. In: Dingledine, R. (ed.) PET 2003. LNCS, vol. 2760, pp. 107–124. Springer, Heidelberg. https://doi.org/10.1007/978-3-540-40956-4 8.

[49] Ashley, P., Hada, S., Karjoth, G., Powers, C., Schunter, M. (2003): Enterprise privacy authorization language (EPAL). IBM Research, 30, 31.

[50] Azraoui, M., Elkhiyaoui, K., Önen, M., Bernsmed, K., De Oliveira, A. S., Sendor, J. (2014): A-PPL: an accountability policy language. In Data privacy management, autonomous spontaneous security, and security assurance (pp. 319-326). Springer, Cham.

[51] Ardagna, C. A., Cremonini, M., De Capitani di Vimercati, S., Samarati, P. (2008): A privacy-aware access control system. Journal of Computer Security, 16(4), 369-397.

[52] Kaye, J., Whitley, E.A., Lund, D., Morrison, M., Teare, H., Melham, K. (2015): Dynamic consent: a patient interface for twenty-first century research networks. Eur. J. Hum. Genet. 23(2), 141.

[53] S. z.B. Grimm, R., Roßnagel, A. (2000): P3P and the Privacy Legislation in Germany: Can P3P Help to Protect Privacy World-wide? htttp://www.w3.org/P3P.

[54] Kim, K. I., Hwang, H. S., Ko, H. J., Lee, H. K., Kim, U. M. (2006): Multi-policy access control considering privacy in ubiquitous environment. In 2006 international conference on hybrid information technology (Vol. 1, pp. 216-222). IEEE.

Anmerkungen

[55] Pappachan, P. et. al (2017): Towards Privacy-Aware Smart Buildings: Capturing, Communicating, and Enforcing Privacy Policies and Preferences. In Distributed Computing Systems Workshops (ICDCSW), 2017 IEEE 37th International Conference on, pages 193– 198. IEEE.

[56] Gassen, M., Fhom, H. S. (2016): Towards Privacy-preserving Mobile Location Analytics. In EDBT/ICDT Workshops; A. Das, M. Degeling, D. Smullen, and N. Sadeh. Personalized privacy assistants for the internet of things: An infrastructure for notice and choice in the internet of things. IEEE Pervasive Computing, 17(3):35– 46, Jul 2018; Das, A. et al. (2017): Satyanarayanan. Assisting users in a world full of cameras: A privacyaware infrastructure for computer vision applications. In 2017 IEEE Conference on Computer Vision and Pattern Recognition Workshops (CVPRW), pages 1387–1396.

[57] Medienpädagogischer Forschungsverbund Südwest (MPFS) (2019): KIM-Studie 2018. Kinder, Internet, Medien. Basisuntersuchung zum Medienumgang 6-13-Jähriger. Stuttgart, 9, 82.

[58] Medienpädagogischer Forschungsverbund Südwest (MPFS) (2019): KIM-Studie 2018. Kinder, Internet, Medien. Basisuntersuchung zum Medienumgang 6-13-Jähriger. Stuttgart, 33 f.

[59] Deutsches Institut für Vertrauen und Sicherheit im Internet (DIVSI) (2018): DIVSI U25-Studie: Euphorie war gestern. Die „Generation Internet" zwischen Glück und Abhängigkeit. Hamburg, 61.

[60] Diese gilt in Deutschland als einfaches Gesetz.

[61] S. Roßnagel, A. (2020): Der Datenschutz von Kindern in der DS-GVO, Vorschläge für die Evaluierung und Fortentwicklung. In: ZD – Zeitschrift für Datenschutz, Nr. 2, S. 88 ff.

[62] S. hierzu Kap. 3.5.

[63] S. hierzu z.B. Roßnagel, A., Geminn, C. (i.E.): Datenschutz-Grundverordnung verbessern! – Änderungsvorschläge aus Sicht der Verbraucher, DuD-Fachbeiträge, Wiesbaden: Springer Vieweg, S. 33 ff.

[64] S. hierzu Artikel 29-Datenschutzgruppe (2018): Leitlinien in Bezug auf die Einwilligung, WP 259 rev.01. Brüssel, S. 26; Roßnagel, A. in: Simitis, S., Hornung, G., Spiecker gen. Döhmann, I. (2019): Datenschutzrecht-Kommentar. Baden-Baden: Nomos, Art. 5 Rn. 47.

[65] S. hierzu auch Roßnagel (2018): Datenschutzgrundsätze – unverbindliches Programm oder verbindliches Recht?, Bedeutung der Grundsätze für die datenschutzrechtliche Praxis. In: ZD – Zeitschrift für Datenschutz, Nr. 8, S. 340.

[66] S. zur Verbesserung der DSGVO allgemein Roßnagel, A., Geminn, C. (i.E.): Datenschutz-Grundverordnung verbessern! – Änderungsvorschläge aus Sicht der Verbraucher, DuD-Fachbeiträge, Wiesbaden: Springer Vieweg.

[67] S. hierzu z.B. Roßnagel, A., Geminn, C. (i.E.): Datenschutz-Grundverordnung verbessern! – Änderungsvorschläge aus Sicht der Verbraucher, DuD-Fachbeiträge, Wiesbaden: Springer Vieweg, S. 94f.

[68] S. hierzu z.B. Roßnagel, A., Geminn, C. (i.E.): Datenschutz-Grundverordnung verbessern! – Änderungsvorschläge aus Sicht der Verbraucher, DuD-Fachbeiträge, Wiesbaden: Springer Vieweg, S. 96f.

[69] S. hierzu Roßnagel, A., Geminn, C. (i.E.): Datenschutz-Grundverordnung verbessern! – Änderungsvorschläge aus Sicht der Verbraucher, DuD-Fachbeiträge, Wiesbaden: Springer Vieweg, S. 108.

Anmerkungen

[70] S. näher Roßnagel, A., Geminn, C. (i.E.): Datenschutz-Grundverordnung verbessern! – Änderungsvorschläge aus Sicht der Verbraucher, DuD-Fachbeiträge, Wiesbaden: Springer Vieweg, S. 97f.

Anmerkungen

IMPRESSUM

Presse und Kommunikation:
Barbara Ferrarese, M.A.
Fraunhofer-Institut für System- und Innovationsforschung ISI
Breslauer Straße 48
76139 Karlsruhe

Telefon +49 721 6809-678
E-Mail presse@forum-privatheit.de

Projektkoordination:
Michael Friedewald
Fraunhofer-Institut für System- und Innovationsforschung ISI
Breslauer Straße 48
76139 Karlsruhe

Telefon +49 721 6809-146
Fax +49 721 6809-315
E-Mail info@forum-privatheit.de

www.isi.fraunhofer.de
www.forum-privatheit.de

Schriftenreihe:
Forum Privatheit und selbstbestimmtes Leben in der digitalen Welt
ISSN-Print 2199-8906
ISSN-Internet 2199-8914

1. Auflage
Juli 2020

Zitiervorschlag:
Roßnagel et al. (2020): White Paper Einwilligung. Möglichkeiten und Fallstricke aus der Konsumentenperspektive. Hrsg.: Michael Friedewald et al., Forum Privatheit und selbstbestimmtes Leben in der digitalen Welt, Karlsruhe: Fraunhofer ISI.

Dieses Werk ist lizenziert unter einer Creative Commons Namensnennung – Nicht kommerziell – Keine Bearbeitungen 4.0 International Lizenz.

forum <privatheit>
selbstbestimmtes_leben_in_der_digitalen_welt

GEFÖRDERT VOM

Bundesministerium für Bildung und Forschung

PROJEKTPARTNER

Fraunhofer

Natur Technik Kultur Gesellschaft
UNIKASSEL VERSITÄT

provet
Projektgruppe verfassungsverträgliche Technikgestaltung

UNIVERSITÄT DUISBURG ESSEN
Offen im Denken

EBERHARD KARLS UNIVERSITÄT TÜBINGEN
INTERNATIONALES ZENTRUM FÜR ETHIK IN DEN WISSENSCHAFTEN

LMU LUDWIG-MAXIMILIANS-UNIVERSITÄT MÜNCHEN

ULD
Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein