Kommunikation & Recht

Betriebs-Berater für
● Medien ● Telekommunikation ● Multimedia

2
K&R

24. Jahrgang **Februar 2021** Seiten 73 – 144

dfv Mediengruppe · Frankfurt am Main

Kommunikation & Recht

K&R 2/2021

RAin Frederike Kollmar, MLE und RAin Maya El-Auwad*

Grenzen der Einwilligung bei hochkomplexen und technisierten Datenverarbeitungen

Kurz & Knapp

In diesem Beitrag, der auf einen Vortrag bei der DSRI-Herbstakademie 2021 zurückgeht, werfen die Verfasserinnen erneut die Frage auf, inwieweit die Einwilligung die richtige und praktikable Rechtsgrundlage, insbesondere im Zusammenhang mit hochkomplexen und technisierten Verarbeitungen darstellen kann und ob ein Ausbalancieren nicht auch mit anderen Instrumenten des Datenschutzes möglich ist.

I. Einleitung

Die Einwilligung zählt zu den favorisierten Verarbeitungsgrundlagen im Datenschutz – haftet ihr doch der Ruf an, die Rechte der Betroffenen dank der Freiwilligkeit am besten zu schützen. Zugleich ermöglicht die Einwilligung den datenschutzrechtlich Verantwortlichen, personenbezogene Daten über gesetzlich legitimierte Zwecke hinaus zu verarbeiten. Sie wird daher gern als Schlüssel zu einem unbegrenzten Datenzugang verstanden und als solcher auch von Verantwortlichen gegenüber vermeintlich strengeren gesetzlichen Erlaubnistatbeständen bevorzugt.

Bei neuen und komplexen technologischen Entwicklungen, bei denen die Verantwortlichen mitunter selbst nicht genau vorhersagen können, welchen Zwecken die Verarbeitung dient, erweisen sich die notwendige Informiertheit und Bestimmtheit von Einwilligungen als problematisch. Ein alleiniger Fokus auf die Entscheidungsfreiheit des Individuums lässt dabei nicht nur den grundrechtlich geschützten Interessen der Verantwortlichen, sondern auch dem Gemeinwohlgedanken des Grundrechtsschutzes oft zu wenig Raum.

Die DSGVO selbst bietet wegen der deklarierten Technikneutralität auf den ersten Blick wenige Antworten auf komplexe hochtechnisierte Verarbeitungsszenarien. Bei genauerer Betrachtung lassen sich ihr aber durchaus Instrumente entnehmen, die bei risikoorientierter Betrachtung auch Datenverarbeitungen unter Einsatz innovativer Technologien, jenseits der Einwilligung, ermöglichen. Zudem bieten neue technische Lösungen zur Stärkung der Datensouveränität den Betroffenen Möglichkeiten, den Selbstdatenschutz zu stärken. Geht all dies Hand in Hand, wird Europa als Technologiestandort insgesamt gestärkt.

II. Historie und Grundlagen der Einwilligung

Die datenschutzrechtliche Einwilligung kann in Deutschland wie in Europa auf eine mehrere Jahrzehnte andauernde Geschichte zurückblicken. Bereits im „Gesetz zum Schutz vor Missbrauch personenbezogener Daten bei der Datenverarbeitung“[1] von 1977, dem ersten Bundesdatenschutzgesetz, fand sich in § 3 eine Regelung zur Einwilligung, allerdings lediglich für Datenverarbeitungen öffentlicher Stellen. Unternehmen konnten sich nur auf berechtigte Interessen oder die Vertragserfüllung als Erlaubnistatbestände berufen (§ 22). Mit dem Volkszählungsurteil des BVerfG[2] und der Entwicklung des Rechts auf informationelle Selbstbestimmung ist der Gedanke der aktiven Betätigung der Grundrechtsausübung in Form der Einwilligung entstanden.[3]

Die EU-Grundrechte-Charta (EU-GRCh) erkennt die Einwilligung in Art. 8 Abs. 2 S. 1 für den Schutz personenbezogener Daten explizit an. Sie soll als Ausdruck des Selbstbestimmungsrechts des Einzelnen im Zeitalter der Digitalisierung wirken.[4] Jedoch war sie bereits zuvor fester Bestandteil auch des europäischen Datenschutzrechts, war sie doch schon in der „Richtlinie zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr“ 95/46/EG (Datenschutz-Richtlinie bzw. DS-RL) anerkannt.

Schließlich löste die VO (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. 4. 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der RL 95/46/EG (Datenschutzgrundverordnung bzw. DSGVO) die Datenschutz-Richtlinie ab. Ziel der DSGVO war es, auf die zunehmenden Massen an Datenverarbeitungen personenbezogener Daten durch technologische Entwicklungen und Globalisierung zu reagieren und den technologischen Fortschritt zu begleiten, um das Risiko der Betroffenen, durch übermäßigen und unzulässigen Datenumgang benachteiligt zu werden, abzufedern. Dabei sollte vor allem der Grundsatz der Technikneutralität eine bedeutende Rolle spielen mit dem Ergebnis, dass die Verordnung Fragen zu aktuellen Themen wie „Big Data“,

* Der Beitrag geht auf einen Vortrag bei der DSRI-Herbstakademie 2021 zurück, der veröffentlicht wurde im Tagungsband von *Taeger* (Hrsg.), Den Wandel begleiten – IT-rechtliche Herausforderung der Digitalisierung, 2020. Er ist überarbeitet und aktualisiert zum Stand 7. 10. 2020. Mehr über die Autorinnen erfahren Sie auf S. VIII. Alle zitierten Internetquellen wurden zuletzt abgerufen am 7. 10. 2020.

1 BGBl. Teil I Nr. 7 vom 1. 2. 1977.

2 BVerfG, 15. 12. 1983 – BvR 209/83, BVerfGE 65, 1 - 71.

3 Vgl. dazu *Geiger*, NVwZ 1989, 35.

4 *Albrecht*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2019, Art. 6 Rn. 4. Umstritten ist allerdings, ob es sich bei Art. 8 Abs. 2 EU-GRCh um eine Konkretisierung der Schutzgewährleistung des Abs. 1 handelt, die Einwilligung also bereits einen Eingriff ausschließt, oder ob es sich bei Abs. 2 um eine Schrankenregelung handelt, die Einwilligung also einen Grundrechtseingriff rechtfertigt.

„Internet of things“ oder „Machine Learning“ augenscheinlich offenlässt – auch im Hinblick auf die Einwilligung in diese Phänomene betreffende Datenverarbeitungen.

Art. 7 DSGVO normiert die grundlegenden Erfordernisse, die an eine wirksame Einwilligung zu stellen sind.

Eine Art. 7 DSGVO vergleichbare Regelung gab es in der DS-RL und der entsprechenden deutschen Umsetzung im BDSG zuvor nicht.[5] Grund dafür war vor allem die Rechtsnatur als Richtlinie, die den Mitgliedsstaaten die Konkretisierung und Umsetzung der Regelungsinhalte – und damit auch der Einwilligung – und der auf ihr beruhenden Datenverarbeitungsvorgänge überließ. Nichtsdestotrotz waren auch schon in der DS-RL die zentralen Wirksamkeitsvoraussetzungen der Freiwilligkeit, Bestimmtheit und Informiertheit einer Einwilligung vorgegeben. Mit der DSGVO, die als europäische Verordnung Anwendungsvorrang gegenüber den nationalen datenschutzrechtlichen Regelungen genießt, war der europäische Gesetzgeber im Bereich des Datenschutzrechts erstmalig aufgefordert, alle als wesentlich erscheinenden Anforderungen an die Wirksamkeit einer Einwilligung selbst zu definieren.

Auch aktuell stehen die Gesetzgebungsaktivitäten auf europäischer Ebene nicht still. Nachdem die E-Privacy-Richtlinie die Notwendigkeit einer Einwilligung ausdrücklich im Bereich des Online-Marketings etabliert hat, wobei in Deutschland mangels wirksamer Umsetzungen Besonderheiten gelten, wird auch an einer unmittelbar in den Mitgliedstaaten geltenden E-Privacy-Verordnung gearbeitet – allerdings mit ungewissem Ausgang.

III. Anforderungen an die Einwilligung

Soll eine Verarbeitung personenbezogener Daten auf eine Einwilligung gestützt werden, sind die Voraussetzungen aus Art. 6 Abs. 1 S. 1 lit. a i. V. m. Art. 7 und Art. 4 Nr. 11 DSGVO zu erfüllen. Art. 4 Nr. 11 DSGVO definiert die Einwilligung als eine

„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.“

Mit Wirksamwerden der DSGVO haben sich die gesetzlichen Anforderungen an die Einwilligung verschärft. Das gilt einmal in formaler Hinsicht: So stellen nach Erwägungsgrund (ErwG) 32 zur DSGVO ein stillschweigendes Einverständnis, vorangekreuzte Kästchen oder die Untätigkeit keine wirksame Abgabe einer Einwilligungserklärung dar. Gänzlich ausgeschlossen ist die konkludente Einwilligung im Rahmen der Verarbeitung von Gesundheitsdaten, vgl. Art. 9 Abs. 1 lit. a DSGVO. Soll die Einwilligung mit anderen Erklärungen zusammen abgegeben werden, ist sie besonders hervorzuheben (Art. 7 Abs. 2 DSGVO). Weiter hat der Verantwortliche die betroffene Person bereits vor Abgabe der Einwilligungserklärung deutlich auf die jederzeitige Widerrufsmöglichkeit hinzuweisen und dieser Widerruf muss ebenso leicht möglich sein wie die Abgabe der Einwilligungserklärung selbst (Art. 7 Abs. 3 DSGVO). Der Nachweis der Abgabe einer diesen Anforderungen genügenden Einwilligung obliegt dem Verantwortlichen (Art. 7 Abs. 1 DSGVO, ErwG 42 DSGVO).

In materieller Hinsicht sind die Freiwilligkeit und die Informiertheit besonders hervorzuheben. Sie sollen dem Gedanken der Selbstbestimmung des Betroffenen Rechnung tragen. Für die Einwilligungsfähigkeit ist Art. 8 maßgeblich, der die Einwilligung von Kindern normiert. Beachtung verdient daneben vor allem Art. 9 DSGVO. Dieser fordert ein besonderes Maß an Bestimmtheit und Zweckgebundenheit, was sich jedoch dann faktisch kaum erfüllen lässt, wenn es sich um sensitive Daten der ersten Kategorie gemäß Art. 9 Abs. 1 DSGVO handelt. So lässt sich im Zusammenhang mit Big Data-Anwendungen, selbst im Falle einst anonymisierter Daten, kaum gänzlich ausschließen, dass aus dem verarbeiteten Datenbestand Rückschlüsse z. B. auf die politische Meinung oder auf die religiöse oder weltanschauliche Überzeugung hervorgehen.

Art. 7 Abs. 2 S. 2 DSGVO stellt klar, dass eine Einwilligung unwirksam ist, wenn sie unter Verstoß gegen die Vorgaben der Verordnung eingeholt worden ist.

Die zunehmenden Verschärfungen an die Anforderungen der Einwilligung und die Zulässigkeit von Datenverarbeitungsprozessen zeigt sich auch in der höchstrichterlichen Rechtsprechung sowie in der Bußgeldpraxis der Datenschutzbehörden. Die niederländische Datenschutzbehörde verhängte kürzlich ein 725 000-Euro-Bußgeld[6] gegen ein Unternehmen, das für die Zutrittskontrolle Fingerabdrücke seiner Mitarbeiter nutzte. Im Rahmen der Wirksamkeitsprüfung der Einwilligung nach Art. 9 Abs. 2 lit. a DSGVO (Verarbeitung biometrischer Daten) kam die Behörde zu dem Schluss, dass das Unternehmen seine Arbeitnehmer nicht ausreichend über die Rechtsgrundlage, die Möglichkeit des Widerrufs und die Freiwilligkeit der Einwilligung informiert hatte.

1. Kritik

Seit jeher steht die Einwilligung daher als Erlaubnistatbestand im datenschutzrechtlichen Diskurs in der Kritik.[7]

Bereits vor der DSGVO gab es auf europäischer Ebene eine breite Diskussion zu der Frage, wo die Grenzen der Einwilligung zu ziehen seien. Teilweise wurde beispielsweise bestritten, dass die Einwilligung eine Übermittlung in ein Drittland legitimieren könne, indem kein gleichwertiges Datenschutzniveau bestünde. Dadurch käme es im Übermittlungsland gem. Art. 52 Abs. 1 EU-GRCh zu einer Verletzung des Wesensgehalts von Art. 7, 8 EU-GRCh.[8] Die Diskussion hierum ist nach dem jüngsten Urteil des EuGH in der Rechtssache Schrems II[9] neu entfacht. Vergleichbare Diskussionen fanden auch in Deutschland statt, wo die Einwilligung als Ausdruck des Grundrechts auf informationelle Selbstbestimmung gesehen wird[10] und der Betroffene demnach gar nicht befugt sei, über eine Verletzung in den Wesensgehalt seines Grundrechts zu disponieren.[11]

Auch die DSGVO hat diese Entwicklungen im Auge gehabt und zumindest mit den Erfordernissen der Eindeutigkeit und Unmissverständlichkeit der Einwilligung der Opt-out-Einholung von Einwilligungen eine Absage erteilt, was der EuGH und der BGH nun auch in den „Planet49“-

5 *Kühling/Buchner*, in: Buchner/Kühling, DSGVO, 2. Aufl. 2018, Art. 7 Rn. 3.
6 Abrufbar unter https://autoriteitpersoonsgegevens.nl/nl/nieuws/boete-voor-bedrijf-voor-verwerken-vingerafdrukken-werknemers.
7 *Buchner/Kühling*, in: Kühling/Buchner (Fn. 5), Art. 7 Rn. 10.
8 Positionspapier des ULD zum Safe-Harbor-Urteil des EuGH v. 6. 10. 2015 – C-362/14 v. 14. 10. 2015 unter 3. a.
9 EuGH, 6. 7. 2020 – C-311/18, K&R 2020, 588 ff.
10 *Kühling*, in: Wolff/Brink, BDSG, 19. Aufl. 2017, § 4a Rn. 1.
11 Positionspapier des ULD zum Safe-Harbor-Urteil des EuGH v. 6. 10. 2015 – C-362/14 v. 14. 10. 2015 unter 3. a.

Entscheidungen[12] bestätigt haben. Mit Wirksamwerden der DSGVO muss eine Verarbeitung personenbezogener Daten aufgrund einer Einwilligung zudem die in Art. 5 DSGVO niedergelegten Grundsätze erfüllen. Auch hier kann sich der Verantwortliche nicht von seinen datenschutzrechtlichen Pflichten einer Abwägung der sich gegenüberstehenden Interessen entledigen.

Trotzdem stellt sich insbesondere bei hochkomplexen und technisierten Datenverarbeitungsprozessen zunehmend die Frage, ob die Anforderungen an die Einwilligung faktisch überhaupt erfüllt werden können oder ob die Einwilligung als Grundlage für eine Datenverarbeitung von vornherein fragwürdig ist.

Denn gerade die vielbeschworene Datensouveränität des Einzelnen, der sich ein klares Bild über die Bedeutung und das Ausmaß seiner Einwilligung machen können soll und anschließend selbstbestimmt und frei von jeglichen Zwängen eine Entscheidung treffen soll, stellt in vielen Konstellationen nur noch eine „Fiktion“[13] dar: Immer häufiger sind sich die Betroffenen der Tragweite ihrer Entscheidungen und der Auswirkungen, die diese auch auf ihr Persönlichkeitsrecht haben, nicht mehr bewusst und können es auch gar nicht mehr sein.

2. Freiwilligkeit

Die Freiwilligkeit der Einwilligung ist nicht erst seit Geltung der DSGVO eine der zentralen Voraussetzungen für die Wirksamkeit der datenschutzrechtlichen Einwilligung. Sie setzt voraus, dass die Einwilligung ohne Druck oder Zwang auf den Betroffenen erklärt werden soll.[14] ErwG 42 S. 5 zur DSGVO konkretisiert dieses Erfordernis, indem er festhält, dass „nur dann davon ausgegangen werden (soll), dass (die betroffene Person) ihre Einwilligung freiwillig gegeben hat, wenn sie eine echte oder freie Wahl hat und somit in der Lage ist, die Einwilligung zu verweigern oder zurückzuziehen, ohne Nachteile zu erleiden.“

ErwG 43 zur DSGVO benennt als Ausschlusskriterium für die Freiwilligkeit der Einwilligung „ein klares Ungleichgewicht“ und zeigt beispielhaft die Konstellation auf, dass es sich bei dem für die Verarbeitung Verantwortlichen um eine Behörde handelt. Doch ist die Grenze, welche Druck oder Zwang konstituiert, nicht immer sofort ersichtlich. Das Kriterium des Ungleichgewichts kann etwa auch bei übermäßigen finanziellen Anreizen zum Tragen kommen.[15] Auch selbstbestimmte Einwilligungserklärungen können nicht „freiwillig“ erfolgen und damit als unwirksam gelten, wenn die betroffene Person keine wirkliche Wahlmöglichkeit in Form einer vernünftigen Alternative hat, etwa den Verzicht auf die Abgabe der Einwilligung. Gleichzeitig scheint es unangemessen, für bestimmte Konstellationen stets und pauschal von einem die Unwirksamkeit auslösenden Ungleichgewicht auszugehen. Dagegen spricht auch die Tatsache, dass nach ErwG 155 zur DSGVO gerade für das Paradebeispiel eines Über-/Unterordnungsverhältnisses, nämlich das Arbeitsverhältnis, die Einwilligung als zulässiger Verarbeitungstatbestand gesehen wird.

Ergänzende Vorgaben zur Bestimmung der Freiwilligkeit finden sich in Art. 7 Abs. 4 DSGVO und dem sogenannten Kopplungsverbot, das jedoch nicht absolut gilt, sondern lediglich eine besondere Prüfpflicht für Fälle fordert, in denen eine vertragliche Leistung von der Abgabe einer Einwilligung abhängig gemacht werden soll.[16] Auch ErwG 43 zur DSGVO stellt für die Beurteilung der Freiwilligkeit der Einwilligung konsequenterweise auf den „speziellen Fall“ ab und etabliert damit die Einzelfallprüfung. Damit spielen verschiedenste Faktoren bei der Beurteilung der Freiwilligkeit eine Rolle, so etwa auch die konkrete Ausgestaltung der Einwilligung.[17]

3. Informiertheit

Das Erfordernis der Informiertheit greift das grundrechtliche Konzept der Selbstbestimmtheit auf – ohne Eingriff.[18] Die Umstände der Datenverarbeitung sollen so verständlich aufgearbeitet werden, dass eine Willensbildung möglich ist. Die Betroffenen müssen abschätzen können, welche Auswirkungen die Erteilung einer Einwilligung für sie hat, sie müssen die Umstände der Datenverarbeitung und die Tragweite ihrer Einwilligung eindeutig und klar erkennen können.[19] Denn nur so ist es Betroffenen überhaupt erst möglich, zu einer freiwilligen Entscheidung zu gelangen. Während etwa im Rahmen der Interessenabwägung allein die Verantwortlichen ihre Grundrechtspositionen mit denen der betroffenen Personen abzuwägen und für diese die Verantwortung zu tragen haben, ist für die Erreichung eines gleichwertigen Schutzniveaus unter Rückgriff auf die Einwilligung zwingend, die betroffene Person vor Abgabe der Erklärung in die Lage zu versetzen, sich ein klares Bild über Bedeutung und Ausmaß der Entscheidung zu machen, um diese Abwägungsentscheidung für sich selbst vornehmen zu können. Dazu benötigt sie zumindest Kenntnis von der Identität der Verantwortlichen, Informationen zum Zweck sowie zum datenschutzrechtlichen Widerrufsrecht. Ebenso sind Angaben über die Risiken und möglichen Folgen, wie zum Beispiel eine Datenübermittlung an Dritte, erforderlich.

Der Grundsatz der Einwilligung „in informierter Weise“ (Art. 4 Nr. 11 DSGVO) ist dabei eng mit dem Transparenzgebot aus Art. 7 Abs. 2 S. 1 DSGVO verbunden, wonach „das Ersuchen um Einwilligung in verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache so zu erfolgen (hat), dass es von den anderen Sachverhalten klar zu unterscheiden ist“. Die Informationen müssen also auch für einen durchschnittlichen Verbraucher ohne besondere juristische Vorbildung verständlich sein.[20]

Für den Fall, dass besondere Kategorien personenbezogener Daten, wie etwa Gesundheitsdaten, im Sinne des Art. 9 Abs. 1 DSGVO verarbeitet werden, müssen zudem auch dieser Umstand und die konkreten Daten der betroffenen Person deutlich kommuniziert werden. Das folgt schon aus der Tatsache, dass Art. 9 Abs. 2 lit. a DSGVO die „ausdrückliche“ Einwilligung in die Verarbeitung dieser Daten vorsieht.

IV. Grenzen individueller Entscheidungsfreiheit bei hoch komplexen und technisierten Verarbeitungsvorgängen

Grundsätzlich liegt der Einwilligung also die Wertung zugrunde, dass der Betroffene im konkreten Fall selbst ent-

12 EuGH, 1. 10. 2019 – C-673/17, K&R 2019, 705 ff.
13 *Simitis*, in: Simitis, BDSG, 8. Aufl. 2014, § 4a Rn. 1 ff.
14 *Schulz*, in: Gola (Hrsg.), DSGVO, 2. Aufl. 2018, Art. 7 Rn. 21.
15 *Schulz*, in: Gola (Fn. 14), Art. 7 Rn. 21. Zum Kopplungsverbot in der DSGVO auch *Spindler/Dalby*, in: Spindler/Schuster (Hrsg.), DSGVO, 4. Aufl. 2019, Art. 7 Rn. 14.
16 *Schulz*, in: Gola (Fn. 14), Art. 7 Rn. 26.
17 *Buchner/Kühling*, in: Kühling/Buchner (Fn. 5), Art. 7 Rn. 45.
18 *Simitis*, in: Simitis/Hornung/Spiecker gen. Döhmann (Fn. 4), Art. 7 Rn. 72.
19 *Heckmann/Paschke*, in: Ehmann/Selmayr, DSGVO, 2. Aufl. 2018, Art. 7 Rn. 58.
20 *Buchner/Kühling*, in: Kühling/Buchner (Fn. 5), Art. 7 Rn. 60.

scheiden können soll, ob er das Risiko des Zugriffs auf seine personenbezogenen Daten tragen möchte. Die Einwilligung soll ja gerade auch solche Datenverarbeitungsvorgänge legitimieren, für die keine gesetzliche Erlaubnis vorliegt. Die Herausforderung liegt darin, den Betroffenen in die Lage zu versetzen – wenn die sonstigen Wirksamkeitsvoraussetzungen erfüllt sind – eine Entscheidung nach seinen Präferenzen und seiner Risikobereitschaft zu treffen. Trotz der zentralen Rolle der Selbstbestimmung der betroffenen Person für den Schutz personenbezogener Daten, die sich auch in der Erwähnung an erster Stelle in Art. 8 Abs. 2 der EU-GRCh widerspiegelt, können die Anforderungen der Freiwilligkeit und Informiertheit in der Praxis aber allzu häufig faktisch nicht erfüllt werden. Gerade bei komplexen Datenverarbeitungsprozessen, die von unverständlichen und überlangen Datenschutzerklärungen begleitet werden und selten die Transparenzanforderungen der Klarheit und Einfachheit erfüllen, wird das Selbstbestimmungselement der betroffenen Person ernsthaft in Frage gestellt. Anzahl und Komplexität der dem Einzelnen abverlangten Entscheidungen sowie die Unabsehbarkeit der Auswirkungen dieser Entscheidung drohen bei neuen, hochtechnisierten Anwendungen dazu zu führen, dass der Einzelne mit dieser Entscheidung überfordert wird; und Verantwortliche vergessen bei einem Rückgriff auf die Einwilligung allzu oft, dass sowohl die europäische Grundrechtecharta als auch die DSGVO fordern, jeden Grundrechtseingriff, unabhängig von der gewählten Rechtsgrundlage, einer Verhältnismäßigkeitsprüfung zu unterziehen.

Unter anderen hat etwa die Datenethikkommission der Bundesregierung in ihrem Gutachten vom 23. 10. 2019 angemahnt, das „dass der Einzelne durch Anzahl und Komplexität der ihm abverlangten Entscheidungen bezüglich einer datenschutzrechtlichen Einwilligung ebenso wie durch die Unabschätzbarkeit aller Auswirkungen einer Datenverarbeitung systematisch überfordert wird".[21] Konsequenz sei ein „Vertrauensverlust" in der Bevölkerung darin, dass der Staat hinreichende rechtliche Rahmenbedingungen schaffe, in denen sich jeder „sicher und relativ sorglos bewegen" könne, ohne die Zufügung erheblicher Schäden zu befürchten. Ein unsachgemäßer Umgang mit dem Rechtsinstitut der Einwilligung kann damit letztlich innovationshemmend wirken. Die Datenethikkommission fordert dann aber nur eine AGB-ähnliche Prüfung der Einwilligung.[22]

Gleichzeitig droht bei einem ausschließlichen Rückgriff auf die Einwilligung als Ausdruck individueller Entscheidungsfindung das Datenschutzniveau insgesamt abzusinken, da sie zwar zu einer Vielzahl von Individualentscheidungen führt, jedoch wegen des alleinigen Fokus auf Individualinteressen nicht auch zwingend dazu, dass eine Entscheidung auch dem Interesse der kollektiv Betroffenen dient. Denn der Einzelne, der eine Entscheidung für sich selbst treffen muss, wird dadurch noch nicht in die Lage versetzt, deren Auswirkungen für potenziell von der individuellen Entscheidung beeinträchtigte Dritte zu erkennen. Das hat auch der Gesetzgeber erkannt und in Art. 9 Abs. 2 lit. a 2. HS DSGVO einen vollständigen bzw. teilweisen Ausschluss eines Rückgriffs auf die Einwilligung auf Grundlage europarechtlicher oder nationaler Rechtsvorschriften vorgesehen. Das ist jedenfalls denkbar, wenn die Verarbeitung besonderer Kategorien personenbezogener Daten diskriminierende Wirkung für andere hat oder sonst Rechte Dritter beeinträchtigt. Verbindet sich damit eine automatisierte Entscheidung im Sinne von Art. 22 DSGVO, ist wegen Art. 9 DSGVO zugleich der Rückgriff auf vertragliche Zwecke (als weitere Form des Ausdrucks individueller Entscheidungsfindung), wie ansonsten von Art. 22 Abs. 2 DSGVO vorgesehen, versperrt, wenn die Entscheidung auf besonderen Kategorien personenbezogener Daten fußt.[23]

Daran ändert auch die als Teil der „Strategie für einen digitalen Binnenmarkt" verabschiedete „RL (EU) 2019/770 des Europäischen Parlaments und des Rates vom 20. 5. 2019 über bestimmte vertragsrechtliche Aspekte der Bereitstellung digitaler Inhalte und digitaler Dienstleistungen"[24] (Digital-RL) nichts, die den Ansatz einer europäischen Harmonisierung im Bereich von Verträgen über die Bereitstellung digitaler Inhalte oder digitaler Dienstleistungen zum Ziel hat und ihrem Anwendungsbereich nach auch solche Verträge umfasst, bei denen die Gegenleistung des Verbrauchers aus personenbezogenen Daten besteht (Art. 3).[25] Gemäß ErwG 24 zur Richtlinie soll mit der Erweiterung der Gegenleistung auf personenbezogene Daten lediglich sichergestellt werden, dass Verbraucher im Zusammenhang mit solchen Geschäftsmodellen Anspruch auf vertragliche Rechtsbehelfe haben. Die datenschutzrechtliche Rechtfertigungsgrundlage für die Verarbeitung der personenbezogenen Daten wird dadurch aber nicht vorweggenommen. Eine Verarbeitung personenbezogener Daten im Zusammenhang mit einem Vertrag, der in den Anwendungsbereich der Digital-RL fällt, ist daher weiterhin nur rechtmäßig, wenn sie mit den Bestimmungen der DSGVO im Einklang steht (ErwG 38).

V. Antworten der DSGVO

1. Anonymisierung

Eine absolute Anonymisierung mit der Folge, dass eine Verarbeitung gänzlich aus dem Anwendungsbereich der DSGVO fällt, dürfte schon wegen der technischen Möglichkeiten der De-Anonymisierung praktisch nicht immer möglich sein, ist von der DSGVO aber auch nicht gefordert. Vielmehr ist gemessen am Stand der Technik zu fragen, ob eine Re-Identifizierung praktisch nur mit unverhältnismäßigem Aufwand an Zeit, Kosten und Arbeitsaufwand möglich ist.

2. Ausweichen auf sonstige Rechtsgrundlagen

Wie gezeigt stellt die Einwilligung den Verantwortlichen gerade in komplexen Verarbeitungskonstellationen vor die kaum zu bewältigende Herausforderung, umfassend, aber zugleich in einer für den Betroffenen verständlichen Weise zu informieren. Gelingt ihm dies nicht, ist die Einwilligung unwirksam (Art. 7 Abs. 2 S. 2 DSGVO). Aber selbst wenn eine Einwilligung sämtliche Anforderungen erfüllt, ist sie doch gemäß Art. 7 Abs. 3 DSGVO stets frei widerrufbar. Die Widerruflichkeit gilt zwar nur ex nunc, also erst ab dem Zeitpunkt, an dem der Widerruf erfolgt. Allerdings ist mit

21 Datenethikkommission, Gutachten vom 23. 10. 2019, S. 96, abrufbar unter https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/it-digitalpolitik/gutachten-datenethikkommission.html.

22 Datenethikkommission (Fn. 21), S. 96.

23 *Schneider*, ZD 2017, 303, 306.

24 Abrufbar unter https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:32019L077.

25 *El-Auwad*, Gewährleistung beim Download von Musik, Videos, Apps – Folgen der EU-Richtlinie zur Bereitstellung digitaler Inhalte und Dienstleistungen, abrufbar unter https://www.haerting.de/neuigkeit/gewaehrleistung-beim-download-von-musik-videos-apps-folgen-der-eu-richtlinie-zur-bereitstellung-digitaler-inhalte-und-dienstleistungen.

erfolgtem Widerruf die Verarbeitung unverzüglich zu beenden, was oft nur schwer umzusetzen ist, denkt man an Machine Learning, sogar unmöglich sein kann.[26] Je komplexer und technisierter die Verarbeitung also ist, desto weniger eignet sich die Einwilligung als taugliche Rechtsgrundlage.[27]

Die Einwilligung ist jedoch nach dem Gesetz weder die vorzugswürdige[28] noch die einzige mögliche Rechtsgrundlage. Das ergibt sich bereits aus Art. 8 Abs. 2 EU-GRCh, aber auch der Wortlaut von Art. 6 DSGVO geht dahin. Der Verantwortliche ist also grundsätzlich erst einmal frei, ob er eine Einwilligung einholen, oder die Verarbeitung personenbezogener Daten auf eine sonstige Rechtsgrundlage aus Art. 6 DSGVO stützen will. Geht es um innovative Technologien, kommen dann berechtigte Interessen und Vertrag in Betracht, die zudem eher geeignet sind, einen schonenden Ausgleich zwischen den Interessen der Betroffenen und der Verantwortlichen sowie sonstiger Dritter zu ermöglichen.

3. Zweckänderung und Kumulation von Rechtsgrundlagen

Der Wortlaut von Art. 6 Abs. 1 DSGVO deutet zudem darauf hin, dass die Rechtsgrundlagen in Art. 6 Abs. 1 nicht nur gleichrangig zueinander sind, sondern auch gleichzeitig nebeneinander verwirklicht werden können.[29] Dass ein aus Sicht des Betroffenen einheitlicher Verarbeitungsvorgang zugleich auf mehrere Rechtsgrundlagen gestützt werden kann, dürfte spätestens seit dem Urteil des EuGH in der Rechtssache Fashion-ID[30] als geklärt gelten. Denn auf die Vorlage, auf wessen berechtigte Interessen bei einer gemeinsamen Verantwortlichkeit abzustellen ist, konstatierte der EuGH, dass jeder an einer Verarbeitung Beteiligte seine Rechenschaftspflichten selbst erfüllen müsse. Für die Frage der Rechtmäßigkeit der Verarbeitung folgert er daraus, dass jeder Akteur einer gemeinsamen Verarbeitung jeweils ein eigenes berechtigtes Interesse nachweisen müsse. Das Urteil, das sich allerdings noch auf die Datenschutz-Richtlinie bezieht, zeigt zudem, dass es in bestimmten Konstellationen durchaus auf eine phasenweise Betrachtung von Verarbeitungsvorgängen, auch bei gleichbleibenden Zwecken, ankommen kann. Denn hieran sind Umfang und Reichweite der gemeinsamen Verantwortlichkeit zu messen.[31] Sofern hierüber vorab transparent informiert wird, ist daher auch eine Kumulation von beispielsweise Einwilligung und berechtigten Interessen möglich.

Zwar ist es möglich, die Einwilligung, auch für mehrere Verantwortliche zugleich abzufragen. Um der Nachweispflicht zu genügen, sollten sich Verantwortliche aber nicht auf vertragliche Zusicherungen anderer, ebenfalls an einer Verarbeitung beteiligten Akteure zum Einholen einer solchen Einwilligung verlassen. Denn eine solche vertragliche Zusicherung begründet allenfalls Ausgleichsansprüche im Innenverhältnis, lässt die gesamtschuldnerische Haftung im Außenverhältnis aber nicht entfallen, wenn die Einwilligung entgegen der vertraglichen Abrede nicht ordnungsgemäß eingeholt wird. Auch deshalb kann es ratsam sein, Verarbeitungen nicht nur auf eine einzige Rechtsgrundlage zu stützen.

In komplexen Verarbeitungskonstellationen, in denen Daten zu einem anderen Zweck weiterverarbeitet werden, als zu dem sie ursprünglich erhoben wurden, kommt Art. 6 Abs. 4 DSGVO und dem Kompatibilitätstest besondere Bedeutung zu.

4. Risikobasierter Ansatz

Die begrenzte Eignung der Einwilligung, hochkomplexe Verarbeitungskonstellationen zu rechtfertigen, stellt Systemarchitekten wie Rechtsanwender vor die Herausforderung, Potenzial und Risiken angemessenen auszutarieren.

Vor diesem Hintergrund kommt auch dem Gedanken des Datenschutzes durch Technikgestaltung, insbesondere den Grundsätzen des privacy by design und privacy by default, kaum zu überschätzende Bedeutung zu. Daher sollten angesichts der Schwierigkeiten hinsichtlich der Verteilung der Verantwortlichkeit und der Durchsetzung von Betroffenenrechten die Nutzung pseudonymisierter Daten und der Einsatz von DSGVO-konformen Datenspeicheroptionen angestrebt werden. Ein risikobasierter Ansatz, wie in der DSGVO formuliert, ist für eine innovationsoffene Gesamtbetrachtung notwendig. Andernfalls droht Europa seine Chancen und seine Einflussmöglichkeit in dem Zukunftsmarkt langfristig zu verlieren.

Aus verfahrensrechtlicher Sicht bieten schließlich Konsultationen, Erarbeitung von Verhaltensregeln und Prüfverfahren der Kommission geeignete Instrumente, Grundrechtsschutz und Innovationsinteresse jeweils zu mehr Wirksamkeit zu verhelfen.

VI. Antworten der Praxis

Derzeitige technische Bestrebungen haben im Blick, dass Betroffene den Schutz ihrer personenbezogenen Daten und ihrer Privatsphäre in der Theorie hochschätzen, tatsächlich aber wenig unternehmen, um die eigenen Daten aktiv zu schützen und diese häufig leichtfertig und freiwillig preisgeben. Dieses widersprüchliche, unter dem Begriff „privacy paradox“[32] bekannte Verhalten spricht unter anderem dafür, dass viele Betroffene die langfristigen Risiken ihrer Zustimmung nur schwer bewerten können bzw. häufig gar nicht wissen, ob und in welchem Umfang ihre Daten tatsächlich verarbeitet werden. Hinzu kommen wahrscheinlich eine Scheu vor dem Aufwand, sich mit datenschutzrechtlichen Risiken für die eigene Privatsphäre ernsthaft auseinanderzusetzen sowie die Unkenntnis darüber, welche datenschutzfreundlichen Alternativen bestehen.

Erwähnenswert im Rahmen einwilligungsbasierter Datenverarbeitungsprozesse sind die – zumeist technischen – Möglichkeiten für die Betroffenen, selbst Maßnahmen zum Datenschutz zu treffen. In Rede stehen dabei vor allem Datenmanagement- und Datentreuhandsysteme. Etwaige Bedenken, dass dadurch die Verantwortung für den Datenschutz unsachgemäß verlagert werden könnte, sind unberechtigt: Die Datenschutzgesetze sind eindeutig, was die Adressaten der datenschutzrechtlichen Pflichten betrifft.

Zu den Datenmanagementsystemen werden Anwendungen zur vereinfachten Einwilligungsverwaltung gezählt, wie z. B. Dashboards, aber auch KI-Tools, die individuelle Nutzerpräferenzen automatisch umsetzen (sog. Daten-

26 *Niemann/Kevekordes*, CR 2020, 17, 23.
27 *Veil*, NVwZ, 2018, 686, 688.
28 A. A. *Frenzel*, in: Paal/Pauly, DSGVO, 2. Aufl. 2018, Art. 6 Rn. 10; wie hier *Schulz*, in: Gola (Fn. 14), Art. 6 Rn. 10; *Schantz*, in: Simitis/Hornung/Spiecker gen. Döhmann (Fn. 4), Art. 6 Rn. 11 f.; *Taeger*, in: Taeger/Gabel, DSGVO, 3. Aufl. 2019, Art. 6 Rn. 23; *Plath*, DSGVO, 3. Aufl. 2018, Art. 6 Rn. 5; *Veil*, NVwZ 2018, 686, 688; jeweils m. w. N.
29 *Krusche*, ZD 2020, 232, 233 f.
30 EuGH, 29. 7. 2019 – C-40/17, K&R 2019, 562 ff. = NVwZ 2019, 1749.
31 Vgl. insgesamt dazu *Kollmar*, NVWZ 2019, 1740 ff.
32 Forschungsgruppe Security/Usability/Society (SECUSO), Privacy Paradox, abrufbar unter https://secuso.aifb.kit.edu/951.php.

agenten). Daneben spielen vor allem Personal Information Management-Systeme (kurz „PIMS“) eine Rolle, bei denen die Dienstleistung im Vordergrund stehen. Diese zwischengeschalteten Systeme ermöglichen in der Regel die lokale Speicherung sowie die individuelle Verwaltung der eigenen personenbezogenen Daten, indem die betroffene Person auswählen kann, mit wem und wann sie welche Daten teilen möchte. Dadurch soll Dritten für konkrete Zwecke und bestimmte Zeiträume vorbehaltlich der von den natürlichen Personen selbst festgelegten Bedingungen und aller vom anzuwendenden Datenschutzrecht vorgesehenen Garantien die Verwendung personenbezogener Daten erlaubt werden.[33] Einige PIMS bieten die Möglichkeit, Daten über die Online-Präsenz des Nutzers (wie Browserverlauf, Lesezeichen, Adressbücher, Anmeldedaten, Ortungsdaten, Finanzdaten, Aktivitäten in sozialen Netzwerken) aufzuspüren und sie im PIMS zu organisieren.[34]

Einige dieser Anwendungen reichen bis zur vollständigen Fremdverwaltung der Daten der Nutzer (sog. Treuhand-Modelle), wie sie etwa im Bereich der Mobilitätsdaten[35] diskutiert werden. Treuhand-Modellen liegt der Gedanke zugrunde, dass diese Systeme kein über die Verwaltung hinausgehendes Eigeninteresse an den Daten haben und damit neutral und professionell agieren können.

Ziel aller sog. „Selbstschutz-Systeme“ ist die Befähigung des Einzelnen, seine personenbezogenen Daten zu kontrollieren und die Entlastung von Entscheidungen, die ihn überfordern.[36] Derzeit steckt diese Entwicklung allerdings noch in den Kinderschuhen.

VII. Fazit

Die Komplexität technisierter Verarbeitungsvorgänge führt bei alleinigem Abstellen auf eine Einwilligung zu einer unsachgemäßen Verlagerung von Abwägungs-Entscheidung auf den Betroffenen und zu Überforderungen. Die DSGVO bietet wegen der deklarierten Technikneutralität nur augenscheinlich zu wenige Antworten. Unter gebotener risikoorientierter Betrachtung sind bei genauerer Betrachtung auch hochkomplexe Datenverarbeitungen unter Einsatz innovativer Technologien möglich. Verantwortliche sollten sich dabei nicht vorschnell unter Rückgriff auf die Einwilligung ihrer Verpflichtungen aus Art. 5 DSGVO entledigt sehen. Das schon deshalb, weil sie gut beraten sind, vorab zu prüfen, ob ein ergänzender Rückgriff auf solche Rechtsgrundlagen, die einen angemessenen Ausgleich der betroffenen Grundrechtspositionen erlauben (vor allem Vertrag und berechtigte Interessen), möglich ist. Durch ein hohes Maß an Transparenz, Verteilung der Entscheidungshoheit zwischen Betroffenen und Verantwortlichen, unter Zuhilfenahme technischer Lösungen zur Stärkung der Datensouveränität sowie risikominimierende Technikgestaltung lassen sich so Fehleranfälligkeit und Widerruflichkeit der Einwilligung abfedern. Zugleich bieten Techniklösungen den Betroffenen heute neue Möglichkeiten, den Selbstdatenschutz zu stärken.

Zu wünschen ist auch, dass die Aufsichtsbehörden ihre Skepsis berechtigten Interessen und dem Gedanken der Kumulation von Rechtsgrundlagen gegenüber ebenso überdenken, wie eine allzu strenge Interpretation des Kopplungsverbotes.

Geht all dies Hand in Hand, wird Europa als Technologiestandort insgesamt gestärkt.

33 EDSB Stellungnahme 9/2016, abrufbar unter https://edps.europa.eu/sites/edp/files/publication/16-10-20_pims_opinion_de.pdf, Rn. 53.
34 EDSB Stellungnahme 9/2016 (Fn. 33), Rn. 16.
35 *Brockmeyer*, ZD 2018, 258, 259.
36 DEK, Abschlussgutachten, S. 133 (Handlungsempfehlung Nr. 46) sowie S. 99 f., abrufbar unter https://datenethikkommission.de/wp-content/uploads/191028_DEK_Gutachten_bf.pdf.

RA Dipl.-Jur. Oliver Huq und RA Dr. Jan Verheyen*

Messenger datenschutzkonform in Unternehmen einsetzen

Kurz und Knapp

Die Kommunikation über „Sofortnachrichten“ („Instant-Messages“) verbreitet sich seit dem Einzug der Smartphones vor allem über mobile Apps (Stichwort „Mobile Messaging“) immer weiter. Auch für Unternehmen wird diese Art der Kommunikation für den Kunden- und Mitarbeiterkontakt immer interessanter. Auf Grund der Corona-Pandemie und der damit verbundenen vermehrten Auslagerung der Arbeit ins Homeoffice[1] hat sich dieser Trend noch zusätzlich beschleunigt. Der vorliegende Beitrag widmet sich dem Thema aus datenschutzrechtlicher Sicht und bewertet die aktuellen Möglichkeiten zur datenschutzkonformen Nutzung von Messengern in Unternehmen.

I. Messenger in Unternehmen

In Unternehmen stellt sich insbesondere seit der Einführung der DSGVO zum 25. 5. 2018 die Frage, inwieweit der Einsatz sogenannter Messenger-Dienste wie Facebook Messenger, iMessage, Signal, Telegram, Threema, WhatsApp und Co. rechtskonform möglich ist.[2] Viele Unternehmen erlauben ihren Mitarbeitern dabei die private Nutzung ihrer Firmen-Smartphones. Dadurch hat sich allein die Anzahl derjenigen, die ihr Smartphone außerhalb der Arbeitszeit für berufliches verwenden, im Zeitraum von 2017

* Mehr über die Autoren erfahren Sie auf S. VIII. Alle zitierten Internetquellen wurden zuletzt abgerufen am 30. 12. 2020.
1 Zum Datenschutz im Homeoffice vgl. *Verheyen/Elgert*, K&R 2020, 476.
2 Bezüglich WhatsApp s. *Hessel/Leffer*, CR 2020, 139.