3 Die Datenschutz-Grundverordnung aus Verbrauchersicht

Vor diesem Hintergrund erfolgt eine nach einzelnen Artikeln der Datenschutz-Grundverordnung geordnete Evaluation der Regelungen der Verordnung aus Verbrauchersicht. Wo dies erforderlich ist, werden mitgliedstaatliche Umsetzungen und Ausgestaltungen der Datenschutz-Grundverordnung in Deutschland mitberücksichtigt.

3.1 Ausübung persönlicher oder familiärer Tätigkeiten

Die Regelung, den Anwendungsbereich der Datenschutz-Grundverordnung bei Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten auszuschließen, muss vor dem Hintergrund der Entwicklung der Datenverarbeitung kritisch hinterfragt werden.

Nach Art. 2 Abs. 2 lit. c DSGVO findet die Datenschutz-Grundverordnung keine Anwendung auf die Verarbeitung personenbezogener Daten, wenn diese durch natürliche Personen zur Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten stattfindet. Erwägungsgrund 18 Satz 1 DSGVO präzisiert dies insofern, als kein Bezug zu einer beruflichen oder wirtschaftlichen Tätigkeit vorgenommen werden darf. Satz 2 des Erwägungsgrundes enthält Beispiele, für die die Anwendung der Datenschutz-Grundverordnung ausgeschlossen sein „könnte". Dies ist das Führen eines Schriftverkehrs oder von Anschriftenverzeichnissen oder die Nutzung sozialer Netze und Online-Tätigkeiten im Rahmen solcher Tätigkeiten. Satz 3 stellt fest, dass der Ausschluss der Anwendung für den Verantwortlichen nicht für die Verantwortlichen oder Auftragsverarbeiter gilt, die die Instrumente für die Verarbeitung personenbezogener Daten für solche persönlichen oder familiären Tätigkeiten bereitstellen. Persönliche Tätigkeiten sind im Ergebnis Tätigkeiten, die der eigenen Selbstentfaltung und Freiheitsausübung in der Freizeit oder im privaten Raum dienen, während familiäre Tätigkeiten solche Tätigkeiten sind, die der Pflege familiärer Beziehungen und des familiären Zusammenhalts dienen.[110]

Der vollständige Ausschluss des Anwendungsbereichs der Datenschutz-Grundverordnung gilt generell und auch dann, wenn besondere Kategori-

110 Roßnagel, in: Simitis/Hornung/Spiecker, 2019, Art. 2 Rn. 25.

en personenbezogener Daten verarbeitet werden.[111] Eine Einzelfallabwägung findet auch bei hohen tatsächlichen Risiken durch die Datenverarbeitung nicht statt. Es wird deshalb eine enge Auslegung der Regelung gefordert.[112] Zu beachten ist, dass durch die Verwendung des Begriffs „ausschließlich" in der Vorschrift eine Verarbeitung, die zu einem Teil auch außerhalb des persönlichen oder familiären Bereichs liegt, trotz der teilweisen Verortung in der persönlichen oder familiären Sphäre der Datenschutz-Grundverordnung unterliegt.[113]

Nicht unter die Ausnahme des Art. 2 Abs. 2 lit. c DSGVO fällt der Austausch von Informationen mit und in einem größeren Kreis von Kommunikationsteilnehmern.[114] Problematisch ist es dabei festzustellen, wo die Grenze zwischen persönlicher Kommunikation und Kommunikation in einem größeren Teilnehmerkreis verläuft. Klar ist lediglich, dass der Anwendungsbereich der Datenschutz-Grundverordnung eröffnet ist, wenn der Empfängerkreis personenbezogener Daten eine unbestimmte Größe hat.[115] Dies hat in der Praxis zu Unsicherheiten geführt, die sich in Fällen von Ubiquitous Computing[116] künftig noch steigern werden. Findet etwa eine Datenverarbeitung im Smart Home statt, so ist im Zweifel, wenn eine Nutzungsbeschränkung auf den Wohnungsinhaber und seine Familie nicht sichergestellt ist, von der Anwendbarkeit der Datenschutz-Grundver-

111 S. Ennöckl, in: Sydow, 2018, Art. 2 Rn. 11.

112 EuGH C-212/13, EuZW 2015, 234 Rn. 28 f. – Ryneš; Husemann, in: Roßnagel, 2018, § 3 Rn. 9; Kühling/Raab, in: Kühling/Buchner, 2018, Art. 2 Rn. 23; Zerdick, in: Ehmann/Selmayr, 2018, Art. 2 Rn. 10; zum Gebot der restriktiven Auslegung, um der Datenschutzkonvention des Europarats (Konvention 108, BGBl. II 1985, 538) zu genügen, die diese Ausnahme nicht kennt, s. Ennöckl, in: Sydow, 2018, Art. 2 Rn. 10; Dammann, in: Simitis, BDSG, 2014 § 1 Rn. 148.

113 S. z.B. Dammann, in: Simitis, BDSG, 2014, § 1 Rn. 150; Simitis, in: Simitis, BDSG, 2014, § 27 Rn. 47 ff.; Buchner, in: Taeger/Gabel, BDSG, 2013, § 27 Rn. 19; a.A. Gola/Lepperhoff, ZD 2016, 9 (10).

114 Roßnagel, in: Simitis/Hornung/Spiecker, 2019, Art. 2 Rn. 29.

115 S. EuGH C-101/01, EuZW 2004, 245 Rn. 37 ff. – Lindquist, Anm. Roßnagel, MMR 2004, 99 f.; Dammann, RDV 2004, 19; s. auch Ernst, in: Paal/Pauly, 2018, Art. 2 Rn. 21; Ennöckl, in: Sydow, 2018, Art. 2 Rn. 13; Kühling/Raab, in: Kühling/Buchner, 2018, Art. 2 Rn. 25; Albrecht/Jotzo, 2017, Teil 3 Rn. 30; Gola, in: Gola, 2018, Art. 2 Rn. 16; Dammann, in: Simitis, BDSG, 2014, § 1 Rn. 151; a.A. von Lewinski, in: Auernhammer, 2018, Art. 2 Rn. 24; Buchner, FamRZ 2019, 665 (666 f.).

116 Für eine Einschränkung der Ausnahme argumentiert Roßnagel, 2007, 131, 192 f.

ordnung auszugehen.[117] Erfassen Wearables oder das Smart Car personenbezogene Daten im öffentlichen Raum, so ist die Verordnung ebenfalls anwendbar.[118] Unklar aber ist bei der gegenwärtigen Formulierung, wo die Grenzen liegen. Dadurch entstehen hohe Befolgungsrisiken bei den Personen, die Daten für persönliche und familiäre Zwecke verarbeiten.

3.1.1 Datenschutzrisiken

Auch jenseits von Abgrenzungsproblemen, denen durch Konkretisierungen durch den Europäischen Datenschutzausschuss zusätzlich zu der bereits erfolgten Rechtsprechung des Europäischen Gerichtshofs[119] abgeholfen werden sollte, liegen Probleme. So hat der einzelne Verbraucher heute Zugriff auf hochkomplexe Technik, die etwa über Aktivitätsberichte oder direkt über Video und Audio auch zur Überwachung von Kindern[120] oder des Lebenspartners eingesetzt werden kann.[121]

Soweit das Risiko der Datenverarbeitung über anerkannte Fallgruppen persönlicher und familiärer Tätigkeiten hinausgeht, ist zu fordern, dass die Ausnahme eingeschränkt wird – zumindest in Fällen, in denen eine deutliche Risikosteigerung vorliegt. Dies sollte in jedem Fall dann angenommen werden, wenn durch die Datenverarbeitung eine umfassende Überwachung ermöglicht wird. Eine vollständige Ausnahme auch dieser Art von Datenverarbeitung wird dem Schutzbedürfnis der betroffenen Personen,

---

117 S. hierzu Geminn, DuD 2015, 575; von Lewinski, in: Auernhammer, 2018, Art. 2 Rn. 30; Skistims, 2016, 393 ff. Werden Daten etwa an den Energieversorger oder Dienstleister weitergegeben oder werden von Gästen, Handwerkern, Postboten etc. erfasste Daten weitergegeben, entfällt der persönliche oder familiäre Zweck.

118 Dies aber z.B. umstritten mit Blick auf sog. Dashcams; s. z.B. Reibach, DuD 2015, 157; Kinast/Kühnl, NJW 2014, 3057; Greger NVZ 2015, 114. Zu Drohnen s. Bischof DuD 2017, 142 (144 f.). Zu Kamerasystemen s. Stöber, NJW 2016, 3681 (3682); EuGH C-212/13, EuZW 2015, 234, Rn. 34 f. – Ryneš. Zu Wearables s. Rose, DuD 2017, 137 (138 f.); Solmecke/Kocatepe, ZD 2014, 22; Schwenke, DuD 2015, 161. Zum Smart Car s. Roßnagel u.a., 2016, 59 f.; Roßnagel/Hornung, 2019.

119 EuGH C-101/01, EuZW 2004, 245 Rn. 37 ff. – Lindqvist, Anm. Roßnagel MMR 2004, 99 f.; Dammann, RDV 2004, 19; EuGH C-212/13, EuZW 2015, 234 Rn. 34 f. – Ryneš.

120 S. z.B. Buchner, FamRZ 2019, 665 (667 f.).

121 Gola/Lepperhoff, ZD 2016, 9 (12); Roßnagel/Kroschwald, ZD 2014, 495; s. Husemann, in: Roßnagel, 2018, § 3 Rn. 9.

insbesondere Minderjähriger, nicht gerecht.[122] Deren Schutz ist aber gerade auch verfassungsrechtlich mit Blick auf Art. 7 und 8 GRCh geboten. Die Quantität der Datenverarbeitung sollte indes nicht entscheidend sein,[123] sondern es sollte auf die Zwecke der Verarbeitung abgestellt werden.

Bei Social Networks, Messengern und ähnlichen Diensten besteht überdies häufig das Problem, dass alle eingebrachten Daten dem Betreiber bekannt werden.[124] Damit besteht gleichzeitig das Risiko einer Weitergabe an Dritte – sowohl an befreundete Unternehmen des Anbieters, Werbetreibende und staatliche Stellen.[125]

Zusammenfassend ist zu konstatieren, dass die Ausnahme des Art. 2 Abs. 2 lit. c DSGVO ein Beispiel für die Unzulänglichkeiten der Datenschutz-Grundverordnung bei der Gewährleistung eines risikoadäquaten Schutzes der betroffenen Personen ist. Ihre Übernahme aus Art. 3 DS-RL wird den seit den 1990er Jahren erfolgten enormen technischen Entwicklungen nicht gerecht. Diese Entwicklung betrifft nicht nur Rechenleistung, sondern auch Speicherkapazitäten und Möglichkeiten zur Datenübermittlung. Darüber hinaus wurde Sensorik verschiedenster Art auf dem Verbrauchermarkt verfügbar und kann im privaten und familiären Bereich eingesetzt werden.[126] Eine vollständige Ausnahme, wie sie Art. 2 Abs. 2 lit. c DSGVO darstellt, kann vor dem Hintergrund dieser Entwicklung und der damit verbundenen Risiken nicht gerechtfertigt werden.[127] Vielmehr ist auch bei persönlichen und familiären Tätigkeiten risikoadäquat zu differenzieren und nur bei – näher zu bestimmenden – geringen Risiken auf eine Anwendung des Datenschutzrechts zu verzichten.

---

122 In diese Richtung auch Albrecht/Jotzo, 2017, Teil 3 Rn. 30; Buchner, FamRZ 2019, 665 (667 f.).

123 So aber z.B. Dammann, in: Dammann/Simitis, DSRL, 1997, Art. 2 Rn. 8; Dammann, in: Simitis, BDSG, 2014, § 1 Rn. 150.

124 Dies gilt z.B. nicht für die Inhalte der Kommunikation, wenn Messenger-Dienste diese Ende-zu-Ende-verschlüsseln.

125 Buchner, FamRZ 2019, 665 (666) weist zurecht darauf hin, dass sich z.B. Facebook in seinen Nutzungsbedingungen eine „nicht-exklusive, übertragbare, unterlizenzierbare und weltweite Lizenz" einräumen lässt, die Inhalte seiner Nutzer „zu hosten, zu verwenden, zu verbreiten, zu modifizieren, auszuführen, zu kopieren, öffentlich vorzuführen oder anzuzeigen, zu übersetzen und abgeleitete Werke davon zu erstellen" (Ziff. 3.1; https//de-de.facebook.com/legal/terms).

126 S. hierzu ausführlich Roßnagel, 2007, 192 ff.; Roßnagel u.a., 2016, 1 ff.

127 Roßnagel/Nebel/Richter, ZD 2015, 455; Gola/Lepperhoff, ZD 2016, 9 (12).

3.1.2 Beschränkte Anwendung der Datenschutz-Grundverordnung

Umgekehrt ist festzustellen, dass Datenverarbeitungen im privaten Handlungskontext aufgrund der enormen technischen Möglichkeiten, die ein Nutzer bereits heute und erst recht künftig hat, zwar in den Geltungsbereich der Verordnung fallen, aber dennoch sozial üblich sind. Da die Datenschutz-Grundverordnung keine Differenzierungen kennt, sind auf diese Handlungen, wenn sie unter die Verordnung fallen, alle Anforderungen der Datenschutz-Grundverordnung anzuwenden. Diese sind den (privaten) Verantwortlichen gegenüber weder zu vermitteln noch effektiv durchzusetzen. Das in der Praxis vielleicht relevanteste Beispiel dürfte die Veröffentlichung von Gruppenbildern auf einer privat genutzten Webseite oder auf einem Social Network sein. Die Veröffentlichung im Internet gehört nach Ansicht des Europäische Gerichtshofs „offensichtlich nicht" zum Privat- und Familienleben von Einzelpersonen.[128] Doch selbst wenn eine Einwilligung der abgebildeten Personen eingeholt und dokumentiert wurde, fehlt es in der Regel an datenschutzkonformer Information, Dokumentation, Systemgestaltung und Sicherungsmaßnahmen. Diese millionenfach durch Aufsichtsmaßnahmen einzufordern und durch Sanktionen durchzusetzen, wäre sozial inadäquat und unverhältnismäßig.

Sowohl um bei der Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten unvertretbare Risiken für betroffene Personen zu vermeiden als auch um bei sozial üblichem und vertretbarem Verhalten außerhalb dieses Bereichs unverhältnismäßige Datenschutzmaßnahmen nicht ergreifen zu müssen, sollte die Datenschutz-Grundverordnung einen Handlungsbereich definieren, der bei erhöhten Risiken zwar Datenschutzpflichten begründet, aber die Verordnung nicht vollständig zur Anwendung kommen lässt. Für diesen Bereich sollten nur ausgewählte Regelungen gelten.[129] Denkbar wären etwa die Regelungen der Datenschutz-Grundverordnung zur Interessenabwägung, zum Schadensersatz, zur Datensicherung und zur Auftragsverarbeitung sowie angepasste Regelungen zur Signalisierung der Einwilligung und Identifizierung betroffener Personen sowie zur Auskunft.[130]

---

128 EuGH C-101/01, EuZW 2004, Rn. 47; s. auch EuGH C-73/ 07. S. auch Kühlung/Raab, in: Kühling/Buchner, DSGVO, 2018, Art. 2 Rn. 25.

129 S. etwa Jandt/Roßnagel, ZD 2011, 160; Roßnagel/Richter/Nebel, ZD 2013, 104.

130 S. z.B. Roßnagel, in: Simitis/Hornung/Spiecker, 2019, Art. 2, Rn. 55.

3.2 Aufenthaltsprinzip

Der räumliche Anwendungsbereich der Datenschutz-Grundverordnung wurde im Vergleich zur Datenschutzrichtlinie deutlich ausgeweitet. Die Ausweitung des Anwendungsbereichs der Datenschutz-Grundverordnung in Art. 3 Abs. 2 DSGVO gilt in zwei Fällen – wenn ein Datenverarbeiter personenbezogene Daten von Personen verarbeitet, die sich in der Union aufhalten, nämlich wenn er entweder der betroffenen Person Waren oder Dienstleistungen anbietet (Marktort) oder die Datenverarbeitung der Beobachtung ihres Verhaltens dient (Beobachtungsort).[131] Dadurch will die Datenschutz-Grundverordnung auf dem europäischen Markt für Wettbewerbsgleichheit zwischen Anbietern in der Union und Anbietern außerhalb der Union sorgen und die Wahrnehmung von Betroffenenrechten vereinfachen. Mit der Ausweitung ist die Geltung des europäischen Datenschutzrechts nicht mehr an die Niederlassung des Verantwortlichen geknüpft, sondern hängt auch vom Aufenthaltsort der betroffenen Person in der Europäischen Union ab.

Möglich gewesen wäre indes auch eine Ausweitung des räumlichen Anwendungsbereichs, die sich nicht auf das Anbieten von Waren oder Dienstleistungen oder die Verhaltensbeobachtung beschränkt. Eine Erstreckung des Anwendungsbereichs auf jede Form der Verarbeitung personenbezogener Daten von betroffenen Personen, die sich in der Europäischen Union aufhalten, hätte Abgrenzungsschwierigkeiten zwischen Art. 3 Abs. 2 lit. a und b DSGVO vermieden und eine weitere Steigerung des Schutzniveaus bedeutet.[132] Zudem bereitet auch die Frage, wann ein Angebot („anbieten“) an betroffene Personen in der Europäischen Union vorliegt, Schwierigkeiten.[133] Die Erwägungsgründe 23 und 24 DSGVO allein reichen zur Klarstellung dieser relevanten Abgrenzungsprobleme nicht aus. Problematisch gestaltet sich beispielsweise das Angebot von Waren oder Dienstleistungen auf einer Webseite in einer Sprache, die auch außerhalb der Europäischen Union Landessprache ist.[134] Sofern hier nicht direkt Personen in der Europäischen Union angesprochen werden, ist fraglich, ob „offensichtlich“ im Sinn von Erwägungsgrund 23 DSGVO betroffene Personen in einem oder mehreren Mitgliedstaaten adressiert werden.

131 Die Bezeichnung Marktortprinzip trifft dementsprechend nur für Art. 3 Abs. 2 lit. a DSGVO zu, nicht aber für lit. b.
132 S. Husemann, in: Roßnagel, 2018, § 3 Rn. 17.
133 S. zur Problematik Klar, in: Kühling/Buchner, 2018, Art. 3 Rn. 80 ff.
134 S. Klar, in: Kühling/Buchner, 2018, Art. 3 Rn. 87.

In der Literatur wird ein Rückgriff auf Art. 57 Abs. 1 AEUV und Richtlinie 2006/123/EG (bezogen auf Dienstleistungen) sowie Art. 28 ff. AEUV (bezogen auf Waren) diskutiert.[135] Dies entspräche dem Gebot einer autonomen Auslegung der Datenschutz-Grundverordnung am Maßstab des europäischen Rechts, steht jedoch vor dem Problem, dass die dort befindlichen Definitionen nicht ohne Anpassungen übernommen werden können.[136] In jedem Fall ist eine weite Auslegung der Begriffe angezeigt, um Schutzlücken auszuschließen.

Den Abgrenzungsschwierigkeiten könnte zwar eine Klarstellung durch den Europäischen Datenschutzausschuss abhelfen, die insbesondere auf die Begriffe „Waren", „Dienstleistungen" und „anbieten" konkretisierend eingeht.[137] Wirksamer und eindeutiger wäre jedoch die Einschränkung auf das Angebot von Waren und Dienstleistungen zu streichen.

Von besonderer Bedeutung ist für die Wahrnehmung des Datenschutzrechts in dem neu beschriebenen Anwendungsbereich, dass sich bei den Aufsichtsbehörden Praktiken herausbilden, die eine effektive Rechtsdurchsetzung auch jenseits der Grenzen der Europäischen Union ermöglichen. Hier wird kritisiert, dass insbesondere ein Durchgriff auf kleine Anbieter Schwierigkeiten bereiten dürfte,[138] aber auch allgemein grundsätzliche Durchsetzungsprobleme außerhalb der Grenzen der Europäischen Union bestehen.[139] Eine Beschlagnahme etwa von in der Europäischen Union befindlichem Vermögen ist nicht möglich, wenn ein solches Vermögen gar nicht existiert. Auch eine Durchsetzung gegenüber dem Vertreter in der Europäischen Union[140] scheidet aus, wenn gar kein Vertreter bestellt wurde. Schon die Zustellung eines Bußgeldbescheides kann auf globaler Ebe-

135 So etwa Klar, in: Kühling/Buchner, 2018, Art. 3 Rn. 71 ff. bzw. 76 ff. S. auch Zerdick, in: Ehmann/Selmayr, 2018, Art. 3 Rn. 18.

136 So auch Klar, in: Kühling/Buchner, 2018, Art. 3 Rn. 73 bzw. 79.

137 S. Hornung, in: Simitis/Hornung/Spiecker, 2019, Art. 3 Rn. 48 ff.; Ennöckl, in: Sydow, 2018, Art. 3 Rn. 13 f.

138 S. etwa Schwartmann, in: Schwartmann u.a., 2018, Art. 4 Rn. 38. Deutscher Industrie- und Handelskammertag, 2019, 5, fordert die Durchsetzung vor allem gegenüber großen Unternehmen aus Drittländern.

139 S. Klar, in: Kühling/Buchner, 2018, Art. 3 Rn. 27, der darauf verweist, dass „Ermittlungs- und Rechtsdurchsetzungsbefugnisse im EU-Ausland nur nach Maßgabe bislang nicht existierender zwischenstaatlicher Verträge bestehen"; vgl. Geminn, DVBl. 2018, 1593 (1594).

140 S. Art 27 Abs. 1 DSGVO. Auch die faktische Möglichkeit der Überprüfung des Vorliegens der Ausschlusskriterien von Art. 27 Abs. 2 DSGVO ist von der Kooperation des nicht in der Europäischen Union niedergelassenen Verantwortlichen oder Auftragsverarbeiters abhängig.

ne leicht scheitern. Die Diskussion um Lösungsansätze steckt hier noch in den Anfängen.

3.3 Grundsätze der Datenverarbeitung

Die gesetzliche Festlegung der Datenschutzgrundsätze in Art. 5 DSGVO ist ein großer Fortschritt im Vergleich zu Art. 6 Abs. 1 DSRL. Sie sollte jedoch hinsichtlich des Grundsatzes „Treu und Glauben" präzisiert und um den Grundsatz der Datenvermeidung, der nicht im Grundsatz der Datenminimierung enthalten ist, ergänzt werden.

3.3.1 Grundsatz der Fairness

Nach Art. 5 Abs. 1 lit. a DSGVO und Art. 8 Abs. 2 Satz 1 GRCh müssen personenbezogene Daten nach Treu und Glauben verarbeitet werden. Der Grundsatz von Treu und Glauben ist in seiner Tragweite jedoch umstritten. Der Europäische Gerichtshof hat festgestellt, er verpflichte etwa „eine Verwaltungsbehörde, die betroffenen Personen davon zu unterrichten, dass die personenbezogenen Daten an eine andere Verwaltungsbehörde weitergeleitet werden, um von dieser […] weiterverarbeitet zu werden".[141] Dabei sind aber die Unterschiede zwischen Art. 5 Abs. 1 lit. a DSGVO und Art. 6 Abs. 1 DSRL zu beachten, zu dem die Entscheidung erging. Bezogen auf Art. 5 Abs. 1 lit. a DSGVO dürfte die vom Europäischen Gerichtshof formulierte Anforderung im Transparenzprinzip aufgehen. Dem Grundsatz von Treu und Glauben muss also ein darüberhinausgehender Gehalt zukommen. Im deutschen Recht ist der Begriff bereits zivilrechtlich besetzt, muss aber in der Datenschutz-Grundverordnung autonom ausgelegt werden. Um hier Missverständnisse zu vermeiden, sollte die deutsche Sprachfassung der Datenschutz-Grundverordnung Treu und Glauben durch Fairness übersetzen.[142] Der Begriff wird auch in der englischen Fassung verwendet und ist auch als deutscher Begriff im Duden zu finden.

Bezogen auf Gehalt und Tragweite des Grundsatzes von Treu und Glauben ist zu verhindern, dass er einerseits durch den Grundsatz der Transparenz, andererseits durch den Grundsatz der Rechtmäßigkeit der Verarbei-

141 EuGH, C-201/14, ZD 2015, 577 (578) Rn. 56 – Bara.

142 So Reimer, in: Sydow, 2018, Art. 5 Rn. 14; Wolff, in: Schantz/Wolff, 2017, Rn. 392; Roßnagel, in: Simitis/Hornung/Spiecker, 2019, Art. 5 Rn. 47.

tung überflüssig ist. Er könnte die Rolle einer Auffangklausel einnehmen, wenn eine Verarbeitung zwar formell und materiell rechtmäßig erfolgt, dies aber in einem bestimmten Fall als unbillig erscheint, etwa weil das Machtgefälle zwischen Anbieter und Verbraucher „unfair" zum Nachteil des Verbrauchers ausgenutzt wurde.[143] Der Europäische Datenschutzausschuss sieht im Grundsatz von Treu und Glauben eine Würdigung der „reasonable expectations" der betroffenen Person mit Blick auf die Machtasymmetrie zwischen dieser und dem Verantwortlichen.[144] Zusammenfassend ist der Gehalt des Grundsatzes von Treu und Glauben in der Datenschutz-Grundverordnung zu präzisieren, denn er ist in höchstem Maße ausfüllungsbedürftig. Dies könnte etwa in Erwägungsgrund 39 DSGVO geschehen, so wie es dort auch bezogen auf den Grundsatz der Transparenz geschehen ist. Zudem sollte seine Rolle in der Interessenabwägung und der Bewertung der Wirksamkeit der Einwilligung[145] gestärkt werden.

Aber auch die weiteren Grundsätze für die Verarbeitung personenbezogener Daten bedürfen der Präzisierung. Statt solche Präzisierungen vorzunehmen, ist die Datenschutz-Grundverordnung wie an vielen Stellen auch hier von der Verwendung unbestimmter Begriffe geprägt,[146] die äußerst interpretationsoffen sind.[147] Der Europäische Datenschutzausschuss sollte hier durch die Formulierung von entsprechenden Leitlinien tätig werden.

3.3.2 Grundsatz der Datenvermeidung

§ 3a BDSG a.F. enthielt das Gebot von Datenvermeidung und Datensparsamkeit. Obwohl es zu den allgemeinen Datenschutzprinzipien zählte, war es nicht sanktionsbewehrt und blieb unspezifisch; seine praktische Relevanz war denkbar gering. In Art. 5 Abs. 1 lit. c DSGVO spricht die Datenschutz-Grundverordnung nun von „Datenminimierung". Es handelt sich

143 So Dammann, in: Dammann/Simitis, 1997, Art. 6 Rn. 3 für die Datenschutzrichtlinie; ebenso Reimer, in: Reimer, 2018, Art. 5 Rn. 14; Herbst, in: Kühling/Buchner, 2018, Art. 5 Rn. 17 für die DSGVO.

144 Draft Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects, version for public consultation, 9 April 2019, 5.

145 S. hierzu Kap. 3.4.

146 Z.B. „nachvollziehbar", „geeignet", „angemessen", „legitim", „vereinbar", „erheblich", „erforderlichenfalls".

147 S. Richter, DuD 2015, 735 (739); Roßnagel/Nebel/Richter, ZD 2015, 455 (457 f.); Frenzel, in: Paal/Pauly, 2018, Art. 5 Rn. 55.

dabei um eine Fortführung des Grundsatzes der Erforderlichkeit der Verarbeitung aus Art. 6 Abs. 1 lit. c DSRL. Daten dürfen nur insoweit verarbeitet werden, als sie als Mittel zur Erreichung des Zwecks der Verarbeitung erforderlich sind; der Verantwortliche ist aber frei, den Zweck der Verarbeitung zu wählen und auszugestalten. Dieser Zweck wird vom Grundsatz der Datenminimierung nicht weiter hinterfragt. § 3a BDSG a.F. forderte hingegen, die Vermeidung von personenbezogenen Daten bereits bei der Zweckfestlegung zu berücksichtigen, mithin den Zweck so auszuwählen, dass möglichst wenige personenbezogene Daten erforderlich werden.[148] Geht es etwa um die Abrechnung der Nutzung eines Dienstes, so wäre ein Abrechnungsverfahren zu wählen, das möglichst wenige personenbezogene Daten erfordert.[149] Umgangssprachlich zwar nahe verwandt, sind Datenminimierung und Datensparsamkeit damit nicht gleichbedeutend.[150] Datenvermeidung kann als Gebot allenfalls aus Erwägungsgrund 78 Satz 3 DSGVO herausgelesen werden, der fordert als Teil von Art. 25 DSGVO die Verarbeitung personenbezogener Daten zu minimieren. Zudem kann er als Teil des Verhältnismäßigkeitsgrundsatzes in die Auslegung von Verarbeitungserlaubnissen der Datenschutz-Grundverordnung Eingang finden, wonach ein Eingriff in grundrechtlich geschützte Positionen so gering wie möglich gehalten werden muss.[151] Aus Gründen der Rechtssicherheit sollte ein § 3a BDSG a.F. entsprechendes Grundprinzip dennoch explizit Eingang in die Datenschutz-Grundverordnung finden. Hierzu böte sich vor allem Art. 5 Abs. 1 lit. c DSGVO an. Dann würden auch Verstöße gegen das Prinzip mit Sanktionen belegt werden können.

Abgesehen von den angesprochenen Problemen im Einzelfall ist den Grundsätzen der Datenverarbeitung gemein, dass sie mit moderner, insbesondere mit smarter Informationstechnik in Konflikt geraten. Sie müssen deshalb modernisiert und risikoadäquat weiterentwickelt werden.[152]

148 Roßnagel, in: Eifert/Hoffmann-Riem, 2011, 41 ff. m.w.N.

149 So bereits Roßnagel/Pfitzmann/Garstka, 2001, 101.

150 Roßnagel, DuD 2016, 561 (562); Herbst, in: Kühling/Buchner, 2018, Art. 5 Rn. 55. Trotz anderslautender Stimmen in der deutschsprachigen Fachliteratur, z.B. Albrecht/Jotzo, 2017, 52; Buchner, DuD 2016, 155 (156); Heberlein, in: Ehmann/Selmayr, 2018, Art. 5 Rn. 22; Frenzel, in: Paal/Pauly, 2018, Art. 5 Rn. 53; Wolff, in: Schantz/Wolff, 2017, Rn. 427; Pötters, in: Gola, 2018, Art. 5 Rn. 21.

151 S. bezogen auf die Verarbeitung personenbezogener Daten EuGH, C-293/12 und C-594/12, NJW 2014, 2169 – Digital Rights Ireland; EuGH, C-362/14, NJW 2015, 3151 – Schrems; EuGH, C-203/15 und C-698/15, NJW 2017, 717 – Tele2 Sverige; BVerfGE 65, 1 (43, 46).

152 S. hierzu näher Kap. 5.3.

3.4 Einwilligung und andere Erlaubnistatbestände

Nach dem Geltungsbeginn der Datenschutz-Grundverordnung im Mai 2018 waren die E-Mail-Postfächer vieler Verbraucher voll von Nachrichten, die vor dem Hintergrund der Verordnung zur Abgabe einer Einwilligung aufforderten. Diese Aufforderungen erfolgten oftmals, obwohl bereits eine Verarbeitungserlaubnis nach Art. 6 Abs. 1 UAbs. 1 lit. b oder lit. f DSGVO bestand.[153] Dies führte durch die bürokratische Aufforderung und die notwendige Zusatzarbeit nicht nur zu einem Prestigeverlust des Datenschutzes; lange gehegte Vorurteile sahen sich bestätigt. Vielmehr führt die Inanspruchnahme einer Einwilligung nach Art. 6 Abs. 1 lit. a oder 9 Abs. 2 lit. a DSGVO neben einem weiteren gesetzlichen Erlaubnistatbestand zu einer Verwirrung über die Voraussetzungen und Rechtsfolgen der Datenverarbeitung.[154]

Einerseits suggeriert Art. 6 Abs. 1 UAbs. 1 DSGVO durch die Verwendung des Begriffs „mindestens", dass mehrere Erlaubnistatbestände nebeneinander Anwendung finden können.[155] Dies wird unterstützt durch die Regelung des Art. 17 Abs. 1 lit. b DSGVO, nach der ein Widerruf der Einwilligung nur dann einen Anspruch auf Datenlöschung begründet, wenn es „an einer anderweitigen Rechtsgrundlage für die Verarbeitung" fehlt.[156] Dieser Vorbehalt betrifft nicht die Verpflichtung zur Datenverarbeitung gemäß Art. 6 Abs. 1 lit. c DSGVO. Denn bei einer solchen Verpflichtung gelten nach Art. 17 Abs. 3 lit. b DSGVO die Abs. 1 und 2 dieser Vorschrift überhaupt nicht. Der Löschanspruch nach Art. 17 Abs. 1 lit. b DSGVO ist somit dann ausgeschlossen, wenn eine Datenverarbeitung auf die Erlaubnistatbestände des Art. 6 Abs. 1 UAbs. 1 lit. b oder lit. f DSGVO gestützt wird.

Dennoch verstößt bezogen auf die Einwilligung die Nutzung mehrerer Tatbestände gegen den Grundsatz von Treu und Glauben, da der Verantwortliche hier das Vertrauen der betroffenen Person missbraucht.[157] Ähn-

153 S. hierzu und zum Folgenden auch Roßnagel, DuD 2018, 741 (745).

154 Klärungsbedarf sieht auch die Bundesregierung, in: Rat, ST 12756/1/19, 14; Deutsche Telekom, 2019, 6.

155 So auch Schulz, in: Gola, 2018, Art. 6 Rn. 11 f.; Buchner/Kühling, in: Kühling/Buchner, 2018, Art. 7 Rn. 17; Schantz, in: Simitis/Hornung/Spiecker, 2019, Art. 6 Abs. 1 Rn. 12.

156 S. Dix, in: Simitis/Hornung/Spiecker, 2019, Art. 17 Rn. 13; Herbst, in: Kühling/Buchner, 2018, Art. 17 Rn. 24 f.

157 S. Erwägungsgrund 43 DSGVO. S. auch Brink/Hertfelder, in: Roßnagel/Hornung, 2019, 75 ff.; Wolff, in: Schantz/Wolff, 2017, Rn. 475; Buchner/Petri,

lich hat sich auch die Artikel 29-Datenschutzgruppe geäußert. In den Leitlinien zur Einwilligung nach der Datenschutz-Grundverordnung weist sie darauf hin, dass der Verantwortliche, der seine Verarbeitung auf eine Einwilligung stützt, bereit sein müsse, „die Entscheidung zu respektieren und den Teil der Verarbeitung zu beenden, wenn eine Einzelperson ihre Einwilligung widerruft".[158] Die Artikel 29-Datenschutzgruppe beruft sich dabei zumindest indirekt auf den Grundsatz von Treu und Glauben, indem sie feststellt, es „wäre gegenüber Einzelpersonen ein in höchstem Maß missbräuchliches Verhalten, ihnen zu sagen, dass die Daten auf der Grundlage der Einwilligung verarbeitet werden, wenn tatsächlich eine andere Rechtsgrundlage zugrunde gelegt wird".[159] Die Datenschutzgruppe erwartet, dass der Verantwortliche sich vor Datenerhebung auf eine Rechtsgrundlage festlegen muss.[160] Zudem hat die Artikel 29-Datenschutzgruppe klargestellt, dass die Formulierung des Art. 17 Abs. 1 lit. b DSGVO, wonach personenbezogene Daten unverzüglich zu löschen sind, wenn die betroffene Person ihre Einwilligung widerruft und es an einer anderweitigen Rechtsgrundlage für die Verarbeitung fehlt, auf Fälle abzielt, in denen ein Datensatz zu unterschiedlichen Zwecken aufgrund unterschiedlicher Rechtsgrundlagen verarbeitet wird.[161] Dies dürfte auch für die Formulierung von Art. 6 Abs. 1 UAbs. 1 DSGVO zutreffen.

Die Regelung der Datenschutz-Grundverordnung ist derzeit widersprüchlich. Sie sieht für die Einwilligung andere Voraussetzungen, Einwirkungsmöglichkeiten und Rechtsfolgen vor, wie für eine Datenverarbeitung, die auf die Erforderlichkeit einer Vertragserfüllung oder eines überwiegenden berechtigten Interesses gestützt wird. Es geht jeweils um die gleiche Datenverarbeitung. Diese kann nicht zugleich unterschiedlichen Regelungskomplexen unterliegen. Auch sieht die Datenschutz-Grundverordnung keine Wahlfreiheit des Verantwortlichen darüber vor, welche Regelungen für die Datenverarbeitung gelten sollen.

---

in: Kühling/Buchner, 2018, Art. 6 Rn. 22; Buchner/Kühling, in: Kühling/Buchner, 2018, Art. 7 Rn. 18, 21; Uecker, ZD 2019, 248; Verbraucherzentrale Bundesverband, Evaluation, 2019, 5; Forum Privatheit, 2019, 4 f.; a.A. z.B. Schulz, in: Gola, 2018, Art. 6 Rn. 11 f.

158 Artikel 29-Datenschutzgruppe, Leitlinien in Bezug auf die Einwilligung, WP 259 rev.01, 27.

159 Leitlinien in Bezug auf die Einwilligung, WP 259 rev.01, 27.

160 Leitlinien in Bezug auf die Einwilligung, WP 259 rev.01, 28.

161 Artikel 29-Datenschutzgruppe, Leitlinien in Bezug auf die Einwilligung, WP 259 rev.01, 26.

Mit der Einwilligung oder der Berufung auf einen gesetzlichen Erlaubnistatbestand sind unterschiedliche Informationspflichten verbunden. So muss der Verantwortliche nach Art. 13 Abs. 1 lit. c und 14 Abs. 1 lit. d DSGVO über die Rechtsgrundlagen der Datenverarbeitung informieren, ob er sich also auf Einwilligung, Vertrag oder überwiegende berechtigte Interessen beruft. Bei einer Berufung auf eine für ihn günstige Interessenabwägung nach Art. 6 Abs. 1 UAbs. 1 lit. f DSGVO muss er nach Art. 13 Abs. 1 lit. d und 14 Abs. 2 lit. b DSGVO über seine berechtigten Interessen informieren. Er muss bei einer Einwilligung nach Art. 13 Abs. 2 lit. c DSGVO und nach Art. 14 Abs. 2 lit. d DSGVO auf die Möglichkeit und die Folgen eines Widerrufs hinweisen. Bei einer Datenverarbeitung, die auf eine Interessenabwägung nach Art. 6 Abs. 1 UAbs. 1 lit. f DSGVO gestützt wird, muss er dagegen nach Art. 13 Abs. 2 lit. b und Art. 14 Abs. 2 lit. c DSGVO über die Möglichkeit eines Widerspruchs nach Art. 21 DSGVO informieren. Widerruf und Widerspruch haben jedoch unterschiedliche Voraussetzungen und Wirkungen.

Informiert der Verantwortliche darüber, dass seine Datenverarbeitung sowohl durch eine Einwilligung als auch durch eine Interessenabwägung legitimiert ist, muss er also der betroffenen Person widersprüchliche Informationen zur gleichen Datenverarbeitung präsentieren. Lässt er sich nur eine Einwilligung geben und informiert über die durch Einwilligung gerechtfertigte Datenverarbeitung korrekt und beruft sich später auf eine Interessenabwägung, hat er die betroffene Person über ihre Rechte aus der Einwilligung getäuscht und ihr die notwendigen Informationen zur Datenverarbeitung aufgrund einer Interessenabwägung vorenthalten.

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 das Vertrauen des Verbrauchers, wenn er zusätzlich eine Einwilligung verlangt. Dies wird dem Prinzip von Treu und Glauben aus Art. 5 Abs. 1 lit. a DSGVO nicht gerecht. Obwohl er ihn nach Art. 7 Abs. 3 Satz 3 DSGVO auf sein Widerrufsrecht hinweisen muss, wird er nach einem Widerruf die weitere Datenverarbeitung trotzdem auf der Grundlage des gesetzlichen Erlaubnistatbestands fortführen.

Außerdem könnte für bestimmte Formen der Datenverarbeitung – wie z.B. Profilbildung oder personalisierte Werbung – der Verantwortliche dem Verbraucher mit der Bitte um eine Einwilligung das Recht vorgaukeln, dass er mit diesen Verarbeitungsformen nur nach einem Opt-in rechnen muss. Dieses mindert sich für ihn aber nachträglich zu einem Recht auf Opt-out, wenn der Verantwortliche auf den gesetzlichen Erlaubnistatbestand des überwiegenden berechtigten Interesses wechselt.

Informiert der Verantwortliche den Verbraucher von Anfang an über beide Erlaubnistatbestände – Einwilligung einerseits und Vertragserfüllung oder berechtigte Interessen andererseits – und die mit ihnen verbundenen unterschiedlichen Regelungsregime, gibt er ihm widersprüchliche Informationen und behält sich die Wahl des Erlaubnistatbestands, auf den er sich später berufen will, vor. Dies wäre ein unzulässiges perplexes Verhalten, das nur dazu führen kann, den Verbraucher zu verwirren.

Schließlich haben beide Rechtfertigungen der Datenverarbeitung unterschiedliche Rechtsfolgen. Mit der Einwilligung ist das Recht der betroffenen Person verbunden, eine Datenübertragung nach Art. 20 DSGVO einzufordern. Dies kann für die Entscheidung einzuwilligen bedeutsam sein. Wenn der Verantwortliche die Datenverarbeitung aber auch auf eine Interessenabwägung stützen kann, ist er in der Lage, dem Verbraucher dieses Recht zu nehmen, indem er sich auf den gesetzlichen Erlaubnistatbestand des überwiegenden berechtigten Interesses beruft. Für diesen Anspruch der betroffenen Person sieht Art. 20 DSGVO aber kein Wahlrecht des Verantwortlichen vor.

Alle diese Ungereimtheiten erfordern eine Klarstellung in der Verordnung. Diese kann nur darin bestehen, 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. Ansonsten suggeriert er dem Verbraucher durch den durch Art. 7 Abs. 3 Satz 3 DSGVO geforderten Hinweis auf das Widerrufsrecht, er könne durch Widerruf die weitere Datenverarbeitung verhindern, obwohl dies aber bei einem bestehenden weiteren gesetzlichen Erlaubnistatbestand faktisch nicht der Fall ist.[162]

Der notwendige Vorrang der Einwilligung sollte nicht nur aus Art. 5 Abs. 1 lit. a DSGVO als einzig faire Form der Datenverarbeitung abgeleitet werden müssen,[163] sondern – zur Rechtssicherheit für alle Beteiligten – in den Text des Art. 6 Abs. 1 UAbs. 1 DSGVO aufgenommen werden.[164] Eine

162 Eine maßvolle Begrenzung der Widerruflichkeit einer Einwilligung fordert Schulz, DuD 2020, 302.

163 S. hierzu Kap. 3.4.

164 S. hierzu Verbraucherzentrale Bundesverband, 2013, 7; Verbraucherzentrale Bundesverband, Evaluation, 2019, 5.

Klarstellung der Formulierung in Art. 6 Abs. 1 UAbs. 1 DSGVO könnte Unsicherheiten abbauen und Missbrauch verhindern.

3.5 Bestimmung des Vertragszwecks

Die extrem weite Fassung des Erlaubnistatbestands der „Erfüllung eines Vertrags" kann so genutzt werden, dass der vom Anbieter definierte Vertragszweck auf umfassende Verarbeitungen der personenbezogenen Daten einer Verbrauchers im Rahmen eines Persönlichkeitsprofils zielt und die Erhebung einer großen Zahl von Daten erforderlich macht.[165] Hier ist eine Präzisierung des Erlaubnistatbestands zu empfehlen.[166]

Art. 6 Abs. 1 UAbs. 1 lit. b DSGVO erklärt die Verarbeitung personenbezogener Daten für rechtmäßig, die zur Erfüllung eines Vertrages erfolgt, dessen Vertragspartei die betroffene Person ist. Dies schließt auch vorvertragliche Maßnahmen ein, die auf Anfrage der betroffenen Person erfolgen. Der Europäische Datenschutzausschuss weist darauf hin, dass eine Verarbeitung, die nicht zur Erfüllung des Vertrages notwendig ist, auf eine andere Grundlage gestellt werden kann, insbesondere auf lit. a und f, die dem Betroffenen dann auch mitzuteilen ist.[167] Zugleich müsse streng zwischen Einwilligung und Vertragserfüllung differenziert werden, da für diese unterschiedliche Voraussetzungen und Rechtsfolgen gelten. Der Bereich notwendiger Einwilligungen darf nicht durch die Ausweitung des Erlaubnistatbestands des Art. 6 Abs. 1 UAbs. 1 lit. b DSGVO eingeschränkt werden.

Die notwendige datenschutzrechtliche Eingrenzung des Erlaubnistatbestands des Art. 6 Abs. 1 UAbs. 1 lit. b DSGVO kann nicht allein durch die Kontrolle der Allgemeinen Geschäftsbedingungen (AGB)[168] erreicht wer-

165 Dieses Problem sieht auch der Europäische Datenschutzausschuss; s. Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects, v2.0, 8. October 2019, 6 f.

166 S. auch Wendehorst/Graf v. Westphalen, NJW 2016, 3745 (3749 f.), die sich mit einer teleologischen Reduktion behelfen.

167 Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects, v2.0, 8 October 2019, 7.

168 S. RL 93/13/EWG.

den.[169] Die AGB-Kontrolle schützt den Verbraucher lediglich vor unfairen allgemeinen für eine Vielzahl von Verträgen vorformulierten Vertragsbedingungen, die eine überraschende Regelung enthalten (§ 305c BGB) oder den Verbraucher entgegen den Geboten von Treu und Glauben unangemessen benachteiligen (§ 307 Abs. 1 BGB). Dies gilt nach § 307 Abs. 2 Nr. 1 BGB insbesondere, wenn eine AGB-Bestimmung mit wesentlichen Grundgedanken der gesetzlichen Regelung, von der abgewichen wird, nicht zu vereinbaren sind. Die AGB-Kontrolle erfasst nach § 305 Abs. 1 Satz 3 BGB jedoch gerade nicht die Bestimmung des individuellen Vertragszwecks – wie weit und wie gezielt auf die Verarbeitung personenbezogene Daten er auch immer ausgerichtet sein mag.

Die notwendige datenschutzrechtliche Eingrenzung verstößt auch nicht gegen den Grundsatz der Privatautonomie und insbesondere den Grundsatz der Vertragsfreiheit. Zwar hat der Verbraucher grundsätzlich die Freiheit, auch in für ihn nachteilige Verträge einzutreten. Daher wird argumentiert, dass das Datenschutzrecht ihm diese Freiheit nicht nehmen dürfe. Das Argument der Freiheit der Vertragsparteien unterliegt jedoch dem Gesetzesvorbehalt. Das Datenschutzrecht schützt die Grundrechte und Freiheiten der betroffenen Person gegen übergroße Machtasymmetrien – vor allem aus Wissensmacht. Insbesondere dann, wenn soziale, rechtliche und sonstige Zwänge zur Nutzung bestimmter Angebote bestehen, bei denen ein weit definierter Vertragszweck den Verbraucher in eine umfassende Verarbeitung seiner personenbezogenen Daten drängen würde, muss die staatliche Schutzpflicht für machtausgleichende Regelungen sorgen. Dieser Schutz fordert eine eingrenzende Bestimmung des Erlaubnistatbestands des Art. 6 Abs. 1 UAbs. 1 lit. b DSGVO.

Zur Frage, was für die Erfüllung eines Vertrages erforderlich ist, darf nicht auf die Vertragsformulierung oder auf den Willen des Verantwortlichen abgestellt werden. Ansonsten könnte der Verantwortliche den Vertragstext so formulieren oder den Vertragsgegenstand und den Vertragszweck so bestimmen, dass er jede von ihm gewünschte Datenverarbeitung durchführen kann – z.B. auch Datenverarbeitungen zu Werbemaßnahmen, zur Profilbildung, zur Weitergabe von Daten an Dritte, zur Durchführung von Sicherungsmaßnahmen, zur Erhebung der Kundenzufriedenheit, zur Verbesserung der Waren und Dienste und vieles mehr. Diese Zu-

169 So aber Engeler, ZD 2018, 55 (57 f.). Über „erprobte zivilrechtliche Werkzeuge wie die Prüfung von Treuwidrigkeit, Verstoß gegen die guten Sitten und die AGB-Kontrolle“ könne eine ausreichende Präzisierung erfolgen (ebd., 60); s. auch Wendehorst/Graf v. Westphalen, NJW 2016, 3745.

satzzwecke sollen nur nach einer Einwilligung der betroffenen Person oder nach der umfassenden und dokumentierten Abwägung der berechtigten Interessen der Verantwortlichen mit den Interessen und Freiheiten der betroffenen Person eine Datenverarbeitung rechtfertigen können. Daher fordert der Ausschuss, für die Zulässigkeit der Datenverarbeitung nach lit. b auf die objektive Erforderlichkeit der Datenverarbeitung für den Hauptzweck des Vertrags abzustellen.[170] Es kann nicht auf das bloße Vorhandensein einer Vertragsklausel ankommen, die der betroffenen Person unilateral auferlegt wird.[171] Entscheidend muss sein, dass die Vertragsleistung funktional ohne die Verarbeitung der relevanten personenbezogenen Daten nicht erbracht werden kann.[172]

Dies sollte zur Rechtssicherheit für alle Beteiligten im Text des Art. 6 Abs. 1 UAbs. 1 lit. b DSGVO klargestellt werden. Ohne Klarstellung, dass die funktional objektive Erforderlichkeit der Datenverarbeitung für den zentralen Vertragszweck entscheidend ist, wird es über die Reichweite des Erlaubnistatbestands des Art. 6 Abs. 1 UAbs. 1 lit. b DSGVO immer wieder zu interessengeleiteten Streitereien kommen. Die dadurch verursachte Rechtsunsicherheit wird den Vollzug des Datenschutzes erheblich behindern.

3.6 Verarbeitung der Daten von Kindern

Kinder wachsen heute in einer digitalisierten Welt auf. Sie sind Objekte der Datenverarbeitung im Säuglingsalter etwa durch Baby-Fon-Apps, im Kinderzimmer durch Smart Toys,[173] Sprachassistenten[174] und Tablet-Computer und im Kindergarten durch Lernroboter und Videoüberwachung. In der Schule werden ihre Verwaltungs-, Verhaltens- und Leistungsdaten

170 Draft Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects, version for public consultation, 9.4.2019, 7 f.; s. auch Johannes, ZD-aktuell 2019, 06821, ZD 2019, Heft 12, VI f.

171 Unter Verweis auf Stellungnahme 6/2014 zum Begriff des berechtigten Interesses des für die Verarbeitung Verantwortlichen gemäß Artikel 7 der Richtlinie 95/46/EG, WP 217, 21 f.

172 S. hierzu auch Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, 2019, 8; Verbraucherzentrale Bundesverband, Evaluation, 2019, 6.

173 S. z.B. Gilga, ZD-aktuell 2019, 06822, ZD 12/2019, V.

174 Wissenschaftliche Dienste des Deutschen Bundestags, Zulässigkeit der Transkribierung und Auswertung von Mitschnitten der Sprachsoftware „Alexa" durch Amazon, WD 10-3000-032/19, 2019, 9.

durch Schulmanagementsysteme, biometrische Daten zum Zugangsschutz und ihre Konsumdaten durch Systeme für bargeldloses Bezahlen in der Schulkantine verarbeitet.[175] Außerdem sind sie in der Welt des Electronic Commerce und der Social Networks, des Ubiquitous Computing und des Big Data den gleichen Praktiken der Datensammelei und der Profilbildung unterworfen wie die Erwachsenen.[176]

Sehr oft wenden sich Verantwortliche direkt an Kinder und verarbeiten deren Daten auf vielfältige Weise und speichern diese für lange Zeit. Dies gilt insbesondere für die Nutzung von Social Networks und Angebote im E-Commerce, die sich an Kinder richten. Z.B. nutzten in der Altersgruppe der 6- bis 13-jährigen im Jahr 2016 57% der Kinder WhatsApp, 50% YouTube und 30% Facebook mehrmals in der Woche oder am Tag.[177] Das durchschnittliche Alter der Erstanmeldung bei Facebook lag 2016 bei 10 Jahren.[178] 2018 nutzten z.B. 73% der 14- bis 17-Jährigen Instagram.[179] Die Datenverarbeitung von Kindern ist somit im Internet keine Ausnahme sondern ein Massenphänomen.[180]

Kinder unterliegen einer besonderen strukturell bedingten Gefährdungslage: Sie verstehen die meist langfristigen Nachteile der Verarbeitung ihrer personenbezogenen Daten noch unzureichend, sind aber für die meist kurzfristigen positiven Effekte der Nutzung von Internet-Diensten sehr offen und für Verführungen zu ihrer Nutzung leicht zugänglich. Wissen über Handlungsfolgen und -möglichkeiten müssen sich bei Kindern erst nach und nach herausbilden und festigen. Ihnen ist nicht klar, dass aus den Daten, die sie preisgeben und die durch die Beobachtung ihres Verhaltens entstehen, neue Daten über sie generiert werden, die ihr Weltverständnis bestimmen, ihre sozialen Beziehungen beeinflussen, ihr Selbstbild prägen und Vorhersagen über ihr Verhalten ermöglichen. Kinder können die Risiken der Verarbeitung ihrer Daten weniger gut vermeiden und sich gegen Eingriffe in ihre Grundrechte weniger gut wehren, als Erwachsene dies können. Schließlich ist zu berücksichtigen, dass Kinder in der Regel ihre eigenen Rechte als betroffene Person nicht kennen. Selbst wenn sie ihnen bekannt wären, sind sie meist nicht in der Lage, sie wahr-

175 S. z.B. Artikel 29-Datenschutzgruppe, WP 147, 16.
176 S. hierzu Roßnagel/Richter, 2017, 205 (209 ff.).
177 MPFS, KIM-Studie 2016, 33.
178 MPFS, KIM-Studie 2016, 41.
179 MPFS, KIM-Studie 2018,39.
180 S. ähnliche Zahlen in BITKOM, 2017, 8.

zunehmen. Aus diesen Gründen haben Kinder einen besonderen Bedarf an Schutz und Fürsorge.[181]

Diese besondere Schutz- und Fürsorgepflicht berücksichtigt auch die Datenschutz-Grundverordnung in vielen Zusammenhängen – allerdings nicht in allen notwendigen Aspekten. Nach Erwägungsgrund 38 Satz 1 DSGVO verdienen Kinder „bei ihren personenbezogenen Daten besonderen Schutz, da Kinder sich der betreffenden Risiken, Folgen und Garantien und ihrer Rechte bei der Verarbeitung personenbezogener Daten möglicherweise weniger bewusst sind". Wen die Datenschutz-Grundverordnung unter den Begriff „Kind" versteht, hat sie zwar nicht definiert.[182] Dennoch ist davon auszugehen, dass sie unter „Kind" jede Person versteht, die das 18. Lebensjahr noch nicht erreicht hat.

Die besondere Schutzbedürftigkeit von Kindern berücksichtigt die Datenschutz-Grundverordnung in sechs Regelungen für unterschiedliche datenschutzrechtliche Zusammenhänge:[183]

– Nach Art. 8 Abs. 1 Satz 1 DSGVO gilt die Einwilligung eines Kindes bei einem Angebot von Diensten der Informationsgesellschaft, das einem Kind direkt gemacht wird, schon als rechtmäßig, wenn das Kind das sechzehnte Lebensjahr vollendet hat. Nach Art. 8 Abs. 1 Satz 1 DSGVO dürfen Mitgliedstaaten diese Grenze sogar auf das dreizehnte vollendete Lebensjahr senken. In anderen Fällen ist das Kind erst mit Volljährigkeit einwilligungsfähig. Von der Öffnungsklausel des Art. 8 Abs. 1 UAbs. 2 DS-GVO hat jedoch die Mehrzahl der Mitgliedstaaten Gebrauch gemacht[184] und diese Grenze durch gesetzliche Regelung gesenkt.[185] Neun haben die Altersgrenze auf 13 Jahre festgesetzt,[186] sechs

181 S. zum Schutzbedarf z.B. Artikel 29-Datenschutzgruppe, WP 147, 3 ff.; Datenethikkommission, 2019, 114 f.; Roßnagel, in: Ammicht Quinn u.a. 2020, i.E.; Roßnagel, ZD 2020, 88.

182 Anders Art. 4 Nr. 18 Entwurf der Kommission und Entwurf des Parlaments, die ein Kind als „jede Person bis zur Vollendung des achtzehnten Lebensjahres" definierten.

183 S. hierzu näher Roßnagel, ZD 2020, 88 (89 f.); Roßnagel, in: Ammicht Quinn u.a. 2020, i.E.

184 Frankreich, in: Rat, ST 12756/1/19, 28, und Niederlande, in: Rat, ST 12756/1/19, 46 f., setzen sich für eine unionseinheitliche Altersbestimmung ein.

185 S. hierzu auch die Kritik der Europäischen Kommission, Commission Staff Working Document, 17.

186 Diese Grenze richtet sich wohl nach den Nutzungsbedingungen der großen amerikanischen Plattformen.

auf 14 Jahre, vier auf 15 Jahre und neun Staaten haben die Altersgrenze der DS-GVO beibehalten.[187]

- Nach Art. 6 Abs. 1 UAbs. 1 Satz 1 lit. f DSGVO muss eine Interessenabwägung die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person in besonderer Weise berücksichtigen, „wenn es sich bei der betroffenen Person um ein Kind handelt".[188] Allerdings wird vom Wortlaut kein bestimmter Zweck und keine bestimmte Form der Datenverarbeitung ausgeschlossen.[189] Daher wird vertreten, die Vorschrift fordere nur eine intensivere Abwägung durch den Verantwortlichen.[190]
- Nach Art. 12 Abs. 1 Satz 1 DSGVO sind Informationen nach Art. 13 und 14 DSGVO sowie Mitteilungen nach Art. 15 DSGVO „in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache zu übermitteln". Dies soll umso mehr für Informationen gelten, die sich speziell an Kinder richten.[191] „Wenn sich die Verarbeitung an Kinder richtet, sollten" nach Erwägungsgrund 58 Satz 4 DSGVO „aufgrund der besonderen Schutzwürdigkeit von Kindern Informationen und Hinweise in einer dergestalt klaren und einfachen Sprache erfolgen, dass ein Kind sie verstehen kann".[192]
- Eine Löschung personenbezogener Daten hat nach Art. 17 Abs. 1 lit. f. DSGVO zu erfolgen, wenn die Daten aufgrund einer Einwilligung von einem Kind nach Art. 8 Abs. 1 DSGVO erhoben worden sind. Die Vorschrift will erreichen, dass Kinder beim Übergang in das Erwachsenen-

187 S. die Übersicht von Nebel/Dräger, ZD-aktuell 8/2019, VIII.

188 Hier sehen die Bundesregierung, in: Rat, ST 12756/1/19, 12, und Irland, in: Rat, ST 12756/1/19, 20, einen Bedarf an Konkretisierung. Irland bedauert, dass die Mitgliedstaaten diese Klausel nicht konkretisieren dürfen.

189 Nach Buchner/Petri, in: Kühling/Buchner, 2018, Art. 6 Rn. 155, sollen bei einem Kind unter 16 Jahren regelmäßig die schutzwürdigen Interessen überwiegen; ähnlich Artikel 29-Datenschutzgruppe, WP 147, 14, für die Verarbeitung von Kinderdaten für Werbezwecke; s. dagegen Reimer, in: Sydow, Aufl. 2018, Art. 6 Rn. 64: nur „besonders gewichtig".

190 S. z.B. Schantz, in: Simitis/Hornung/Spiecker, 2019, Art. 6 Abs. 1 Rn. 112.

191 Hier verweist die Artikel 29-Datenschutzgruppe auf die Konvention über die Rechte des Kindes – Für Kinder erklärt des Kinderhilfswerks der Vereinten Nationen als gelungenes Beispiel für kindgerechte Sprache; Leitlinien für Transparenz, WP 260 rev.01, 12.

192 Hier verweist die Art. 29-Datenschutzgruppe, Leitlinien für Transparenz, WP 260 rev.01, 2018, 12, auf die „Konvention über die Rechte des Kindes – Für Kinder erklärt" des Kinderhilfswerks der Vereinten Nationen als gelungenes Beispiel für kindgerechte Sprache.

alter nicht von „Jugendsünden" verfolgt werden, deren langfristige Folgen sie im Kindesalter noch nicht abschätzen konnten.[193]

- Nach Art. 40 und 41 DSGVO können Verbände Verhaltensregeln für ihre jeweilige Branche beschließen, mit denen sie die Anwendung der Verordnung präzisieren. Diese Verhaltensregeln sind den Aufsichtsbehörden vorzulegen und von diesen zu genehmigen, wenn sie der Datenschutz-Grundverordnung entsprechen. Sie sind dann für die weitere Aufsichtstätigkeit verbindlich.[194] Art. 40 Abs. 2 lit. g DSGVO sind auch „Unterrichtung und Schutz von Kindern und Art und Weise, in der die Einwilligung des Trägers der elterlichen Verantwortung für das Kind einzuholen ist," mögliche Regelungsgegenstände.[195]
- Nach Art. 57 Abs. 1 lit. b DSGVO ist es eine von vielen Aufgaben der Aufsichtsbehörden, „die Öffentlichkeit für die Risiken, Vorschriften, Garantien und Rechte im Zusammenhang mit der Verarbeitung (zu) sensibilisieren und sie darüber auf(zu)klären. Besondere Beachtung finden dabei spezifische Maßnahmen für Kinder." Diese Aufklärungsmaßnahmen sollen besonders sowohl auf den Schutz von Kindern gerichtet sein als auch sich an Kinder richten.[196]

Das sind allerdings nicht alle Situationen, in denen der besondere Schutz von Kindern erforderlich ist oder ihre besonderen Interessen zu berücksichtigen sind. In allen anderen Regelungen behandelt die Datenschutz-Grundverordnung Kinder zwar wie Erwachsene. Für sie gelten beispielsweise die gleichen Erlaubnistatbestände und die gleichen Verarbeitungsgrundsätze. Sie haben die gleichen Rechte wie Erwachsene. Die Verantwortlichen haben ihnen gegenüber grundsätzlich die gleichen Verpflichtungen und können ihre Daten unter den gleichen Voraussetzungen in Staaten außerhalb des Geltungsbereichs der Datenschutz-Grundverordnung übertragen.[197] In all diesen Fällen fordert die Datenschutz-Grundverordnung aber gerade nicht, die Schutzbedürftigkeit von Kindern besonders zu berücksichtigen.

Die Datenschutz-Grundverordnung schützt Kinder in einer ihrer Schutzbedürftigkeit entsprechenden Weise somit nur punktuell, jedoch nicht in allen Situationen, in denen ein besonderer Schutz erforderlich ist.

---

193 S. Erwägungsgrund 65 DSGVO; s. hierzu z.B. Herbst, in: Kühling/Buchner, 2018, Art. 17 Rn. 31.

194 S. hierzu Roßnagel, in: Simitis/Hornung/Spiecker, 2019, Art. 40 Rn. 67 ff.

195 Hier sehen der Rat, ST 14994/2/19, Rn. 13, und Irland, in: Rat, ST 12756/1/19, 21, eine Möglichkeit, Kindern adäquaten Schutz zu bieten.

196 Polenz, in: Simitis/Hornung/Spiecker, 2019, Art. 57 Rn. 11 und 20.

197 S. hierzu Niederlande, in: Rat, ST 12756/1/19, 47.

Hinter den wenigen Regelungen ist kein Gesamtkonzept erkennbar.[198] Daher sollte der Wortlaut der Verordnung z.B. in folgenden Vorschriften diesen besonderen Aspekt zusätzlich und ausdrücklich berücksichtigen:[199]

- Die Prüfung der Vereinbarkeit eines neuen Verarbeitungszwecks mit dem bisherigen Verarbeitungszweck nach Art. 6 Abs. 4 DSGVO sollte auch berücksichtigen, wenn die Daten eines Kindes für einen anderen Zweck verwendet werden sollen. In diesem Fall sollte die Feststellung der Vereinbarkeit einer Zweckänderung mit dem ursprünglichen Zweck restriktiver erfolgen als bei Daten von Erwachsenen.
- In den Normtext des Art. 8 DSGVO sollte die Wertung des Erwägungsgrunds 38 Satz 2 DSGVO übernommen werden: „Ein solch besonderer Schutz sollte insbesondere die Verwendung personenbezogener Daten von Kindern für Werbezwecke oder für die Erstellung von Persönlichkeits- oder Nutzerprofilen und die Erhebung von personenbezogenen Daten von Kindern bei der Nutzung von Diensten, die Kindern direkt angeboten werden, betreffen." Der Unionsgesetzgeber sollte in Art. 8 DSGVO festlegen, dass die Verwendung personenbezogener Daten von Kindern für Werbezwecke oder für die Erstellung von Persönlichkeits- oder Nutzerprofilen unzulässig ist.[200] Ein solches Verbot würde die Werbung für Spiele und Spielsachen nicht ausschließen, sondern nur die Nutzung von Persönlichkeits- oder Nutzerprofilen und andere Sammlungen von Kinderdaten für Werbezwecke. Dabei sollte es keinen Unterschied machen, ob diese Datenverarbeitung auf eine Einwilligung des Kindes oder seiner Erziehungsberechtigten oder auf überwiegende berechtigte Interessen gestützt wird.
- Von der Ausnahme des Verbots der Verarbeitung besonderer Kategorien von personenbezogenen Daten bei einer Einwilligung nach Art. 9 Abs. 2 lit. a DSGVO sollte die Einwilligung eines Kindes ausgenommen werden. Eine Einwilligung oder Zustimmung durch den Träger der elterlichen Verantwortung bliebe weiterhin möglich. Die Zielsetzung des Erwägungsgrunds 38 Satz 3 DSGVO, dass „die Einwilligung des

198 Besonders kritisch Irland, in: Rat, ST 12756/1/19, 20: „inadequate", „both fragmented and disjointed" „resemble a jigsaw puzzle but, unlike a complete jigsaw, they do not provide a coherent picture of protection for children"; s. auch Niederlande, in: Rat, ST 12756/1/19, 47; Däubler, in: Däubler/Wedde/Weichert/Sommer, 2018, Art. 8 DSGVO, Rn. 2; Verbraucherzentrale Bundesverband, Evaluation, 2019, 6 f.

199 S. hierzu ausführlich Roßnagel, ZD 2020, 88 (90 ff.); Roßnagel, in: Ammicht Quinn u.a. 2020, i.E.

200 So auch Glatzner, DuD 2020, 312.

Trägers der elterlichen Verantwortung … im Zusammenhang mit Präventions- oder Beratungsdiensten, die unmittelbar einem Kind angeboten werden, nicht erforderlich sein" sollte, hat im Text der Verordnung keinen Ansatzpunkt gefunden. Sie könnte ebenfalls in Art. 9 DSGVO geregelt werden.[201] Ein Kind sollte in psychischen Zwangslagen z.B. eine Sucht- oder Schwangerschaftsberatung in Anspruch nehmen können, ohne befürchten zu müssen, dass die Eltern davon erfahren.[202]

- Nicht nur bei der Forderung nach Löschung, sondern auch beim Widerspruch nach Art. 21 Abs. 1 DSGVO sollte es in besonderer Weise berücksichtigt werden, wenn die personenbezogenen Daten im Kindesalter erhoben worden sind. Kinder sind sich gemäß Erwägungsgrund 38 Satz 1 DSGVO „der betreffenden Risiken, Folgen und Garantien und ihrer Rechte bei der Verarbeitung personenbezogener Daten möglicherweise weniger bewusst". Um hier Missverständnisse auszuschließen und Rechtsklarheit zu schaffen, sollte der Wortlaut des Art. 21 Abs. 1 DSGVO klarstellen, dass der Verantwortliche bei der Prüfung der Berechtigung des Widerspruchs den Umstand, dass er Daten von Kindern verarbeitet, besonders berücksichtigen muss. Dies würde auch mit der Pflicht des Verantwortlichen nach Art. 6 Abs. 1 UAbs. 1 lit. f DSGVO korrespondieren, bei seiner Interessenabwägung die entgegenstehenden Interessen oder Grundrechte und Grundfreiheiten in besonderer Weise zu berücksichtigen, „wenn es sich bei der betroffenen Person um ein Kind handelt".
- Von der Ausnahme des Verbots der Verarbeitung personenbezogener Daten bei einer automatisierten Entscheidung aufgrund einer Einwilligung nach Art. 22 Abs. 2 lit. c DSGVO sollte die Einwilligung eines Kindes ausdrücklich ausgenommen werden.[203] Die Wertung von Erwägungsgrund 71 Satz 5 DSGVO („Diese Maßnahme sollte kein Kind betreffen") findet bisher im Normtext keinen Niederschlag, sollte sich aber in diesem wiederfinden.[204] Die Einwilligung des Erziehungsberechtigten bliebe danach allerdings weiterhin möglich.
- Bei der datenschutzgerechten Systemgestaltung nach Art. 25 Abs. 1 DSGVO[205] sollte der Schutz der Grundrechte und Interessen von Kin-

201 S. z.B. auch Verbraucherzentrale Bundesverband, Evaluation, 2019, 7.
202 S. hierzu auch Klement, in: Simitis/Hornung/Spiecker 2019, Art. 8 Rn. 16.
203 Noch weitergehender Verbraucherzentrale Bundesverband, 2013, 17.
204 Europäische Akademie für Informationsfreiheit und Datenschutz, 2020, 4, fordert bei der Begrenzung der Erlaubnis Daten von Kindern besonders zu berücksichtigen.
205 S. hierzu allgemein Kap. 3.14.

dern in besonderer Weise gefordert werden. Gerade bei der Systemgestaltung wäre ein grundlegender Schutz von Kindern – vor allem in Social Networks und anderen Angeboten mit datengetriebenen Geschäftsmodellen – besonders wichtig – und meist auch leicht zu realisieren.
- Auch bei der datenschutzfreundlichen Voreinstellung nach Art. 25 Abs. 2 DSGVO[206] sollte der Schutz von Kindern in besonderer Weise gefordert werden. Sie übernehmen – mehr noch als Erwachsene – die voreingestellten Werte und konzentrieren sich allein auf die Nutzung des Geräts oder des Dienstes. Diese spezifische Voreinstellung für Kinder ist vor allem für Social Networks wichtig.[207] Gerade von Kindern kann nicht angenommen werden, dass sie Voreinstellungen erkennen und deren Bedeutung für ihre informationelle Selbstbestimmung verstehen. Sie sind in besonderer Weise darauf angewiesen, dass die Grundeinstellung jedes Risiko für ihren Datenschutz vermeidet.
- In der Datenschutzfolgenabschätzung nach Art. 35 DSGVO sollte das besondere Risiko und der besondere Schutzbedarf von Kindern in adäquater Weise berücksichtigt werden. Daher sollte sowohl für die Bestimmung der Notwendigkeit einer Datenschutzfolgenabschätzung nach Abs. 2 bis 4 als auch bei der Risikoanalyse und bei der Festlegung der Schutzmaßnahmen nach Abs. 7 dem Schutz der Grundrechte und Interessen von Kindern eine besondere Aufmerksamkeit entgegengebracht werden.[208]

Diese Schutzregelungen können mit geringem Aufwand, aber hoher Wirkung in den Text der jeweiligen Vorschrift aufgenommen werden. Über die besondere Schutzbedürftigkeit von Kindern dürfte auch kein politischer Streit entstehen.

3.7 Informationspräsentation

Die Informationspflichten wurden in Art. 13 und 14 DSGVO im Vergleich zu den Vorgängerregelungen der Datenschutzrichtlinie zwar inhaltlich ausgeweitet, aber an vielen Stellen sehr unscharf umschrieben. Vom Zweck der Informationspflichten, dem Verbraucher die Wahrnehmung seiner Rechte zu ermöglichen, sollten in der Form weiterentwickelt und im Inhalt präzisiert werden. Eine intensivere Überarbeitung ist für den

206 S. hierzu allgemein Kap. 3.15.
207 S. auch Roßnagel/Richter, 2017, 205 (242 f., 254 f.).
208 Anders noch der Kommissionsentwurf in Art. 32 Abs. 2 lit. d.

Text der Informationspflichten nach Art. 13 Abs. 2 lit. f und Art. 14 Abs. 2 lit. g DSGVO erforderlich.

3.7.1 Interessengerechte und an der Aufnahmekapazität ausgerichtete Information

Aus Verbrauchersicht von besonderer Relevanz ist zunächst die Form der Informationsvermittlung. Die Ausgestaltung der Information stellt für Verbraucher regelmäßig eine signifikante Hürde dar, tatsächlich Umfang und Tragweite einer Datenverarbeitung zu erfassen. Nach Art. 12 Abs. 1 Satz 1 DSGVO sind Informationen nach Art. 13 und 14 DSGVO sowie Mitteilungen nach Art. 15 DSGVO „in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache zu übermitteln". Dies soll umso mehr für Informationen gelten, die sich speziell an Kinder richten.[209] In der Praxis ergeben sich hier zwei Problemkreise. Einerseits werden entsprechende Erklärungen unter Umständen in Sprache und Form bewusst so gestaltet, dass sie beschwichtigend auf aktive oder potenzielle Nutzer wirken. Andererseits ist die Datenverarbeitung auch bei bestem Willen des Verantwortlichen, die betroffenen Personen bestmöglich zu informieren, unter Umständen so komplex, dass eine leicht zu erfassende Darstellung nicht gelingt.[210] Um den Zweck des Grundrechtsschutzes durch Information zu erreichen, müssten die Informationen so angeboten werden, dass sie den jeweiligen Interessen und der jeweiligen Aufnahmekapazität der betroffenen Person entsprechen. Sie müssten daher in unterschiedlichem Umfang und unterschiedlichen Konkretisierungsstufen (z.B. Icon, Informationen auf einer einzigen Seite oder umfangreiche Darstellung), die die betroffene Person wählen kann, präsentiert werden. Sie müsste somit der Nutzungssituation angemessen in unterschiedlichen Modi zur Verfügung gestellt werden. Dies wird so von Art. 12 DSGVO nicht ausdrücklich gefordert.

209 Hier verweist die Artikel 29-Datenschutzgruppe als auf die Konvention über die Rechte des Kindes – Für Kinder erklärt des Kinderhilfswerks der Vereinten Nationen als gelungenes Beispiel für kindgerechte Sprache; Leitlinien für Transparenz, WP 260 rev.01, 12.

210 Die Europäische Kommission kritisiert eine legalistische Übung der Verantwortlichen, Commission Staff Working Document, 21.

3.7.2 Mediengerechte Information

Die Übermittlung der Information sollte praktikabel sein. Sie soll zwar grundsätzlich im gleichen Medium übermittelt werden, wie die Datenerhebung erfolgt. Ein Medienbruch bei der Information sollte jedoch dann zulässig sein, wenn das Ausgangsmedium keinen Raum für eine ausreichende Information lässt oder keine geeignete Information ermöglicht. 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.[211] Gleichzeitig darf der Medienbruch nicht zu einer Umgehung von Informationspflichten missbraucht werden oder dem Verbraucher die Informationserlangung erschweren. Dabei ist auch die jeweilige Adressatengruppe und deren Technikaffinität zu berücksichtigen. Ein Medienbruch wäre damit nur unter engen Voraussetzungen zulässig und entsprechend begründungspflichtig.

3.7.3 Situationsadäquate Information

Um ihren gesetzlichen Zweck zu erfüllen, müssten die Informationen situationsadäquat, also dann gegeben werden, wenn der Verbraucher eine Entscheidung zu treffen hat – z.B. unmittelbar vor einer Einwilligung, vor der Nutzung eines Dienstes oder vor der Übertragung von Daten. Nach Art. 13 Abs. 1 DSGVO müssen die Daten „zum Zeitpunkt der Erhebung" mitgeteilt werden. In der bisherigen Praxis erfolgt die Mitteilung meist bei Vertragsabschluss oder beim ersten Kontakt mit der betroffenen Person. Dabei werden in Form von Datenschutzerklärungen oder Allgemeinen Geschäftsbedingungen alle Eventualitäten künftiger Datenverarbeitungen beschrieben.[212] Die Mitteilung kann dadurch Jahre vor der Datenerhebung liegen. Keine betroffene Person wird sich an die umfassenden Inhalte dieser Mitteilung erinnern, wenn die Daten tatsächlich erhoben werden. Diese Praxis entspricht nicht der Forderung, die Informationen „zum Zeitpunkt der Erhebung" mitzuteilen. Die Mitteilung muss vielmehr zum

211 S. hierzu z.B. Bundesrat, BR-Drs. 570/19, 5; Bundesregierung, ST 12756/1/19, 16; Datenschutzkonferenz, Erfahrungsbericht, 2019, 8; Deutscher Industrie- und Handelskammertag, 2019, 5, 7; Gesellschaft für Datenschutz und Datensicherheit, 2019, 2; Deutsche Telekom, 2019, 4; Jaspers/Jaquemain, DuD 2020, 297.

212 S. z.B. Dorfleitner/Hornuf, 2018, 2, 4, für die FinTech-Unternehmen in Deutschland.

richtigen Zeitpunkt erfolgen: zum Zeitpunkt der Datenerhebung und – aus dem Blickwinkel der Selbstbestimmung – vor einer notwendigen oder möglichen Entscheidung der betroffenen Person.[213] Dies sollte im Normtext dadurch zum Ausdruck gebracht werden, dass die *relevante* Information *jeweils* zum Zeitpunkt der Erhebung dieser Daten" erfolgt.[214]

Eng mit dem Zweck der Information für den Grundrechtsschutz hängt die Frage zusammen, wie gesichert werden kann, dass die Informationen für die betroffene Person handlungsrelevant sind. Dies ist die für die Selbstbestimmung letztlich die entscheidende Frage. In einer Situation extremer Machtasymmetrie oder in einem Anschluss an eine Infrastruktur (Take it or Leave it) gibt es für die betroffene Person keine Selbstbestimmung hinsichtlich der Datenverarbeitung, wenn sie auf die Leistung der anderen Seite angewiesen ist. Daher kommt es darauf an, künftige Datenverarbeitungssysteme so zu gestalten, dass für die betroffene Person ein hohes Maß an Auswahlmöglichkeiten besteht. Dies ist eine zentrale Aufgabe der von Art. 25 Abs. 1 DSGVO geforderten Gestaltung der Funktion des Datenverarbeitungssystems.[215]

Die Leitlinien der Artikel 29-Datenschutzgruppe für Transparenz[216] geben zwar wertvolle Hilfestellungen zur Auslegung der Art. 12 ff. DSGVO, jedoch ist die Befolgung der dort formulierten Praxis noch deutlich verbesserungsbedürftig. Präzision und Redlichkeit bei der Information sind aber zentral, da der Verbraucher sonst nur schwer abschätzen kann, welche Reichweite seine Einwilligung hat, welche Datenverarbeitung ihn betrifft und welche Rechte er geltend machen kann. Bleibt der Verantwortliche hier vage, indem er beispielhaft verkürzt, anstatt vollständige Angaben zu machen, oder angibt, dass „möglicherweise" mit bestimmten Handlungen seinerseits zu rechnen ist, anstatt definitive Angaben zu präsentieren, so können die mit den Transparenzpflichten der Grundverordnung verfolg-

213 S. auch Europäische Akademie für Informationsfreiheit und Datenschutz, 2020, 6 f.: „data processing actually intended"; Verbraucherzentrale Bundesverband, Evaluation, 2019, 8

214 Gesellschaft für Datenschutz und Datensicherheit, 2019, 2, fordert „im persönlichen Kontakt, beim Austausch von Visitenkarten, bei der Erst-Kontaktaufnahme per E-Mail oder der Erhebung von Daten am Telefon" die Information über die Datenverarbeitung, wenn sie nicht ohnehin sozial üblich ist, später bekannt geben zu dürfen. Andernfalls würde „häufig der erste (persönliche) Kontakt mit bürokratischen Transparenzpflichten konterkariert". S. hierzu auch Der Landesbeauftragte für Datenschutz und Informationsfreiheit Baden-Württemberg, Evaluierung, 2019, 6; Jaspers/Jaquemain, DuD 2020, 297.

215 S. hierzu Kap. 3.14.

216 Artikel 29-Datenschutzgruppe, Leitlinien für Transparenz, WP 260 rev.01.

ten Ziele nicht erreicht werden. Es sollte im Text des Art. 12 DSGVO festgehalten werden, dass sich die Information auf die gegenwärtig vorgesehene Datenverarbeitung beziehen muss. Künftige Änderungen in der Datenverarbeitung sollten zu neuen, dann wiederum aktuellen, Informationen führen. Es sollte ausdrücklich nicht zulässig sein, seine Informationspflicht zu erfüllen, indem alle denkbaren künftigen Datenverarbeitungen mit vagen Hinweisen auf künftige Möglichkeiten in eine einmalige Information aufgenommen werden.

3.7.4 Information durch Bildsymbole

Art. 12 Abs. 7 DSGVO sieht die Möglichkeit vor, die bereitzustellenden Informationen mit standardisierten Bildsymbolen zu kombinieren. Trotz initialer Rückschläge bei der Frage der konkreten Gestaltung dieser Bildsymbole stellt diese Neuerung einen äußerst begrüßenswerten Ansatz dar, in dem großes Potential steckt. Er sollte deshalb konsequent weiterverfolgt werden. In die gleiche Richtung geht letztlich die Etablierung von datenschutzspezifischen Zertifizierungsverfahren sowie von Datenschutzsiegeln und -prüfzeichen.[217] Hier geht es darum, den Verbraucher zu entlasten, der sich eine eigene Überprüfung der durch den Verantwortlichen bereitgestellten Informationen ersparen kann, wenn diese nachgewiesener Weise bereits durch einen vertrauenswürdigen Dritten erfolgt ist.

3.7.5 Technik- und bereichsspezifische Informationen

Außerdem sollte die Information für spezielle Anwendungsbereiche und Technologien bereichsspezifisch geregelt werden. Dies könnte im Rahmen von Verordnungen geschehen, die bereichsspezifisch etwa die Datenverarbeitung im intelligenten Fahrzeug regeln.[218] Der technologieneutrale Ansatz der Datenschutz-Grundverordnung gerät hier an seine Grenzen.

217 S. zum Stand der Einführung solcher Verfahren Maier/Bile, DuD 2019, 478.
218 S. hierzu Husemann, in: Roßnagel/Hornung, 2019, 367 ff.

3.8 Informationspflichten des Verantwortlichen

Bezogen auf konkrete Informationspflichten des Verantwortlichen zu Beginn der Datenverarbeitung sind einige Kritikpunkte zu erörtern.

3.8.1 Informationen über Empfänger

In Art. 13 Abs. 1 lit. e und Art. 14 Abs. 1 lit. e DSGVO sollte die Formulierung aufgenommen werden, dass über „die Empfänger, *soweit sie bestimmbar sind*, oder Kategorien von Empfängern der personenbezogenen Daten" zu informieren ist. Da die personenbezogenen Daten sehr oft weitergegeben werden, kann die betroffene Person ihre Rechte nur dann effektiv geltend machen, wenn sie die Empfänger kennt.[219] Soweit der Verantwortliche die Empfänger, denen er die Daten der betroffenen Person weitergibt, kennen kann, sollte er diese der betroffenen Person mitteilen, damit diese auch den Datenempfängern gegenüber ihre Rechte geltend machen kann.[220] Für den Verantwortlichen ist dies ein geringer Mehraufwand, für die betroffenen Personen aber die Grundvoraussetzung, um von ihren Rechten nach der Datenschutz-Grundverordnung überhaupt Gebrauch machen zu können.

3.8.2 Konflikt zwischen rechtlich geschützten Geheimnissen und Informationspflicht

Probleme bereitet auch die Information im Kontext von automatisierter Entscheidungsfindung im Einzelfall gemäß Art. 13 Abs. 2 lit. f und 14 Abs. 2 lit. g DSGVO. Die Reichweite der Informationspflicht wie auch des Auskunftsrechts nach Art. 15 Abs. 1 lit. h DSGVO bezogen auf Art. 22 Abs. 1 und 4 DSGVO umfasst dabei „aussagekräftige Informationen über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung für die betroffene Person". Diese zu-

219 Dies findet in Deutschland selten statt – s. z.B. Dorfleitner/Hornuf, 2018, 2, 26 ff. für die FinTech-Unternehmen in Deutschland.

220 S. z.B. auch Europäische Akademie für Informationsfreiheit und Datenschutz, 2020, 6; Verbraucherzentrale Bundesverband, Evaluation, 2019, 8; auf gegenteilige Forderungen weist Der Landesbeauftragte für Datenschutz und Informationsfreiheit Baden-Württemberg, Evaluierung, 2019, 6, hin.

nächst weit erscheinende Formulierung erfährt durch Erwägungsgrund 63 Satz 5 DSGVO jedoch eine einschränkende Auslegung. So sollen insbesondere Geschäftsgeheimnisse und Rechte des geistigen Eigentums nicht dem Auskunftsrecht unterfallen. Zwar stellt Erwägungsgrund 63 Satz 6 DSGVO klar, dass das Vorliegen eines Geschäftsgeheimnisses oder geistigen Eigentums nicht dazu führen darf, dass der betroffenen Person jegliche Auskunft verweigert wird. Dies beinhaltet jedoch nur eine Grenzziehung nach unten, dass eine Information der betroffenen Person nicht vollständig entfallen darf. Wie der Konflikt zwischen Informationsanspruch und Geheimnisschutz oberhalb dieser Grenze gelöst werden soll, lässt die Datenschutz-Grundverordnung offen und gibt die Entscheidung damit in die Hand des Verantwortlichen. Hier ist eine Abwägung des Gesetzgebers notwendig, der zumindest eine Grundregel für die Auflösung des Konflikts festlegen müsste. Diese könnte zum Beispiel so lauten, dass – unter Wahrung des Geschäftsgeheimnisses oder des geistigen Eigentums – dennoch ein möglichst hohes Maß an Information bereitgestellt werden muss.[221] Hier könnten Überlegungen ansetzen, in der Praxis die bereitzustellenden Informationen im Bereich des Geheimnisses zu „verrauschen" und so etwa geheim zu haltende Bestandteile des Entscheidungsverfahrens zu schützen, gleichzeitig aber ein Maximum an Information zu ermöglichen.[222]

3.8.3 Informationen über automatisierte Entscheidungsverfahren

Der Verantwortliche hat „aussagekräftige" Informationen „über die involvierte Logik sowie die Tragweite" für die betroffene Person zu geben. Über den Umfang und die Tiefe dieser Information ist großer Streit entbrannt. Hier sollte in einer Überarbeitung der Vorschrift klargestellt werden, dass die Information über die Tragweite auch die rechtlichen und tatsächlichen Auswirkungen auf die betroffene Person umfasst. Hinsichtlich der Information über die „involvierte Logik" müssen auch die abstrakten Kriterien[223] für die Entscheidung und ihre Gewichtung enthalten sein.[224] Die betroffene Person muss nach der Information in der Lage sein, ihr Verhalten

221 S. auch Netzwerk Datenschutzexpertise, 2019, 7 f.

222 S. z.B. Bäcker, in: Kühling/Buchner, 2018, Art. 13 Rn. 54 unter Verweis auf Kugelmann, DuD 2016, 566 (568).

223 Im Gegensatz zur Auskunft nach Art. 15 Abs. 1 lit. h DSGVO – s. Kap. 3.9.2.

224 Artikel 29-Datenschutzgruppe, Leitlinien zu automatisierten Entscheidungen im Einzelfall einschließlich Profiling, WP 251 rev.01, 30; Verbraucherzentrale Bundesverband, 2013, 13; Verbraucherzentrale Bundesverband, Algorithmen-

so anzupassen, dass sie die entscheidenden Kriterien erfüllt oder zumindest konkret nachvollziehen kann, warum die Entscheidung nicht zu ihren Gunsten ausfällt.[225] Nur so kann verhindert werden, dass sie als Persönlichkeit einem für sie unverständlichen algorithmenbasierten System unterworfen wird.

Aussagekräftig sind die Informationen, wenn sie in der Lage sind, bei der betroffenen Person das genannte Verständnis hervorzurufen. Dies fordert vom Verantwortlichen, „einfache Möglichkeiten [zu] finden, die betroffene Person über die der Entscheidungsfindung zugrunde liegenden Überlegungen bzw. Kriterien zu informieren".[226] Komplexität ist „keine Entschuldigung" für mangelhafte Information. Dies dürfte gerade bei selbstlernenden Systemen eine Herausforderung für den Verantwortlichen darstellen. Gerade deshalb sollte diese Klarstellung zumindest in einen Erwägungsgrund aufgenommen werden.

An dem Eingriff in das Datenschutzrecht und die informationelle Selbstbestimmung der betroffenen Person ändert sich gar nichts, wenn die automatisierte Entscheidung arbeitsteilig getroffen wird. Daher darf eine Arbeitsteilung nicht dazu führen, dass die Information unterbleibt oder verkürzt erfolgt. Findet das arbeitsteilige automatisierte Entscheidungsverfahren in einem Auftragsverhältnis nach Art. 28 DSGVO statt, hat der Auftraggeber die umfassende Information zu geben. Findet das arbeitsteilige automatisierte Entscheidungsverfahren durch mehrere Kooperationspartner statt, sollte jeder über den Teil samt den Schnittstellen zu allen anderen Teilen informieren, den er verantwortet. Dies sollte in der Vorschrift festgehalten werden.

Im Ergebnis darf eine arbeitsteilige Durchführung der automatisierten Entscheidung etwa in der Form, dass die Auskunftei A ein Verbraucherprofil erstellt, aus dem der Bonitätsprüfer B einen Score-Wert errechnet, der im Kreditvergabesystem des Online-Händlers C zu einem Verbraucherkredit oder einer bestimmten Bezahlweise führt,[227] nicht dazu führen, dass Informationslücken für die betroffene Person entstehen. In diesem Fall muss es so sein, dass alle drei Verantwortlichen die betroffene Person über

---

kontrolle, 2019, 13; Netzwerk Datenschutzexpertise, 2019, 7; Glatzner, DuD 2020, 312.

225 Artikel 29-Datenschutzgruppe, Leitlinien zu automatisierten Entscheidungen im Einzelfall einschließlich Profiling, WP 251 rev.01, 28.

226 Artikel 29-Datenschutzgruppe, Leitlinien zu automatisierten Entscheidungen im Einzelfall einschließlich Profiling, WP 251 rev.01, 28.

227 S. ähnlich Artikel 29-Datenschutzgruppe, Leitlinien zu automatisierten Entscheidungen im Einzelfall einschließlich Profiling, WP 251 rev.01, 28.

ihren jeweiligen Beitrag zum automatisierten Entscheidungsverfahren informieren müssen, ganz gleich ob sie die eigentliche Entscheidung treffen oder diese lediglich vorbereiten. Dies muss die Vorschrift klarstellen.

Inhaltliche Erweiterungen würde die Vorschrift indirekt erfahren, wenn das Verbot des Art. 22 Abs. 1 DSGVO den Vorschlägen dieses Gutachtens entsprechend erweitert würde.[228]

3.8.4 Information über Profiling

Profiling ist in Art. 4 Nr. 4 DSGVO definiert und in Art. 22 Abs. 1 DSGVO sowie in Art. 13 Abs. 2 lit. f, 14 Abs. 2 lit. g und 15 Abs. 12 lit. h DSGVO in der eigentümlichen Form „einschließlich Profiling" erwähnt. Profiling hat in der Datenschutz-Grundverordnung jedoch keine eigenständige Regelung erfahren, obwohl dies nach dem risikobasierten Absatz der Verordnung erforderlich gewesen wäre. Profiling als automatisierte Sammlung von Persönlichkeitsmerkmalen zur Bewertung einer betroffenen Person ist ein tiefer Eingriff in die Grundrechte auf Datenschutz und informationelle Selbstbestimmung. Von solchen Bewertungsprofilen gehen insbesondere für Verbraucher besondere, über die normale Verarbeitung personenbezogener Daten hinausgehende Risiken für die freie Entfaltung und Entscheidung und die gerechte Beurteilung aus. Daher sollte die betroffene Person zumindest über jedes Profiling informiert werden, auch wenn dieses nicht unmittelbar mit einer automatisierten Entscheidung verbunden ist, sondern für andere Bewertungszwecke verwendet wird.[229] Daher sollten die Vorschriften der Art. 13 Abs. 2 lit. f und 14 Abs. 2 lit. g DSGVO dahingehend ausgeweitet werden, dass über jede automatisierte Entscheidung und über jedes Profiling informiert werden muss.[230]

228 S. näher Kap. 3.11.

229 S. z.B. auch Martini, 2019, 10; Glatzner, DuD 2020, 312; Europäische Akademie für Informationsfreiheit und Datenschutz, 2020, 4; Niederlande, ST 12756/1/19, 42, 44, fordert eine entsprechende Transparenz, insbesondere, wenn das Profil zu individueller Preisbildung genutzt wird.

230 Zu weiteren Regelungsvorschlägen hinsichtlich algorithmenbasierter Systeme s. Kap. 3.11.

3.9 Das Auskunftsrecht der betroffenen Person

Ähnlich wie für die Informationspflichten sind die Informationen, die zur Erfüllung des Auskunftsrechts nach Art. 15 DSGVO zu geben sind, zu präzisieren, um die grundrechtsschützende Funktion des Auskunftsrechts zu wahren.[231]

3.9.1 Auskunft über Empfänger

Das Gleiche, wie zu Art. 13 Abs. 1 lit. e und Art. 14 Abs. 1 lit. e DSGVO hinsichtlich der Empfänger von personenbezogenen Daten aufgeführt, gilt erst recht bei einem Auskunftsanspruch nach Art. 15 Abs. 1 lit. c DSGVO.[232] Die Auskunft soll der betroffenen Person die Informationen verschaffen, um ihre Rechte nach der Datenschutz-Grundverordnung wahrnehmen zu können.[233] Hierzu gehört in erster Linie die Identität aller Verantwortlichen, um ihnen gegenüber ihr Recht gelten machen zu können. Wenn der Verantwortliche, gegenüber dem die betroffene Person ihr Auskunftsrecht geltend macht, durch die Weitergabe der Daten dafür verantwortlich ist, dass die Empfänger auch zu Verantwortlichen geworden sind, die Daten der betroffenen Person verarbeiten, dann ist es auch gerechtfertigt, von ihm die Mitteilung zu verlangen, an wen er die Daten weitergeleitet hat. Denn diese Weiterleitung ist ein gesonderter Eingriff in das Grundrecht auf Datenschutz der betroffenen Person. Dieser Eingriff mag gerechtfertigt sein, eventuell auch die weitere Datenverarbeitung durch den Empfänger. Aber die betroffene Person sollte in der Lage sein, dies zu überprüfen. Der Verantwortliche sollte daher verpflichtet sein, alle

231 S. aber auch die Stimmen, die unter Verweis auf missbräuchliches Verhalten eine Einschränkung des Auskunftsrechts fordern: s. z.B. Der Landesbeauftragte für Datenschutz und Informationsfreiheit Baden-Württemberg, Evaluierung, 6 („Pervertierung des Auskunftsrechts als Instrument der ‚Selbstjustiz'"); Digitaleurope, 2020, 8 f.; Deutsche Telekom, 2019, 5 („Ein erheblicher Teil der Auskunftsanfragen wird durch professionelle Anbieter erzeugt, die zur Geltendmachung von Auskunftsansprüchen motivieren. Diese Anbieter verfolgen häufig durch die Generierung einer möglichst hohen Anzahl von Auskunftsanfragen ein eigenes kommerzielles Interesse gegenüber dem Verantwortlichen."); s. auch Schulz, DuD 2020, 302.

232 S. hierzu auch Verbraucherzentrale Bundesverband, 2013, 12.

233 Erwägungsgrund 63 DSGVO; s. z.B. auch Der Hessische Beauftragte für Datenschutz und Informationsfreiheit, 2019, 76; Brink/Joos, ZD 2019, 483 (384).

Empfänger der personenbezogenen Daten zu protokollieren und der betroffenen Person das sie betreffende Protokoll bekanntzugeben.[234]

3.9.2 Auskunft über automatisierte Entscheidungsverfahren

Nach Art. 15 Abs. 1 lit. h DSGVO hat die betroffene Person einen Anspruch auf „aussagekräftige Informationen über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung für die betroffene Person". Im Gegensatz zur Information nach Art. 13 Abs. 2 lit. f und Art. 14 Abs. 2 lit. g DSGVO,[235] die die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen nur abstrakt beschreiben muss, ist die Auskunft über diese Themen personenspezifisch zu erteilen. Diese Auskunft muss um die relevanten Merkmale und deren Bedeutung für die automatisierte oder automatisiert vorbereitete Entscheidung ergänzt werden. Nur mit dieser Information kann die betroffene Person ihr Verhalten so einrichten, dass sie Chancen hat, die gewünschte Entscheidung zu erreichen.[236]

Eine gesonderte Information sollte nach einem geänderten Art. 15 Abs. 1 lit. h DSGVO der betroffenen Person auch für jedes Profiling, dessen Umfang, Inhalt, Zielsetzung und Verwendungszweck gegeben werden müssen.[237]

3.9.3 Recht auf Erhalt einer Kopie

Nach Art. 15 Abs. 3 Satz 1 DSGVO hat der Verantwortliche der betroffenen Person auf Antrag „eine Kopie der personenbezogenen Daten, die Gegenstand der Verarbeitung sind, zur Verfügung" zu stellen.[238] Kaum eine Regelung in der Datenschutz-Grundverordnung ist so misslungen und daher umstritten.[239] Dies beginnt schon mit der Frage, ob das „Recht auf Er-

234 S. Europäische Akademie für Informationsfreiheit und Datenschutz, 2020, 6 f.
235 S. Kap. 3.8.3.
236 S. auch Kap. 3.9.
237 S. hierzu auch Kap. 3.11.
238 Hier sieht auch die Bundesregierung einen Konkretisierungsbedarf – Bundesregierung, ST 12756/1/19, 13; Bundesrat, BR-Drs. 570/19, 6; Gesellschaft für Datenschutz und Datensicherheit, 2019, 3.
239 S. z.B. Zikesch/Sörup, ZD 2019, 239 (239, 243); Wybitul, ZD 2019, 278; Lapp, NJW 2019, 345 (347); Härting, CR 2019, 219 (221 ff.); Engeler/Quiel, NJW

halt einer Kopie“ (Art. 15 Abs. 4 DSGVO) ein eigenständiger Anspruch der betroffenen Person ist[240] oder nur eine Form der Auskunft nach Art. 15 Abs. 1 DSGVO.[241] Der Streit geht weiter mit der Frage, was eine Kopie ist,[242] ob diese eine umfassende Wiedergabe aller zu einer betroffenen Person vorhandenen Datensätze beinhalten muss,[243] welcher „Gegenstand der Verarbeitung“ kopiert werden muss[244] und endet nicht in den Problemen, ob der Anspruch auf eine Kopie eigens geltend gemacht werden muss[245] oder nicht[246] sowie in welcher Form die Kopie übergeben werden muss.[247]

Dieses „Recht auf Erhalt einer Kopie“ ist vom Ansatz her eine sinnvolle Lösung:[248] Der Verantwortliche wird durch eine schlichte Kopie eines Da-

---

2019, 2201; Wybitul/Brams, NZA 2019, 672; Brink/Joos, ZD 2019, 483; Weik, DuD 2020, 98; Schulz, DuD 2020, 302; Jaspers/Jaquemain, DuD 2020, 297; LAG Baden-Württemberg, ZD 2019, 276. Der Bundesrat spricht von „großer Unsicherheit“: BR-Drs. 570/19, 5; s. auch Der Landesbeauftragte für Datenschutz und Informationsfreiheit Baden-Württemberg, Evaluierung, 2019, 6; Datenschutzkonferenz, Erfahrungsbericht, 2019, 9; Gesellschaft für Datenschutz und Datensicherheit, 2019, 3; Deutschland, in: Rat, ST 12756/1/19, 13; Digitaleurope, 2020, 8; Deutsche Telekom, 2019, 2.

240 So z.B. Bäcker, in Kühling/Buchner, 2018, Art. 15 Rn. 39; Schwartmann/Klein, in: Schwartmann u.a., 2018, Art. 15 Rn. 34; Spindler, DB 2016, 937 (944); Härting, CR 2019, 219 (220); Engeler/Quiel, NJW 2019, 2201 (2202); Brink/Joos, ZD 2019, 483 f.; Weik, DuD 2020, 98 (100 ff.).

241 So z.B. Der Hessische Beauftragte für Datenschutz und Informationsfreiheit, 2019, 77 f.; Bayerisches Landesamt für Datenschutz, 2019, 46; Raith 2019, 223 f.; Paal, in: Paal/Pauly, 2018, Art. 15 Rn. 33; Franck, in: Gola, 2018, Art. 15 Rn. 27; Specht, in: Sydow, 2018, Art. 15 Rn. 18; Veil, in: Gierschmann/Schlender/Stenzel, 2018, Art. 15 Rn. 209; Zikesch/Sörup, ZD 2019, 239 (240); Wybitul, ZD 2019, 278 (279); Kamlah, in: Plath, 2018, Art. 15 Rn. 16.

242 S. z.B. Der Hessische Beauftragte für Datenschutz und Informationsfreiheit, 2019, 77 f.; Härting, CR 2019, 219 (221 ff.); Engeler/Quiel, NJW 2019, 2201 (2202 f.).

243 So z.B. Dix, in: Simitis/Hornung/Spiecker, 2019, Art. 15 Rn. 36; Engeler/Quiel, NJW 2019, 2201 (2203); a.A. Dausend, ZD 2019, 103; Zikesch/Sörup, ZD 2019, 239 (243); Specht, in: Sydow, 2018, Art. 15 Rn. 18; Wybitul 2016, Kap. IV, Rn. 166.

244 S. z.B. Härting, CR 2019, 219 (222).

245 S. z.B. Bäcker, in Kühling/Buchner, 2018, Art. 15 Rn. 39.

246 S. z.B. Dix, in: Simitis/Hornung/Spiecker, 2019, Art. 15 Rn. 29; Ehmann, in: Ehmann/Selmayr, 2018, Art. 15 Rn. 25; Engeler/Quiel, NJW 2019, 2201 (2205).

247 S. z.B. z.B. Der Hessische Beauftragte für Datenschutz und Informationsfreiheit, 2019, 78. Engeler/Quiel, NJW 2019, 2201 (2204).

248 So z.B. auch Jaspers/Jaquemain, DuD 2020, 297; a.A. IHK München und Oberbayern, 2019, 1.

tensatzes nur wenig belastet.[249] Eine Mitteilung aller verarbeiteten Daten ist dann nicht notwendig. Für die betroffene Person gibt die „Kopie der personenbezogenen Daten, die Gegenstand der Verarbeitung sind," eine geeignete Prüfgrundlage für die Fragen, welche Daten von ihr in welchem Verarbeitungszusammenhang verarbeitet werden und ob diese Datenverarbeitung rechtmäßig ist. Allerdings kann eine Kopie der verarbeiteten Daten eine Erläuterung erforderlich machen, wenn sie für die betroffene Person ansonsten nicht verständlich wäre. Wenn das „Recht auf Erhalt einer Kopie" sich vom Recht auf Auskunft unterscheidet, sollte dieses Recht ausdrücklich eingefordert werden müssen.[250]

Umstritten ist jedoch, was eine „Kopie der personenbezogenen Daten, die Gegenstand der Verarbeitung sind," sein kann. Dies ist leicht zu beantworten, soweit die Daten der betroffenen Person in einem Datensatz oder in einem Dateiordner gespeichert sind, wie dies etwa ein Account, eine Personalakte, eine Kunden- oder eine Krankenakte, ein Persönlichkeitsprofil oder ähnlich geschlossene Datensammlungen sind. Schwierig ist es jedoch die „personenbezogenen Daten, die Gegenstand der Verarbeitung sind", von anderen Daten, auf deren Kenntnis die betroffene Person kein Recht hat, abzugrenzen, wenn sie mit anderen Daten in Geschäftsvorgängen, Protokollen, Logdateien, Backup-Dateien, Kommunikationsverläufen, Infrastruktur- oder Geräteprozessen verarbeitet werden, die nicht nach betroffenen Personen geordnet sind und auch nicht nach diesen strukturiert werden können.[251] Dass ein Datum der betroffenen Person in einem Geschäftsvorgang vorkommt, kann nicht dazu führen, ihr den gesamten – unter Umständen sehr umfangreichen – Geschäftsvorgang in Kopie zur Kenntnis zu geben. Die Rechtsunsicherheit, wo die Grenze des berechtigten Anspruchs auf eine Kopie liegt, führt dazu, dass betroffene Personen davor zurückschrecken, dieses Recht in Anspruch zu nehmen, und dass Verantwortliche sich weigern, diesen Anspruch zu erfüllen. Daher ist es notwendig, dass das Recht auf eine „Kopie der personenbezogenen Daten, die Gegenstand der Verarbeitung sind", in einer Weise präzisiert wird, dass

249 S. den Hinweis des Erwägungsgrunds 63 DSGVO auf die Verwendung von Datendownloadtools. Diese werden von Social-Media-Anbieter überwiegend angewendet – s. zu den unzureichenden Ergebnissen jedoch Scheibel/Horn/Öksüz, 2018, 13 ff.

250 S. auch Litauen, in: Rat, ST 12756/1/19, 36: „In our view Article 15(3) of the Regulation could be amended to provide that a data subject should only receive a copy of their personal data if they so request."

251 S. z.B. Zikesch/Sörup, ZD 2019, 239.

es in der Praxis handhabbar wird, und der Verbraucher in die Lage versetzt wird, es gezielt in Anspruch zu nehmen.

Kann der Verantwortliche keine Kopie zur Verfügung stellen, ist eine strukturierte, aufgearbeitete Liste aller verarbeiteten Daten notwendig, damit die betroffene Person überprüfen kann, ob die über sie gespeicherten Daten korrekt sind und ihre Verarbeitung durch den angegebenen Erlaubnistatbestand erlaubt ist. Die Angabe der Kategorien personenbezogener Daten, die verarbeitet werden, nach Art. 15 Abs. 1 lit. b DSGVO kann dann nicht ausreichen. Für diese Fälle ist Abs. 1 um die Angabe der verarbeiteten Daten zu ergänzen. In bestimmten Fällen, in denen die Kopie eines Dokuments oder eines Auszugs aus einem komplexen Datensatzes notwendig ist, um die Rechtmäßigkeit der Datenverarbeitung zu überprüfen, ist eine solche Kopie oder ein solcher Auszug vorzulegen.[252]

Diese Klarstellung sowie die im folgenden Kapitel vorgeschlagene Klarstellung zum Anwendungsbereich des Rechts auf Datenübertragung nach Art. 20 DSGVO würde auch den Unterschied zwischen der Übermittlung einer Kopie und der Übertragung von Daten der betroffenen Person verdeutlichen:[253] Die Kopie würde die der betroffenen Person zugeordnete Datensammlung betreffen, unabhängig davon, ob die betroffene Person die Daten „bereitgestellt" hat und unabhängig davon, auf welcher Rechtsgrundlage die Daten verarbeitet werden. Dagegen besteht das Recht auf Datenübertragung nur unter zwei Voraussetzungen, die für das Recht auf eine Kopie nicht gelten: Zum einen kann die Datenübertragung nur gefordert werden, wenn die Verarbeitung personenbezogener Daten „auf einer Einwilligung gemäß Art. 6 Abs. 1 UAbs. 1 lit. a oder Art. 9 Abs. 2 lit. a oder auf einem Vertrag gemäß Art. 6 Abs. 1 UAbs. 1 lit. b DSGVO beruht". Zum anderen gilt sie nur für alle die Datensammlungen, die die betroffene Person verursacht oder veranlasst hat, auch wenn dies Daten von Dritten mit umfasst, die die betroffene Person rechtmäßig verarbeitet hat. Außerdem muss die Kopie nicht in einer weiterverarbeitbaren Form übermittelt werden, während die Datenübertragung nur dann Sinn macht, wenn sie vom Empfänger weiterverarbeitet werden kann.

252 Der Hessische Beauftragte für Datenschutz und Informationsfreiheit, 2019, 78; Zikesch/Sörup, ZD 2019, 239 (243).

253 Dies übersehen z.B. Der Hessische Beauftragte für Datenschutz und Informationsfreiheit, 2019, 77 f.; Zikesch/Sörup, ZD 2019, 239 (241); Jaspers/Jaquemain, DuD 2020, 297; s. zum Problem auch Deutsche Telekom 2019, 2 f.

3.10 Das Recht auf Datenübertragung

Während die Rechte der betroffenen Personen aus dem Katalog der Datenschutz-Grundverordnung im Wesentlichen dem entsprechen, was auch bereits unter dem Regime der Datenschutzrichtlinie galt, stellt das Recht auf Datenübertragung eine der prominentesten Neuerungen des neuen Datenschutzrechts dar.[254] Es gibt der betroffenen Person das Recht, Daten, die sie dem Verantwortlichen bereitgestellt hat, auf einen anderen Datenverarbeiter zu übertragen. Diese nicht zuletzt auf soziale Netzwerke abzielende Regelung[255] soll sog. Lock-in-Effekte reduzieren helfen und den Wettbewerb zwischen Anbietern steigern.[256]

Die Bezeichnung des Rechts ist missglückt. Art. 20 DSGVO regelt einen Anspruch auf eine Handlung und eine Pflicht zu einer Handlung, nämlich die Bereitstellung personenbezogener Daten (Abs. 1) und deren Übertragung durch die betroffene Person (Abs. 1) oder den Verantwortlichen (Abs. 2), nicht ein Recht zur Herstellung einer Möglichkeit. Wie die anderen Rechte der betroffenen Person nicht mit Informierbarkeit, Korrigierbarkeit, Löschbarkeit oder Einschränkbarkeit überschrieben sind, sondern mit Auskunft, Berichtigung, Löschung und Einschränkung die geforderte Handlung nennen, sollte auch Art. 20 DSGVO mit „Recht auf Übertragung" überschrieben werden.[257]

Die Nutzung dieses Rechts ist für Verbraucher jedoch durch drei Probleme, die der Normtext verursacht, gefährdet: erstens durch den zu engen Anwendungsbereich[258] des Rechts auf Datenübertragung und zweitens durch die zu geringe Bestimmtheit über das Format, in dem die Daten übergeben werden sollen.[259] Schließlich ist die Regelung zu eng, weil sie eine bestehende Einwilligung oder einen bestehenden Vertrag voraussetzt.

---

254 Roßnagel, DuD 2019, 467 (468).

255 S. Gesellschaft für Datenschutz und Datensicherheit, 2019, 3 und Jaspers/Jaquemain, DuD 2020, 297, die mit Verweis auf die Genese der Norm eine Beschränkung ihres Anwendungsbereichs auf (Online-)Portale fordert.

256 S. Europäische Kommission, COM(2020) 264 final, 8; Commission Staff Working Document,21; Kühling/Sackmann, 2018, 21; Stiftung Datenschutz, 2018, 10, 13 ff.

257 Das Recht als „Marketing-Gag" ersatzlos zu streichen, fordert Schulz, DuD 2020, 302.

258 S. Niederlande, in: Rat, ST 12756/1/19, 41: „quite narrow".

259 Den Mangel an Standards stellt selbst die Kommission fest, COM(2020) 264 final, 8; Commission Staff Working Document, 21.

3.10.1 Anwendungsbereich der Vorschrift

Das Recht auf Datenübertragung sollte nicht nur für die von der betroffenen Person „bereitgestellten" personenbezogenen Daten gelten, sondern auch für die von der betroffenen Person verursachten Daten. Zwar könnte mit einer umstrittenen[260] Auslegung vertreten werden, „bereitgestellten" Daten seien nicht nur die aktiv in das Dienstangebot eingestellten Daten, sondern auch personenbezogene Daten, die das Ergebnis der Beobachtung der Tätigkeit der betroffenen Person sind.[261] Die Bereitstellung durch den Nutzer erfolge dabei durch die Nutzung des Dienstes oder Geräts.[262] Beispiele sind Suchverläufe, Playlists, Verkehrs- und Standortdaten, Fitnessdaten oder ähnliche Daten.[263] Als eingegeben sollten auf jeden Fall auch Daten gelten, die der Verbraucher mittels eines Trackers erhebt und über eine Schnittstelle in das System des Verantwortlichen eingibt. Als nicht bereitgestellt sollen dagegen Daten gelten, die der Verantwortliche aus der Analyse und Zusammenführung der bereitgestellten Daten gewonnen hat – wie etwa Bonitäts-Scores und andere Profiling-Ergebnisse.[264]

Dieses Verständnis überzeugt vor dem Hintergrund des Normzwecks, der in einer Stärkung des Wettbewerbs und dem Schutz der Verbraucher liegt.[265] Letztlich geht es darum, Einflusssphären zwischen Verantwortlichem und betroffener Person abzugrenzen und den Beitrag zum Entstehen der Daten zu würdigen. Aus ihrem Beitrag zum Entstehen der Daten leitet sich die Verfügungsbefugnis der betroffenen Person ab. Soweit die betroffene Person das Entstehen der Daten verursacht hat, der Verantwortliche aber hierzu wenig beigetragen hat, indem er etwa lediglich die Infrastruktur bereitstellt, sollen die entstandenen Daten auch unter der Verfügungs-

260 S. a.A. z.B. Piltz, in: Gola, 2018, Art. 20 Rn. 14; Richter, PinG 2017, 231; Kamann/Braun, in: Ehmann/Selmayr, 2018, Art. 20 Rn. 13; Westphal/Wichtermann, ZD 2019, 191 (192).

261 Artikel 29-Datenschutzgruppe, Leitlinien zum Recht auf Datenübertragbarkeit, WP 242 rev.01, 11; Kühling/Sackmann, 2018, 21.

262 S. Verbraucherzentrale Bundesverband, 2016, 6; Scheibel/Horn/Öksüz 2018, 4.

263 Artikel 29-Datenschutzgruppe, Leitlinien zum Recht auf Datenübertragbarkeit, WP 242 rev.01, 11; Niederlande, ST 12756/1/19, 41; Dix, in Simitis/Hornung/Spiecker, 2019, Art. 20 Rn. 8; Herbst, in: Kühling/Buchner, 2018, Art. 20 Rn. 11.

264 Artikel 29-Datenschutzgruppe, Leitlinien zum Recht auf Datenübertragbarkeit, WP 242 rev.01, 11 nennen diese „abgeleitete" Daten. S. hierzu auch Westphal/Wichtermann, ZD 2019, 191.

265 S. Roßnagel/Richter/Nebel, ZD 2013, 103 (107); Nebel/Richter, ZD 2012, 407 (413); Schantz, NJW 2016, 1841 (1845).

und Nutzungsgewalt der betroffenen Person stehen.[266] Aus dieser Logik heraus wird klar, dass eine Erstreckung von Art. 20 DSGVO auch auf Rohdaten erfolgen muss, die vom Verhalten der betroffenen Person verursacht werden.[267]

Auch für Daten Dritter, die die betroffene Person in ihrem Bereich auf der Plattform verarbeitet hat, soll sie ein Recht auf Datenübertragung haben, wenn sie diese Daten rechtmäßig verarbeitet. Dies gilt etwa für ihre Kontaktdaten[268] oder ihre Bilder, auf denen auch andere Personen zu sehen sind. Gerade Daten, die von anderen Personen an die betroffene Person übermittelt worden sind, werden vom Wortlaut der Vorschrift nicht erfasst, müssten aber von der Zielsetzung der Vorschrift erfasst sein. Dies gilt insbesondere bei Kommunikationsvorgängen. Zumindest sollten alle die Daten von der Vorschrift erfasst werden, die sich ausschließlich in der Sphäre der betroffenen Person befinden, wie z.B. E-Mails im Eingangspostfach. Dass die Nachrichten im Ausgangspostfach – weil von der betroffenen Person eingegeben – übertragen werden können, die Nachrichten im Eingangspostfach aber nicht, wäre widersinnig. Das Gleiche muss aber auch für Chats oder Messenger-Dienste gelten, auf die auch andere Personen zugreifen können. Wenn sich Beitrag an Beitrag reiht und die betroffene Person zur Kommunikation beigetragen hat, wäre es unverständlich, wenn sie nur ihre Beiträge übertragen könnte, nicht aber die Beiträge anderer, auf die sich ihre Beiträge beziehen. Bei beiden Gruppen handelt es sich um nachträglich nicht mehr veränderbare Nachrichten einer Person an die betroffene Person als Empfänger. Der Empfänger muss davon ausgehen können, dass eine persönliche Nachricht (auch) an ihn zu seiner freien Verfügung steht.[269] Im Ergebnis muss dies auch für Geschäftsvorgänge gel-

266 S. auch Europäische Akademie für Informationsfreiheit und Datenschutz, 2020, 7: „It should also be ensured that the right covers all data processed by automated means that the data subject has generated (including metadata) and not only those that he has deliberately entered into a system."

267 S. zum Streit Kamann/Braun, in: Ehmann/Selmayr, 2018, Art. 20 Rn. 13. S. wie hier auch Europäische Akademie für Informationsfreiheit und Datenschutz, 2020, 7: „including metadata"; Verbraucherzentrale Bundesverband, Evaluation, 2019, 9; a.A. Deutsche Telekom 2019, 3, die eine Klarstellung fordert, dass das Recht „keine Daten erfasst, die bei der Nutzung des Dienstes durch die betroffene Person automatisch vom Dienst erzeugt wurden (z.B. Logdateien, Verkehrs- oder Standortdaten)".

268 Artikel 29-Datenschutzgruppe, Leitlinien zum Recht auf Datenübertragbarkeit, WP 242 rev.01, 10 f.; Niederlande, ST 12756/1/19, 41.

269 Ähnlich auch Artikel 29-Datenschutzgruppe, Leitlinien zum Recht auf Datenübertragbarkeit, WP 242 rev.01, 11; Schantz, NJW 2016, 1841 (1845).

ten, die die betroffene Person betreffen, wie etwa Einzahlungen oder Belastungen auf ihren Konten. So würde einer Lösung jede Plausibilität fehlen, wenn sie nur die von ihr veranlassten Überweisungen oder Einzahlungen übertragen könnte, nicht aber die Überweisungen Dritter auf ihr Konto oder die Abbuchungen Dritter von ihrem Konto. Der Begriff „bereitgestellt" ist daher zu eng und sollte, um sinnvolle Ergebnisse zu erzielen, durch „verursacht oder veranlasst" ersetzt werden.

3.10.2 Beschränkung auf geltende Einwilligungen oder Verträge

Das Recht auf Datenübertragung besteht nach Art. 20 Abs. 1 DSGVO nur, wenn die Verarbeitung auf einer Einwilligung gemäß Art. 6 Abs. 1 UAbs. 1 lit. a oder Art. 9 Abs. 2 lit. a DSGVO oder auf einem Vertrag gemäß Art. 6 Abs. 1 UAbs. 1 lit. b DSGVO beruht. Ungeklärt ist die Frage, ob dieser Anspruch auch noch zu dem Zeitpunkt besteht, wenn die Einwilligung widerrufen oder der Vertrag beendet worden ist.[270] Für diesen Fall wird vertreten, dass eine Übertragung der Daten nicht mehr gefordert werden kann, weil die Datenverarbeitung nach dem Widerruf oder der Vertragsbeendigung nicht mehr auf einer Einwilligung oder einem Vertrag beruht.[271] Gerade nach einem Widerruf oder einer Beendigung des Vertrags besteht aber in besonderer Weise der Bedarf der Übertragung der Daten an die betroffenen Person oder an den neuen Provider. Der Zielsetzung der Vorschrift des Art. 20 DSGVO würde ein solcher Anspruch erst recht entsprechen. Für sie kann es keinen Unterschied machen, ob die betroffene Person zuerst die Einwilligung wiederrufen oder den Vertrag beendet hat und dann ihren Anspruch auf Datenübertragung geltend gemacht hat oder umgekehrt. Den Anspruch der betroffenen Person zu versagen, nur weil der Wortlaut des Art. 20 Abs. 1 DSGVO unpassend formuliert ist, wäre ungerechtfertigt. Daher sollte der Text dieser Vorschrift dahingehend verbessert werden, dass er die Datenübertragung auch noch nach Beendigung der Verarbeitungserlaubnis ermöglicht. Allerdings sollte dieser Anspruch in einem angemessenen zeitlichen Zusammenhand zum Widerruf oder zur Vertragsbeendigung geltend gemacht werden.

Ohne Einwilligung oder ohne Vertrag müssen die Daten nach Art. 17 Abs. 1 lit. a, b oder d DSGVO gelöscht werden. Dies wird in der Praxis

270 Die Datenübertragung ist keine nachvertragliche Pflicht und dient nicht der Vertragserfüllung – s. Westphal/Wichtermann, ZD 2019, 191 (192).

271 S. z.B. Westphal/Wichtermann, ZD 2019, 191 (192).

aber nicht sofort nach dem Widerruf oder der Vertragsbeendigung geschehen, sondern entsprechend dem jeweiligen Löschkonzept in einer angemessenen darauffolgenden Zeitspanne. Der Anspruch auf Datenübertragung kann nur geltend gemacht werden, solange die Daten noch im System des Verantwortlichen gespeichert sind. Daher wäre die Zeitspanne bis zur Löschung der Daten auch der notwendige und zugleich ein angemessener Zeitraum, um die Datenübertragung einfordern zu können.[272] Der Verantwortliche hätte es dann in der Hand, durch eine baldige Löschung der Daten auch von seiner Pflicht zur Datenübertragung frei zu werden.

3.10.3 Form der Datenübertragung

Besteht ein Recht auf Datenübertragung aus Art. 20 Abs. 1 DSGVO, ist unklar, welche Form der Datenübertragung und welches Format der Daten der Verbraucher fordern darf. Das Recht auf Datenübertagung ist durch die Verwendung unbestimmter Rechtsbegriffe (z.B. „strukturiertes gängiges und maschinenlesbares Format", „ohne Behinderung", „technisch machbar"), gekennzeichnet,[273] die von Anbietern höchst unterschiedlich und oft zum Nachteil der Verbraucher ausgelegt werden.[274] So gibt die Datenschutz-Grundverordnung keine konkreten Formate vor. Der Begriff „ohne Behinderung" lässt offen, ob lediglich ein Unterlassen von Behinderung gemeint oder eine weite Auslegung vorzunehmen ist.[275] Bei einer weiten Auslegung dürfte die aktuelle Bereitstellungspraxis überwiegend einen Verstoß gegen Art. 20 DSGVO darstellen. Die Datenschutz-Grund-

272 S. hierzu auch Artikel 29-Datenschutzgruppe, Leitlinien zum Recht auf Datenübertragbarkeit, WP 242 rev.01, Anhang, Frage 5; Westphal/Wichtermann, ZD 2019, 191 (193 f.), die allerdings eine Datenübertragung nach Widerruf der Einwilligung ausschließen wollen.

273 S. z.B. Niederlande, ST 12756/1/19, 41; Strubel, ZD 2017, 355; Jülicher/Röttgen/Schönfeld, ZD 2016, 358.

274 Sie sind nach Erwägungsgrund 68 nicht verpflichtet, „technisch kompatible Datenverarbeitungssysteme zu übernehmen oder beizubehalten". Sie „sollten dazu aufgefordert werden interoperable Formate zu entwickeln, die die Datenübertragbarkeit ermöglichen". S. zur Praxis von Social-Media-Anbieter Scheibel/Horn/Öksüz, 2018, 15 ff.

275 Artikel 29-Datenschutzgruppe, Leitlinien zum Recht auf Datenübertragbarkeit, WP 242 rev.01, 18: „jedwede rechtliche, technische oder finanzielle Hürde […], durch die ein Verantwortlicher den Datenzugriff, die Datenübertragung oder die Datenwiederverwendung vonseiten der betroffenen Person oder eines anderen Verantwortlichen verlangsamen oder verhindern möchte.

verordnung bestimmt auch nicht, was gängige Formate sind. So wären E-Mails, die als PDF-Datei übergeben werden, oder Chats, die als Screenshots in einem gängigen Bildformat herausgegeben werden, wohl nicht sachgerecht, obwohl es gängige Formate sind. Für welche spätere Funktion, die herauszugebenden Daten geeignet sein müssen, lässt die Verordnung jedoch offen. Die technische Machbarkeit soll etwa auch bei der Möglichkeit einer Bereitstellung der Daten auf einem physischen Medium „unter Umständen" nicht entfallen,[276] was wiederum Kosten beim Verarbeiter verursacht. Gerade für dieses Betroffenenrecht bleiben alle die Problembereiche im Streit, die der europäische Gesetzgeber nicht gelöst, sondern nur vertuscht hat. Vorschläge zur Verankerung von Interoperabilität im Normtext sowie zur Verpflichtung des Verantwortlichen zur Bereitstellung in einem von der betroffenen Person weiter verwendbaren Format[277] wurden im Trilog nicht akzeptiert. Die mit der Einführung dieser rechtlichen Innovation bezweckten Regelungsziele werden durch die bestehenden Unsicherheiten gefährdet und durch die Anbieter von Social Networks weitgehend unterlaufen.[278]

Die Lösung dieser Problembereiche kann nur in der rechtlichen Forderung nach Interoperabilität der verwendeten Formate liegen.[279] Der Aufruf des Erwägungsgrundes 68 DSGVO, Verantwortliche zur Entwicklung interoperabler Formate für die Datenübertragung aufzufordern, hat bislang indes kaum Nachhall gefunden. Interoperabilität der Formate benötigt klare und verbindliche Vorgaben. Diese sollten in der Verordnung gefordert und deren bestimmte Festlegung als verbindliche Pflichtaufgabe des Europäischen Datenschutzausschuss gewährleistet werden. Dieser sollte aufgefordert werden, verbindliche Formatvorgaben für die Übergabe der Daten zu bestimmen.

Hilfreich hierfür könnten die Leitlinien zum Recht auf Datenübertragbarkeit der Artikel 29-Datenschutzgruppe vom Dezember 2016 sein. Interoperabilität wird dort als „gewünschte[s] Ergebnis" der sich aus den Begrif-

276 So die vagen Vorgaben der Artikel 29-Datenschutzgruppe, Leitlinien zum Recht auf Datenübertragbarkeit, WP 242 rev.01, 17.

277 „In einem interoperablen gängigen elektronischen Format […], das sie weiterverwenden kann", Art. 15 Abs. 2a Parl-E; „in einem von ihr weiter verwendbaren strukturierten gängigen elektronischen Format", Art. 18 Abs. 1 KOM-E.

278 S. z.B. Scheibel/Horn/Öksüz, 2018, 15 ff.

279 So auch Niederlande, in: Rat, ST 12756/1/19, 41; Verbraucherzentrale Bundesverband, 2013, 15; Europäische Akademie für Informationsfreiheit und Datenschutz, 2020, 7; Verbraucherzentrale Bundesverband, Evaluation, 2019, 9; Kühling/Sackmann, 2018, 21.

fen „strukturiert", „gängig" und „maschinenlesbar" ergebenden „Leistungsvorgaben" bezeichnet. Das erwartete Dateiformat, in dem Daten der betroffenen Person bereitzustellen sind, muss „mit einer Weiterverwendung vereinbar" sein.[280] Der dem Verbraucher bereitgestellte Datensatz soll mit Standardsoftware kompatibel sein.

Neben Interoperabilität der Formate fordert das Recht auf Datenübertragung weitere gesetzlich Klärungen: So sollte festgelegt werden, dass die Daten durch den Verantwortlichen in der deutschen oder englischen Sprache bereitgestellt werden sollen.

Rechtspolitisch besteht demnach Klärungs- und Präzisierungsbedarf bezüglich des Rechts auf Datenübertragung, um sicherzustellen, dass es die ihm zugedachten verbraucher- und wettbewerbsstärkenden Funktionen tatsächlich erfüllen kann. Daher sollte der Unionsgesetzgeber die vorgeschlagenen Änderungen in den Normtext der Datenschutz-Grundverordnung aufnehmen.

3.11 Automatisierte Entscheidungen im Einzelfall

Für Art. 22 DSGVO ist weniger entscheidend, was die Vorschrift verbietet, sondern was sie erlaubt.[281] Ihre geltende Fassung verursacht für Verbraucher folgende Probleme, die eine Anpassung erfordern: Zum einen ist das Verbot automatisierter Entscheidungen im Einzelfall zu eng gefasst. Zum anderen erwähnt sie zwar das Problem des Profiling, ohne dessen spezifische Risiken zu regeln. Drittens rechtfertigt sie in Abs. 2 eine automatisierte Entscheidung im Einzelfall, wenn sie für den Abschluss oder eines Vertrags erforderlich ist, ohne dass die betroffene Person dem zustimmen muss.[282]

3.11.1 Ausweitung des Anwendungsbereichs der Vorschrift

Art. 22 Abs. 1 DSGVO enthält das „Recht, nicht einer ausschließlich auf einer automatisierten Verarbeitung beruhenden Entscheidung – ein-

280 Artikel 29-Datenschutzgruppe, Leitlinien zum Recht auf Datenübertragbarkeit, WP 242 rev.01, 19.

281 S. Roßnagel, in: Baule u.a., 2019, 33 ff.

282 Mit keiner dieser Fragen befasst sich der Evaluationsbericht der Europäischen Kommission.

schließlich Profiling – unterworfen zu werden, die ihr gegenüber rechtliche Wirkung entfaltet oder sie in ähnlicher Weise erheblich beeinträchtigt". Auch hier handelt es sich um eine Übernahme aus dem alten Datenschutzrecht; hier wurde der über 20 Jahre alte Art. 15 der Datenschutzrichtlinie fast wörtlich in die Datenschutz-Grundverordnung überführt. Diese Regelung wird ca. 25 Jahre nach ihrem Entstehungsprozess den Grundrechtsrisiken algorithmenbasierter Entscheidungen nicht ausreichend gerecht.

Ihr Anwendungsbereich ist in dreifacher Weise eingeschränkt: Zunächst ist er begrenzt auf Entscheidungen und erstreckt sich nicht auf Verarbeitungen personenbezogener Daten, die den Entscheidungen zugrunde liegen, sodann ist er beschränkt auf „ausschließlich auf einer automatisierten Verarbeitung beruhende Entscheidungen" und schließlich ist er begrenzt auf Entscheidungen mit einer rechtlichen Wirkung oder einer ähnlichen erheblichen Beeinträchtigung. Durch diese Einschränkungen erfasst die Vorschrift nur einen Bruchteil der Grundrechtsbeeinträchtigungen von Verbrauchern und wird daher der Schutzpflicht des Gesetzgebers für die Grundrechte der Verbraucher nicht gerecht.

Beispiele für automatisierte Entscheidungsverfahren sind die personalisierte Preissetzung von Gütern und Diensten, KI-basierte Gesundheitsratgeber, die Bestimmung individueller Kreditausfallrisiken, Smart-Home-Anwendungen, digitale Assistenzsysteme, Portfoliomanagement für Finanzanleger sowie das autonome Fahren.[283] Alle diese Entscheidungsverfahren berühren die Grundrechte und Interessen der betroffenen Person in beträchtlicher Weise.

Nicht erfasst von Art. 22 Abs. 1 DSGVO ist die auf einer automatisierten Verarbeitung beruhende Vorbereitung einer Entscheidung, sondern lediglich die Entscheidung selbst.[284] Die vorausgehende Verarbeitung personenbezogener Daten richtet sich in ihrer Rechtmäßigkeit nach den risikoneutralen Erlaubnistatbeständen des Art. 6 Abs. 1 und 4 DSGVO. Das damit verbundene Problem einer adäquaten Regulierung der Risiken des Profiling wird im folgenden Unterkapitel aufgegriffen.[285]

Nicht erfasst sind zum anderen alle Entscheidungen, die nicht „ausschließlich" auf einer automatisierten Verarbeitung beruhen. Die Vor-

283 S. Verbraucherzentrale Bundesverband, Algorithmenkontrolle, 2019, 7 f. m.w.N.

284 Kritisch Martini, 2018, 19 f.; Verbraucherzentrale Bundesverband, Algorithmenkontrolle, 2019, 12; Glatzner, DuD 2020, 312; Weichert, DuD 2020, 293.

285 S. Kap. 3.12.

schrift erfasst damit nicht die Risiken, die durch eine teilautomatisierte Entscheidung oder eine arbeitsteilig durchgeführte automatisierte Entscheidung entstehen. Möglich bleiben dadurch Entscheidungen im Einzelfall, die in mehreren Stufen automatisiert vorbereitet werden, die am Ende zwar ein Mensch trifft, der aber die automatische Entscheidungsvorbereitung nicht zu verantworten hat, eventuell nicht einmal ihre Kriterien kennt, aber ihr Ergebnis übernimmt. Dadurch entstehen erhebliche Schutzlücken gegenüber den Risiken automatisierter Entscheidungen für die Grundrechte.[286] Die Vorschrift des Art. 22 Abs. 1 DSGVO sollte daher auf die Einschränkung „ausschließlich" verzichten, um eine Erstreckung auch auf teilautomatisierte Entscheidungen zu erreichen.

Auch innerhalb einer Organisation ist die Beschränkung auf automatisierte Entscheidungen aus Verbrauchersicht problematisch. Das Recht nach Art. 22 Abs. 1 DSGVO gilt nicht, wenn am Ende ein Mensch entscheidet. Dieser wird in der Praxis die Vorgabe des Systems ungeprüft übernehmen. Zudem wird ihm zumeist das Fachwissen fehlen, diese Vorgabe kritisch zu hinterfragen. Der Mensch ist in solchen Fällen nur formal der Entscheider; die tatsächliche Entscheidung wird vom automatisierten System getroffen.

Nicht erfasst werden schließlich die automatisiert entstandenen Entscheidungen im Einzelfall, die keine Rechtswirkung entfalten oder den Betroffenen auf ähnliche Weise erheblich beeinträchtigen. Laut Erwägungsgrund 71 DSGVO sollen die automatische Ablehnung eines Online-Kreditantrags oder eines Online-Einstellungsverfahrens ohne jegliches menschliche Eingreifen erfasst sein. Aufgrund dieser Beschränkung soll die Vorschrift aber keine Anwendung finden etwa auf die automatisierte Beschränkung von Zahlungsmöglichkeiten im E-Commerce oder die Verweigerung bestimmter Vertragskonditionen.[287] Umstritten ist die Anwendbarkeit auf verhaltensbedingte Werbung und individualisierte Preise.[288]

Notwendig wäre in Art. 22 Abs. 1 DSGVO eine Ergänzung um ein Verbot, automatisiert vorbereiteten Entscheidungen ausgeliefert zu sein, die

286 S. auch Jaspers/Jaquemain, DuD 2020, 297; Glatzner, DuD 2020, 312; s. zu dem damit verbundenen Anspruch auf aussagekräftige Informationen s. Kap. 3.8.

287 Buchner, in: Kühling/Buchner, 2018, Art. 22 DSGVO, Rn 26; Born, ZD 2015, 66; Abel, ZD 2018, 304; s. auch Atzert, in: Schwartmann u.a., 2018, Art. 22 Rn. 51.

288 Dagegen Martini, in: Paal/Pauly, 2018, Art. 22 Rn. 23; Artikel 29-Datenschutzgruppe, Leitlinien zu automatisierten Entscheidungen im Einzelfall einschließlich Profiling, WP 251 rev.01, 24; dafür Hladjk, in: Ehmann/Selmayr, 2018, Art. 22 Rn. 9.

der menschliche Entscheider im Regelfall unbesehen übernimmt, ohne dass die betroffene Person *vor* der Entscheidung eine Möglichkeit hat, ihren Standpunkt vorzutragen.[289] Hierzu benötigt sie zuvor eine aussagekräftige Information gemäß Art. 13 Abs. 2 lit. f und Art. 14 Abs. 2 lit. g DSGVO aufgeführt oder eine Auskunft gemäß Art. 15 Abs. 1 lit. h DSGVO „über die involvierte Logik, die einzelnen Profilmerkmale und deren Bedeutung sowie die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung für die betroffene Person".[290]

Schließlich sollte Abs. 1 auf die Einschränkung verzichten, dass die Entscheidung der betroffenen Person gegenüber rechtliche Wirkung entfaltet oder sie *„in ähnlicher Weise erheblich"* beeinträchtigt. Für die Geltung des Art. 22 Abs. 1 DSGVO sollte genügen, dass die betroffene Person in ihren Grundrechten und Freiheiten beeinträchtigt wird.[291] Wenn von ihr höhere Preise verlangt werden oder wenn sie durch personalisierte Werbung belästigt wird, sollte dies als Beeinträchtigung ausreichen. Eine Benachteiligung wie bei einer negativen rechtlichen Wirkung zu verlangen, bevorzugt den Verantwortlichen und benachteiligt die Verbraucher in ungerechtfertigter Weise.

3.11.2 Automatisierte Entscheidungen Dritter als Bedingung

Zudem soll Art. 22 Abs. 1 DSGVO nach Abs. 2 lit. a nicht greifen, wenn automatisierte Entscheidungen Dritter zur Bedingung der Entscheidung eines Anbieters werden.[292] Dies ist etwa dann der Fall, wenn eine Bonitätsprüfung eingeholt wird, die dann über die Vergabe eines Kredits entscheidet. Art. 22 Abs. 2 lit. b DSGVO ermöglicht die Festsetzung weitere Aus-

289 S. auch Verbraucherzentrale Bundesverband, Evaluation, 2019, 10; Glatzner, DuD 2020, 312; im Unterschied dazu zielt Art. 22 Abs. 3 DSGVO nur auf eine nachträgliche nochmalige Überprüfung, wenn die vollautomatisierte Entscheidung im Einzelfall auf den Erlaubnistatbeständen des Abs. 2 lit. a oder c beruht – s. z.B. Scholz, in: Simitis/Hornung/Spiecker, 2019, Art. 22 Rn. 56 und 59; Hladjk, in: Ehmann/Selmayr, 2019, Art. 22 Rn. 15.

290 S. hierzu Kap. 3.8 und 3.9.

291 S. auch Verbraucherzentrale Bundesverband, 2013, 17; Verbraucherzentrale Bundesverband, Algorithmenkontrolle, 2019, 3 f., 12; Verbraucherzentrale Bundesverband, Evaluation, 2019, 10; Europäische Akademie für Informationsfreiheit und Datenschutz, 2020, 4.

292 Die Niederlande, ST 12756/1/19, 41, halten diese Regelung für rechtsunsicher.

nahmen durch mitgliedstaatliches Recht, was in Deutschland in Form von § 37 BDSG geschehen ist.

Art. 22 Abs. 2 lit. a DSGVO sollte entweder vollständig entfallen oder zumindest um die Formulierung „mit Einwilligung der betroffenen Person" ergänzt werden. Dass eine Bank, ein Vermieter oder ein Verkäufer mit einer Auskunftei vereinbart haben, dass ein Scoring Voraussetzung für einen Vertragsabschluss oder die Erfüllung eines Vertrags mit der betroffenen Person sein soll, kann nicht dafür genügen, dass Abs. 1 zu Lasten der betroffenen Person ersatzlos ausfällt. Vielmehr sollte die betroffene Person auch in diesen Fällen das genannte Auskunfts- und Reklamationsrecht haben.

3.11.3 Qualitative Anforderungen

Jede auf einer automatisierten Verarbeitung beruhende Entscheidung sollte immer qualitativen Anforderungen unterliegen. Diese Anforderungen könnten sich an den Bedingungen des Erwägungsgrunds 71 DSGVO und des § 31 BDSG für Scoring und Bonitätsauskünften orientieren.[293] Zumindest sollte gefordert werden, dass die Entscheidung unter Zugrundelegung eines wissenschaftlich anerkannten mathematisch-statistischen Verfahrens nachweisbar für die Entscheidungsfindung erheblich ist und dass die Prognosetauglichkeit für das Verhalten einer Person, die Validität und Reliabilität des verwendeten mathematisch-statistischen Verfahren wissenschaftlich nachgewiesen werden kann.[294]

3.11.4 Pflicht zur Erläuterung der Entscheidung

Nach Abs. 3 des Art. 22 DSGVO hat der Verantwortliche in den Fällen des Abs. 2 lit. a oder c „angemessene Maßnahmen" zu treffen, „um die Rechte und Freiheiten sowie die berechtigten Interessen der betroffenen Person zu wahren." Zu diesen Maßnahmen gehören „mindestens" die Rechte „auf

293 S. auch Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, 2019, 8.

294 S. auch Verbraucherzentrale Bundesverband, Algorithmenkontrolle, 2019, 21; Verbraucherzentrale Bundesverband, Evaluation, 2019, 11; weitergehende Forderungen auch in Netzwerk Datenschutzexpertise, 2020, 8; Verbraucherzentrale Bundesverband, Evaluation, 2019, 13; Datenethikkommission 2019, 180 ff.; Weichert, DuD 2020, 293; Glatzner, DuD 2020, 312.

Erwirkung des Eingreifens einer Person seitens des Verantwortlichen, auf Darlegung des eigenen Standpunkts und auf Anfechtung der Entscheidung". Diese Vorschrift gewährleistet der betroffenen Person ein Recht auf Reklamation und auf nochmalige Überprüfung der automatisiert getroffenen Entscheidung durch einen Menschen. Der Wortlaut fordert keine Begründungen, Erklärungen oder Erläuterungen der automatisiert getroffenen Entscheidung. In der Kommentarliteratur wird dies zwar als Inhalt des Abs. 3 gefordert,[295] aber auch bestritten.[296]

Um hier für Klarheit zu sorgen und einen Interessenausgleich sicherzustellen, sollte der Text des Abs. 3 eindeutig feststellen, dass der Verantwortliche im Fall einer Reklamation die wesentlichen Gründe der automatisiert getroffenen Entscheidung und deren Auswirkungen erläutern muss. Der betroffenen Person muss deutlich werden, welche Beurteilungsmaßstäbe der Entscheidung zugrunde lagen und welche Gesichtspunkte und Erkenntnisse in ihrem Fall ausschlaggebend waren.[297] Soweit dies möglich ist, sollte er auch verpflichtet sein, anzugeben unter welchen Voraussetzungen die Entscheidung für die betroffene Person positiv ausgegangen wäre.[298]

3.12 Nichtabdingbarkeit von Rechten der betroffenen Person

Die Datenschutz-Grundverordnung lässt es zu, dass die Rechte der betroffenen Person durch Rechtsgeschäft[299] beschränkt werden. Diese Möglichkeit ist für Verbraucher besonders nachteilig. Sie erlaubt Verantwortlichen, ihre Macht über den Interessenausgleich, den die Datenschutz-Grundverordnung zwischen ihnen und betroffenen Person als angemessen festgelegt hat, hinaus dadurch auszuweiten, dass sie die Rechte der betrof-

295 S. z.B. Scholz, in: Simitis/Hornung/Spiecker, 2019, Art. 22 Rn. 57 f.; Schulz, in: Gola 2019, Art. 22 Rn. 42 – jeweils unter Berufung auf Erwägungsgrund 71 UAbs. 1 Satz 4.

296 S. z.B. nicht erwähnt in der Kommentierung von Helfrich, in: Sydow, 2018, Art. 22 Rn. 69 bis 73.

297 S. z.B. Verbraucherzentrale Bundesverband, Evaluation, 2019, 10; Scholz, in: Simitis/Hornung/Spiecker, 2019, Art. 22 Rn. 57 f.

298 S. hierzu auch Niederlande, in: Rat, ST 12756/1/19, 44; Verbraucherzentrale Bundesverband, Evaluation, 2019, 10.

299 Ein Rechtsgeschäft besteht aus einer einseitigen oder mehreren aufeinander bezogenen Willenserklärungen, die eine Rechtsfolge herbeiführen sollen – s. z.B. Dix, in: Simitis, BDSG, 2014, § 6 Rn. 11.

fenen Personen durch Rechtsgeschäft beschränken. Dies ist vor allem dann unfair, wenn diese aus sozialen oder beruflichen Gründen gezwungen sind, die Angebote der Verantwortlichen anzunehmen und zu nutzen. Die Datenschutz-Grundverordnung sollte in diesen Fällen einseitiger Machtausübung die betroffene Person als schwächere Partei nicht im Stich lassen. Sich auf die fehlende Fairness im Sinn des Art. 5 Abs. 1 lit. a DSGVO zu berufen, ist viel zu unsicher. Und die Vorschrift des Art. 7 Abs. 4 DSGVO bietet einen viel zu schwachen Ansatz. Sie enthält für die Beurteilung, ob eine Einwilligung freiwillig erteilt wurde, nur eine „Berücksichtigungspflicht" und soll im Ergebnis nicht bei den Social Networks greifen, wenn die Einwilligung wirtschaftlich die Gegenleistung für die geldfreien Leistungen der Plattform ist.[300] Bis zum Geltungsbeginn der Datenschutz-Grundverordnung waren die Rechte der betroffenen Person im deutschen Datenschutzrecht nicht abdingbar.[301] Diese Regelung ist mit der Datenschutz-Grundverordnung entfallen. Sie sollte unionsweit (wieder) eingeführt und ausgeweitet werden.[302]

3.13 Anforderungen an Profiling

Ein großes Manko der Datenschutz-Grundverordnung ist, dass sie das Profiling zwar in Art. 4 Nr. 5 DSGVO definiert als „jede Art der automatisierten Verarbeitung personenbezogener Daten, die darin besteht, dass diese personenbezogenen Daten verwendet werden, um bestimmte persönliche Aspekte, die sich auf eine natürliche Person beziehen, zu bewerten, insbesondere um Aspekte bezüglich Arbeitsleistung, wirtschaftliche Lage, Gesundheit, persönliche Vorlieben, Interessen, Zuverlässigkeit, Verhalten, Aufenthaltsort oder Ortswechsel dieser natürlichen Person zu analysieren oder vorherzusagen". Diese Definition ist deswegen notwendig, um durch sie besonders hohe Risiken für die Grundrechte der betroffenen Personen zu erfassen.

Trotz seiner besonderen Risiken regelt die Datenschutz-Grundverordnung Profiling nur punktuell.[303] Gegen Profiling kann nach Art. 21 Abs. 1 und 2 DSGVO Widerspruch angemeldet werden, wenn es der Wahrung

300 S. z.B. *Klement*, in Simitis/Hornung/Spiecker, Datenschutzrecht, 2019, Art. 7 Rn. 58 ff.; Buchner/Kühling, in: Kühling/Buchner, DSGVO, Art. 7 Rn. 48.
301 S. Dix, in: Simitis, BDSG, 2014, § 6 Rn. 7 ff.
302 S. auch Roßnagel, MMR 2020, 222.
303 Kritisch hierzu auch Niederlande, in: Rat, ST 12756/1/19, 42.

berechtigter Interessen, insbesondere dem Direktmarketing, dient. Es ist außerdem nach Art. 22 Abs. 1 DSGVO verboten, wenn es für eine ausschließlich auf einer automatisierten Verarbeitung beruhenden Entscheidung dient, es sei denn eine der Ausnahmen des Art. 22 Abs. 2 DSGVO erlaubt dies. Alle anderen Formen und Gründe für Profiling sowie deren Risiken regelt die Datenschutz-Grundverordnung nirgendwo in einer adäquaten Weise. Auch die allgemeinen Zulässigkeitsregelungen in Art. 6 DSGVO enthalten keine Anforderungen zur Bekämpfung dieser Risiken.[304]

Profiling von Verbrauchern ist jedoch immer ein starker Eingriff in deren Grundrechte, der über die normale Verarbeitung von personenbezogenen Daten hinausgeht. So kann es in Folge einer automatisierten Entscheidung auf Grundlage eines Profils zu einer Preisdiskriminierung im Internet kommen, wenn etwa Kunden, bei denen aufgrund ihres Profils (Einkommen, Interessen, Präferenzen) eine höhere Zahlungsbereitschaft angenommen wird und daher ein höherer Preis verlangt wird, als dies ohne Profil der Fall wäre.[305] Daher bedarf die Datenschutz-Grundverordnung einer risikoadäquaten Regelung, die Datenschutz und Entscheidungsfreiheit schützt und Diskriminierung verhindert.[306] Eine solche Regelung ist nicht nur dann notwendig, wenn das Profil die Grundlage für eine automatisierten Entscheidungsfindung ist, sondern immer dann, wenn die Risiken üblicher Datenverarbeitung durch die Risiken einer Merkmalssammlung in Profilen deutlich gesteigert werden.[307]

Um den spezifischen Risiken zu begegnen, die mit Profiling für die Grundrechte der Verbraucher einhergehen, sind risikoadäquate Regelungen notwendig. Die Datenschutz-Grundverordnung könnte gesetzlich festlegen, für welche Zwecke Profiling zulässig ist und für welche nicht.[308] Vergleichbar mit der Regelung in Art. 9 DSGVO für besondere Kategorien

304 So auch kritisch Datenschutzkonferenz, Erfahrungsbericht, 2019, 24.

305 S. hierzu Niederlande, in: Rat, ST 12756/1/19, 42 ff.

306 S. auch Niederlande, in: Rat, ST 12756/1/19, 42; Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, 2019, 8; Datenschutzkonferenz, Erfahrungsbericht, 2019, 24; Netzwerk Datenschutzexpertise, 2020, 7; Verbraucherzentrale Bundesverband, Evaluation, 2019, 11; Glatzner, DuD 2020, 312.

307 Datenschutzkonferenz, Erfahrungsbericht, 2019, 24; Verbraucherzentrale Bundesverband, Evaluation, 2019, 11; Verbraucherzentrale Bundesverband, Evaluation, 2019, 11; Glatzner, DuD 2020, 312; ähnlich Netzwerk Datenschutzexpertise, 2019, 7; Forum Privatheit, 2019, 7 f.; Europäische Akademie für Informationsfreiheit und Datenschutz, 2020, 4; ähnlich für Profiling mit besonderen Kategorien personenbezogener Niederlande, in: Rat, ST 12756/1/19, 42.

308 S. Datenschutzkonferenz, Erfahrungsbericht, 2019, 24.

personenbezogener Daten könnte die Regelung festlegen, dass Profiling grundsätzlich nicht erlaubt ist und nur in ausdrücklich vorgesehenen Fällen zugelassen ist.[309] Außerdem sollte die Sammlung von Persönlichkeitsmerkmalen immer qualitativen Anforderungen unterliegen. Zu fordern ist, dass die verwendeten Merkmale für den Verarbeitungszweck tatsächlich aussagekräftig sind, dass sie nicht unzulässig diskriminieren, dass die zugrundeliegenden und genutzten Daten für die Zweckerreichung erforderlich und erheblich sind und dass die Schlussfolgerungen, die aus den Daten gezogen werden, wissenschaftlich nachweisbar mit den Merkmalen, die durch die Daten belegt werden sollen, zusammenhängen.

3.14 Datenschutz durch Systemgestaltung

Eine besondere Innovation der Datenschutz-Grundverordnung[310] ist die in Art. 25 Abs. 1 DSGVO geforderte datenschutzgerechte Systemgestaltung. Art. 25 Abs. 1 DSGVO verpflichtet den Verantwortlichen, sowohl zum Zeitpunkt der Festlegung der Mittel für die Verarbeitung als auch zum Zeitpunkt der eigentlichen Verarbeitung geeignete technische und organisatorische Maßnahmen zu ergreifen, die die Datenschutzgrundsätze wirksam umsetzen und den Schutz der Rechte der betroffenen Personen garantieren. Die Forderung einer datenschutzgerechten Systemgestaltung ist indes nicht neu[311] und dennoch zentral für die Verwirklichung von Datenschutz in einem technisierten Alltag.

3.14.1 Unbestimmtheit der Gestaltungspflicht

Die Pflicht ist allerdings sehr weich formuliert („trifft der Verantwortliche"). Ergänzt wird sie in Erwägungsgrund 78 DSGVO dadurch, dass der Verantwortliche interne Strategien festlegen und Maßnahmen ergreifen „sollte", die den Grundsätzen des Datenschutzes durch Technik sowie dem Datenschutz durch datenschutzfreundliche Voreinstellungen Genüge tun. Zur Konkretisierung enthält Erwägungsgrund 78 DSGVO in Satz 3 lediglich die sehr abstrakten Beispiele Datenminimierung, Pseudonymisierung,

309 S. auch Netzwerk Datenschutzexpertise, 2020, 7; Niederlande, in: Rat, ST 12756/1/19, 44, im Regelfall nur nach Einwilligung.
310 S. hierzu Roßnagel, DuD 2019, 467 (468 f.).
311 S. etwa Roßnagel, 1993, 241 ff.

Transparenz, Möglichkeit der Überwachung durch die betroffene Person sowie Schaffung und Verbesserung von Sicherheitsfunktionen durch den Verantwortlichen. Die konkrete Umsetzung bleibt offen.[312]

Zur Problematik hochgradiger Unbestimmtheit treten die zahlreichen Einschränkungen, die Art. 25 Abs. 1 DSGVO enthält. So sollen der Stand der Technik, die Implementierungskosten und die Art, der Umfang, die Umstände und der Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere der mit der Verarbeitung verbundenen Risiken für die Rechte und Freiheiten natürlicher Personen Berücksichtigung finden. Die Bestimmung und Abwägung dieser Faktoren gestalten sich jedoch äußerst schwierig und geben dem Verantwortlichen einen sehr großen Entscheidungs- und Gestaltungsspielraum.[313] Beide Problemkreise – unbestimmte Pflicht und weite Einschränkungsmöglichkeiten – gemeinsam führen in der Praxis dazu, dass die Verpflichtung zur Systemgestaltung nach Art. 25 Abs. 1 DSGVO beim Verantwortlichen meist auf der Strecke bleibt, solange diese Pflicht nicht für bestimmte Techniklinien (wie z.B. Künstliche Intelligenz oder Plattformen) durch bereichsspezifische Regelungen konkretisiert wird.[314]

3.14.2 Fehlende Verpflichtung der Hersteller

Die Pflicht nach Art. 25 Abs. 1 DSGVO trifft überdies nur den Verantwortlichen. Dieser ist häufig darauf angewiesen, dass der Markt geeignete Techniken zur Verfügung stellt und Hersteller von Informationstechnik geeignete Produkte anbieten, die es dem Verantwortlichen erlauben, den Anforderungen der Datenschutz-Grundverordnung gerecht zu werden. Dies ist jedoch oft nicht der Fall: „Diejenigen, die es richtig machen wollten, waren auch nicht glücklich, weil sie feststellten, dass Hersteller von Produkten und Anbieter von Dienstleistungen ihnen oft keine Hilfe waren und es damit schwierig war, die eigene Rechenschaftspflicht zu erfüllen."[315] Gleiches gilt auch für die Verbraucher, wenn sie Software, die zwischen ihnen und dritten Datenverarbeitern steht, wie beispielsweise Webbrowser oder

312 S. Hartung, in: Kühling/Buchner, 2018, Art. 25 Rn. 17.
313 S. z.B. Hansen, in: Simitis/Hornung/Spiecker, 2019, Art. 25 Rn. 37 f.
314 S. hierzu Roßnagel, DuD 2018, 741 (745). Bereichsspezifische risikobezogene Konkretisierungen fordert auch die Bundesregierung, in: Rat: ST 12756/1/19, 15; Europäische Akademie für Informationsfreiheit und Datenschutz, 2020, 5; Datenethikkommission, 2019, 116, 123.
315 Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein, 2019, 10.

Betriebssysteme, oder IT-Geräte, für die es keine Verantwortlichen gibt, verwenden.

Hersteller werden von der Verordnung aber nicht direkt adressiert, sondern durch Erwägungsgrund 78 Satz 4 DSGVO lediglich „ermutigt", das Recht auf Datenschutz bei der Entwicklung und Gestaltung der Produkte, Dienste und Anwendungen zu berücksichtigen und unter gebührender Berücksichtigung des Stands der Technik sicherzustellen, dass die Verantwortlichen und die Verarbeiter in der Lage sind, ihren Datenschutzpflichten nachzukommen.[316]

Die Vorschrift wird allein aus diesem Grund nicht die beabsichtigte Wirkung erzielen, eine Marktdurchdringung möglichst datenschutzfreundlicher Technologien zu erreichen. Konkrete Forderungen können aus der geltenden Fassung der Vorschrift des Art. 25 DSGVO nicht abgeleitet werden. Dies führt dazu, dass sich letztlich stets derjenige durchsetzt, der die Technikgestaltung durchführt, ohne dass Art. 25 DSGVO den Verbrauchern einen Anspruch verleiht, mehr zu verlangen. Eine verpflichtende und bußgeldbewehrte Adressierung der Hersteller wäre weitaus effektiver und würde die Vorschrift nicht lediglich auf einen wohlgemeinten Programmsatz reduzieren.[317] Ohne diese Erstreckung bestehen nicht nur erhebliche Lücken im Schutz personenbezogener Daten, sondern es kommt zu einer Potenzierung von technischem und bürokratischem Aufwand bei dem Versuch, dezentral bei den Anwendern Mängel zu beseitigen, die zentral bei Hersteller verursacht werden. Dies belastet alle Verantwortlichen und Auftragsverarbeiter, wobei KMU überproportional belastet werden.[318]

Für Anbieter von Social Networks ist die Unterscheidung zwischen Hersteller und Anwender weitgehend bedeutungslos. Der Verantwortliche ist auch der Hersteller oder hat auf die Hersteller einen so starken Einfluss, dass er sie zwingen kann, das von ihm gewünschte Maß an Datenschutz zu realisieren. Bei ihnen könnte die Pflicht zur datenschutzgerechten Systemgestaltung theoretisch greifen, sie wird aber von ihnen bisher praktisch ignoriert.

---

316 S. Husemann, in: Roßnagel, 2018, § 5 Rn. 56.

317 Bundesrat, BT-Drs. 570/19, 4; Datenschutzkonferenz, Erfahrungsbericht, 2019, 15 ff.; Verbraucherzentrale Bundesverband, Evaluation, 2019, 12; Der Landesbeauftragte für Datenschutz und Informationsfreiheit Baden-Württemberg, Evaluierung, 2019, 10 f.; Datenethikkommission, 2019, 116, 123.

318 Der Landesbeauftragte für Datenschutz und Informationsfreiheit Baden-Württemberg, Evaluierung, 2019, 10; Datenschutzkonferenz, Erfahrungsbericht, 2019, 16.

Sofern auch Herstellern datenschutzrechtliche Pflichten übertragen werden, sollten sich auch die möglichen Rechtsbehelfe der betroffenen Personen nach Art. 79 DSGVO und ihr Anspruch auf Schadensersatz nach Art. 82 DSGVO auf diese Pflichten beziehen, um den Herstellern ausreichende Anreize zu geben, ihre Pflichten zu erfüllen.[319] Aus dem gleichen Grund sollten auch die Aufsichtsbehörden Anordnungen gegen Hersteller nach Art. 58 DSGVO[320] und Sanktionen nach Art. 83 DSGVO gegen Hersteller anordnen können, die ihre Pflichten vernachlässigen.

3.14.3 Gestaltungsmacht der Verantwortlichen

Zusammenfassend kann also festgehalten werden, dass bezogen auf Datenschutz durch Technikgestaltung vornehmlich Konkretisierungen dieser Verpflichtungen und eine Ausweitung des Adressatenkreises notwendig sind. Die Pflicht zur Systemgestaltung als zentrale Neuerung des Datenschutzrechts kann nur dann volle Wirkung entfalten, wenn auch die Hersteller von IT-Produkten und -Programmen rechtlich bindend verpflichtet werden.[321] Entsprechend sollten auch die Regelungen zum Recht auf einen wirksamen gerichtlichen Rechtsbehelf in Art 79 und zum Schadensersatz nach Art. 82 auf Hersteller erstreckt werden.[322]

Eine Präzisierung dessen, was Datenschutz durch Technikgestaltung konkret bedeutet, kann auf Unionsebene durch den Europäischen Datenschutzausschuss, auf mitgliedstaatlicher Ebene durch die Aufsichtsbehörden erfolgen.[323] Zudem sind Verbänderegulierung und Normung als Instrumente denkbar. Eine Verpflichtung der Hersteller könnten sowohl die

319 S. hierzu Datenschutzkonferenz, Erfahrungsbericht, 2019, 16 f.; Europäische Akademie für Informationsfreiheit und Datenschutz, 2020, 6.

320 S. hierzu Der Landesbeauftragte für Datenschutz und Informationsfreiheit Baden-Württemberg, Evaluierung, 2019, 11.

321 Bundesrat, BR-Drs. 570/19, 4; Datenschutzkonferenz, Erfahrungsbericht, 2019, 15 ff.; Verbraucherzentrale Bundesverband, Evaluation, 2019, 12; Der Landesbeauftragte für Datenschutz und Informationsfreiheit Baden-Württemberg, Evaluierung, 2019, 10 f.; Europäische Akademie für Informationsfreiheit und Datenschutz, 2020, 5 f.

322 Datenschutzkonferenz, Erfahrungsbericht, 2019, 17.

323 S. hierzu Roßnagel, 2017, 122 ff. So etwa geschehen durch die spanische Datenschutzaufsichtsbehörde: Agencia Española de Protección de Datos, Guía de Privacidad desde el Diseño, Oktober 2019.

mitgliedstaatlichen Gesetzgeber,[324] besser aber der Unionsgesetzgeber vorsehen.

Eine abstrakte Regelung, wie sie Art. 25 Abs. 1 DSGVO enthält, zeichnet sich zwar durch Offenheit für technische Neuerungen aus, hat jedoch auch den handfesten Nachteil, zu Auseinandersetzungen von Interessenvertretern über ihren Bedeutungsgehalt einzuladen.[325] Hier besteht die Gefahr, dass die Interessen der Verarbeiter und Hersteller sich im Diskurs gegenüber den Interessen der betroffenen Personen und insbesondere der Verbraucher durchsetzen. Machtasymmetrien spielen auch innerhalb der Verantwortlichen eine Rolle. Mahnt die Datenschutzabteilung eines Unternehmens zu bestimmten Maßnahmen, um Datenschutz durch Technikgestaltung sicherzustellen, so kann die Gegenseite sich leicht auf den Katalog der Einschränkungen aus Art. 25 Abs. 1 DSGVO zurückziehen und die geforderten Maßnahmen ablehnen. Auch dies gerät dem Verbraucher letztlich zum Nachteil.

3.15 Datenschutz durch datenschutzfreundliche Voreinstellungen

Das Prinzip des „Privacy by Default" nach Art. 25 Abs. 2 DSGVO unterliegt nicht den fünf Einschränkungen des Abs. 1.[326] Jedoch sollen sich die Voreinstellungen für den Nutzer nach der Erforderlichkeit der Verarbeitung für den jeweiligen Verarbeitungszweck richten. Dies lässt dem Verantwortlichen sehr große Freiheiten, durch die Bestimmung des Zwecks die Voreinstellungen so zu wählen, dass er durch diese die gewünschten Daten erhalten kann. Auch hier sind Präzisierungen erforderlich, wenn die Vorschrift ihr rechtspolitisches Ziel erreichen soll. Diese können durch die Aufsichtsbehörden, den mitgliedstaatlichen Gesetzgeber (für einzelne Technikbereiche),[327] den Europäischen Datenschutzausschuss, aber auch durch Verbänderegulierung erfolgen.

Außerdem sollte der mögliche Zweck auf die Funktionalität des jeweiligen Dienstes beschränkt werden. Art. 25 Abs. 2 DSGVO nimmt eine solche Beschränkung nicht vor, sondern richtet die Voreinstellungen an der Er-

---

324 S. Hansen, in: Simitis/Hornung/Spiecker, 2019, Art. 25 Rn. 21.
325 S. Roßnagel, DuD 2018, 741 (745).
326 S. Hartung, in: Kühling/Buchner, 2018, Art. 25 Rn. 29; Hansen, in: Simitis/Hornung/Spiecker, 2019, Art. 25 Rn. 45.
327 Barlag, in: Roßnagel, Europäische Datenschutz-Grundverordnung, 2017, § 3 Rn. 247.

forderlichkeit für den jeweiligen Verarbeitungszweck aus. Diesen aber bestimmt allein der Verantwortliche – nach seinen Verarbeitungsinteressen. Setzt er seine Zwecke großzügig, so läuft letztlich der als Beschränkung vorgesehene Art. 25 Abs. 2 DSGVO weitgehend leer.

Hier könnte das Prinzip der Datenvermeidung, das auch den Zweck unter das Gebot, mit möglichst wenigen personenbezogenen Daten auszukommen, nimmt, in einer Ergänzung des Art. 5 Abs. 1 DSGVO helfen.[328] Bei der Zweckbestimmung müsste eine vergleichbare Einschränkung erfolgen wie sie zur Bestimmung des Vertragszwecks ihm Rahmen des Art. 6 Abs. 1 UAbs. 1 lit. b DSGVO vorgeschlagen wurde.[329]

3.16 Effektive Datenschutzaufsicht

Ein in der Praxis effektives Datenschutzregime ist auf eine funktionierende Datenschutzaufsicht angewiesen. Die Datenschutz-Grundverordnung hat mit ihren Regelungen zu Aufgaben und Befugnissen der Aufsichtsbehörden zur Zusammenarbeit und Kohärenz sowie mit den Entwicklungen in den Bereichen Rechtsbehelfe, Rechtsmittel, Haftung und Schadensersatz sowie Sanktionen eine deutliche Verbesserung bewirkt.[330] Das Funktionieren des Kohärenzmechanismus muss sich in der Praxis indes noch beweisen. Zudem bleibt trotz personeller Anpassungen das Problem einer unzureichenden personellen wie auch finanziellen Ausstattung des Europäischen Datenschutzausschusses[331] und der nationalen Aufsichtsbehörden.[332] Ergänzende Regelungen könnten hilfreich sein.

Die Aufsichtsbehörden sind die Instanzen, für die die Datenschutz-Grundverordnung die größten Veränderungen bewirkt und den größten Zuwachs an neuen Aufgaben bewirkt hat.[333] Ihre Ausstattung ist angesichts dieser neuen Aufgaben zwar in den meisten Fällen verbessert wor-

328 S. hierzu Kap. 3.3.
329 S. hierzu Kap. 3.5.
330 Europäische Kommission, COM(2020) 264 final, 5 f.; Commission Staff Working Document, 4 ff.
331 Zur Überforderung des EDSA s. Landesbeauftragte für Datenschutz und Akteneinsicht Brandenburg, 2019, 11; Roßnagel, DuD 2019, 467 (472).
332 Europäische Kommission, COM(2020) 264 final, 6; Commission Staff Working Document, 12 ff. und Annex 2.
333 S. hierzu ausführlich Roßnagel, 2017.

den.[334] Dennoch sind sie vom Umfang und der Größe der zusätzlichen Aufgaben durch die Datenschutz-Grundverordnung weiterhin überfordert.[335] Die Beanspruchung durch Beschwerden, Beratungsanforderungen und Meldungen von Datenschutzverstößen haben sich um ein Vielfaches erhöht und binden in beträchtlichem Umfang Personal.[336] Die Herstellung von Vollzugsgleichheit in den Bundesländern und in den Mitgliedstaaten ist für den Erfolg der Datenschutz-Grundverordnung zentral.[337] Um alle praktisch relevanten Fragen der Datenschutz-Grundverordnung beantworten und um alle notwendigen Vorbedingungen für die Durchsetzung der Datenschutzregelungen zu gewährleisten, sind noch weitere Personalaufstockungen erforderlich.[338]

3.17 Sanktionen

Eine wichtige Stärkung des Datenschutzes liegt in der Möglichkeit, drastische Sanktionen zu verhängen. Die Unsicherheit bezogen auf die zu abstrakten Bußgeldtatbestände des Art. 83 Abs. 4 und 5 DSGVO behindert jedoch die Nutzung dieses Instruments. Diese sind daher zur Gewährleistung ihrer Praktikabilität zu präzisieren.

Bei dem im Vergleich zum alten Bundesdatenschutzgesetz deutlich erweiterten Spielraum zur Sanktionierung von Rechtsbrüchen handelt es sich um die wahrscheinlich meistbeachtete Innovation der Datenschutz-Grundverordnung.[339] Die Datenschutzrichtlinie hatte die Ausgestaltung solcher Sanktionen noch den Mitgliedstaaten überlassen. Das Bundesdatenschutzgesetz sah in seiner alten Fassung eine Höchstbuße von 300.000

334 S. näher Europäische Kommission, Commission Staff Working Document, 13 f. und Annex 2.

335 S. z.B. Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit, 2019, 18; Bayerisches Landesamt für Datenschutzaufsicht, 2019, 2; Sachsen-Anhalt, 2019, 6.

336 S. Schulzki-Haddouti, Implodierende Aufsichtsbehörden, PinG-Blog vom 29.3.2019; Landesbeauftragte für Datenschutz und Akteneinsicht Brandenburg, 2019, 11; Der Landesbeauftragte für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern, 2019, 10.

337 Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit, 2019, 22.

338 S. Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit 2019, 18; Der Landesbeauftragte für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern, 2019, 10; Roßnagel, DuD 2019, 467 (471 f.).

339 S. hierzu Rost, DuD 2019, 467 (471 f.).

Euro vor.[340] Die in der aufsichtsbehördlichen Praxis verhängten Bußgelder lagen indes zumeist im vierstelligen Bereich. Art. 83 Abs. 4, 5 und 6 DSGVO ermöglichen nun, Geldbußen in Höhe von bis zu 10 Millionen Euro oder bei Unternehmen von bis zu 2% des gesamten weltweit erzielten Jahresumsatzes des vorausgegangenen Geschäftsjahres bzw. 20 Millionen Euro oder 4 % des Jahresumsatzes zu verhängen.

Art. 83 Abs. 1 und 2 DSGVO enthalten die Maßstäbe, die bei der Verhängung von Geldbußen anzulegen sind. Hier sind General- und Spezialprävention wesentliche Aspekte, wobei insbesondere die Negativprävention durch die Verwendung des Begriffs „abschreckend" in Art. 83 Abs. 1 DSGVO hervorgehoben wird. Ebenso hervorgehoben werden die Effektivität der verhängten Geldbußen („wirksam") sowie der Grundsatz der Verhältnismäßigkeit. Art. 83 Abs. 2 Satz 2 DSGVO enthält eine Auflistung von Faktoren, die sich verschärfend oder mildernd auf die Geldbuße auswirken sollen.

Es ist zu konstatieren, dass die Möglichkeiten zur Sanktionierung von Verstößen, die die Datenschutz-Grundverordnung bietet, bislang noch eher zurückhaltend ausgenutzt werden,[341] auch wenn einzelne Bußgelder herausstechen.[342] Ein Grund hierfür dürfte in der Spannbreite der möglichen Sanktionen liegen, die durch die abstrakten Vorgaben des Art. 83 Abs. 2 Satz 2 DSGVO nur unzureichend eingeengt wird. Hier wird zurecht kritisiert, die Bußgeldtatbestände in Art. 83 Abs. 4 und 5 DSGVO seien zu unbestimmt, um rechtssicher Bußgelder in Millionenhöhe verhängen zu können.[343] In der Praxis sicher handhabbar dürfte allein das Bußgeld nach Art. 83 Abs. 6 DSGVO sein, das bei Nichtbefolgung einer Anweisung einer Aufsichtsbehörde nach Art. 58 Abs. 2 DSGVO verhängt werden kann. Die Anweisung der Aufsichtsbehörde muss dabei allerdings auch vollziehbar sein. Dabei ist davon auszugehen, dass insbesondere finanzstarke Verarbeiter eine gerichtliche Überprüfung des Bußgelds anstreben werden. Diese

340 § 43 Abs. 3 Satz 1 BDSG a.F.

341 S. näher Martin/Friedewald, DuD 2019, 493 ff.; Rost, DuD 2019, 488 (491 f.).

342 Z.B. gegen ein dänisches Taxiunternehmen im April 2019 in Höhe von etwa 2,8% des Jahresumsatzes des Unternehmens; gegen Google in Höhe von 50 Millionen Euro durch die französische CNIL im Januar 2019; in Italien im Kontext des Telemarketing (Newsletter des italienischen Datenschutzbeauftragten Nr. 453 vom 30. Mai 2019); im Juli 2019 in Großbritannien 183,4 Millionen GBP (ca. 1,5% des weltweiten Jahresumsatzes) gegen British Airways und 99.2 Millionen GBP gegen Marriott.

343 S. etwa Bergt, DuD 2017, 555; Eckhardt/Menz, DuD 2018, 139; Faust/Spittka/Wybitul, ZD 2016, 120.

Prozesse auch über mehrere Instanzen binden wiederum Ressourcen der Aufsichtsbehörden. Der Vollzug der Datenschutz-Grundverordnung hätte deshalb von Anfang an durch eine Präzisierung der Bußgeldtatbestände gestärkt werden müssen.[344] Diese könnte nachträglich durch eine Leitlinie des Europäischen Datenschutz-Ausschusses nach Art. 70 Abs. 1 Satz 2 lit. k DSGVO erreicht werden. Eine erste Leitlinie zu den Kriterien des Art. 83 Abs. 2 Satz 2 DSGVO hat die Artikel 29-Datenschutzgruppe zwar bereits 2017 vorgenommen,[345] es verbleibt jedoch weiterer Präzisierungsbedarf.[346] Die notwendige Präzisierung könnte indes auch auf mitgliedstaatlicher Ebene von der Konferenz der Datenschutzaufsichtsbehörden geleistet werden, indem diese einen unverbindlichen Bußgeldkatalog erstellt.[347] Als Beispiel können die Feststellungen der Konferenz der unabhängigen Datenschutzaufsichtsbehörden in Deutschland vom Oktober 2019 gelten.[348] Nur so kann dem sowohl im primären Unionsrecht als auch mitgliedstaatlich verankerten Bestimmtheitsgebot Genüge getan und eine einheitliche Anwendung der Bußgeldvorschriften in der gesamten Union erreicht werden. Hierfür wäre auch eine Verpflichtung der Aufsichtsbehörden hilfreich, eine jährliche Statistik ihrer Bußgeldpraxis zu veröffentlichen. Jedenfalls sind alle sinnvollen Maßnahmen zu ergreifen, um hinsichtlich der Sanktionen keinen Anreiz zu einem Forum Shopping zu bieten.

Denkbar wäre auch eine Reform des Umgangs mit erfolgreich verhängten Bußgeldern. Die so erlangten Geldmittel fließen in Deutschland überwiegend in die allgemeinen Haushalte des Bundes und der Länder. Hier wäre mit Blick auf andere Mitgliedstaaten wie Frankreich auch eine Ausgestaltung denkbar, bei der Bußgelder direkt in den Haushalt der jeweiligen Aufsichtsbehörde fließen. Wird dieser Weg aus Angst vor einem überschießenden Gebrauch des Instruments nicht gegangen, so ist zumindest eine weitere personelle und finanzielle Aufstockung der Aufsichtsbehörden angezeigt[349] – verbunden mit einer Übernahme anfallender Prozesskosten durch den Bund und die Länder.[350]

344 S. Roßnagel, 2017, 131 ff.
345 Artikel 29-Datensachutzgruppe, WP 253.
346 So auch Bundesregierung, in: Rat, ST 12756/1/19, 18.
347 Braun/Hohmann, in: Roßnagel, 2018, § 6 Rn. 152.
348 Datenschutzkonferenz, Konzept zur Bußgeldzumessung vom 14.10.2019.
349 S. Roßnagel, 2017, 191 ff.
350 Miedzianowski, in: Roßnagel, 2018, § 4 Rn. 75; Dieterich, ZD 2016, 266.