Datenschutz im digitalen Zeitalter: Umsetzung der Datenschutzgrundverordnung (DSGVO) – Bilanz ein Jahr nach Inkrafttreten

Gutachten im Auftrag der Fraktion Bündnis 90/Die Grünen im Deutschen Bundestag

Peter Schaar

Dr. Alexander Dix, LL.M.

Vorgelegt am 16. Mai 2019

Inhaltsverzeichnis

1. Vorbemerkung

Mit der Datenschutz-Grundverordnung[1] gibt es seit dem 25. Mai 2018 in Europa erstmals ein **Europäisches Datenschutzgesetz**, wie es der Vertrag von Lissabon schon 2007 ins Auge gefasst hatte.[2] Die mit dem Vertrag erfolgte Aufwertung der EU-Grundrechtecharta (EUGrCh) hat die datenschutzrechtliche Landschaft stark verändert. Art. 7 der Charta verlangt — wie schon Art. 8 der Europäischen Menschenrechtskonvention[3] – die Achtung des Privat- und Familienlebens, Art. 8 EUGrCh garantiert den Schutz personenbezogener Daten und schreibt eine unabhängige Datenschutzaufsicht vor. Insofern war klar gestellt, dass der Datenschutz als europäisches Grundrecht eines effektiven Schutzes in der gesamten Union bedürfe.

Der bereits zuvor bestehende, durch die Datenschutz-Richtlinie von 1995[4] gesetzte europarechtliche Rahmen war von den Mitgliedstaaten sehr unterschiedlich ausgefüllt worden. Angesichts des datenschutzrechtlichen Flickenteppichs und des damit einhergehenden unterschiedlichen Datenschutzniveaus in den Mitgliedstaaten sah sich die Europäische Kommission veranlasst, die Schaffung eines verbindlichen, einheitlichen und kohärenten Rechtsrahmens vorzuschlagen, weil diese Unterschiede den gleichmäßigen Schutz der Unionsbürgerinnen und -bürger vereiteln, ein „Hemmnis für die unionsweite Wirtschaftstätigkeit darstellen, den Wettbewerb verzerren und die Behörden an der Erfüllung“ ihrer unionsrechtlichen Pflichten hindern können.[5]

Die Aufwertung des Datenschutzes durch die Grundrechtecharta hatte gravierende Konsequenzen: So hat der Gerichtshof der Europäischen Union (EuGH) in verschiedenen Urteilen verdeutlicht, dass er sich - ebenso wie schon der Straßburger Gerichtshof für Menschenrechte – nun als Hüter der EU-Grundrechte auf Privatsphäre und Datenschutz versteht und sich nicht mehr auf die Rolle eines EU-Verwaltungsgerichtshofs beschränkt. Diese neue Rollenbestimmung der EuGH wurde besonders deutlich in den Urteilen zur Vorratsdatenspeicherung[6] und zu Safe Harbour[7] - eine angesichts der zunehmenden

---

[1] Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rats vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) - EU Amtsblatt v. 4.5.2016, L119/1.

[2] Art. 16 Abs 2 AEUV.

[3] Konvention zum Schutz der Menschenrechte und Grundfreiheiten (Europäische Menschenrechtskonvention) v. 4. 11.1950.

[4] Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, EG-Amtsblatt 23.11.1995, L 281.

[5] Erwägungsgrund 9 DSGVO.

[6] EuGH, Urteil vom 8. April 2014, (verbundene Rechtssachen C-293/12 und C-594/12); Urteil v. 21.12.2016 (verbundene Rechtssachen 203/15 und 698/15).

[7] EuGH, Urteil vom 6.10.2015 (Rechtssache C-362/14).

Bedeutung der Informationstechnologie und anschwellender transnationaler Datenströme uneingeschränkt positiv zu beurteilende Entwicklung.

Inwieweit die Ziele der DSGVO, allen voran die der **Harmonisierung des Datenschutzes** und eines **effektiven Schutzes gegen Datenschutzverstöße** - erreicht worden ist, lässt sich nach nur einem Jahr noch nicht seriös bewerten. Die Europäische Kommission ist nach Art. 97 DSGVO verpflichtet, die Anwendung und Wirkungsweise der Verordnung laufend zu überprüfen und darüber erstmals am 25. Mai 2020 zu berichten und erforderlichenfalls Vorschläge zur Änderung und Weiterentwicklung der Verordnung zu machen.

Die folgende Darstellung hat insofern vorläufigen Charakter. Sie konzentriert sich zudem auf die in Deutschland geführte Debatten und auf die Umsetzung durch die Gesetzgeber des Bundes und der Länder, einschließlich der hier noch bestehenden Handlungsbedarfe.

2. In der öffentlichen Debatte diskutierte Folgen der DSGVO

Trotz der zweijährigen Vorlaufzeit zwischen der Verkündung des EU-Rechtsakts am 4. Mai 2016[8] und dessen voller Anwendbarkeit am 25. Mai 2018 waren viele Rechtsanwender auf die Anforderungen nur **unzureichend vorbereitet**. So ergab eine im Dezember 2017 veröffentlichte Umfrage, dass mehr als der Hälfte der deutschen Unternehmen die DSGVO nicht bekannt war oder dass sie sich noch nicht mit ihr beschäftigt hätten.[9]

Zwar hatte die Europäische Kommission rechtzeitig eine Website[10] mit Fragen und Antworten in allen Sprachen der Mitgliedsländer zur Verfügung gestellt. Damit konnte sie aber naturgemäß nur Fragen beantworten, die sich aus dem Text der DSGVO selbst ergaben, nicht jedoch aus dem Zusammenspiel von europäischem und nationalem Recht. Dies ist insbesondere deshalb bedeutsam, weil die Mitgliedstaaten - allen voran die deutsche Bundesregierung[11] - im Rat eine Vielzahl von Öffnungs- und Konkretisierungsklauseln für die nationalen Gesetzgeber durchgesetzt hatten[12], die unterschiedlich genutzt wurden.

Die damit verbundenen **Rechtsunsicherheiten** waren und sind in Deutschland besonders ausgeprägt, weil das hiesige Datenschutzrecht maßgeblich durch Spezialregelungen geprägt ist und sich vielfach die Frage stellt, in welcher Beziehung die bereichsspezifischen Datenschutzvorschriften zu den Vorgaben der DSGVO stehen. Hinzu kommt die föderale Differenzierung des deutschen Datenschutzrechts, die in keinem anderen Mitgliedsland eine Entsprechung findet.

---

[8] Vgl. Fn. 1.
[9] ZEW, Dezember 2017
[10] https://ec.europa.eu/info/law/law-topic/data-protection/reform_de?pk_source=google_ads&pk_medium=paid&pk_campaign=gdpr2019 (abgerufen am 30.4.2019).
[11] Schaar, Deutscher Sonderweg beim Datenschutz?, vorgänge 221-222/2018, 31.
[12] Roßnagel, Umsetzung der Unionsregelungen zum Datenschutz, dud 12/2018, 741.

Schließlich haben sich die Bundesregierung und die Landesregierungen nur sehr begrenzt um eine Klärung offener Rechtsfragen und um die Vermittlung von Kenntnissen über den neuen europäischen Rechtsrahmen zum Datenschutz bemüht. Vielmehr ging es sowohl bei Gesetzgebungsaktivitäten (vgl. Abschnitt 3) als auch in der Öffentlichkeitsarbeit augenscheinlich darum, die Position der datenverarbeitenden öffentlichen Stellen und der Unternehmen zu stärken und sie gegen vermeintliche datenschutzrechtliche Zumutungen zu schützen. So plädierte die für Digitales zuständige Staatsministerin im Kanzleramt Dorothee Bär für eine „smarte Datenkultur“ und beklagte in Deutschland existiere in „ein Datenschutz wie im 18. Jahrhundert“.[13]

Statt den Datenschutz als Chance zu begreifen und so das Vertrauen in digitale Prozesse in Staat und Wirtschaft zu stärken, wurde der Eindruck erzeugt, Datenschutz bedrohe den Wohlstand, verhindere sinnvolle IT-Projekte und erschwere das Leben von Vereinen und kleinen Unternehmen. Die Wahrnehmung der DSGVO als „Innovationsbremse“ oder „Bürokratiemonster“ wurde verstärkt durch vielfach unbegründete Behauptungen und zweifelhafte Rechtsauslegungen, auf die im Folgenden beispielhaft eingegangen werden soll.

2.1. Die überstrapazierte Einwilligung

Ein zentraler Kritikpunkt an der DSGVO richtet sich gegen die wahrgenommene „Bürokratisierung“ des Datenschutzes. Dabei spielte (und spielt) die Frage eine zentrale Rolle, wann die Verarbeitung personenbezogener Daten **rechtmäßig** ist. Hier hält sich hartnäckig das Gerücht, dass der Verantwortliche seit dem 25. Mai 2018 grundsätzlich eine Einwilligung des Betroffenen in die Datenverarbeitung benötige. Diese Vorstellung ist deshalb falsch, weil – wie schon nach dem alten Datenschutzrecht – die Einwilligung nur erforderlich ist, soweit kein anderer gesetzlicher Erlaubnistatbestand gegeben ist.

Gemäß Art. 6 Abs. 1 DSGVO ist die Verarbeitung nur rechtmäßig, wenn „mindestens eine der nachfolgenden Bedingungen“ erfüllt ist. Die Einwilligung ist zwar die erste dieser Bedingungen, aber bei weitem nicht die einzige.

Die Verarbeitung personenbezogener Daten durch ein Unternehmen (oder einen Verein) erfolgt hauptsächlich im Zusammenhang mit **Vertragsverhältnissen** mit den Kunden bzw. mit den Beschäftigten oder Mitgliedern. Nach Art. 6 Abs. 1 lit b DSGVO sind Verarbeitungen rechtmäßig, wenn sie *„für die Erfüllung eines Vertrags, dessen Vertragspartei die betroffene Person ist, oder zur Durchführung vorvertraglicher Maßnahmen erforderlich, die auf Anfrage der betroffenen Person erfolgen“*.

Hinzu kommt ggf. (etwa in Bezug auf Werbung) zur **Wahrung berechtigter Interessen** des Verantwortlichen oder eines Dritten (Art. 6 Abs. 1 lit. f DSGVO). Hier ist allerdings eine

[13] Interview mit der Bild-Zeitung am 5.3.2018, https://www.bild.de/politik/inland/dorothee-baer/im-interview-55009410.bild.html (abgerufen am 30.4.2019).

Abwägung mit den schutzwürdigen Betroffenenrechten erforderlich. Zudem haben die Betroffenen in diesen Fällen ein Widerspruchsrecht gem. Art. 21 DSGVO.

Natürlich kann man zwar zusätzlich auch die Einwilligung (lit. a) erbitten. Im Regelfall ist dies aber wenig sinnvoll. Wenn die Verarbeitung auf einer Einwilligung basiert, hat die betroffene Person ein jederzeitiges Recht, diese Einwilligung zu widerrufen (Art. 6 Abs. 3 DSGVO). Dann müssen die Daten unverzüglich gelöscht werden. Schon deshalb ist von der unnötigen Verwendung der Einwilligung abzuraten. Für die Verarbeitung zur Anbahnung bzw. Erfüllung eines Vertrags (Art. 6 Abs. 1 lit. b DSGVO) besteht weder ein Widerspruchsrecht noch ein Widerrufsrecht, sondern lediglich das Recht, einen Vertrag gemäß BGB zu kündigen. Aus der Vertragsauflösung resultiert keine unmittelbare Löschungsverpflichtung: Die Daten müssen zwar frühestmöglich gelöscht werden, sie dürfen aber solange gespeichert bleiben, wie dies für die Abwicklung des Vertrags und seine Dokumentation erforderlich oder - insb. durch steuerliche Regelungen zur Aufbewahrung von Unterlagen nach der Abgabenordnung - vorgeschrieben ist.

2.2. Umgang mit digitalen Fotografien

> *„Datenschutz-Grundverordnung: Fotoverbot in Münchner Kita“*[14] *„EU-Datenschutz Kita schwärzt alle Erinnerungsfotos wegen neuer Verordnung“*[15] *„Folge der DSGVO: Diözese Freiburg sagt alle Livestreams von Gottesdiensten ab“*[16]

Die zitierten Schlagzeilen belegen, dass bei dem datenschutzgerechten Umgang mit der Digitalfotografie Verunsicherung besteht, von der naturgemäß diejenigen in besonderem Maß betroffen sind, die beruflich fotografieren oder Fotos verbreiten. Vielfach wurde von Medien die Behauptung aufgestellt, digitale Fotografien oder deren Veröffentlichung seinen generell nur noch mit ausdrücklicher, informierter Einwilligung der abgebildeten Personen zulässig, ansonsten aber verboten. Die Unsicherheiten resultieren maßgeblich daraus, dass weder die EU-Verordnung selbst noch die zu ihrer Umsetzung erlassenen deutschen Rechtsvorschriften zum Umgang mit Fotos, auf denen Personenabgebildet sind, konkrete Vorgaben enthalten.

Tatsächlich hat sich durch die DSGVO **an der Rechtslage aber kaum etwas geändert**: Weiterhin ist gilt für die Fotografie im Rahmen „ausschließlich familiärer oder persönlicher Tätigkeiten“ das Datenschutzrecht von vornherein nicht (Art. 3 Abs. 2, 2. Anstrich DSGVO). Dies ist beispielsweise immer dann der Fall, wenn ein Familienmitglied auf einer privaten Familienfeier fotografiert oder Videos anfertigt und diese nicht veröffentlicht.

Soweit das Datenschutzrecht doch anzuwenden ist (etwa bei Verwertung durch Firmen oder Institutionen oder bei einer Veröffentlichung in Social Media), können Fotos – vielfach auf der Grundlage eine Interessenabwägung aufgenommen und weiterverarbeitet werden (Art.

[14] Welt-Online v. 14.6.2018
[15] Kölner Stadt-Anzeiger, 1.8.2018.
[16] Meedia.de v. 28.5.2018, https://meedia.de/2018/05/28/kuriose-folge-der-dsgvo-dioezese-freiburg-sagt-alle-livestreams-von-gottesdiensten-wegen-datenschutz-ab/ (abgerufen am 16.52019).

6 Abs. 1 lit. f DSGVO). Dabei gilt die Faustformel: Je geringer in das Persönlichkeitsrecht eingegriffen wird (etwa bei Überblicksaufnahmen, Panoramen usw.), umso eher fällt diese Interessenabwägung zu Gunsten des Fotografierenden aus. Dies kann auch bei Aufnahmen von Kindern gelten, soweit damit Interessen des Kindes selbst und anderer Kinder verfolgt werden – wie im Fall von Fotoalben als Abschlussgeschenk im Kindergarten. Hingegen ist eine ausdrückliche Einwilligung nur in wenigen Fällen notwendig, vor allem dann, wenn die Interessen des Betroffenen nicht aufgenommen zu werden, überwiegen. Dies gilt etwa für Porträts.

Inzwischen haben Vertreter des Bundesinnenministerium und der Datenschutzbehörden klargestellt, dass die Vorgaben des **Kunst-Urheber-Gesetzes (KUG)** auch weiterhin gelten, mit dem das Recht am eigenen Bild geschützt wird.[17] Danach ist es zulässig, Fotos von Versammlungen oder Aufzügen wie Volksfesten, Festumzügen usw. ohne Einwilligung der abgebildeten Personen zu veröffentlichen. Diese durch die Rechtsprechung bestätigte Rechtslage hat sich durch die DSGVO nicht geändert.

Andererseits erscheint es und durchaus **sinnvoll, die sich aus dem Nebeneinander des KUG und der DSGVO ergebenden Rechtsunsicherheiten**[18] **durch eine klarstellende gesetzliche Regelung zu beseitigen**. So hält der Deutsche Journalisten-Verband wegen der durch eine Umfrage bei Fotojournalistinnen und -journalisten belegte Unsicherheit

> *„die Schaffung von Rechtssicherheit für Bildjournalistinnen und -journalisten für dringend erforderlich, um die Foto- und Filmfreiheit wiederherzustellen."*[19]

Die Möglichkeit zu einer solchen Klarstellung ergibt sich aus Art. 85 DSGVO, der die Mitgliedstaaten dazu verpflichtet, einen Ausgleich zwischen den Datenschutzvorschriften und dem Recht auf freie Meinungsäußerung und Informationsfreiheit zu schaffen (vgl. unten 3.). Offenbar sieht die Bundesregierung bisher hierzu keine Notwendigkeit. Weder das zusammen mit der DSGVO am 25. Mai 2018 in Kraft getretene deutsche Datenschutzanpassungsgesetz[20] noch der Entwurf eines weiteren Datenschutzanpassungsgesetzes[21] enthalten entsprechende Bestimmungen.

2.3. Internet und soziale Medien: Welches Recht gilt?

---

[17] Vgl. etwa 27. TB des BfDI, 29.
[18] Krüger/Wiencke: Bitte recht freundlich – Verhältnis zwischen KUG und DS-GVO, mmr 2019, 76.
[19] Fotofreiheit, „DJV-Umfrage: Bildjournalisten fordern Rechtssicherheit", http://fotofreiheit.org/2019/04/10/djv-umfrage-bildjournalisten-fordern-rechtssicherheit/ (abgerufen am 7.5.2019).
[20] Gesetz zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 (Datenschutz-Anpassungs- und -Umsetzungsgesetz EU - DSAnpUG-EU) G. v. 30.06.2017 BGBl. I S. 2097 (Nr. 44).
[21] Entwurf eines Zweiten Gesetzes zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 (Zweites Datenschutz-Anpassungs- und Umsetzungsgesetz EU - 2. DSAnpUG-EU) (BT-Drs. 19/4674).

Angesichts ihrer zunehmenden Reichweite und der damit verbundenen sehr umfangreichen Sammlung personenbezogener Daten kommt dem Internet und den sozialen Medien besondere datenschutzrechtliche Bedeutung zu. Gerade hier besteht jedoch erhebliche Unsicherheit, die einerseits aus dem **Nebeneinander der sog. ePrivacy-Richtlinie der EU[22] und der DSGVO** resultiert und andererseits durch die lang anhaltende Arbeitsverweigerung der Bundesregierung bei der Umsetzung europarechtlicher Regelungen verursacht wurde.

Der im Jahr 2009 durch die sog. „**Cookie-Richtlinie**“[23] neu gefasste Art. 5 Abs. 3 der ePrivacy RL enthält strikte Vorgaben zur Einwilligung hinsichtlich der Nutzer bei der Verwendung von Cookies oder ähnlichen Tracking-Methoden:

> *„(3) Die Mitgliedstaaten stellen sicher, dass die Speicherung von Informationen oder der Zugriff auf Informationen, die bereits im Endgerät eines Teilnehmers oder Nutzers gespeichert sind, nur gestattet ist, wenn der betreffende Teilnehmer oder Nutzer auf der Grundlage von klaren und umfassenden Informationen, die er gemäß der Richtlinie 95/46/EG u. a. über die Zwecke der Verarbeitung erhält, seine Einwilligung gegeben hat. ….“*

Das 2007 vom Bundestag beschlossene und seither mehrfach geänderte **Telemediengesetz (TMG)**[24] hat diese Vorgaben nicht nachvollzogen. § 15 Abs. 3 TMG erlaubt weiterhin - entgegen der klaren europarechtlichen Vorgabe - das Tracking für Werbezwecke auch ohne Einwilligung, soweit die entsprechenden Nutzerprofile unter Pseudonym geführt werden und räumt dem Nutzer lediglich ein Widerspruchsrecht ein.

Die wiederholt von Datenschutzseite vorgebrachten Forderungen zur Umsetzung der europarechtlichen Verpflichtungen wurden von der Bundesregierung nicht aufgegriffen, mit dem Ergebnis, dass sich die deutschen Anbieter allein dem (insoweit europarechtswidrigen) TMG verpflichtet fühlten. „Die fortgesetzte Untätigkeit der Bundesregierung und des Gesetzgebers hat zur Folge, dass gegenwärtig die Betroffenen ihre Ansprüche zur Wahrung der Privatsphäre aus Artikel 5 Absatz 3 der E-Privacy-Richtlinie gegenüber Anbietern in Deutschland, bei denen das TMG zur Anwendung kommt, nur unzureichend wahrnehmen können. Damit wird den Bürgerinnen und Bürgern faktisch ein europarechtlich vorgesehenes, wesentliches Instrument zur Wahrung ihrer Privatsphäre bei der Nutzung des Inter-nets vorenthalten“, kritisierte etwa die Konferenz der Datenschutzbeauftragten des Bundes und der Länder in einer bereits 2015 beschlossenen Entschließung.[25] Gerade die Weiterentwicklung von neuen Technologien zur Sammlung und Analyse des

---

[22] Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation) EU-Amtsblatt v. 31.7.2002, L 201.

[23] Richtlinie 2009/136/EG des Europäischen Parlaments und des Rates vom 25. November 2009 zur Änderung der Richtlinie 2002/22/EG über den Universaldienst und Nutzerrechte bei elektronischen Kommunikationsnetzen und -diensten, der Richtlinie 2002/58/EG über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation und der Verordnung (EG) Nr. 2006/2004 über die Zusammenarbeit im Verbraucherschutz EU Amtsblatt v. 18.12.2009, L 337.

[24] Telemediengesetz (TMG) v. 26.3.2007, BGBl I. S. 179.

[25] Umlaufentschließung der Datenschutzbeauftragten des Bundes und der Länder vom 05. Februar 2015, https://www.bfdi.bund.de/SharedDocs/Publikationen/Entschliessungssammlung/DSBundLaender/Entschliessung_Cookies.html?cms_templateQueryString=e-privacy&cms_sortOrder=score+desc (abgerufen am 10.5.2019).

Nutzerverhaltens im Internet mache moderne und effiziente Regelungen zum Schutz der Privatsphäre der Nutzer unabdingbar.

Am 25. Mai 2018 hat sich Rechtslage erheblich geändert, weil die DSGVO als EU-Verordnung **direkt anwendbares Recht in den Mitgliedsstaaten** ist, anders als die DSRL v. 1995 und die ePrivacy RL, die erst mit ihrer Umsetzung in nationales Recht wirksam wurden. Deshalb haben die deutschen Datenschutzbehörde festgestellt, dass die entsprechenden **Bestimmungen des TMG nach dem Inkrafttreten der DSGVO nicht mehr gültig** sind:

> *„Die Vorschrift des Artikels 95 DSGVO findet keine Anwendung auf die Regelungen im 4. Abschnitt des TMG … Damit können die §§ 12, 13, 15 TMG bei der Beurteilung der Rechtmäßigkeit der Reichweitenmessung und des Einsatzes von Tracking-Mechanismen, die das Verhalten von betroffenen Personen im Internet nachvollziehbar machen, ab dem 25. Mai 2018 nicht mehr angewendet werden."*[26]

So nachvollziehbar diese Position der Datenschutzbehörden ist, so unklar sind deren Konsequenzen. Natürlich können Datenschutzbehörden kein vom Gesetzgeber beschlossenes Gesetz aufheben oder außer Kraft setzen. Die Erklärung ist insofern lediglich eine Interpretation der Rechtslage, deren Konsequenzen unklar bleiben. Die Wirtschaft und die Nutzer stehen vor dem Dilemma, dass unklar ist, nach welchen Vorgaben sie personenbezogene Daten in elektronischen Diensten verarbeiten dürfen. Zudem praktizieren deutsche Webanbieter weiterhin **umfangreiches Nutzertracking**, ohne entsprechende Einwilligungen einzuholen, weil weder die DSGVO noch das TMG dies ausdrücklich verbieten.

Die einzige praktikable Lösung würde in einer **Neufassung des TMG** bestehen, die sowohl der DSGVO als auch den Vorgaben der ePrivacy RL entspricht. Die Bundesregierung lässt - unter Berufung auf die auf EU-Ebene geführte Debatte über eine neue ePrivacy-*Verordnung* (vgl. unten 4.2) keinerlei Absicht erkennen, hier tätig zu werden.[27] Auch der Entwurf des Zweiten DSAnpG sieht hier keine klarstellende Regelung vor.[28] Im Ergebnis bleibt es also bis auf weiteres bei den Unsicherheiten, zumal derzeit nicht absehbar ist, ob und wann es zu einer ePrivacy-Verordnung kommen und welchen Inhalt sie ggf. haben wird.

2.4. Wo bleibt die Abmahnwelle?

Immer wieder wurde in Medien eine von der DSGVO verursachte Abmahnwelle heraufbeschworen, die vor allem kleine und mittlere Unternehmen oder Vereine treffe. Die

---

[26] Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder, Entschließung 26. April 2018, https://www.bfdi.bund.de/SharedDocs/Publikationen/Entschliessungssammlung/DSBundLaender/95DSK_Positionsbestimmung_TMG.html?nn=5217228 (abgerufen am 10.5.2019).

[27] Vgl. Antwort der Bundesregierung auf eine Kleine Anfrage der FDP-Fraktion, Drs. 19/2653 v. 11.6.2018, S.9.

[28] Vgl. Fn. 21.

Verunsicherung reichte in die bis in die Arztpraxen. So verabschiedete der Ärztetag eine *„Resolution gegen DSGVO-Verunsicherung und Abmahn-Angst“*[29]

Der Bundesdatenschutzbeauftragte Ulrich Kelber stellte hierzu in seinem jüngsten Tätigkeitsbericht fest, dass von der vorhergesagten Abmahnwelle in seinem Haus bis Ende 2018 fünf Beschwerden über Abmahnungen übrig geblieben seien.[30] Die Berichte anderer Datenschutzbehörden bestätigen die Diagnose, dass von massenhaften Abmahnungen nicht die Rede sein kann.

Mitbewerber, klageberechtigte Vereine und Verbände sowie die Industrie- und Handelskammern können auf Grund von § 3a i. V. m. § 8 UWG Verstöße gegen Datenschutzvorschriften abmahnen, soweit diese Vorschriften zumindest auch im Interesse der Marktteilnehmer das Marktverhalten regeln.

Von den UWG-basierten Abmahnmöglichkeiten zu unterscheiden sind zivilrechtliche Unterlassungs- und Beseitigungsansprüche wegen eines Verstoßes gegen datenschutzrechtliche Vorschriften, dies sich aus dem Unterlassungsklagegesetz (UKlaG) ergeben. Diese Ansprüche stehen gemäß § 3 Abs. 1 UKlagG lediglich Verbraucher-, Branchen- und Berufsverbänden und Kammern zu. Wettbewerber sind nicht klageberechtigt. So bestehen Unterlassungsansprüche, wenn Unternehmer datenschutzrechtlichen Vorschriften zuwiderhandeln, die die Zulässigkeit der Erhebung, Verarbeitung oder Nutzung von Verbraucherdaten regeln, wenn die Daten zu den Zwecken der Werbung, der Markt – und Meinungsforschung, des Betreibens einer Auskunftei, des Erstellens von Persönlichkeits- und Nutzungsprofilen, des Adresshandels, des sonstigen Datenhandels oder zu vergleichbaren kommerziellen Zwecken erhoben werden. Darunter können auch Vorschriften der DSGVO oder des neu gefassten BSDG fallen. Missbrauchsfälle sind hier überhaupt nicht bekannt geworden.

Bereits im Hinblick auf das frühere Datenschutzrecht war die **Abmahnfähigkeit von Datenschutzverstößen nach dem UWG umstritten**, weil Datenschutzvorschriften primär das Persönlichkeitsrecht der Betroffenen schützen. Auch die DSGVO enthält keine ausdrückliche Aussage darüber, ob Regelungen und Rechtsbehelfe zum Schutz des Wettbewerbs bei Datenschutzverstößen ausgeschlossen werden. Die deutsche Rechtsprechung zu diesem Thema ist bislang uneinheitlich.[31] Letztlich bleibt die Beantwortung dieser Frage dem EuGH vorbehalten.[32]

Angesichts der zwischenzeitlichen Erfahrungen und der noch ausstehenden Klarstellung durch den EuGH erscheint es **derzeit nicht vordringlich, dass der deutsche Gesetzgeber hier zusätzliche Regelungen gegen Abmahnungen bei Datenschutzverstößen** trifft.

---

[29] Ärzte-Zeitung v. 22.6.2018.
[30] BfDI, 27.TB, 29.
[31] Vgl. etwa LG Bochum, 07.08.2018 - I-12 O 85/18; LG Würzburg, 13.09.2018 - 11 O 1741/18; OLG Hamburg, 25.10.2018 – 3 U 66/17, sowie Baumgartner/Sitte, Abmahnungen von DS-GVO-Verstößen, ZD 2018, 555 ff. mwN.
[32] Antwort der Bundesregierung (Fn. 26), S. 13.

Keinesfalls sollte an den Klagemöglichkeiten von Verbraucher- und Datenschutzverbänden nach dem UKlagG gerüttelt werden, die hinter entsprechenden Möglichkeiten anderer EU-Staaten zurückbleiben. Art. 80 Abs. 2 DSGVO erlaubt es den Mitgliedstaaten vorzusehen, dass Bürgerrechts- oder Datenschutzorganisationen unabhängig von einem Auftrag der betroffenen Person das Recht hat, bei der zuständigen Aufsichtsbehörde eine Beschwerde einzulegen und gerichtlich durchzusetzen, wenn ihres Erachtens die Rechte einer betroffenen Person gemäß dieser Verordnung infolge einer Verarbeitung verletzt worden sind. Von dieser Möglichkeit hat der deutsche Gesetzgeber bislang keinen Gebrauch gemacht. Es erscheint deshalb sachgerecht, in Ausfüllung der Öffnungsklause in Art. 80 Abs. 2 DSGVO das bereits im UKlagG angelegte **datenschutzrechtliche Verbandsklagerecht zu stärken, indem auch Datenschutz- und Bürgerrechtsverbände in den Kreis der Klageberechtigten aufgenommen werden**.

2.5. Behindert die DSGVO die „Bagatellkommunikation“?

> *„Datenschutz-Irrsinn: Unsere Klingelschilder sollen weg!“*[33] *„Begrüßung mit Namen – Kundin beklagt fehlenden Datenschutz“*[34] *„Datenschutz beim Arzt: Dürfen Patienten noch mit Namen aufgerufen werden?“*[35] *„DSGVO: Jetzt werden sogar Visitenkarten zur Datenschutz-Falle“*[36]

Die in diesen Schlagzeilen beschworenen Folgen der DSGVO zeugen von geringer Rechtskenntnis, denn in keinem der beschriebenen Fälle hat sich etwas an der Rechtslage geändert. Bisweilen drängt sich sogar der Eindruck auf, als werde hier unter den Stichwort „DSGVO-Irrsinn aus Brüssel“ eine **Kampagne gegen den Datenschutz** geführt.

So hat die Befürchtung, die Annahme und Erfassung einer Visitenkarte löse umfangreiche Informationspflichten aus, skurrile Züge. Da die Übergabe einer Businesscard regelmäßig durch den Inhaber erfolgt, damit der Empfänger Kontakt mit ihm aufnimmt, ist er damit informiert und daran interessiert, dass der Empfänger die Karte auch verwendet und die Kontaktdaten etwa in seinem Adressverzeichnis auf dem Smartphone erfasst. Wer damit nicht einverstanden ist, verzichtet auf die Übergabe der Karte. Eine ausdrückliche Informationspflicht des Empfängers gem. Art. 14 DSGVO wird demgemäß nicht ausgelöst. Eine Einwilligung braucht man schon gar nicht. Datenschutzrechtliche Informationspflichten und die Notwendigkeit zum Einholen einer Einwilligung bestehen nur, wenn die Daten zu anderen Zwecken, etwa zur Überprüfung der Kreditwürdigkeit, herangezogen würden.

---

[33] Bild-Zeitung v. 18.10.2018 (Titelseite)
[34] Berliner Morgenpost, 14.12.2018, https://www.morgenpost.de/vermischtes/article215988685/Datenschutz-DSGVO-Metzgerei-Kundin-wehrt-sich-gegen-namentliche-Begruessung.html (abgerufen am 10.5.2019).
[35] Mitteldeutsche Zeitung, 31.5.2018.
[36] Die Welt (online), 18.5.2018, https://www.welt.de/wirtschaft/article176468214/DSGVO-Visitenkarten-werden-durch-neue-EU-Regel-zum-Datenschutz-Problem.html (abgerufen am 10.5.2019).

In einer Reihe der skandalisierten Fälle ist das Datenschutzrecht nicht einmal anzuwenden. Die DSGVO gilt nämlich nur für automatisierte Datenverarbeitungen oder für gegenwärtige bzw. geplante Verarbeitungen in Dateisystemen (Art. 2 Abs. 1 DSGVO). Das gute Namensgedächtnis einer Verkäuferin ist ganz gewiss kein Dateisystem im Sinne der DSGVO.[37] Metzger und Bäcker dürfen also ihre Kunden weiterhin mit Namen begrüßen. Wenn sich ein Kunde dagegen verwahrt, kann er sich jedenfalls nicht auf die DSGVO berufen. Und der weit verbreitete Namensaufruf von Patientinnen und Patienten in der Arztpraxis ist nicht in erster Linie datenschutzrechtlich, sondern vor dem Hintergrund der ärztlichen Schweigepflicht zu beurteilen.

Auch bei den Klingelschildern dürfte die DSGVO meist deshalb nicht greifen, weil keine strukturierte Datensammlung vorliegt. Anders sieht es ggf. bei elektronischen „Klingelbrettern" aus und bei Wohnungsunternehmen, bei denen die Daten der Mieter in einer Datei gespeichert und die Klingelschilder automatisiert erzeugt werden. Aber auch hier führt die DSGVO nicht etwa zu einem Verbot. Der Vermieter braucht nicht einmal eine Einwilligung, da im Regelfall ein berechtigtes Interesse (Art. 6 Abs. 1 lit f DSGVO) vorliegt, etwa damit Boten Pakete und Briefe zustellen können oder bei Besuchern. Da hier allerdings eine Interessenabwägung vorgenommen werden muss, hat der Vermieter einen individuellen, begründeten Widerspruch des Mieters gegen die Nennung seines Namens zu beachten.

2.6. Betriebliche Datenschutzbeauftragte als Bürde?

„Unternehmen müssen zukünftig einen Datenschutzbeauftragten einstellen"[38]

Die Behauptung, mit der DSGVO würde für Unternehmen und Vereine eine unverhältnismäßige Verpflichtung eingeführt, einen Datenschutzbeauftragten zu bestellen, ist gleich mehrfach irreführend. So gab es **auch nach dem bisherigen deutschen Datenschutzrecht eine Verpflichtung zur Bestellung eines (betrieblichen bzw. behördlichen) Datenschutzbeauftragten** (§ 4f BDSG aF). Auch daran, welche Stellen einen DSB zu benennen haben, hat sich nichts wesentliches geändert. Der Schwellenwert für nicht-öffentliche Stellen (*„soweit sie in der Regel mindestens 10 Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigen"*) bleibt unverändert. Er ist § 38 Abs. 1 BDSG nF festgelegt, nicht in der DSGVO. Neu ist nur, dass Art. 37 DSGVO - wie bisher schon das BDSG - Unternehmen mit besonders risikoträchtiger Datenverarbeitung und öffentliche Stellen in sämtlichen EU-Mitgliedstaaten zur Bestellung eines DSB verpflichtet. Angesichts der zunehmenden Digitalisierung von Wirtschaft und Verwaltung ist dies ohne Einschränkung zu begrüßen.

---

[37] BfDI, vgl. Fn. 30.

[38] Focus Online Money, 25.5.2018, „EU paradox: Bürokratie soll abgebaut werden - und dann kommt die DSGVO", https://www.focus.de/finanzen/experten/joachim_haedke/strengerer-datenschutz-eu-paradox-buerokratie-soll-abgebaut-werden-und-dann-kommt-die-dsgvo_id_8982955.html (abgerufen am 10.5.2019).

Die Aufregung über die seit 1977 in Deutschland bestehende Verpflichtung zur Benennung von DSB ist - wie bei zahlreichen anderen, seit letztem Jahr hochgekochten Kritikpunkten an einem „überzogenen Datenschutz“- in erster Linie damit zu erklären, dass die bestehenden Verpflichtungen zu wenig bekannt waren und vielfach nicht befolgt wurden, jetzt aber angesichts höherer Bußgelddrohungen für Datenschutzverstöße Ernst genommen werden müssen.

Kurios mutet es an, dass selbst Regierungsressorts, die in den internen Datenschutzbeauftragten zuvor ein praktisches Mittel zur Verankerung von Datenschutz-Know How in den Unternehmen gesehen hatten, diese nunmehr als bürokratisches Hindernis in Frage stellen. So fand die Forderung, die Bestellpflicht von DSB zu lockern, in der Politik Rückhalt und wurde von dem Bundeswirtschaftsministerium unterstützt. Der Bundesrat lehnte am 19. Oktober 2018 zwar eine vom Freistaat Bayern initiierte Änderung ab, die Bestellpflicht gemäß § 38 Abs. 1 BDSG nF gänzlich zu streichen. Trotzdem ist diese Frage noch nicht endgültig vom Tisch.[39] Aus diesem Grund hat sich die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder gegen eine Abschaffung oder Schwächung der Datenschutzbeauftragten ausgesprochen.[40] Sie weist darauf hin, dass auch beim Wegfall der nationalen Benennungspflicht von Datenschutzbeauftragten die von den Verantwortlichen einzuhaltenden Pflichten des Datenschutzrechts bestehen blieben. Diese verlören interne Beraterinnen und Berater zu Fragen des Datenschutzes. Der Wegfall könnte zwar kurzfristig als Entlastung empfunden werden, mittelfristig ginge jedoch interne Kompetenz verloren. Eine Aufweichung dieser Benennungspflicht für Unternehmen und Vereine werde diesen deshalb mittelfristig schaden.

Den Bestrebungen, die Bestellpflicht für Datenschutzbeauftragte zu lockern oder sie gar abzuschaffen, sollte weiterhin entgegengetreten werden.

2.7. Wer vertritt die deutschen Datenschutzbehörden im Europäischen Datenschutzausschuss?

> *„Wahl eines deutschen Ländervertreters im Europäischen Datenschutzausschuss: Die Positionen der Aufsichtsbehörden (= der Landesdatenschutzbeauftragten) werden systematisch ausgeblendet und missachtet. Das kann keinem gefallen, der einen starken, unterstützenden und beratenden Datenschutz will.“*[41]

---

[39] Spaeing, Bundesrat hat gegen Änderung der Bestellpflicht gestimmt, https://www.bvdnet.de/bundesrat-hat-gegen-aenderung-der-bestellpflicht-gestimmt/ (abgerufen am 10.5.2019).

[40] Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder, Entschließung v. 23.4.2019, https://www.bfdi.bund.de/SharedDocs/Publikationen/Entschliessungssammlung/DSBundLaender/DSK_Entschließung_KeineAbschaffungDSB.pdf?__blob=publicationFile&v=1 (abgerufen am 10.5.2019).

[41] Twitter-Nachricht des Landesbeauftragten Baden-Württemberg, https://www.baden-wuerttemberg.datenschutz.de/twitter-nachricht-wahl-eines-deutschen-laendervertreters-im-europaeischen-datenschutzausschuss/ (abgerufen am 13.5.2019).

Eines der wichtigsten Argumente für ein europaweit einheitliches Datenschutzrecht besteht darin, dass im Internetzeitalter grenzüberschreitende Angebote immer mehr zur Regel werden. Bei der Koordination der Datenschutzbehörden kommt dem gemäß Art. 68 DSGVO eingerichteten Europäischen Datenschutzausschuss (EDSA) zentrale Bedeutung zu. Neben einem allgemeinen Informationsaustausch hat er echte Entscheidungsbefugnisse bei der Auslegung der Verordnung und der Lösung von Einzelfällen, etwa bei dem Vorgehen gegen Datenschutzverstöße internationaler Unternehmen.

Deshalb kommt der Entscheidung, wer Deutschland im EDSA vertritt, besondere Bedeutung zu. Gemäß § 17 BDSG ist gemeinsamer deutscher Vertreter zwar der Bundesbeauftragte, bei Angelegenheiten in ausschließlicher Länderkompetenz hat dieser jedoch die Verhandlungsführung und das Stimmrecht auf einen **gemeinsamen Ländervertreter** zu übertragen. Im Hinblick darauf, dass nach dem BDSG die Landesdatenschutzbehörden für den Datenschutz in der Wirtschaft zuständig sind, ist es von großer Bedeutung, wie der Ländervertreter benannt wird.

Die Datenschutzkonferenz hatte sich dafür ausgesprochen, dass die Landesdatenschutzbehörden den Ländervertreter bestimmen können. Dem sind weder der Bundestag noch der Bundesrat gefolgt. Gemäß § 17 BDSG nF wird der Vertreter allein vom Bundesrat bestimmt. Die Wahl des Ländervertreters durch den Bundesrat ist mit der Unabhängigkeit der Datenschutzaufsichtsbehörden der Länder unvereinbar. Deren Leiter werden in Deutschland – ebenso wie die Bundesbeauftragte – von den jeweiligen Parlamenten gewählt. Damit ist es nicht zu vereinbaren, wenn die Landesregierungen den Vertreter der Landesaufsichtsbehörden im Europäischen Datenschutzausschuss bestimmen könnten. Zumindest hätte den Landesdatenschutzbehörden das alleinige Vorschlagsrecht hierfür eingeräumt werden müssen.[42] **Die Benennung des Ländervertreters sollte deshalb gesetzlich neu geregelt und dabei verbindlich festgeschrieben werden, dass der Vertreter durch die Leitungen der unabhängigen Landesaufsichtsbehörden für den Datenschutz gewählt wird.**

Geradezu skandalös ist es, dass es der Bundesrat bis heute (Stand: 14.5.2019) versäumt hat, den Ländervertreter zu benennen. Deshalb **muss der Bundesrat unverzüglich seiner Verpflichtung aus § 17 Abs. 1 BDSG nachkommen und einen Vertreter der Länder für den Europäischen Datenschutzausschuss benennen.** Er sollte dabei dem Votum der unabhängigen Landesaufsichtsbehörden für den Datenschutz folgen.

3. Rechtliche Umsetzung bzw. Nicht-Umsetzung in Deutschland

Ein Jahr nach dem Wirksamwerden der DSGVO fällt die Zwischenbilanz zur Umsetzung und Anwendung der DSGVO in Deutschland – bezogen auf die bereits beschlossenen und im Entwurf vorliegenden Gesetze auf Bundes- und Länderebene **überwiegend negativ** aus. Die Gesetzgeber des Bundes und der Länder haben die in der Grundverordnung enthaltenen

[42] Stellungnahme der EAID zum Gesetzentwurf v. 22.2.2017, https://www.eaid-berlin.de/?page_id=1656 (abgerufen am 30.4.2019).

Öffnungsklauseln teilweise überstrapaziert, teilweise wurden Bestimmungen unter Verstoß gegen das unionsrechtliche Wiederholungsverbot schlicht in das deutsche Recht übernommen. In Teilen sind Gesetzgebungsaufträge der Grundverordnung nicht erfüllt worden.

Das Hauptanliegen des Bundesgesetzgebers war und ist es offenbar, den rechtlichen Status quo in Sachen Datenschutz in Deutschland auch nach dem Inkrafttreten der Grundverordnung soweit wie möglich unverändert zu lassen. Diesem unambitionierten Beispiel sind die Landesgesetzgeber weitgehend gefolgt. Das aber widerspricht dem Anliegen des Unionsgesetzgebers, der mit der Grundverordnung auf die rasanten technischen Entwicklungen reagiert hat[43] und offenbar auch sicherstellen will, dass der Rechtsrahmen laufend an diese angepasst wird, wie man dem Evaluationsauftrag an die Kommission entnehmen kann.[44]

Das alte BDSG war seit 2001 unverändert geblieben, weshalb es notwendig gewesen wäre, diesen Rechtszustand anlässlich des Inkrafttretens der Grundverordnung der technischen Entwicklung anzupassen, statt ihn schlicht beizubehalten und teilweise wörtlich in das neue BDSG zu übernehmen. Zudem hat der Bundesgesetzgeber den Spielraum überschätzt, den die Grundverordnung den Mitgliedstaaten bei der Umsetzung eröffnet. Die Bundesregierung hat gemeinsam mit anderen Mitgliedstaaten zwar Öffnungsklauseln insbesondere für den öffentlichen Bereich in der Grundverordnung gerade mit der Absicht durchgesetzt, die in Deutschland geltenden Regeln sowohl im allgemeinen als auch im bereichsspezifischen Datenschutzrecht beibehalten zu können. Diese Öffnungsklauseln sind aber nicht unbegrenzt und rechtfertigen es auch nicht, das bisher in Deutschland geltende unterschiedliche Datenschutzniveau für den öffentlichen und den nicht-öffentlichen Bereich aufrechtzuerhalten. Schon die Datenschutzrichtlinie von 1995[45] wollte prinzipiell einheitliche Regeln für beide Bereiche etablieren. Diesen Ansatz verfolgt die Grundverordnung weiter, wobei sie den Mitgliedstaaten für die im öffentlichen Interesse liegende oder der Ausübung öffentlicher Gewalt dienende Datenverarbeitung bestimmte Abweichungsmöglichkeiten eröffnet hat. Die Beibehaltung ganzer Regelungssysteme für den Datenschutz im Bereich der staatlichen Verwaltung wird dadurch jedoch nicht legitimiert. Die deutschen Umsetzungsgesetze überdehnen die Öffnungsklauseln der Grundverordnung in mehrfacher Hinsicht oder füllen sie in unzureichender Weise aus und enthalten redundante und das Unionsrecht in unzulässiger Weise wiederholende Regelungen.

So enthält das mit dem Datenschutz-Anpassungs- und Umsetzungsgesetz EU v. 30.6.2017 neugefasste Bundesdatenschutzgesetz zahlreiche Vorschriften, die **mit Unionsrecht unvereinbar** sind. Das gilt für die blankettartige Zweckänderungsbefugnis für öffentliche Stellen „zur Abwehr erheblicher Nachteile für das Gemeinwohl“ wie zur „Wahrung

[43] Erwägungsgrund 6 der DSGVO.
[44] Art. 97 Abs. 5 DSGVO.
[45] S. Fn. 4.

erheblicher Belange des Gemeinwohls“ in § 23 Abs. 1 Nr. 3 BDSG[46] ebenso wie für die Zweckänderungsbefugnis für nichtöffentliche Stellen zur Geltendmachung zivilrechtlicher Ansprüche in § 24 Abs. 1 Nr. 2 BDSG.[47] Des weiteren sind auch die Beschränkungen der Betroffenenrechte und der Informationspflichten der Datenverarbeiter in mehrfacher Hinsicht unionsrechtswidrig. Das gilt sowohl für die Beschränkung der Informationspflicht und des Auskunftsanspruchs bei Informationen, die „ihrem Wesen nach“ geheim gehalten werden müssen (§ 29 Abs. 1 S. 1 BDSG)[48] als auch für die Beschränkungen der Kontrollbefugnisse der Aufsichtsbehörden gegenüber Berufsgeheimnisträgern (§ 29 Abs 3 BDSG)[49] und für die Einschränkungen der Informationspflichten bei analoger Kommunikation mit Betroffenen und ihre Folgeregelungen (§ 32 Abs. 1 Nr. 1, Abs. 2 u. 3 BDSG), für die es in der Grundverordnung keine Basis gibt bzw. die deren Voraussetzungen nicht genügen.[50] In gleicher Weise verstößt die Beschränkung des Auskunftsrechts jedenfalls gegenüber nichtöffentlichen Stellen insoweit gegen Unionsrecht, als die Auskunft nach § 34 Abs. 1 Nr. 2 BDSG verweigert werden kann, wenn die Daten aufgrund von Aufbewahrungsvorschriften aufbewahrt werden oder ausschließlich der Datensicherung oder Datenschutzkontrolle dienen.[51] Schließlich ist auch die Beschränkung des Löschungsanspruchs in Fällen des für den Verantwortlichen unverhältnismäßigen Aufwands (§ 35 Abs. 1 BDSG) mit der Grundverordnung nicht vereinbar.[52] Gleiches gilt für die Beschränkung des Widerspruchsrechts in § 36 BDSG, die nicht nur überflüssig ist, sondern gegen das unionsrechtliche Verbot der Normwiederholung verstößt. Dieses soll sicherstellen, dass eine unionsweit einheitliche Rechtsauslegung durch den Europäischen Gerichtshof stattfinden kann.[53] Zwar lässt die Grundverordnung im Erwägungsgrund 8 Normwiederholungen zu, soweit sie erforderlich sind, um die Kohärenz zu wahren und die Verständlichkeit der nationalen Rechtsvorschriften für die Normadressaten zu erhöhen. Beide Voraussetzungen sind aber nicht erfüllt. Das neugefasste Bundesdatenschutzgesetz und die bereichsspezifischen Gesetze führen im Gegenteil durch seine Regelungen – nicht allein soweit sie wederholenden Charakter haben - zu **erhöhter Rechtsunsicherheit** bei den Betroffenen und Rechtsanwendern. Auch die Vorschriften zum Scoring (§ 31 BDSG) und zur

---

[46] Kühling/Buchner/Herbst (2. Aufl.), § 23 BDSG Rn. 20.

[47] Kühling/Buchner/Herbst (2. Aufl.), § 24 BDSG Rn. 13 f.

[48] Vgl. die Stellungnahme der EAID zum Gesetzentwurf v. 22.2.2017, https://www.eaid-berlin.de/?page_id=1656 (abgerufen am 30.4.2019); Kühling/Buchner/Herbst (2. Aufl.), § 29 BDSG Rn. 8, hält eine verordnungskonforme Auslegung dieser Bestimmung für möglich und geboten. S. auch Simitis/Hornung/Spiecker/Dix, Datenschutzrecht, Art. 14 Rn. 30.

[49] Vgl. Stellungnahme der EAID zum Referentenentwurf für ein 2. Datenschutz-Anpassungs- und Umsetzungsgesetz EU v. 16.7.2018, https://www.eaid-berlin.de/wp-content/uploads/2018/07/EAID-Stellungnahme-Referentenentwurf-2.-DSAnpUG-EU.pdf (abgerufen am 30.4.2019); Kritik an der Unklarheit der Vorschrift übt auch Kühling/Buchner/Herbst, (2. Aufl.), § 29 BDSG Rn. 30.

[50] Kühling/Buchner/Golla (2. Aufl.), § 32 BDSG Rn. 5, 23 u. 26. S. auch Simitis/Hornung/Spiecker/Dix, Datenschutzrecht, Art. 14 Rn. 28.

[51] Kühling/Buchner/Herbst, (2. Aufl.), § 34 BDSG Rn. 4, 11 f.

[52] Kühling/Buchner/Herbst, (2. Aufl.), § 35 BDSG Rn. 15 f.

[53] Kühling/Buchner/Herbst, (2. Aufl.), § 36 BDSG Rn. 14, 18 mwN auf die Rechtsprechung des EuGH.

automatisierten Entscheidungsfindung einschließlich Profiling (§ 37 BDSG) sind in Teilen unionsrechtswidrig, weil sie (im Fall des Scoring) den bisher geltenden Rechtszustand beibehalten wollen, obwohl die Grundverordnung dafür keine Grundlage enthält,[54] und weil sie (im Fall der automatisierten Einzelentscheidung) von einer fehlerhaften Interpretation der Grundverordnung ausgehen.[55]

Das Gleiche gilt im Wesentlichen für die dem BDSG in weiten Teilen entsprechenden Vorschriften im novellierten Steuer- und Sozialrecht.[56] Auch der gegenwärtig noch im Gesetzgebungsverfahren befindliche Entwurf der Bundesregierung für ein Zweites Datenschutz-Anpassungs- und Umsetzungsgesetz EU setzt die Tendenz fort, das geltende bereichsspezifische Datenschutzrecht für den öffentlichen Bereich unabhängig von seiner Vereinbarkeit mit Unionsrecht beizubehalten und lässt die **Chancen der Grundverordnung** für eine Vereinheitlichung und Modernisierung des Datenschutzrechts **ungenutzt**. So sind die geplanten Vorschriften im BSI-Gesetz zur Durchbrechung der Zweckbindung sowie zur Beschränkung der Informationspflichten und der Betroffenenrechte so weitgehend und unbestimmt begründet, dass sie mit der Grundverordnung nicht zu vereinbaren sind.[57] Das gilt auch für die geplanten Änderungen des Bundesmeldegesetzes, die ebenfalls eine unionsrechtswidrige Einschränkung der Auskunfts- und Löschungsrechte enthalten. [58] Zudem versäumt es der Entwurf, die bereits erfolgte Umwandlung des Melderegisters in einen multifunktionalen Informationspool durch die Stärkung der Betroffenenrechte zu kompensieren, was dem Grundrecht auf informationelle Selbstbestimmung, wie es in der Grundverordnung zum Ausdruck kommt, entsprochen hätte.

Im übrigen hat es der Bundesgesetzgeber versäumt, den Regelungsauftrag des Art. 85 der Grundverordnung für die **Datenverarbeitung zu journalistischen Zwecken** zu erfüllen (vgl. oben 2.2) und ein **Beschäftigtendatenschutzgesetz** zu erlassen, das den Vorgaben des Art 89 Grundverordnung genügt. Das Kunsturheber-Gesetz gilt zwar fort, kann aber die Rechtsunsicherheit bei der Tätigkeit insbesondere von Foto-Journalisten nicht beseitigen (s. auch oben 2.).[59] Die Landesgesetzgeber sind aufgefordert, für den Bereich des Presserechts zu regeln, inwieweit Ausnahmen von den Informationspflichten der Grundverordnung angemessen sind, um die Arbeit von Foto-Journalisten nicht unzulässig zu erschweren. Zudem sind die Gesetzgeber in Bund und Ländern aufgefordert, die Erteilung personenbezogener Auskünfte durch Behörden und deren sonstige Öffentlichkeitsarbeit präziser zu regeln und das bestehende Schutzgefälle für die betroffenen Personen gegenüber Print- und Funkmedien zu beseitigen Schließlich muss die ungerechtfertigte Sonderbehandlung der öffentlich-rechtlichen Rundfunkanstalten, die bisher nur in vier

---

[54] Kühling/Buchner/Buchner, (2. Aufl.), § 31 BDSG Rn 4 f.

[55] Kühling/Buchner/Buchner, (2. Aufl), § 37 BDSG Rn 3.

[56] Vgl. Art. 17 und 24 des Gesetzes zur Änderung des Bundesversorgungsgesetzes und anderer Vorschriften v. 17.7.2017.

[57] Vgl. Stellungnahme der EAID (s.o. FN 8), Abschnitt III.

[58] Vgl. Stellungnahme der EAID (s.o. FN 8), Abschnitt IV.

[59] Vgl. dazu Benedikt/Kranig, DS-GVO und KUG – ein gespanntes Verhältnis, ZD 2019, 4 ff.

Bundesländern (Berlin, Brandenburg, Bremen und Hessen) hinsichtlich der Verarbeitung von Teilnehmerdaten durch den Beitragsservice der Kontrolle durch unabhängige Aufsichtsbehörden unterliegen, beendet werden, um eine unionsrechtskonforme Situation auch in diesem Bereich herbeizuführen.[60] Die Generalklausel des § 26 BDSG zum Beschäftigtendatenschutzgesetz wird den unionsrechtlichen Vorgaben ebenfalls nicht gerecht.[61]

Die unzureichende Umsetzung der Grundverordnung in Deutschland führt allerdings nicht dazu, dass diese keine praktische Wirkung entfaltet. Die Grundverordnung ist vielmehr – wie das gesamte Unionsrecht – stets vorrangig vor dem deutschen Recht anzuwenden, soweit dieses dem Unionsrecht widerspricht und auch nicht (z.B. wegen seines eindeutigen Wortlauts) unionsrechtskonform ausgelegt werden kann. Dieser **Anwendungsvorrang des Unionsrechts** wird deklaratorisch in den deutschen Umsetzungsgesetzen erwähnt.[62] Es ist Aufgabe der Verantwortlichen, der Aufsichtsbehörden und letztlich der Gerichte (in letzter Instanz des Europäischen Gerichtshofs), diesem Anwendungsvorrang Geltung zu verschaffen. Dabei gibt es keinen Entscheidungsvorrang der Gerichte (quasi ein Verwerfungsmonopol) bei der Frage, in welchen Fällen das Unionsrecht vorrangig anzuwenden ist. Jeder Verantwortliche und jede Aufsichtsbehörde in Europa ist verpflichtet, das Unionsrecht vorrangig anzuwenden, soweit ein Konflikt mit innerstaatlichem Recht besteht, der interpretatorisch nicht aufgelöst werden kann. Auch wenn der Unionsgesetzgeber den Harmonisierungsanspruch für den öffentlichen Bereich durch die Aufnahme der Öffnungsklauseln insbesondere in den Art. 6 und 23 relativiert hat, erscheint es verfrüht, die Harmonisierung des Datenschutzes im öffentlichen Bereich als misslungen zu bezeichnen.[63] Denn die notwendigerweise sehr abstrakt formulierte Grundverordnung bedarf der Konkretisierung und Operationalisierung nicht nur durch die nationalen Gesetzgeber, sondern insbesondere durch die Aufsichtsbehörden, die in Deutschland in der Konferenz der unabhängigen Aufsichtsbehörden und in Europa im Europäischen Datenschutzausschuss kooperieren. Sowohl die von der deutschen Datenschutzkonferenz bereits beschlossenen Kurzpapiere zur Interpretation von Schlüsselbestimmungen der Grundverordnung[64] als auch die ersten Richtlinien und Stellungnahmen des Europäischen Datenschutzausschusses[65] verdeutlichen, dass die Aufsichtsbehörden diese Aufgabe ernst nehmen. Diese Präzisierungsarbeit muss intensiviert werden, um der verunsichernden Wirkung der deutschen Gesetzgebung zur Implementierung der Grundverordnung wirksam zu begegnen. Insbesondere sollte der Europäische Datenschutzausschuss Leitlinien zur einheitlichen Bußgeldpraxis der Aufsichtsbehörden verabschieden, die transparent und vorhersehbar gestaltet werden muss (s.o. 2.). Gleichzeitig gibt die immer umfangreichere Rechtsprechung des Europäischen Gerichtshofs und des Europäischen Gerichtshofs für Menschenrechte wichtige Hinweise für die Anwendung der Grundverordnung in der Praxis.

---

[60] Simitis/Hornung/Spiecker/Dix, Datenschutzrecht, Art 85 Rn. 11, 16, 21, 32.

[61] Kühling/Buchner/Maschmann (2. Aufl.), § 26 BDSG Rn. 2.

[62] § 1 Abs 5 BDSG, § 35 Abs. 2 S. 1 SGB I, § 2a Abs 3 AO.

[63] Vgl. demgegenüber Roßnagel, DuD 2018, 741, 743.

[64] https://www.datenschutzkonferenz-online.de/kurzpapiere.html (abgerufen am 1.5.2019).

[65] https://edpb.europa.eu/our-work-tools/general-guidance_de (abgerufen am 1.5.2019).

Die Aufsichtsbehörden müssen allerdings zur Sicherung ihrer **Unabhängigkeit** mit den nötigen personellen, technischen und finanziellen **Ressourcen** ausgestattet werden, um den gewachsenen Aufgabenumfang zu bewältigen (Art, 52 Abs 4 DSGVO). In einigen Bundesländern (z.B. in Hamburg, wo wichtige Internet-Unternehmen ihre Deutschland-Zentrale haben) sind die Aufsichtsbehörden dramatisch unterausgestattet. Für diesen Verstoß gegen Unionsrecht ist die Bundesrepublik als Ganzes verantwortlich. Bayern ist zudem die einzige Region in der EU, wo die Aufsicht über die Wirtschaft und die Verwaltung gespalten ist. Das widerspricht zwar nicht der Grundverordnung, ist aber in hohem Maße bürgerunfreundlich.

4. Weiterentwicklung des Datenschutzrahmens in der EU und international

4.1. Einfluss der DSGVO auf die Datenschutzgesetzgebung in Drittstaaten

Die Datenschutz-Grundverordnung hat schon vor ihrem Inkrafttreten erhebliche Auswirkungen auf die weltweite Diskussion zu Fragen des Datenschutzes gehabt, der sich seit dem 25. Mai 2018 noch intensiviert hat. Die Einschätzung des Europäischen Datenschutzbeauftragten Giovanni Buttarelli, die Grundverordnung sei ein Aufruf zur **Entwicklung eines neuen weltweiten digitalen „Goldstandards**“[66] ist durchaus berechtigt. Mehrere außereuropäische Länder und Bundesstaaten haben inzwischen Gesetze beschlossen, die sich am Vorbild der Grundverordnung orientieren. Zu nennen ist beispielsweise der kalifornische Consumer Privacy Act (CCPA)[67] und das neue thailändische Datenschutzgesetz. Dem US-Kongreß liegen mehrere Entwürfe für Datenschutzgesetze und Gesetze zu damit zusammenhängenden Fragen vor oder werden gegenwärtig parteiübergreifend erarbeitet[68], etwa der Entwurf eines Algorithmic Accountability Act. Auch die großen Internet-Konzerne fordern mittlerweile ein US-Bundesgesetz zum Datenschutz in der Wirtschaft, das bisher fehlt.[69] Marc Zuckerberg hat vor dem US-Kongress und vor dem Europäischen Parlament die europäische Datenschutz-Grundverordnung als vorbildlich bezeichnet. Unabhängig von der Glaubwürdigkeit solcher Aussagen, die in der Folge des Cambridge Analytica-Skandals gemacht wurden, ist unverkennbar, dass der Druck der Wirtschaft auf den US-Kongreß zunimmt, ein Datenschutzgesetz zu erlassen, das ein der

---

[66] Buttarelli, The EU GDPR as a clarion call for a new global digital gold standard, IDPL 2017, 77.

[67] Das Gesetz tritt am 1.1.2020 in Kraft.

[68] Eine Gruppe von Senatoren (Republikaner und Demokraten) erarbeitet gegenwärtig einen Gesetzentwurf für den Datenschutz im Online-Bereich, der noch im Mai 2019 im Handelssausschuss des Senats zur Abstimmung gestellt werden soll, https://www.reuters.com/article/us-usa-privacy-congress/us-lawmakers-struggle-to-draft-online-privacy-bill-idUSKCN1S62NA?mkt_tok=eyJpIjoiWlRsbFpEazNNRFl4TXpVMiIsInQiOiJwSEVYbXJKZFZkZlZpMWpcL3VUVFBGNTYwaUlGem5mblBPQXZ3R3BNMXkzSnhcL1ZxejAxM2l3TFJYT0FIaUYzZFhZTlMwemFRZU5DVjdLeDJIU3N4VE56aTVSbjJSZWZlRUZiT3hlQjVSXC9GbWcwb1lGRmFkb08rSHRpczBQa3ZPeCJ9 (abgerufen am 252019). Siehe auch das Schreiben des Electronic Privacy Information Center (EPIC) an den Handelsausschuss vom 29.4.2019, https://epic.org/testimony/congress/EPIC-SCOM-ConsumerPerspectives-Apr2019.pdf (abgerufen am 2.5.2019).

[69] Der U.S. Privacy Act 1974 gilt nur für die öffentliche Verwaltung.

Grundverordnung adäquates Datenschutzniveau gewährleistet und eine unabhängige Datenschutzaufsicht vorsieht.

4.2. Rechtsrahmen für die Telekommunikation und das Internet

Angesichts der zentralen Bedeutung der elektronischen Kommunikation und der zunehmenden Risiken ihrer Überwachung und der umfassenden Registrierung des Kommunikationsverhaltens muss die Europäische Union dafür sorgen, dass die **Vertraulichkeit und Sicherheit** von technisch vermittelter Kommunikation stärker und effektiver als bisher geschützt wird.

Europarechtliche Vorgaben zum Datenschutz bei elektronischen Kommunikationsdiensten durch den Erlass der Datenschutzgrundverordnung nicht etwa überflüssig geworden. Die gegenwärtigen Vorgaben bedürfen allerdings einer grundlegenden Überarbeitung. Nur so lassen sich der Schutz der Kommunikationsdaten und des **Fernmeldegeheimnisses** auch in Zukunft auf hohem Niveau gewährleisten.

Wie bereits weiter oben ausgeführt (vgl. oben 2.3), bestehen hinsichtlich des Datenschutzes bei elektronischen Diensten erhebliche Unsicherheiten, die sowohl der Nicht-Umsetzung europäischen Rechts durch das TMG als auch dem Nebeneinander von DSGVO und ePrivacy-RL geschuldet sind.

Vor diesem Hintergrund kommt der in den EU-Gremien diskutierten Entwurf einer ePrivacy-Verordnung, die - ebenso wie die DSGVO - in allen Mitgliedstaaten direkt anwendbar wäre, zentrale Bedeutung zu.

Die Europäische Kommission hatte bereits am 10. Januar 2017 den Entwurf[70] einer Verordnung zum Schutz der Privatsphäre für die elektronische Kommunikation (**ePrivacy-Verordnung**) vorgelegt. Die neue Verordnung, die in allen Mitgliedstaaten direkt anwendbar sein soll, soll die bisherige ePrivacy-Richtlinie ersetzen, die von den Mitgliedstaaten unterschiedlich und z.T. unvollständig umgesetzt wurde. Kernstücke des Vorschlags sind die Erstreckung auf Dienste, die hinsichtlich ihrer Funktionalität den Telekommunikationsdiensten entsprechen (sog. **Over the Top Telecommunications – OTT**, z.B. Skype oder WhatsApp und Webmail-Angebote) und die Neufassung der Bestimmungen zur Einwilligung in elektronische Tracking- und Profilingverfahren.

Aus datenschutzrechtlicher Sicht[71] ist eine Weiterentwicklung des EU-Rechtsrahmens für die Telekommunikation, das Internet und soziale Medien unverzichtbar. Er sollte beim Telefonmarketing wie die Versendung von kommerziellen Nachrichten in sozialen Netzwerken die Einwilligung des Betroffenen voraussetzen (**Opt-In-Prinzip**). Schließlich muss jeder das Recht haben, seinen Kommunikationsverkehr (sein Heimnetzwerk, seine E-Mails,

---

[70] Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications), 10.1.2017 COM(2017) 10 final 2017/0003 (COD) https://ec.europa.eu/digital-single-market/en/proposal-eprivacy-regulation (abgerufen am 10.5.2019).

[71] EAID-Stellungnahme zur Konsultation der EU-Kommission zur ePrivacy-Richtlinie: Vertraulichkeit und Sicherheit der elektronischen Kommunikation v. 8.7. 2016, https://www.eaid-berlin.de/?p=1224 (abgerufen am 10.5.2019).

Smartphones und Datenträger) durch Passörter und Verschlüsselung zu sichern und die Anbieter von Kommunikationsdiensten sollten verpflichtet werden, entsprechende Sicherheitsmaßnahmen zumindest anzubieten.

Angesichts der zunehmenden Bedeutung vermeintlich „kostenloser" Dienste, welche die Nutzer tatsächlich mit ihren personenbezogenen bezahlen, besteht die Gefahr, dass der Datenschutz zum Luxusgut für Vermögende wird. Deshalb sollten existenziell bedeutsame Dienste im Sinne eines Universaldienstes kostenlos und ohne überschießende Datensammlung angeboten werden. Die Verarbeitung personenbezogener Daten muss sich hier ausschließlich auf das zu ihrer Erbringung erforderliche Maß beschränken. Cookies von Drittanbietern sollten stets standardmäßig deaktiviert und auch andere Techniken zum Tracking und Targeting nur mit ausdrücklicher Zustimmung der Nutzer eingesetzt werden.

Zur Sicherung einer einheitlichen Rechtsdurchsetzung sollten in allen Mitgliedstaaten die **Datenschutzbehörden für die Umsetzung der ePrivacy-VO zuständig** sein, die im Europäischen Datenschutzausschuss für eine einheitliche Rechtsanwendung sorgen. Damit würden die bisherigen Zuständigkeitsprobleme und Rechtsunsicherheiten behoben, die weder für die Nutzer noch für die Unternehmen nachvollziehbar sind. Schließlich müssen die strengen **Sanktionsmechanismen** der DSGVO (Bußgelder und Untersagungsbefugnisse der Datenschutzaufsichtsbehörden) auch für den Geltungsbereich der ePrivacy VO sichergestellt werden.

5. Fazit und Ausblick

Die Datenschutz-Grundverordnung regelt die Verarbeitung personenbezogener Daten vor dem Hintergrund der gegenwärtig vorherrschenden technologischen Rahmenbedingungen. Es ist absehbar, dass sich diese rasch verändern werden. Deshalb hat der Unionsgesetzgeber eine **Evaluations- und Berichtspflicht** vorgesehen (Art 97 DSGVO), die verhindern soll, dass der neue Rechtsrahmen und die technische und soziale Realität in Kürze auseinanderfallen. Insbesondere kann die Grundverordnung nicht wie die Vorgängerregelung, die Richtlinie 95/46, mehr als zehn Jahre unverändert bleiben. Bei ihren Berichten und Änderungsvorschlägen muss die Kommission Standpunkte und Feststellungen aller „einschlägigen Stellen oder Quellen" berücksichtigen.[72] Dazu zählen auch die Mitgliedstaaten und die Aufsichtsbehörden.[73]

Die Bundesregierung, aber auch die Aufsichtsbehörden sollten deshalb aktiv an der Evaluation durch die Kommission mitwirken und dabei auch auf Mängel in der Grundverordnung hinweisen, die sich nach deren Inkrafttreten gezeigt haben. Dazu zählt insbesondere die Tatsache, dass Art. 22 DSGVO die automatisierte Entscheidungsfindung und insbesondere das **Profiling** nur **unzureichend** regelt. Die Vorschrift beantwortet nicht

[72] Art 97 Abs 4 DSGVO.

[73] Kühling/Buchner/Kühling/Raab, (2. Aufl.), Art 97 Rn 9.

die Frage, wann eine automatisierte Entscheidungsfindung oder die Bildung eines Persönlichkeitsprofils zulässig ist, sondern regelt nur die Bedingungen, unter denen das Ergebnis eines solchen Entscheidungsprozesses genutzt werden darf.[74] Auch aus einem anderen Grund hatte der Unionsgesetzgeber mit dieser Vorschrift die mit derartigen Prozessen verbundenen Risiken für die Rechte des Einzelnen nicht ausreichend berücksichtigt: Art 22 enthält bestimmte Rechte für Personen, die einer *ausschließlich* auf automatisierter Datenverarbeitung einschließlich Profiling unterworfen werden. Dazu zählt unter anderem das Recht, eine menschliche Intervention auf Seiten des Verantwortlichen verlangen zu können.[75] Diese Regelung verkennt die praktische Bedeutung, die rechnergestützte Bewertungen und Vorschläge schon heute auf Entscheidungen haben, auch wenn sie letztlich von einer natürlichen Person getroffen werden („Der Computer hat immer Recht"). Auch die Pflicht zur Aufklärung über die involvierte Logik bei Systemen der **künstlichen Intelligenz** und des **maschinellen Lernens** sollte dahingehend präzisiert werden, dass derartige Systeme nicht eingesetzt werden dürfen und damit auf die Gewinnung bestimmter Informationen verzichtet werden muss, wenn der Verantwortliche die involvierte Logik selbst nicht versteht und sie deshalb der betroffenen Person nicht erklären kann.

Außerdem bedarf die Grundverordnung der Überarbeitung zumindest auch in einem weiteren Punkt: der zunehmende Einsatz von Sensorik etwa im **Internet der Dinge** und die wachsende Bedeutung von **Big-Data-Anwendungen** drohen die in Art 5 DSGVO garantierten Grundsätze des Datenschutzes auszuhöhlen.[76] Bereits die Subsumtion solcher Formen der riskanten Datenverarbeitung mit den Mitteln der Interpretation unter die Normen der Grundverordnung stößt an enge Grenzen. Diese Normen – etwa bezüglich des klassischen Personenbezugs – lassen aber weitergehende Risiken für ganze Personengruppen, für die Meinungsfreiheit und damit eine funktionierende Demokratie bisher außer Acht.[77]

---

[74] Kühling/Buchner/Buchner, (2. Aufl.), § 22 Rn. 11; Simitis/Hornung/Spiecker/Scholz, Datenschutzrecht, Art. 22 Rn. 5.

[75] Art 22 Abs. 3 DSGVO.

[76] Nebel in: Roßnagel, Das neue Datenschutzrecht (2018), § 3 Rn. 93.

[77] Simitis/Hornung/Spiecker/Schantz, Datenschutzrecht, Art 6 Abs. 1 Rn. 102.