DeutscherAnwaltVerein

Stellungnahme

des Deutschen Anwaltvereins durch den Ausschuss Informationsrecht

zum Referentenentwurf eines Zweiten Gesetzes zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie EU 2016/680

Stellungnahme Nr.: 34/2018 Berlin, im Juli 2018

Mitglieder des Ausschusses

- Rechtsanwalt Dr. Helmut Redeker, Bonn (Vorsitzender und Berichterstatter)
- Rechtsanwalt Dr. Simon Assion, Frankfurt (Berichterstatter)
- Rechtsanwältin Dr. Christiane Bierekoven, Nürnberg
- Rechtsanwältin Isabell Conrad, München
- Rechtsanwalt Michael Friedmann, Hannover
- Rechtsanwalt Dr. Malte Grützmacher, LL.M., Hamburg
- Rechtsanwalt Prof. Niko Härting, Berlin (Berichterstatter)
- Rechtsanwalt Peter Huppertz, LL.M., Düsseldorf
- Rechtsanwalt Dr. Robert Selk, LL.M. (EU), München
- Rechtsanwalt Prof. Dr. Holger Zuck, Stuttgart

Zuständig in der DAV-Geschäftsführung

- Referentin Ina Kitzmann

Deutscher Anwaltverein
Littenstraße 11, 10179 Berlin
Tel.: +49 30 726152-0
Fax: +49 30 726152-190
E-Mail: dav@anwaltverein.de

Büro Brüssel
Rue Joseph II 40, Boîte 7B
1000 Brüssel, Belgien
Tel.: +32 2 28028-12
Fax: +32 2 28028-13
E-Mail: bruessel@eu.anwaltverein.de
EU-Transparenz-Registernummer:
87980341522-66

www.anwaltverein.de

Verteiler

Deutschland
Bundesministerium der Justiz und für Verbraucherschutz
Bundesministerium für Wirtschaft und Energie
Ausschuss für Recht und Verbraucherschutz im Deutschen Bundestag
Ausschuss für Wirtschaft und Energie im Deutschen Bundestag
Ausschuss Digitale Agenda im Deutschen Bundestag
SPD-Fraktion im Deutschen Bundestag
CDU/CSU-Fraktion des Deutschen Bundestages, Arbeitsgruppe Recht
Fraktionen BÜNDNIS 90/DIE GRÜNEN im Deutschen Bundestag
Fraktion DIE LINKE im Deutschen Bundestag
Fraktion der ALTERNATIVE FÜR DEUTSCHLAND im Deutschen Bundestag
Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit
Die Datenschutzbeauftragten der Bundesländer

Europäische Kommission - Vertretung in Deutschland
Bundesrechtsanwaltskammer
Bundesnotarkammer
Bundesverband der Freien Berufe
Deutscher Richterbund
Deutscher Notarverein e.V.
Deutscher Steuerberaterverband
Bundesverband der Deutschen Industrie (BDI)
GRUR
BITKOM
DGRI

DAV-Vorstand und Geschäftsführung
Vorsitzende der DAV-Gesetzgebungsausschüsse
Vorsitzende der DAV-Landesverbände
Vorsitzende des FORUMs Junge Anwaltschaft

Presse
Frankfurter Allgemeine Zeitung
Süddeutsche Zeitung GmbH
Berliner Verlag GmbH
Redaktion NJW
Juve-Verlag
Redaktion Anwaltsblatt
Juris
Redaktion MultiMedia und Recht (MMR)
Redaktion Zeitschrift für Datenschutz ZD
Redaktion heise online

Der Deutsche Anwaltverein (DAV) ist der freiwillige Zusammenschluss der deutschen Rechtsanwältinnen und Rechtsanwälte. Der DAV mit derzeit rund 64.500 Mitgliedern vertritt die Interessen der deutschen Anwaltschaft auf nationaler, europäischer und internationaler Ebene.

Der DAV begrüßt, dass der Bundesgesetzgeber nunmehr auch das bereichsspezifische Datenschutzrecht an die Anforderungen der DSGVO anpasst. Die nachfolgende Stellungnahme beschränkt sich auf ausgewählte Teilbereiche. Dabei geht es um vier Teile, nämlich

- einerseits um eine Änderung an § 22 Abs. 1 Nr. 2 Bundesdatenschutzgesetz (BDSG) – (hierzu Abschnitt 1),
- Klärungsbedarf im Bereich der Normen zum automatisierten Abrufverfahren in verschiedenen Gesetzen (hierzu Abschnitt 2),

sowie um Bereiche, in denen das zweite Datenschutzanpassungsgesetz *keine* Änderungen vorsieht, obwohl dies notwendig wäre (Abschnitte 3 und 4). Insbesondere empfiehlt der DAV dem Gesetzgeber, auch die zwei folgenden Aspekte zu regeln:

- Schaffung einer allgemeinen Regelung zum Ausgleich zwischen Datenschutz und den Kommunikationsfreiheiten, insbesondere der Meinungsfreiheit (hierzu Abschnitt 3)
- Anpassung des Telemediengesetzes an die DSGVO (hierzu Abschnitt 4).

1. § 22 BDSG

Art. 10 Nr. 1.1.5 des Referentenentwurfs sieht verschiedene, inhaltlich aber miteinander verbundene textliche Änderungen in § 22 Abs. 1 Nr. 1 BDSG vor. Sachlich geht es in allen diesen Änderungen darum, dass auch private Einrichtungen besondere Kategorien personenbezogener Daten verarbeiten dürfen, wenn dies aus Gründen eines erheblichen öffentlichen Interesses zwingend erforderlich ist und zwar nach § 22 Abs. 1 Nr. 2 BDSG nur und soweit die Interessen der Verantwortlichen an der Datenverarbeitung die Interessen der betroffenen Personen überwiegen. Diese Befugnis stand bislang nur öffentlichen Stellen zu.

Die Begründung zu dieser Änderung führt aus, dass dies auch zivilgesellschaftlichen Trägern im Rahmen von Präventions- und Deradikalisierungsprogrammen gerade im

Bereich religiös motivierten, islamistischen Terrorismus ermögliche, solche Daten zu verarbeiten. Dies erleichtere auch die Zusammenarbeit von öffentlichen Stellen auf Bundes- und Landesebene mit diesen Stellen. Insbesondere werde es über den Verweis in § 24 Abs. 2 BDSG auch möglich, solche Daten zu einem anderen Zweck zu verwenden als dem, zu dem sie erhoben würden. Deswegen erlaube die Änderung den nicht öffentlichen Stellen, die aus einer Beratung gewonnenen Daten mit Sicherheitsrelevanz an die dafür zuständigen öffentlichen Stellen zu übermitteln.[1]

Die Öffnungsklausel dürfte die Verarbeitung auch im Rahmen der Bekämpfung sonstigen politischen Terrorismus erleichtern, weil ja auch Daten über politische Meinungen von Art. 9 DSGVO besonders geschützt werden.

Soweit es dadurch im Rahmen der Präventions- und Deradikalisierungsprogramme für deren Träger leichter wird, gewonnene Erkenntnisse zur Durchführung der Programme zu verwenden, weil sie zum Beispiel auch außerhalb einer konkreten Beratungs- und Betreuungssituation für die Entwicklung von neuen Maßnahmenpaketen eingesetzt werden können, ist die Ergänzung des BDSG auch sinnvoll.

Nach der Begründung geht es aber in erster Linie nicht darum. Vielmehr geht es darum, die Zusammenarbeit zwischen den Sicherheitsbehörden und den Trägern der Präventions- und Deradikalisierungsprogrammen zu intensivieren. Es soll den privaten Trägern dieser Programme möglich werden, ihre Erkenntnisse immer dann an die Sicherheitsbehörden zu übermitteln, wenn dies aus Gründen eines erheblichen öffentlichen Interesses zwingend geboten ist. Der Begriff des erheblichen öffentlichen Interesses ist vage und umfasst sicher mehr als nur den Schutz von Leben und Gesundheit oder vergleichbar gewichtiger Rechtsgüter[2]. Es kann zum Beispiel auch um erhebliche finanzielle Interessen gehen. Der Begriff stammt aus Art. 9 Abs. 2 Buchst. g DSGVO. Dabei handelt es sich aber um eine Öffnungsklausel für anderweitige gesetzliche, meist mitgliedsstaatliche Regelungen, die diesen vagen Begriff konkretisieren sollen. Ihn einfach in eine gesetzliche Regelung zu übernehmen, ohne die Zielrichtung klarer zu bestimmten, ist zweifelhaft.

Die schon wegen der vagen Formulierung bestehenden erheblichen Zweifel an der Regelung verstärken sich, wenn man die – in der Begründung darüber hinaus auf den islamistischen Terror beschränkte – Zielrichtung der Neuregelung betrachtet. Die

[1] S. 210 des Referentenentwurfs.
[2] Paal/Pauly/*Frenzel,* Art. 9 DSGVO Rn. 39.

Präventions- und Deradikalisierungsprogramme müssen bei ihren Zielpersonen Vertrauen erwecken, um überhaupt eine (möglicherweise sogar nur geringe) Chance zu haben, ihre Ziele zu erreichen. Zu diesem Vertrauen gehört es für die Adressaten der Programme auch, sicher zu sein, dass die Informationen, die die Mitarbeiter dieser Programme erhalten, auch dort verbleiben, soweit der Betreute nicht mit ihrer Weitergabe einverstanden ist. Die undifferenzierte Neuregelung ist geeignet, dieses Vertrauen zu zerstören – dürfen die Mitarbeiter der Programme nach dieser Regelung doch solche Daten weitergeben, ohne dass die Weitergabe etwa auf den Schutz des Lebens und der Gesundheit der Bevölkerung beschränkt ist. Die Norm greift ja auf den relativ unbestimmten Begriff eines erheblichen öffentlichen Interesses zurück.

Die weitere Einschränkung, nach der die Interessen des Verantwortlichen an der Datenverarbeitung die Interessen der betroffenen Person überwiegen müssen, – ist schon hinsichtlich des Adressatenkreises – unklar. Nimmt man den Wortlaut dieser Vorschrift ernst und wendet sie auf die privaten Träger der Präventions- und Deradikalisierungsprogramme an, muss es um Interessen dieser privaten Träger gehen. Diese dürften – außer im Fall der Weiterverwendung der Erkenntnisse für ihre eigene Arbeit – keine Interessen haben, die das Interesse des Betroffenen überwiegen. Die Norm stellt ja auf erhebliche öffentliche Interessen ab. Diese sind aber nicht die Interessen des Verantwortlichen. Sieht man dies so, werden die in der Begründung dargestellten Anwendungsfälle der Zusammenarbeit von Öffentlichen und Privaten von der Norm gar nicht erfasst.

Es ist aber nicht ausgeschlossen, dass die Norm nur für die öffentlichen Stellen gilt, die die Daten erhalten. Dafür spricht, dass diese Einschränkung in § 22 Abs. 1 Nr. 2 BDSG steht, einer Norm, die nur für öffentliche Stellen gilt. Sieht man das so, beschränkt sie die Verarbeitungsmöglichkeiten der Privaten gar nicht, weil die Privaten gar nicht Regelungsadressat der Norm sind. Geht man davon aus, verstößt die Norm gegen die Vorgaben von Art. 9 Abs. 2 Buchst. g DSGVO, weil sie im Hinblick auf die privaten Stellen keine irgendwie gearteten Maßnahmen zur Wahrung der Grundrechte und Interessen des Betroffenen trifft. Solche Maßnahmen verlangt Art. 9 Abs. 2 Buchst. g DSGVO aber. Der Gesetzgeber muss die Abwägung mit den Interessen der

Betroffenen auch im Bereich privater Stellen eindeutig regeln. Die in § 22 Abs. 2 BDSG geregelten unveränderten abstrakten Maßnahmen reichen nicht.[3]

Angesichts der recht weiten Formulierung dürfte die Einschränkung darüber hinaus auch die Datenverarbeitung der öffentlichen Stellen kaum beschränken, soweit diese überhaupt den Regelungen der DSGVO unterliegen.

Zu befürchten ist auch, dass die Mitarbeiter der Präventions- und Deradikalisierungsprogramme über andere Regelungen aufgrund der Neuregelung in den Polizeigesetzen gezwungen werden, ihre Informationen weiterzugeben. Ein Schweigerecht im Sinne von § 53 StPO steht ihnen ja nicht zu, wenn nicht die Berater als akademisch ausgebildete Psychologen beziehungsweise staatlich anerkannte Sozialarbeiter oder Sozialpädagogen ein eigenes Schweigerecht haben (vergleiche § 203 Abs. 1 Nr. 2, 6 StGB).

Es bedarf hier zumindest einer starken Beschränkung dieser Voraussetzungen für eine Datenweitergabe, zum Beispiel auf konkret drohende Gefahren für Leben und Gesundheit. Andernfalls würde diese Regelung die Ziele der Präventions- und Deradikalisierungsprogramme gefährden, statt sie zu unterstützen. Die Änderung des BDSG in dieser Entwurfsfassung geht hier zu weit.

2. Veralteter Begriff: Automatisiertes Abrufverfahren

Der Entwurf sieht an einigen Stellen Regelungen zu „automatisierten Abrufverfahren“ vor. Der DAV gibt zu bedenken, dass derartige Regelungen, die an § 10 BDSG a.F. anknüpfen, durch die Regelungssystematik der DSGVO sowie durch die technische Entwicklung überholt sein dürften.

Regelungen zu „automatisierten Abrufverfahren“ finden sich in

- Art. 14 (Bundesmeldegesetz), § 11 Abs. 1 Satz 2;
- Art. 20 (Grundstoffüberwachungsgesetz), § 10 Abs. 2;
- Art. 22 (Transplantationsgesetz), § 2 Abs. 4a;
- Art. 26 (Lebensmittel- und Futtermittelgesetzbuch), § 49 Abs. 4;

[3] Vgl. schon S. 10 der Stellungnahme des DAV zum Entwurf des Referentenentwurfs des Bundesministeriums des Innern vom 23.11.2016 für ein Gesetz zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 (im Folgenden „DSGVO“) und zur Umsetzung der Richtlinie (EU) 2016/680 (Datenschutz-Anpassungs- und Umsetzungsgesetz EU – DSAnpUG-EU, Stellungnahme 87/2016.

- Art. 47 (Aufenthaltsgesetz), § 89a Abs. 5 bis 5c;
- Art. 80 (IHK-Gesetz), § 9 Abs. 3a;
- Art. 99 (Fleischgesetz), § 12 Abs. 4;
- Art. 101 (Gesetz über Meldungen über Marktordnungswaren), § 15 Abs. 7 und 8.

Ausweislich der Entwurfsbegründung finden sich Regelungen, die sich auf „automatisierte Abrufverfahren beziehen“ auch in Art. 6 (BDBOS-Gesetz), § 23.

In der DSGVO findet sich zu § 10 BDSG a.F. keine Parallelnorm. Auch im BDSG n.F. (auf der Grundlage des Datenschutz-Anpassungs- und -Umsetzungsgesetzes) fehlt eine entsprechende Vorschrift.

§ 10 BDSG a.F. stammt aus dem Jahre 1990.[4] Zur damaligen Zeit verfügten nur wenige Behörden über Dateisysteme, die den gezielten Abruf einer Vielzahl personenbezogener Daten ermöglichten. Aus damaliger Sicht hatten derartige Systeme ein hohes datenschutzrechtliches Gefahrenpotenzial. Dies ist einer der Gründe, weshalb es aus damaliger Sicht sinnvoll war, Spezialregelungen zu schaffen, die die spezifischen Gefahren „automatischer Abrufsysteme“ regelten.

Aus heutiger Sicht sind „automatisierte Abrufsysteme“ der Normalfall der Datenverarbeitung.[5] Alle Datenbanken, die Behörden nutzen, sind „automatisiert abrufbar“. Die Google-Suche ist ebenso ein „automatisiertes Abrufsystem“ wie jedes gängige System der elektronischen Aktenverwaltung oder auch die E-Mail-Verwaltung mit Programmen wie Microsoft Outlook. Für all diese Dateisysteme finden sich in der DSGVO risikobasierte Regelungen (beispielsweise in Art. 5, 24, 25 und 32 DSGVO). Dass es bei „automatisierten Abrufsystemen“ ein weitergehendes Gefahrenpotenzial gibt, das durch die DSGVO nicht ausreichend erfasst ist, ist nicht ersichtlich.

§ 10 BDSG a.F. verfolgte im Übrigen den Zweck, die Nutzung „automatisierter Abrufsysteme“ zu ermöglichen (nicht: zu erschweren).[6] Die Vorschrift war notwendig, da die bloße Bereithaltung personenbezogener Daten „zum Abruf“ nach dem BDSG

[4] *Ehmann* in Simitis, BDSG, 8. Aufl. 2014, § 10, Rn. 2; *Schultz-Melling* in Taeger/Gabel, BDSG, 2. Auf. 2013, § 10, Rn. 2.
[5] Vgl. *Ehmann* in Simitis, BDSG, 8. Aufl. 2014, § 10, Rn. 7: „inflationärerer Einsatz“.
[6] *Ehmann* in Simitis, BDSG, 8. Aufl. 2014, § 10, Rn. 2 ff.; *Schultz-Melling* in Taeger/Gabel, BDSG, 2. Auf. 2013, § 10, Rn. 2.

1977 bereits als Übermittlung galt,[7] ohne dass es auf tatsächliche Abrufe ankam. Daher bedurfte es für eine solche Bereithaltung einer Rechtsgrundlage, die durch § 10 BDSG a.F. geschaffen werden sollte.

Nach Art. 4 Nr. 2 DSGVO ist die Übermittlung ein Unterfall der „Offenlegung". Die „Offenlegung" ist wiederum ein Beispielsfall für eine „Verarbeitung" von Daten, die mit dem umfassenden Begriff des „Vorgangs" beziehungsweise der „Vorgangsreihe im Zusammenhang mit personenbezogenen Daten" definiert wird.

Maßstab für die materielle Rechtmäßigkeit jedweder Datenverarbeitung sind die Art. 6 und 9 DSGVO. Dass die Art. 6 und 9 DSGVO Abrufverfahren nicht hinlänglich legitimieren können, wie dies nach dem BDSG 1977/1990 der Fall war, ist nicht ersichtlich.

Der Gesetzgeber ist aufgefordert, die bestehenden Regelungen in den verschiedenen Gesetzen nicht nur weitgehend textlich zu korrigieren (wie zum Beispiel im BMG) oder gar neue Regelungen zu automatisierten Abrufverfahren hinzuzufügen (wie in Art. 22 DSGVO (Transplantationsgesetz nur: § 2 Abs. 4a)), sondern der heutigen Situation angemessene Regelungen für die praktisch überall bestehenden automatisierten Abrufverfahren vorzunehmen.

3. Regelung zum Schutz der Meinungsfreiheit

Der DAV empfiehlt, das BDSG um eine Regelung zu ergänzen, die die allgemeine Öffnungsklausel für ein „Medienprivileg" in Art. 85 DSGVO vollständig nutzt und dabei gleichzeitig einen Rahmen für speziellere landesgesetzliche Regelungen schafft, ohne diese zu verdrängen. Eine solche Regelung sollte einen angemessenen Interessenausgleich zwischen Datenschutz-, Äußerungs- und Öffentlichkeitsinteressen schaffen.

a) Rechtlicher Hintergrund

Art. 85 Abs. 1 DSGVO enthält einen aktiv an die Mitgliedsstaaten gerichteten Ausgestaltungsauftrag:

[7] § 2 Abs. 2 BDSG 1977: „Im Sinne dieses Gesetzes ist … Übermitteln (Übermittlung) das Bekanntgeben gespeicherter oder durch Datenverarbeitung unmittelbar gewonnener Daten an Dritte in der Weise, dass die Daten durch die speichernde Stelle weitergegeben **oder zur Einsichtnahme, namentlich zum Abruf bereitgehalten** werden…"

„Die Mitgliedstaaten bringen durch Rechtsvorschriften das Recht auf den Schutz personenbezogener Daten gemäß dieser Verordnung mit dem Recht auf freie Meinungsäußerung und Informationsfreiheit, einschließlich der Verarbeitung zu journalistischen Zwecken und zu wissenschaftlichen, künstlerischen oder literarischen Zwecken, in Einklang."

Art. 85 Abs. 2 DSGVO ergänzt diese Vorschrift um einen spezielleren Regelungsauftrag speziell zur Datenverarbeitung zu journalistischen, wissenschaftlichen, künstlerischen oder literarischen Zwecken. Die Datenverarbeitung allgemein zum Zweck des Rechts auf freie Meinungsäußerung und Informationsfreiheit wird demgegenüber nur in Absatz 1 erwähnt.

Die fachliche Debatte zu Art. 85 DSGVO hat bisher zu keinem eindeutigen Ergebnis geführt. So wird unter anderem die Ansicht vertreten, dass Art. 85 Abs. 1 DSGVO bereits durch Art. 5 GG ausgefüllt werde, so dass keine speziellen Anpassungsgesetze notwendig seien. Nach dieser Ansicht sollen sich also selbst Vorschriften des Grundgesetzes in die Öffnungsklausel des Art. 85 Abs. 1 DSGVO einfügen und offenbar die DSGVO so modifizieren, dass diese nicht zu Ergebnissen führt, die mit der Meinungsfreiheit und anderen Kommunikationsfreiheiten unvereinbar sind.[8] Auch wird vertreten, dass andere Gesetze zum Schutz der Meinungsfreiheit wie zum Beispiel die §§ 22 und 23 KUG sich unmittelbar unter die Öffnungsklausel des Art. 85 Abs. 1 DSGVO fassen lassen.

Trotz dieser Meinung, die auch von dem für das 2. DSAnpUG federführenden BMI vertreten wird, [9] haben sowohl der Bundes- als auch die Landesgesetzgeber spezielle Vorschriften zum Schutz der Meinungsfreiheit erlassen.[10] Diese beschränken sich allerdings, soweit ersichtlich, bisher weitestgehend auf den Bereich des professionellen Journalismus.[11] In den entsprechenden Gesetzen werden konkrete bestimmte

[8] So u.a. der ehemalige Berichterstatter zur DSGVO im Europaparlament, *Jan-Philipp Albrecht,* in einer Diskussion auf Twitter: https://twitter.com/JanAlbrecht/status/856120709311057920.
[9] Vgl. die „FAQ zur DSGVO", abrufbar unter https://www.bmi.bund.de/SharedDocs/kurzmeldungen/DE/2018/04/faqs-datenschutz-grundverordnung.html.
[10] Überblick zum Landesrecht unter https://emr-sb.de/wp-content/uploads/2018/07/Synopse-zu-den-geplanten-%c3%84nderungen-landesrechtlicher-Regelungen-zur-Umsetzung-des-21.-Rundfunk%c3%a4nderungsstaatsvertrages-und-der-Datenschutz-Grundverordnung-der-EU_Stand-Juli-2018.pdf.
[11] Für den Bereich des Bundes bisher soweit ersichtlich nur die Novelle des DW-Gesetzes (im selben Gesetzesentwurf, Artikel 39); für die Länder s.o. Fn. 10.

Vorschriften der DSGVO modifiziert, um negative Effekte für die journalistische Berichterstattung auszuschließen.

Vergleichbare Regelungen zum Schutz der allgemeinen Meinungs- und Informationsfreiheit sowie zum Schutz von künstlerischen oder literarischen Zwecken liegen bisher nicht vor.

b) Ist eine spezielle gesetzliche Regelung notwendig?

Das BMI hat sich bislang auf den Standpunkt gestellt, besondere gesetzliche Regelungen zum Schutz von Diskursteilnehmern jenseits des professionellen Journalismus seien nicht notwendig, weil das bestehende Recht, wie zum Beispiel Art. 5 GG oder das KUG, diese Kreise bereits ausreichend schütze.

Es ist dann allerdings fraglich, wieso das 2. DSAnpUG für eine spezielle Gruppe von Datenverarbeitern dann doch wieder spezielle Schutzvorschriften enthält, nämlich für die Deutsche Welle und die dort arbeitenden Journalisten. Es ist widersprüchlich, dass der Gesetzentwurf zwar für journalistische Zwecke spezielle Vorschriften zur Modifikation der DSGVO vorsieht, jedoch für literarische oder künstlerische Zwecke der Schutz von Art. 5 GG ausreichen soll.

Nach dem aktuellen Stand werden die speziellen Regelungen des „Medienprivilegs“ in Bund und Ländern sich weitgehend auf professionelle Medien beziehungsweise Journalisten beschränken,[12] aber keine Wirkung für beispielsweise die folgenden Personengruppen entfalten:

- Blogger, Podcaster, Youtuber, Twitter-Nutzer
- Fotografen außerhalb des Bereichs der Pressefotografie (zum Beispiel Street Photography, Stockfotos, Hobbyfotografen)
- Künstler
- Pressesprecher beziehungsweise allgemein Institutionen, die Öffentlichkeitsarbeit und Marketing betreiben (Vereine, Behörden, Unternehmen, NGOs, Parteien)

[12] Konkret: Gemäß § 57 RStV die „in der ARD zusammengeschlossenen Landesrundfunkanstalten, das ZDF, das Deutschlandradio, private Rundfunkveranstalter oder Unternehmen und Hilfsunternehmen der Presse als Anbieter von Telemedien“; nach § 12 LPG RLP „Unternehmen der Presse oder zu diesen gehörende Hilfs- und Beteiligungsunternehmen“. Flexibler beispielsweise § 9 Bln DSG: „Soweit personenbezogene Daten in Ausübung des Rechts auf freie Meinungsäußerung und Informationsfreiheit zu journalistischen, künstlerischen oder literarischen Zwecken, einschließlich der rechtmäßigen Verarbeitung auf Grund der §§ 22 und 23 KUG […].“

- Politiker.

Auch diese Gruppen äußern sich regelmäßig in der Öffentlichkeit und sind ein wichtiger Teil des demokratischen Diskurses. Den Schutz des „Medienprivilegs“ nur auf den professionellen Journalismus beschränken zu wollen, wird der Rolle dieser Gruppen nicht gerecht.[13]

Hinzu kommt, dass die unter anderem vom BMI vertretene These, laut der das bereits bestehende Recht ausreichend die öffentlichen Äußerungen der oben genannten Gruppen absichere, bislang äußerst umstritten ist[14]. Sie wird auch nicht von allen Datenschutzbehörden geteilt. Die gemeinsame Konferenz der Datenschutzbeauftragten von Bund und Ländern hat bereits geäußert, gesetzliche Abweichungen von der DSGVO müssten *konkret* und *spezifisch* sein.[15] Auch der HamBfDI hat in einem längeren Vermerk die Auffassung vertreten, das KUG und das Verfassungsrecht hätten keinen Vorrang gegenüber der DSGVO[16]. Der HamBdDl hat stattdessen den Erlass einer speziellen Schutzvorschrift vorgeschlagen.

Ob die Gerichte sich der Auffassung des BMI anschließen werden oder nicht, ist offen.[17] Jedenfalls spricht angesichts der aktuell sehr kontroversen Debatte viel dafür, dass eine abschließende gerichtliche Klärung der streitigen Rechtsfragen frühestens in mehreren Jahren erfolgen würde. In der Zeit bis dahin läge die Last der rechtlichen Unsicherheit auf den oben genannten Personengruppen. Diese Sachlage führt bereits jetzt zu Einschüchterungseffekten; anschaulich wird dies beispielsweise durch die Twitter-Debatte unter dem Hashtag „#Blogsterben“ oder durch die breit geführte Debatte unter Fotografen[18], PR- und Marketingfachkräften.[19]

---

[13] So auch EG 153 DSGVO, letzter Satz: „Um der Bedeutung des Rechts auf freie Meinungsäußerung in einer demokratischen Gesellschaft Rechnung zu tragen, müssen Begriffe wie Journalismus, die sich auf diese Freiheit beziehen, weit ausgelegt werden.“

[14] Zum Streitstand *Lauber-Rönsberg/Hartlaub*, NJW 2017, 1057, 1060 ff.; vgl. zum teils konfusen, widersprüchlichen Meinungsstand auch *Seiler*, in: Fotorecht Seiler vom 12. Mai 2018, https://www.fotorecht-seiler.eu/dsgvo-fotografie-kug-update/.

[15] Datenschutzkonferenz, Entschließung vom 09.11.2017, https://www.datenschutz-bayern.de/dsbk-ent/DSK_94-Art_85_DSGVO.html.

[16] Vermerk des HamBfDI, S. 3 f., abrufbar unter: https://www.filmverband-suedwest.de/wp-content/uploads/2018/05/Vermerk_DSGVO.pdf.

[17] Das OLG Köln hat in einer Entscheidung des einstweiligen Rechtsschutzes das KUG als vorrangig gegenüber der DSGVO behandelt, allerdings in einem Fall, in dem es offenbar um professionellen Fotojournalismus ging; siehe OLG Köln, Beschluss v. 18.06.2018, 15 W 27/18.

[18] Statt vieler eine Stellungnahme des Bundesverbandes Professioneller Bildverarbeiter (BVPA), abrufbar unter https://bvpa.org/kommentar-stellungnahme-des-bmi-zu-dsgvo-und-fotografie/.

Hinzuweisen ist außerdem darauf, dass die DSGVO ohne ergänzende nationale Gesetze zum Schutz der Meinungs- und Kommunikationsfreiheiten nicht zu angemessenen Ergebnissen führt. Denn die DSGVO stellt zwar für die Verarbeitung „normaler“ personenbezogener Daten mit Art. 6 Abs. 1 Buchst. e und f Rechtsgrundlagen zur Verfügung, die ausreichend flexibel sind, um auch Interessen der Meinungs- und Informationsfreiheit (Art. 11 der EU-Grundrechtecharta) abzudecken. Diese Rechtsgrundlagen sind aber nicht ausreichend für die Verarbeitung personenbezogener Daten, die in die Gruppe der besonders geschützten Datenkategorien (sogenannte „sensible Daten“ – Art. 9 DSGVO) oder unter die „Strafdaten“ (Art. 10 DSGVO) fallen.

Nach der DSGVO reicht es für derartige Datenverarbeitungen nicht aus, dass sie der Erfüllung einer öffentlichen Aufgabe dienen (Art. 6 Abs. 1 Buchst. e DSGVO) oder wenn an der Verarbeitung ein legitimes überwiegendes Interesse besteht (Art. 6 Abs. 1 Buchst. f DSGVO). Vielmehr ist eine spezielle Rechtsgrundlage für die „sensiblen Daten“ notwendig (Art. 9 Abs. 2 DSGVO). Auch für die Verarbeitung von „Strafdaten“ bedarf es einer speziellen gesetzlichen Ermächtigung. Damit geraten beispielsweise die folgenden Szenarien in eine rechtliche Grauzone:

- Ein nicht als Journalist tätiger Fotograf fotografiert eine Personengruppe. Auf den Fotos werden einzelne Personen mit ihren politischen Überzeugungen erkennbar, beispielsweise durch das Tragen von eindeutigen T-Shirt-Motiven (Daten zur politischen Meinung, Art. 9 Abs. 1 DSGVO).
- Ein Politiker fotografiert eine Besuchergruppe und verbreitet das Foto im Internet. Eine Person der Besuchergruppe sitzt in einem Rollstuhl (Gesundheitsdatum, Art. 9 Abs. 1 DSGVO).
- Ein Blogger zitiert in seinem Blog aus Medienberichten über die strafrechtliche Verurteilung einer prominenten Person (Datum über eine strafrechtliche Verurteilung, Art. 10 DSGVO). Im Unterschied zu der zitierten Medienberichten kann der Blogger sich nicht auf das Medienprivileg im RStV beziehungsweise den Landespressegesetzen berufen, da diese auf nicht-journalistische Telemedien keine Anwendung findet.

[19] Siehe insbesondere die Ergebnisse einer Fachkonferenz des Bundesverbandes deutscher Pressesprecher (BdP), hier abrufbar: https://www.bdp-net.de/datenschutzgrundverordnung.

Die drei vorgenannten Beispiele sind Datenverarbeitungen, bei denen offensichtlich ein überwiegendes Interesse daran besteht, dass diese weiter stattfinden. Aus datenschutzrechtlicher Sicht sind diese Szenarien bislang aber nicht abgesichert; für die jeweiligen Fotografen, Politiker, Blogger et cetera bedeuten sie ein erhebliches Risiko. Denn eine schnelle und einfache rechtliche Lösung für derartige Fälle existiert nicht.[20] Die beste Verteidigungsstrategie dieser Personen bestände darin, sich auf die streitige Ansicht zu berufen, dass Art. 5 GG (in der Form mittelbarer Drittwirkung im Privatrechtsverhältnis) über Art. 85 Abs. 1 DSGVO Anwendung findet und deshalb auch Datenverarbeitungen erlaubt, für die die DSGVO selbst keine Rechtsgrundlage bietet. Ob diese Ansicht sich wirklich durchsetzt, ist allerdings fraglich.

Zu der Frage nach der Rechtsgrundlage kommen weitere Regelungsbereiche der DSGVO hinzu, in denen sich Rechtspflichten der DSGVO einschränkend auf die Meinungsfreiheit auswirken können. Hierzu zählen insbesondere die Transparenzpflichten nach Art. 13 und 14 DSGVO und die Betroffenenrechte nach Art. 15 bis 22 DSGVO. In Bezug auf professionelle Medien und Journalisten haben Bund- und Landesgesetzgeber diese Vorschriften deshalb aufgehoben oder modifiziert jedoch nicht in Bezug auf die oben genannten Gruppen.

Es ist festzuhalten, dass sich im Zusammenhang mit dem Inkrafttreten der DSGVO erhebliche Einschüchterungseffekte eingestellt haben. Diese sind – wie typisch für Einschüchterungseffekte[21] – nicht monokausal auf einzelne bestimmte Regelungen der DSGVO zurückzuführen. Vielmehr wirkt die DSGVO gemeinsam mit anderen Einflüssen (und teils verzerrt durch diese) auf die in der Regel juristisch nicht vorgebildeten Personen eher wie eine amorphe „Drohkulisse“. In der Praxis mischen sich zutreffende Rechtseinschätzungen mit rechtlichen Fehlschlüssen. Die Einschüchterungseffekte werden dabei noch dadurch verstärkt, dass anerkannte Experten – Datenschutzbehörden, das BMI und spezialisierte Juristen – zu voneinander abweichenden Einschätzungen kommen.

Aus Sicht der Personen, die am öffentlichen Diskurs teilnehmen, führt dies zu dem Gesamteindruck, dass durch die DSGVO einige Bereiche der „öffentlichkeitsrelevanten“ Datenverarbeitung in rechtliche Grauzonen geraten sind, die erst durch

[20] Denkbar wäre in einigen Fallkonstellationen, sich darauf zu berufen, dass die Betroffenen das Datum selbst offensichtlich öffentlich gemacht hätten (Art. 9 Abs. 2 Buchst. e DSGVO). Allerdings gibt es Fälle, in denen dies gerade nicht der Fall ist.
[21] Vgl. *Assion*, Telemedicus v. 15.05.2014, http://tlmd.in/a/2767.

Gerichtsentscheidungen wieder geklärt werden können.[22] Die Aussicht auf Gerichtsverfahren ist aber gerade für nicht-professionell arbeitende Personen wie Blogger schon grundsätzlich abschreckend, zumal wenn Bußgeldandrohungen und Schadensersatzforderungen in Frage stehen. Datenverarbeiter sind gerade in Bezug auf Öffentlichkeitsarbeit und auf nicht-kommerzielle Tätigkeiten in der Regel nicht bereit, risikoreiche rechtliche Rechtsauffassungen zu vertreten. Eher wird die publizistische Tätigkeit als Ganzes eingestellt.

Unabhängig von der eigenen Rechtsauffassung des BMI sollte der Gesetzgeber bereits diese *Einschüchterungseffekte* zum Anlass nehmen, durch eine gesetzliche Regelung zur Klärung und Beruhigung beizutragen. Die derzeit bestehenden Einschüchterungseffekte auf „Panikmache“ durch Dritte zurückzuführen[23], wird der Sache nicht gerecht. Zum einen gibt die derzeitige Rechtslage zwar keinen Grund zur Panik, durchaus aber tatsächlichen Anlass zur Besorgnis. Zum anderen ist ja gerade die Möglichkeit zur „Panikmache“ eine Folge (auch) der unklaren Rechtslage. Die „Panikmache“ könnte durch eindeutige gesetzliche Regelungen beendet werden. In einer solchen Situation keine Klärung herbeizuführen, wäre aus Sicht des DAV nicht angemessen, zumal andere EU-Mitgliedsstaaten genau diesen Weg beschritten haben (dazu noch unten). Die öffentliche Meinungsbildung bedarf eines besonderen Schutzes gegen Einschüchterungen.

c) Empfehlung

Der DAV empfiehlt , in das BDSG eine Regelung aufzunehmen, die die folgenden Kriterien erfüllt:

- Die Regelung sollte – in Form einer „Generalklausel“ – klarstellen, dass der deutsche Gesetzgeber die Öffnungsklausel des Art. 85 Abs. 1 DSGVO in ihrem vollen Umfang nutzt. Das heißt nicht nur wie bislang für professionelle Medien und Journalisten, sondern auch für die weiteren in Art. 85 Abs. 1 DSGVO

[22] Einen Präzedenzfall, bei dem eine Person ehrenamtlich eine Webseite betrieben hatte und für die Veröffentlichung personenbezogener Daten strafrechtlich (!) belangt wurde, hat der EuGH freilich bereits (noch zum alten Recht) entschieden; vgl. EuGH, Urt. v. 6. November 2003, Rs. C-101/01 (ECLI:EU:C:2003:596) – *Lindqvist*. In der Entscheidung (vor allem Rn. 85 ff.) weist der EuGH die Pflicht, ein angemessenes Gleichgewicht zur Meinungsfreiheit herzustellen, dem Recht der Mitgliedsstaaten zu.
[23] So mit fast gleichlautenden Zitaten die Bundesdatenschutzbeauftragte und das BMI, beide zitiert in Beck-aktuell vom 22.05.2018, https://rsw.beck.de/aktuell/meldung/eu-datenschutzgrundverordnung-ende-der-fotografie-oder-blosse-panikmache.

genannten Zwecke: Meinungsäußerung und Informationsfreiheit sowie wissenschaftliche, künstlerische und literarische Zwecke.[24]

- Die Regelung sollte nicht auf einen einseitigen Vorrang der vorgenannten Interessen abzielen, sondern auf einen gerechten Ausgleich von Öffentlichkeits- und Privatheitsinteressen. Dabei bietet es sich an, auf die bereits bestehenden gesetzlichen Regelungen zu verweisen, auf denen das bisherige Äußerungsrecht aufbaut. Dieser Verweis sollte allgemein erfolgen, wobei der Gesetzgeber in den Gesetzesmaterialien auch konkretisieren kann, welche Vorschriften beziehungsweise Rechtserwägungen er genau meint.[25]
- Insgesamt sollte das Ziel einer solchen Regelung sein, die bisherigen Wertungen des Äußerungsrechts, die auf jahrzehntelang gewachsener Rechtsprechung der Gerichte, einschließlich des BVerfG und des EGMR, aufbaut, zu erhalten. Diese Rechtsprechung räumt dem öffentlichen Diskurs aufgrund von dessen essenzieller Bedeutung für das Funktionieren der Demokratie hohe Bedeutung bei. Es sollte vermieden werden, dass das Datenschutzrecht diese Wertung „überlagert", bloß weil die DSGVO aufgrund ihrer Vorrangwirkung gegenüber dem nationalen Recht Rechtsgrundlagen des Äußerungsrechts verdrängt.
- In Bezug auf Betroffenenrechte und andere Regelungen der DSGVO, die sich indirekt ebenfalls einschränkend auswirken könnten, sollten konkrete Regelungen zu deren Modifikation oder Aufhebung erfolgen. Dabei können die Regelungen im RStV oder im Vorschlag für eine Änderung des Deutsche Welle-Gesetzes als Vorbild dienen.

Vergleichbare Regelungen sind auch in anderen EU-Mitgliedsstaaten bereits erlassen worden. Die Herangehensweisen der Mitgliedsstaaten an Art. 85 DSGVO gehen weit auseinander. Allerdings ist festzustellen, dass kaum ein anderer Staat sich mit Regelungen zum Schutz der Meinungsfreiheit soweit zurückgehalten hat wie Deutschland.[26] Ein Recht großer Teil der Mitgliedsstaaten schützt – anders als Deutschland – zumindest gleichberechtigt zu den journalistischen Zwecken auch die Zwecke der Kunst, der Wissenschaft und der Literatur. Einige Staaten – darunter

[24] Mit einer Empfehlung, zumindest künstlerische Zwecke abzusichern, auch der HamBfDI (oben Fn. 7).
[25] Insbesondere wäre dies § 193 StGB („Wahrnehmung berechtigter Interessen") sowie die Rechtsprechung des BGH zu Unterlassungs- und Schadensersatzansprüchen wegen Verletzungen des allgemeinen Persönlichkeitsrechts (zu § 823 BGB und/oder § 1004 BGB i.V.m. Art. 2 Abs. 1, Art. 1 Abs. 1 GG), sowie die hierzu ergangenen Entscheidungen des BVerfG und des EGMR.
[26] Für einen Überblick vgl. https://www.twobirds.com/en/in-focus/general-data-protection-regulation/gdpr-tracker/personal-data-and-freedom-of-expression.

Irland,[27] Schweden[28] und Österreich[29] – schützen in ihren nationalen Gesetzen ausdrücklich auch die Freiheit der Meinungsäußerung und die Informationsfreiheit.

Orientiert an den bereits vorliegenden Gesetzen anderer EU-Mitgliedsstaaten ließe sich eine gesetzliche Klarstellung in Deutschland beispielsweise wie folgt formulieren:

(1) Die Verarbeitung zum Zweck der Ausübung des Rechts auf freie Meinungsäußerung und Informationsfreiheit ist grundsätzlich zulässig, es sei denn dem steht ein überwiegendes legitimes Interesse der Betroffenen entgegen. Dies gilt insbesondere für die Verarbeitung zu journalistischen, wissenschaftlichen, künstlerischen oder literarischen Zwecken.

(2) Spezielle Regelungen des Bundes- und Landesrechts zur Zulässigkeit der Verarbeitung zu den in Absatz 1 genannten Zwecken, einschließlich der Veröffentlichung, bleiben von der DSGVO unberührt. Ihre Wertungen gelten auch im Rahmen der Interessenabwägung nach Absatz 1.

(3) Ein Verantwortlicher ist zu einer Information der Betroffenen nach Art. 13 und 14 DSGVO nicht verpflichtet, soweit überwiegende Interessen der Freiheit der Meinungsäußerung und Informationsfreiheit entgegenstehen. Das gilt insbesondere für die Verarbeitung zu journalistischen, wissenschaftlichen, künstlerischen oder literarischen Zwecken, Der Verantwortliche ergreift geeignete Maßnahmen zum Schutz der Rechte und Freiheiten sowie der berechtigten Interessen der betroffenen Person, wozu auch die Bereitstellung dieser Informationen für die Öffentlichkeit gehören kann.[30]

(4) Betroffenenrechte nach den Artikeln 15- bis 22 DSGVO sind ausgeschlossen, soweit überwiegendes Interesse der Freiheit der Meinungsäußerung und Informationsfreiheit entgegenstehen. Dies gilt insbesondere für die Verarbeitung zu journalistischen, wissenschaftlichen, künstlerischen oder literarischen Zwecken.

Eine solche Klarstellung könnte im BDSG erfolgen. Insbesondere bestehen keine Bedenken gegen eine Gesetzgebungskompetenz des Bundes. Denn eine solche

[27] Ziffer 43 des irischen Data Protection Act 2018, hier abrufbar: https://data.oireachtas.ie/ie/oireachtas/act/2018/7/eng/enacted/a0718.pdf.
[28] § 7 des schwedischen Datenschutzgesetzes, hier abrufbar: http://rkrattsbaser.gov.se/sfst?bet=2018:218.
[29] § 9 des österreichischen DSG, hier abrufbar: https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=bundesnormen&Gesetzesnummer=10001597.
[30] Orientiert an Art. 14 Abs. 5 Buchst. b DSGVO.

Regelung wäre erkennbar eine Annexregelung zu den übrigen Vorschriften des BDSG und kann sich demzufolge auf dieselben Gesetzgebungskompetenzen stützen wie das. Das BVerfG entscheidet in ständiger Rechtsprechung, dass solche Ergänzungsregelungen zulässig sind, solange sie im Regelungszusammenhang des eigentlichen Regelungsgegenstands verbleiben und mit diesem eine „enge Verzahnung“ besteht.[31] Regelungen zu angrenzenden Sachbereichen sind zulässig, wenn der ursprüngliche Regelungsgegenstand verständigerweise nicht geregelt werden kann, ohne dass zugleich eine nicht ausdrücklich zugewiesene andere Materie mitgeregelt wird.[32]

Vorliegend geht es, wie aus dem oben genannten Beispiel deutlich wird, um eine Regelung, die sich nicht aus dem Rahmen des allgemeinen Datenschutzrechts lösen würde und dabei „medienrechtlichen“ oder „presserechtlichen“ Charakter hätte. Vielmehr versucht diese Regelung lediglich, überschießende und ungewollte negative Effekte der DSGVO auf die in Art. 85 Abs. 1 DSGVO genannten Rechtsgüter zu vermeiden. Sie verweist dabei ausdrücklich auf die Wertungen des einschlägigen Spezialrechts, einschließlich des Landesrechts.

Eine solche Regelung nur den Ländern zu überlassen, wäre demgegenüber nicht sachgerecht. Es käme anderenfalls zu einem „Flickenteppich“ an Landesregelungen, da jedes Land eigene Bestimmungen erlassen würde. Die Folge wäre, dass für die Zulässigkeit von Meinungsäußerungen in jedem Bundesland andere Regeln gälten. Eine solche zersplitterte Rechtslage würde aber ebenfalls zu Einschüchterungseffekten und Erschwernissen beim Gebrauch der Meinungsfreiheit führen, die nicht tragbar und angemessen sind. Eine allgemeine Regelung durch den Bund wäre deshalb die bessere Lösung.

4. Anpassungsbedarf im Telemediengesetz

Der DAV empfiehlt, auch das Telemediengesetz (TMG) an die Rechtslage der DSGVO anzupassen. Eine solche Anpassung nicht vorzunehmen, hätte für alle Beteiligten starke Rechtsunsicherheit zur Folge. Ein Abwarten bis zum Inkrafttreten der ePrivacy-Verordnung (ePrivacy-VO) erscheint nicht angemessen, denn bis zu deren Wirksamwerden kann es noch mehrere Jahre dauern.

[31] Beispielsweise BVerfGE 97, 228, 251 f. – *Kurzberichterstattung*.
[32] BVerfGE 138, 261 – *Ladenöffnungszeiten*.

a) Rechtlicher Hintergrund

Die DSGVO entfaltet im Bereich des Datenschutzrechts grundsätzlich Vollharmonisierungswirkung. Abgesehen von den Bereichen, in denen die DSGVO über Öffnungsklauseln spezielles Datenschutzrecht der Mitgliedsstaaten zulässt, wird deutsches Datenschutzrecht deshalb verdrängt (Anwendungsvorrang des Europarechts). Für Regelungen des TMG sind vor allem die ePrivacy-RL und Art. 95 DSGVO relevant. Nach Art. 95 DSGVO können Regelungen, die in Umsetzung der ePrivacy-RL erlassen wurden, auch neben der DSGVO bestehen bleiben und haben in bestimmten Konstellationen sogar Vorrang.

Für den überwiegenden Teil der datenschutzrechtlichen Regelungen im 4. Abschnitt des TMG (§§ 11 ff.) gibt es allerdings weder eine Grundlage in der ePrivacy-RL, noch ist eine der Öffnungsklauseln der DSGVO einschlägig.

Die ePrivacy-RL regelt ganz überwiegend Sachverhalte des Telekommunikationsrechts, die in den §§ 91 ff. TKG umgesetzt sind. Ein Gesetz zur Anpassung dieser TKG-Vorschriften an die neue Rechtslage ist im 2. DSAnpUG enthalten (Art.134). Die Anpassungen in diesem Artikel heben richtigerweise diejenigen Vorschriften des TK-Datenschutzrechts auf, für die nach Inkrafttreten der DSGVO kein Raum mehrbleibt. Eine vergleichbare Regelung auch für das TMG ist im 2. DSAnpUG nicht enthalten.

Auch in Bezug auf das TMG gibt es allerdings Umsetzungsbedarf. Denn Regelungsgegenstände, die in den Bereich des TMG fallen würden, sind in der ePrivacy-RL weitestgehend nicht enthalten. Lediglich Art. 5 Abs. 3 der ePrivacy-RL hat für das TMG Relevanz. Laut dieser Vorschrift müssen die EU-Mitgliedsstaaten Regeln erlassen für die „Speicherung von Informationen“ im Endgerät des Nutzers und den „Zugriff auf Informationen, die bereits im Endgerät eines Teilnehmers oder Nutzers gespeichert sind“. Art. 5 Abs. 3 der ePrivacy-RL bezieht sich in erster Linie auf Cookies. Ob die Vorschrift im derzeit geltenden TMG umgesetzt ist, ist strittig. Im Übrigen enthält die ePrivacy-RL *keine* weiteren Regelungspflichten, die in den Bereich des TMG fallen. Für die Vorschriften im 4. Abschnitt des TMG gibt es somit ganz überwiegend keine Grundlage im EU-Recht.

Im Ergebnis heißt dies, dass die Vorschriften des 4. Abschnitts des TMG bereits jetzt (seit dem 25.05.2018) von der DSGVO verdrängt werden und demzufolge nicht mehr anwendbar sind, es sei denn sie fallen in eine der folgenden Kategorien:

- Wirksam bleiben Vorschriften, die die ePrivacy-RL umsetzen (somit nach strittiger Auffassung die §§ 13 Abs. 1, § 12 und § 15 TMG – jedoch nur beschränkt auf den Regelungsgegenstand des Art. 5 Abs. 3 ePrivacy-RL).
- Wirksam bleiben außerdem Vorschriften, die einen Regelungsgegenstand haben, der nicht zum Datenschutzrecht zählt und deshalb von der Vollharmonisierungswirkung der DSGVO nicht erfasst wird. Dies ist beispielsweise die in § 13 Abs. 6 TMG geregelte Pflicht, soweit als möglich eine anonyme oder pseudonyme Nutzung zu ermöglichen oder die Verpflichtung zur Wahrung der IT-Sicherheit in angemessenem Umfang auch dort, wo keine personenbezogenen Daten betroffen sind (§ 13 Abs. 7 Nr. 1 und Nr. 2 b) TMG).
- Wirksam bleiben zuletzt auch Regelungen, die in eine der Öffnungsklauseln der DSGVO fallen. In Frage kommen hier die Öffnungsklausel für gesetzliche Verpflichtungen zur Datenverarbeitung (Art. 6 Abs. 1 Buchst. c i.V.m. den Absätzen 2 und 3 DSGVO) und die allgemeine Öffnungsklausel nach Art. 23 DSGVO). In diese Gruppe fallen insbesondere die Auskunftspflichten von Telemediendiensteanbietern nach § 14 Absätze 2-5 und § 15 Abs. 5 Satz 4 TMG.

Vorschriften des 4. Abschnitts des TMG, die nicht in eine dieser Kategorien fallen, sind unwirksam und dürfen nicht angewendet werden.

b) Problematik

Das für diesen Regelungsbereich federführende BMWi hat eine gesetzliche Anpassung der TMG-Vorschriften zwar zunächst erwogen, hiervon jedoch letztlich abgesehen. Als Grund werden insbesondere die Schwebephase bis zum Inkrafttreten der ePrivacy-VO sowie ein derzeit beim EuGH anhängiges Verfahren zur Umsetzung der „Cookie-Regelungen“ in Deutschland genannt.[33] Eine Anpassung des TMG soll deshalb erst

[33] So u.a. eine online abrufbare Präsentation, https://www.bvdnet.de/wp-content/uploads/2018/04/Winfried-Ulmen-E-Privacy-TKG-TMG_NEU.pdf, Folie 18.

erfolgen, wenn der Gesetzgebungsprozess der ePrivacy-VO abgeschlossen ist. Die ePrivacy-VO soll die derzeit geltende ePrivacy-RL ersetzen und dabei zusätzliches bereichsspezifisches „ePrivacy“-Datenschutzrecht festsetzen.

Ein so langes Abwarten wäre allerdings aus Sicht des DAV nicht angemessen. Denn nach aktuellem Stand des Gesetzgebungsverfahrens der ePrivacy-VO ist derzeit nicht sicher absehbar, wann diese überhaupt finalisiert werden kann. Unterstellt, dass das Gesetzgebungsverfahren überhaupt abgeschlossen wird, wäre dies wohl frühestens im Sommer 2019. Falls auch dieser Termin nicht erricht werden kann, könnte wegen der dann neu anstehenden EU-Parlamentswahlen eine Verabschiedung unter Umständen auch deutlich später kommen oder sogar komplett scheitern.

Selbst wenn es zu einer ePrivacy-VO kommen sollte, wird diese nach ihrem Inkrafttreten einen Übergangszeitraum zwischen Inkrafttreten und Wirksamwerden vorsehen. Diesbezüglich werden im Moment Zeiträume von bis zu zwei weiteren Jahren diskutiert.

Im Ergebnis heißt dies, dass die Dauer der Übergangsphase, die das BMWi abwarten möchte, und während der das TMG in großen Umfang unwirksamen Regelungen enthält, derzeit kaum absehbar ist. Voraussichtlich wird sie mindestens mehrere Jahre betragen. Das Wirksamwerden spezifischen „ePrivacy“-Datenschutzrechts wird bei realistischer Betrachtung frühestens 2020, eventuell aber auch erst 2021 oder noch später erfolgen.

Bis zum Ende dieser Übergangsphase wird es für die Rechtsanwender in Deutschland außerordentlich schwierig sein festzustellen, welche Vorschriften des TMG nun Anwendung finden und welche nicht. Dies erfordert, wie oben beschrieben, eine komplexe rechtliche Prüfung. Ohne spezialisiertes Wissen im Bereich des Telemedien- und Datenschutzrechts lässt sich aber kaum herausdestillieren, welche Vorschriften des 4. Abschnitts des TMG Anwendung finden und welche nicht.

Wenn der Bundestag ein deutsches Gesetz, trotz besseren Wissens über dessen Nichtanwendbarkeit, über den Zeitraum von mehreren Jahren stehen lässt, sendet er damit das falsche Signal an die betroffenen Bürgerinnen und Bürger und Unternehmen. Diesen wird vermittelt, dass es auch aus Sicht des Bundestages nicht notwendig (beziehungsweise nicht möglich) ist, sich rechtstreu zu verhalten.

Zudem ist es sowohl für die Unternehmen der Digitalwirtschaft als auch für die Betroffenen der Datenverarbeitung, nicht zumutbar, über einen so langen Zeitraum mit einer so unklaren Rechtslage umgehen zu müssen. Insbesondere gilt dies für kleine und mittlere Unternehmen sowie für nichtkommerzielle Webseitenbetreiber, die keinen Zugriff auf spezialisierte Rechtsberatung haben.

c) Vorschlag

Der DAV plädiert dafür, bereits mit dem hier vorgelegten 2. DSAnpUG den 4. Abschnitt des TMG um die nicht mehr anwendbaren Vorschriften zu bereinigen und stattdessen die Vorschrift des Art. 5 Abs. 3 ePrivacy-VO wortlautgenau umzusetzen. Dies würde den Unternehmen der Digitalwirtschaft, aber auch den Betroffenen und den Aufsichtsbehörden eine klare Rechtslage geben, an der sie sich orientieren können. Zudem würde der Gesetzgeber durch die Aufhebung der sehr feingranularen Vorschriften des 4. Abschnitts des TMG auch für Entlastung der digitalen Wirtschaft sorgen. Gleichzeitig bliebe es beim hohen Schutzstandard der DSGVO, so dass die Interessen der Betroffenen gewahrt blieben.