DeutscherAnwaltVerein

Stellungnahme

des Deutschen Anwaltvereins durch die Ausschüsse Informationsrecht und Gefahrenabwehrrecht

zum Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über die Achtung des Privatlebens und den Schutz personenbezogener Daten in der elektronischen Kommunikation und zur Aufhebung der Richtlinie 2002/58/EG (Verordnung über Privatsphäre und elektronische Kommunikation)

Stellungnahme Nr.: 29/2017 Berlin, im März 2017

Mitglieder des Ausschusses Informationsrecht

- Rechtsanwalt Dr. Helmut Redeker, Bonn (Vorsitzender, 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

- Rechtsanwältin Nicole Narewski

Mitglieder des Ausschusses Gefahrensabwehrrecht

- - Rechtsanwältin Dr. Heide Sandkuhl, Potsdam (Vorsitzende)
- Rechtsanwalt Wilhelm Achelpöhler, Münster
- Rechtsanwältin Dr. Annika Dießner, Berlin (Berichterstatterin)
- Rechtsanwalt Dr. Nikolas Gazeas, LL.M., Köln
- Rechtsanwalt Prof. Dr. Björn Gercke, Köln
- Rechtsanwalt Dr. Stefan König, Berlin
- Rechtsanwältin Dr. Regina Michalke, Frankfurt / Main
- Rechtsanwältin Kerstin Oetjen, Freiburg
- Rechtsanwältin Lea Voigt, Bremen

Zuständig in der DAV-Geschäftsführung

- Rechtsanwalt Max Gröning

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
Transparenz-Registernummer:
87980341522-66

www.anwaltverein.de

Verteiler

Europa

Europäische Kommission
- Generaldirektion Justiz
- Generaldirektion Kommunikationsnetze, Inhalte und Technologien
  Europäisches Parlament
- Ausschuss für Bürgerliche Freiheiten, Justiz und Inneres
- Rechtsausschuss
- Ausschuss für Binnenmarkt und Verbraucherschutz
- Ausschuss für Industrie, Forschung und Energie

Rat der Europäischen Union
Ständige Vertretung der Bundesrepublik Deutschland bei der EU
Justizreferenten der Landesvertretungen
Rat der Europäischen Anwaltschaften (CCBE)
Vertreter der Freien Berufe in Brüssel
DIHK Brüssel
BDI Brüssel

Deutschland

Bundesministerium der Justiz und für Verbraucherschutz
Bundesministerium für Wirtschaft und Energie
Bundesministerium des Innern
Ausschuss für Recht und Verbraucherschutz im Deutschen Bundestag
Ausschuss für Wirtschaft und Energie im Deutschen Bundestag
Ausschuss Digitale Agenda im Deutschen Bundestag
Innenausschuss
Arbeitsgruppen Inneres der im Deutschen Bundestag vertretenen Parteien
Arbeitsgruppen Recht der im Deutschen Bundestag vertretenen Parteien
Justizministerien und –senatsverwaltungen der Länder
Landesministerien und Senatsverwaltungen des Innern
Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit
Die Datenschutzbeauftragten der Bundesländer
Innenausschüsse der Landtage
Rechtsausschüsse der Landtage
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
Gewerkschaft der Polizei (Bundesvorstand)
Deutsche Polizeigewerkschaft im DBB
Ver.di, Recht und Politik
stiftung neue verantwortung e.V.
Institut für Deutsches und Europäisches Strafprozessrecht und Polizeirecht (ISP)

der Universität Trier
DAV-Vorstand und Geschäftsführung
Vorsitzende der DAV-Gesetzgebungs- und Geschäftsführenden Ausschüsse des DAV
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
JurPC

Der Deutsche Anwaltverein (DAV) ist der freiwillige Zusammenschluss der deutschen Rechtsanwältinnen und Rechtsanwälte. Der DAV mit derzeit rund 66.000 Mitgliedern vertritt die Interessen der deutschen Anwaltschaft auf nationaler, europäischer und internationaler Ebene.

Kurzzusammenfassung

Die geplante Verordnung COM(2017)10/F1 (im Folgenden: ePrivacy-VO) soll die E-Privacy-Richtlinie (Richtlinie 202/58/EG vom 12.7.2002 – im Folgenden ePrivacyRL) ablösen. Sie ergänzt die Datenschutzgrundverordnung (VO (EU) 2016/679 v. 27.4.2016, im Folgenden DSGVO) im Hinblick auf Daten, die im Rahmen von Telekommunikationsdiensten anfallen. Dabei geht sie – wie auch die Vorgängervorschrift – von einem weiteren Anwendungsbereich aus: Geschützt werden auch Daten, die sich auf juristische Personen und nicht nur auf natürliche Personen beziehen.

Die vorgeschlagenen Regelungen stellen an vielen Stellen eine bewusste Parallele zu den Regelungen in der Datenschutzgrundverordnung dar. An einigen Stellen wird auf sie auch verwiesen. Solche Parallelen sind nicht immer gerechtfertigt. Dies liegt zum einen daran, dass der Inhalt der Telekommunikation oft sehr privater Natur ist und daher ein hoher Vertraulichkeitsschutz geboten ist. Und auch die Analyse der Metadaten kann sehr persönliche Erkenntnisse über einzelne Nutzer ergeben – von deren politischer Ausrichtung bis hin zu sexuellen Vorlieben. Deswegen hat der EuGH die hohe Bedeutung des Schutzes dieser Daten immer wieder betont (zuletzt Urt. v. 21.12.2016 (C-203/15 und C 698/15)). Dies führt dazu, dass das Schutzniveau in der Regel höher sein muss als bei personenbezogenen Daten allgemein, insbesondere bei möglichen staatlichen Eingriffen. Diese Differenzierungen beachtet der Verordnungsentwurf nicht. Art. 5 und 6 ePrivacy-VO sollten dem spezifischen Schutzbedarf der Vertraulichkeit der Kommunikation vor spezifischen kommunikationsbezogenen Gefahren und Eingriffen Rechnung tragen, statt Kommunikationsinhalte per se wie personenbezogene Daten zu behandeln.

Darüber hinaus ist der Text des Verordnungsentwurfs an einigen Stellen unklar. Auch der europäische Verordnungsgeber sollte aber den Grundsatz der Normklarheit beachten.

Wahl des Rechtsinstrumentes „Verordnung“, Zeitpunkt des Inkrafttretens

Vorschlag:

- An der Gestaltung als Verordnung und an dem Zeitpunkt des Inkrafttretens zum 25.5.2018 sollte festgehalten werden.
- Die Formulierungen sollten so normenklar und präzise sein, wie es für unmittelbar anwendbares Recht notwendig ist.

Begründung:

Der Fachausschuss begrüßt, dass die EU-Kommission eine Rechtsverordnung vorschlägt und den Zeitpunkt des Inkrafttretens mit dem der DSGVO synchronisieren will. Dies vermeidet Unklarheiten im Verhältnis zwischen DSGVO und ePrivacy-RL, die für die Rechtspraxis und damit auch für Betroffene und Wirtschaft negative Folgen ausgelöst hätten.

Indem die ePrivacy-VO und die DSGVO auf eine Stufe gestellt werden, wird klargestellt, dass keiner der beiden Rechtsakte gegenüber dem anderen absolut vorrangig ist. Dies entspricht der tatsächlichen Interessenlage, da die ePrivacy-VO als Ausprägung des Fernmeldegeheimnisses einen anderen Anwendungsbereich und Schutzcharakter als die DSGVO hat und haben muss. Die ePrivacy-VO auf Ebene einer Richtlinie zu belassen, hätte einen Vorrang des Datenschutzrechts gegenüber dem Fernmeldegeheimnis suggeriert, der tatsächlich nicht besteht und auch nicht angemessen wäre. Zur Klarstellung des (Gleich-) Rangverhältnisses von DSGVO und ePrivacy-VO sind allerdings noch einige Klarstellungen nötig (siehe unten, Abschnitt „Verhältnis zur DSGVO“).

Durch den synchronisierten Zeitpunkt des Inkrafttretens wird ein zeitliches Überlappen der Übergangsperioden vermieden. Für Unternehmen würde anderenfalls eine zeitliche Periode von vermutlich nur wenigen Monaten eintreten, in der zwar die DSGVO bereits

in Kraft getreten ist, jedoch gleichzeitig noch die alten Regelungen der ePrivacy-RL und somit teilweise nationales Datenschutzrecht anzuwenden gewesen wären. Diese Regelungen sind schlecht aufeinander abgestimmt (dazu sogleich, Abschnitt „Verhältnis zur DSGVO“). Zudem führt die Synchronisierung zu dem großen Vorteil, dass die Unternehmen die Umsetzungsbemühungen aufeinander abstimmen können, indem sie für beide Rechtsakte, die eng miteinander in Zusammenhang stehen, auf einen einheitlichen Umsetzungstermin zuarbeiten.

Die ePrivacy-VO wird die bestehenden Regelungen im deutschen TKG, insbesondere zum Telekommunikationsdatenschutz (§§ 91 ff. TKG) und zum Fernmeldegeheimnis (§ 88 TKG) verdrängen. Gleiches gilt für die datenschutzrechtlichen Bestimmungen des Telememediengesetzes (§§ 11 TMG). Aus Sicht eines deutschen Rechtsanwenders bedeutet die ePrivacy-VO insofern nur dann eine Verbesserung, wenn die ePrivacy-VO denselben Standard bei der Normenklarheit erreicht wie das bestehende Recht. Diesem Anspruch wird der aktuelle Entwurf nicht gerecht. Er sollte - gerade unter dem Gesichtspunkt der praktischen Handhabung und Anwendbarkeit – überarbeitet werden. Hierzu werden nachfolgend konkrete Vorschläge gemacht.

Verhältnis zur DSGVO

Vorschlag:

- Art. 95 DSGVO sollte durch den folgenden Text ersetzt werden: „Innerhalb ihres Anwendungsbereichs hat die [ePrivacy-Verordnung] gegenüber der (EU) 2016/679 Vorrang.“
- Art. 21 Abs. 5 DSGVO sollte mit Inkrafttreten der ePrivacy-VO herausgenommen werden. Stattdessen sollte in Art. 9 Abs. 2 der ePrivacy-VO geregelt werden, dass auch die Ausübung des Widerspruchsrechts durch Browsereinstellungen erfolgen kann.

Begründung:

Die DSGVO beschränkt sich ausdrücklich auf die Verarbeitung personenbezogener Daten. Somit sind die Verarbeitung von Kommunikationsdaten (die zwar dem Schutz

des Fernmeldegeheimnisses unterfallen, jedoch nicht immer personenbezogenen sind) in der DSGVO außer Betracht. Aufgrund eines politischen Kompromisses innerhalb der EU blieben außerdem alle sonstigen Regelungsbereiche außer Betracht, die Gegenstand der ePrivacy-RL waren (z.B. Cookie-Regelungen). Dies wurde in Art. 95 DSGVO ausdrücklich klargestellt, indem dort eine Regelung aufgenommen wurde, laut der die DSGVO in den Regelungsbereichen der ePrivacy-RL keine zusätzlichen Pflichten auferlegt.

Ausweislich des Wortlauts von Art. 95 gilt dieser Vorrang der ePrivacy-RL jedoch nur unter den folgenden Bedingungen:

- Vorrang der Privacy-RL nur für die „Verarbeitung in Verbindung mit der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste in öffentlichen Kommunikationsnetzen“. Somit kein Vorrang für die Verarbeitung bei einfachen (nicht-öffentlichen) elektronischen Kommunikationsdiensten und Kommunikationsnetzen.

- Vorrang der ePrivacy-RL nur, wenn die in der Richtlinie geregelten Pflichten „dasselbe Ziel verfolgen“. Wann genau dies der Fall ist, wird nicht weiter definiert und somit Auslegungssache.

- Der in Art. 95 DSGVO statuierte (begrenzte) Vorrang der ePrivacy-RL beschränkt sich auf die Richtlinie selbst, jedoch nicht auf die in der Richtlinie gewährten Umsetzungsspielräume. Auf diese Weise wird somit alles nationale (Telekommunikations-) Datenschutzrecht, das über die zwingende Umsetzung der Richtlinie hinausgeht, der DSGVO unterworfen – und von dieser verdrängt. Die Folge ist, dass beispielsweise die Normen des deutschen Telekommunikationsdatenschutzrechts verdrängt werden, insoweit diese über zwingendes Richtlinienrecht hinausgehen (z.B. beziehen sich die Vorschriften der §§ 91 ff. TKG auch auf nicht-öffentlich angebotene Telekommunikationsdienste).

Soweit ersichtlich soll nach den bisherigen Planungen der EU-Kommission Art. 95 nicht geändert werden. Die Folge wäre, dass die Vorschrift gleichermaßen auch auf die neue ePrivacy-VO Anwendung finden würde (vgl. Art. 27 Abs. 2 ePrivacy-VO). Der Wortlaut

des Art. 95 DSGVO würde somit besagen, dass die ePrivacy-VO gegenüber der DSGVO nur begrenzten Anwendungsvorrang hat, nämlich nur in dem von Art. 95 gewährten Umfang (nur bei öffentlichen Diensten, nur bei Identität der „Ziele“ der Regelungen).

Ein Beibehalten von Art. 95 DSGVO würde zu offensichtlichen Abgrenzungsproblemen zwischen den beiden Regelungsakten führen, da die ePrivacy-VO einen Anwendungsbereich haben soll (vgl. vor allem Art. 2 Abs. 1 i.V.m. der nur begrenzten Rückausnahme in Art. 2 Abs. 2 lit. d ePrivacy-VO), der ihr von der DSGVO nicht vollständig gewährt wird.

Der Entwurf der ePrivacy-VO sagt in Ziffer 1.2 der Erläuterungen, dass die ePrivacy-VO „lex specialis“ sein soll. In Art. 1 Abs. 3 der ePrivacy-VO wird geregelt, dass die ePrivacy-VO die DSGVO durch die Festlegung besonderer Vorschriften präzisiert und ergänzt. Dieses Ziel – Vorrang als lex specialis durch Präzisierung und Ergänzung – wird jedoch nur dann zweifelsfrei erreicht, wenn Art. 95 DSGVO wie oben beschrieben abgewandelt wird.

Eine zweite Referenz auf die derzeitige ePrivacy-RL findet sich in Art. 21 Abs. 5 DSGVO. Diese Vorschrift soll offenbar besagen, dass Browser-Einstellungen wie das „Do Not Track“-Feature als automatische Ausübung des Widerspruchsrechts betrachtet werden sollen. Art. 21 Abs. 5 DSGVO fällt in den Anwendungsbereich und steht somit in engem Bezug insbesondere zu Art. 9 Abs. 2 der geplanten ePrivacy-VO (Erteilung der Einwilligung durch Browsereinstellungen). Ein „Auseinanderreißen“ der datenschutzrechtlichen Selbstbestimmungsmöglichkeiten per Browser auf zwei Rechtsakte macht keinen Sinn. Der Aspekt sollte einheitlich und abschließend entweder in der DSGVO oder in der ePrivacy-VO behandelt werden, jedoch nicht verteilt auf zwei Rechtsakte. Dabei wäre auch zu prüfen, ob die Selbstbestimmungsmöglichkeiten der Nutzer auf die Cookie-Regelungen beschränkt sein müssen, oder ob diese vergleichbar Art. 21 Abs. 5 DSGVO auf alle Datenverarbeitungen durch Dienste der Informationsgesellschaft bezogen werden können.

Fehlende Struktur beim personalen Anwendungsbereich

Vorschlag:

- In die Verordnung sollte für alle Vorschriften, bei denen dies bisher nicht der Fall ist, klarstellend aufgenommen werden, für welchen Normadressatenkreis diese gelten. Dabei sollten unterschiedliche Normadressatenkreise unterschieden werden, z.B. Anbieter von elektronischen Kommunikationsdiensten, Anbieter von Diensten der Informationsgesellschaft, Verantwortliche Stellen für die Verarbeitung von Kommunikationsdaten, etc.
- Art. 16 des Entwurfs sollte abgetrennt und in eine inhaltlich passende Regelung des EU-Rechts (z.B. Richtlinie 2005/29/EG, sog. UGP-Richtlinie) überführt werden.

Begründung:

Der Entwurf versucht, in der Art einer „one size fits all"-Regulierung eine Reihe von ganz unterschiedlichen Sachverhalten und Normadressaten zu erfassen. Ausweislich Art. 2 Abs. 1 gilt der Entwurf *„für die Verarbeitung elektronischer Kommunikationsdaten, die in Verbindung mit der Bereitstellung und Nutzung elektronischer Kommunikationsdienste erfolgt, und für Informationen in Bezug auf die Endeinrichtungen der Endnutzer".*

Dies ist bereits im Ausgangspunkt unzutreffend, da der Entwurf auch Regelungsbereiche jenseits der Verarbeitung elektronischer Kommunikationsdaten und von Endnutzer-Endeinrichtungen hat. Insbesondere gilt dies für Art. 16. Dieser regelt unter der Überschrift „Unerbetene Kommunikation" Fragen des Direktmarketings, ohne dabei einen Bezug zu Kommunikationsdaten oder Endnutzer-Endeinrichtungen herzustellen. Es handelt sich bei dieser Norm schlicht um eine Regelung des Werbe- und Verbraucherschutzrechts, die in der ePrivacy-VO systematisch falsch einsortiert ist. Diese Vorschrift sollte aus Gründen der Normenklarheit aus der ePrivacy-VO herausgenommen und in einer der EU-Vorschriften mit Bezug zum Marketing ergänzt werden. Dabei wäre auch zu prüfen, ob es einer solchen Regelung überhaupt noch bedarf, oder ob der Themenbereich bereits ausreichend geregelt ist.

Schwerer wiegt, dass der Entwurf der ePrivacy-VO beim personalen Anwendungsbereich jede Struktur vermissen lässt. Dies galt so im Grundsatz auch für die vorhergehende ePrivacy-RL. Allerdings blieb es den Mitgliedsstaaten bisher

aufgrund des Richtliniencharakters überlassen, die Regelungen auf die jeweils „passenden“ Gesetze aufzuteilen und somit klarzustellen, wer jeweils der Adressat der jeweiligen Regelung ist. In Deutschland ist dies erfolgt, indem die Regeln der bisherigen ePrivacy-RL teils in das Telekommunikationsgesetz, teils in das Telemediengesetz und teils in das Bundesdatenschutzgesetz aufgenommen wurden. Hieraus ergab sich dann auch, ob die betreffenden Regelungen für die Anbieter von Telekommunikationsdiensten (≈electronic communication services, ECS) und Betreiber von Telekommunikationsnetzen (≈electronic communication networks, ECN), für die Anbieter von Telemedien (≈Information Society Services, ICS) oder für alle Verantwortlichen im Sinne des Datenschutzrechts gelten sollten.

Eine solche Klarstellung wird ab dem Inkrafttreten der ePrivacy-VO nicht mehr möglich sein. Vielmehr gelten dann unmittelbar die Regeln der ePrivacy-VO. Deren Normen sind aber ganz überwiegend so formuliert, als ob es beim personalen Anwendungsbereich keinerlei Einschränkungen gibt. Damit scheint angedeutet zu werden, dass sich letztlich jeder an die Regeln der ePrivacy-VO halten muss. Dieser Ansatz ist schon grundsätzlich rechtsdogmatisch betrachtet problematisch, da die ePrivacy-VO erkennbar *kein* „Jedermannsrecht“ sein soll, sondern Teil einer Spezialregulierung für einen ganz bestimmten Wirtschaftssektor und eine bestimmte Gruppe von Normadressaten.
Hinzu kommt, dass viele der Regelungen offensichtlich auf einen ganz konkreten spezifischen Adressatenkreis ausgerichtet wurden (z.B. auf Betreiber von Webseiten oder Anbieter von elektronischen Kommunikationsdiensten), ohne dass dies aber klargestellt würde. Der Effekt ist, dass eine Vielzahl von Rechtsbestimmungen auch an Personen adressiert wird, die für diese gar nicht umsetzbar sind. Einige Vorschriften, z.B. Art. 3 Abs. 1 lit. b) sind aufgrund dieser Tatsache sogar völlig unverständlich.
Die Problematik zieht sich wie ein roter Faden fast durch den gesamten Verordnungsentwurf, weshalb auch der gesamte Entwurf überarbeitet und ggf. re-strukturiert werden sollte (z.B. durch Aufteilung der Regelungsbereiche, geordnet nach Normadressaten in verschiedene Abschnitte). Auf einige Fälle wird im Folgenden noch gesondert eingegangen.

Ausdehnung auf OTT-Dienste

Vorschlag:

- Hinsichtlich der Anwendung auf OTT-Dienste sollte die Kommission prüfen, ob alle Regelungen der ePrivacy-VO auch für innovative Diensteanbieter angemessen sind und unter verhältnismäßigen Bedingungen umgesetzt werden können.
- Insbesondere sollte geprüft werden, ob für die Verarbeitung von Kommunikationsdaten flexible Erlaubnistatbestände analog Art. 6 Abs. 1 lit. b und lit. f DSGVO ergänzt werden können (Verarbeitung zur Vertragserfüllung sowie auf Basis legitimer Interessen bei gleichzeitiger Interessenabwägung).
- In Erwägungsgrund 18 sollte präzisiert werden, dass ein Kopplungsverbot bei der Einwilligung nur betreffend grundlegender Internetzugangs- und Sprachkommunikationsdienste gilt, jedoch nicht für innovative OTT-Dienste.

Begründung:

Die ePrivacy-VO will ihren Anwendungsbereich ausweislich ihrer Erwägungsgründe auch auf sog. OTT-Dienste ausdehnen. Während dies in den Darstellungen der Kommission zum bisherigen Gesetzgebungsverfahren und in den Erwägungsgründen ausführlich dargestellt wird, beschränkt sich im eigentlichen Text der Verordnung der Verweis auf die OTT-Dienste auf den Definitionsteil in Art. 4 Abs. 1, wo auf den European Electronic Communications Code (EECC) verwiesen wird.

Nach Auffassung des Fachausschusses gehört das OTT-Thema in der Tat eher zum Gesetzgebungsverfahren des EECC, und weniger zur ePrivacy-VO. Die Anwendbarkeit der Spezialregulierung für elektronische Kommunikationsdienste ist eine allgemeine und generelle Frage mit vielen Ausprägungen, von denen die Regelungsbereiche der ePrivacy-VO nur eines ist. Der Fachausschuss betont deshalb, dass die Frage der Regulierung von OTT-Diensten nicht isoliert als Angelegenheit der ePrivacy-VO betrachtet werden sollte sondern allgemein, im Rahmen der Erstellung des EECC, beantwortet werden sollte.

Speziell zu der Frage der OTT-Regulierung nach der ePrivacy-VO ist anzumerken, dass zwar unter dem Aspekt des „Level Playing Field“ viel dafür sprechen mag, Anbieter mit demselben Geschäftsmodell auch gleichartig, d.h. technologieneutral zu regulieren. Jedoch sollte auch berücksichtigt werden, dass OTT-Dienste häufig deutlich

innovativer sind und den Nutzern neue Funktionen und Features anbieten. Auch die klassischen Anbieter von elektronischen Kommunikationsdiensten und Kommunikationsnetzen werden zunehmend innovativer. Unter den Stichworten „unified communications“, „IoT“ und „M2M“ werden neue Produkte und Geschäftsmodelle entwickelt. Häufig beruhen diese auf einer innovativen Verbindung verschiedener Stufen der Wertschöpfungskette (z.B. der Verbindung der Funktion einer Telefonanlage mit dem Angebot des Internetzugangs) oder neuartigen Auswertungsverfahren für personenbezogene und nicht-personenbezogene Daten. Der ganz überwiegende Teil dieser Dienste stellt für sich betrachtet keine gesteigerte Bedrohung für die Privatsphäre der Endnutzer dar, sondern einfach ein zusätzliches innovatives Produkt auf dem Markt.

Innovative Produkte, seien sie aus dem Bereich von OTT oder aus dem klassischen Telekommunikationsbereich, erfordern häufig eine Verwendung von Kommunikationsdaten, die vom Gesetzgeber nicht antizipiert worden ist. Dies spricht gegen eine zu starke Verengung der Erlaubnistatbestände, da diese sonst nicht flexibel genug sind, um auf innovative Dienste zu reagieren. Insbesondere ist es deshalb kritisch zu sehen, dass eine Erlaubnisregelung analog Art. 6 Abs. 1 lit. b (Verarbeitung zur Vertragserfüllung) und lit. f DSGVO (überwiegende Interessen des Datenverarbeiters) in der ePrivacy-VO fehlt (zu den Erlaubnistatbeständen siehe auch noch unten, Abschnitt „Erlaubnisregelungen in Art. 6“). Im Rahmen der Interessenabwägung wäre der gesteigerte Vertraulichkeitsanspruch von Kommunikationsdaten zu berücksichtigen.

Zudem besteht seitens der Nutzer an OTT-Dienste nicht immer die gleiche Vertraulichkeitserwartung wie bei „klassischen“ elektronischen Kommunikationsdiensten. Im Gegenteil wird ein Nutzer häufig eher erwarten, dass ihm ein OTT-Dienst einen Mehrwert bietet, beispielsweise bei der Verwaltung oder dem Teilen seiner personenbezogenen Daten. Auch diesen strukturellen Unterschied zwischen OTT-Diensten und „klassischen“ Diensten sollte die ePrivacy-VO berücksichtigen.

Daraus folgt nach Auffassung des Fachausschusses nicht, dass die ePrivacy-VO ihren technologieneutralen Ansatz aufgeben sollte. Jedoch sollten die Regelungen der

ePrivacy-VO so angepasst werden, dass den Bedürfnissen der OTT-Anbieter Rechnung getragen wird, anstatt diese mit auf sie schlecht angepassten Regelungen zu „erschlagen“.

Insbesondere muss deshalb für OTT-Anbieter die Möglichkeit bestehen, bei den Betroffenen bzw. Endnutzern eine Einwilligung einzuholen, die ihnen die Erbringung ihrer innovativen Dienste ermöglicht. Zu hohe Anforderungen an eine wirksame Einwilligung wären damit nicht vereinbar. Insbesondere muss es den Anbietern möglich sein, überhaupt eine wirksame Einwilligung einholen zu können. Dies setzt voraus, dass diese Anbieter die Erbringung ihrer Dienste von der Abgabe einer Einwilligung zur Verwendung ihrer (personenbezogenen) Kommunikationsdaten abhängig machen können (sog. Kopplung), denn häufig ist eine solche Einwilligung erst Voraussetzung für die Legalität solcher Dienste.

Ob eine Einwilligung „freiwillig“ und damit wirksam ist, wenn die Einwilligung an die Erbringung einer Dienstleistung gekoppelt wird, wird in Anbetracht von Art. 7 Abs. 4 DSGVO häufig bezweifelt. Genau dies muss aber möglich sein, wenn die Anwendung der ePrivacy-VO auf OTT-Dienste nicht zu unverhältnismäßigen Folgen führen soll (was auch eine starke Verärgerung der massenhaft betroffenen Nutzer dieser Dienste zur Folge hätte). Erwägungsgrund 18 der ePrivacy-VO geht in diesem Punkt bereits in die richtige Richtung. Dort wird – ohne dies deutlich auszudrücken – angedeutet, dass das Kopplungsverbot nur dann greift, wenn das Erfordernis der Einwilligung mit einem „unverzichtbaren“ Dienst gekoppelt wird. Dies bezieht sich nach Erwägungsgrund 18 auf „grundlegende und breitbandige Internetzugangs- und Sprachkommunikationsdienste“ – und somit gerade nicht auf OTT-Dienste. Dieser Ansatz ist zu begrüßen, sollte jedoch präzisiert werden. Im genauen Wortlaut besagt Erwägungsgrund 18 bisher nicht, dass nicht-grundlegende Dienste vom Kopplungsverbot nicht erfasst werden.
Diese Präzisierung sollte im Rahmen von Erwägungsgrund 18 noch erfolgen. Die Präzisierung zur erlaubten Kopplung von Dienstleistung und Einwilligung sollte sich auf alle Anbieter von elektronischen Kommunikationsdiensten sowie auf die Dienste der Informationsgesellschaft beziehen.

Ausdehnung auf Kommunikationsdienste, die nur als Nebenfunktion angeboten werden

Vorschlag:

Art. 4 Abs. 2 des Entwurfs sollte nicht übernommen werden.

Begründung:

Über die Ausweitung auf OTT-Dienste hinaus besagt Art. 4 Abs. 2 der ePrivacy-VO, dass unter den Begriff „interpersonaler Kommunikationsdienst“ (und somit auch den regulierten elektronischen Kommunikationsdienst) zukünftig auch Dienste fallen sollen, *„die eine interpersonelle und interaktive Kommunikation lediglich als untrennbar mit einem anderen Dienst verbundene untergeordnete Nebenfunktion ermöglichen.“*

Diese Bestimmung würde dazu führen, dass die Telekommunikationsregulierung – noch über die Regulierung von OTT-Diensten hinaus – auch auf solche Dienste ausgeweitet würde, die nicht einmal im Schwerpunkt elektronische Kommunikationsdienste sind. Dies ist keine Frage der technologieneutralen Gleichbehandlung, sondern der Versuch, den Anwendungsbereich der Telekommunikationsregulierung insgesamt auszudehnen. Insbesondere stellt Art. 4 Abs. 2 des Verordnungsentwurf einen Bruch mit dem Paradigma dar, dass als Anbieter eines elektronischen Kommunikationsdienstes nur reguliert wird, wer einen Dienst erbringt, der *ganz oder überwiegend* in der Übermittlung von Signalen über elektronische Kommunikationsnetze besteht (so bisher Art. 2 lit. c der Rahmenrichtlinie 2002/21/EG). Unbenommen bleibt die – bereits auf Basis des bestehenden Rechts mögliche – Anwendbarkeit des Telekommunikationsrechts auf Dienstbestandteile, die sich gedanklich abtrennen und als eigenständiger Dienst betrachten lassen. Auf diese Dienste kann bereits jetzt die Telekommunikationsregulierung Anwendung finden.

Eine Ausweitung der ePrivacy-Verordnung auf „Nebendienste“ würde demgegenüber beispielsweise Kommunikationsdienste erfassen, die ergänzend zu Computerspielen (z.B. Chat-Möglichkeiten oder TeamSpeak) oder zu Online-Bearbeitungstools für Dokumente (z.B. Chat- und Kommentarfunktionen bei Google Docs) angeboten

werden. Die Regelungen der Telekommunikationsregulierung sind jedoch auf professionelle und spezialisierte Anbieter von elektronischen Kommunikationsdiensten und –Netzen ausgelegt. Sie haben für Dienste, bei denen Kommunikation nur eine Nebenfunktion darstellt und auch keine Vertraulichkeitserwartung der Nutzer i.S.d. Fernmeldegeheimnisses besteht, keinen sinnvollen Anwendungsbereich.

Zudem sollte der Anbieterbegriff schon aus Gründen der Normenklarheit einheitlich im EECC definiert werden. Auch aus diesem Grund sollte eine Sonderregelung in der ePrivacy-VO unterbleiben.

Präzisierung des Anwendungsbereichs: Keine Anwendung auf anonymisierte Metadaten

Vorschlag:

In Art. 4 Abs. 3 lit. c sollte die folgende Ergänzung aufgenommen werden: „Daten gelten nicht als elektronische Kommunikationsdaten, wenn sie sich nicht auf natürliche oder juristische Personen beziehen oder beziehbar sind."

Begründung:

Der Entwurf der ePrivacy-VO ist bisher bei der Frage, ob anonyme bzw. anonymisierte Daten als Kommunikationsdaten geschützt werden, unklar.

Art. 7 Abs. 1 und Abs. 2 scheinen davon auszugehen, dass die ePrivacy-VO (wie auch die DSGVO) auf vollständig anonymisierte Daten keine Anwendung findet. Erwägungsgrund 17 scheint ebenfalls davon auszugehen, dass nicht-personenbezogene Metadaten von vornherein nicht dem Verbot mit Erlaubnisvorbehalt unterfallen. Eine explizite Klarstellung diesbezüglich fehlt aber in dem Entwurf. Und insbesondere die Definitionen der Begriffe „elektronische Kommunikationsdaten" (Art. 4 Abs. 3 lit. a); „elektronische Kommunikationsinhalte" (Art. 4 Abs. 3 lit. b) und „elektronische Kommunikationsmetadaten" (Art. 4 Abs. 3 lit. c) scheinen Daten unabhängig davon zu erfassen, ob sie sich auf eine konkrete (natürliche oder juristische) Person beziehen bzw. beziehbar sind oder nicht.

Es erscheint angemessen, bei dieser Frage zu differenzieren.

- Die Vertraulichkeit von Kommunikations*inhalten* sollte auch dann geschützt sein, wenn diese Daten keinen Personenbezug haben. Denn Kommunikationsinhalte können, auch unabhängig von ihrem Personenbezug, Informationen von hohem Geheimhaltungs- oder Privatsphäreninteresse enthalten (z.B. Unternehmensgeheimnisse).
- Bei *Meta*daten ist demgegenüber nicht nachvollziehbar, wieso der Schutz der ePrivacy-VO diese auch dann erfassen soll, wenn die Daten anonymisiert wurden. An solchen Daten besteht im Fall eines fehlenden Personenbezugs bzw. nach der Anonymisierung kein legitimes Geheimhaltungs- oder Datenschutzinteresse mehr.

Für die digitale Wirtschaft und insbesondere Anbieter elektronischer Kommunikationsdienste ist die Nutzbarkeit von nicht personenbezogenen Daten essenziell, z.B. für die Nutzung bei „Internet der Dinge“-Angeboten (M2M-Kommunikation) oder für andere innovative Produkte (siehe auch oben zu OTT-Diensten). Der digitalen Wirtschaft sollten keine unnötigen Steine in den Weg gelegt werden, indem auch Daten ohne Bezug zur Privatsphäre besonders geschützt werden müssen.

Präzisierung des Anwendungsbereichs des Telekommunikationsgeheimnisses in Art. 5

Vorschlag:

In Art. 5 sollte klargestellt sein, dass der Adressatenkreis der Verpflichtung zur Wahrung der Vertraulichkeit der Kommunikation ausschließlich Anbieter von elektronischen Kommunikationsdiensten, Betreiber von elektronischen Kommunikationsnetzen und solche Personen sind, die an der Erbringung solcher Dienste bzw. dem Betrieb solcher Netze mitwirken.

Begründung:

Art. 5 der Verordnung enthält das Telekommunikationsgeheimnis. Die Norm ist freilich so konturlos formuliert, dass das klassische Telekommunikationsgeheimnis aus ihr kaum erkennbar wird.

Das Telekommunikationsgeheimnis ist eine Ausprägung des Grundrechts auf Wahrung der Vertraulichkeit der Kommunikation. Dieses Grundrecht ist im Ausgangspunkt als Abwehrrecht des Bürgers gegen den Staat gerichtet; auf Ebene des EU-Rechts stellt es eine Ausprägung des allgemeinen Schutzes der Fernkommunikation dar (Art. 7 EU-GrCh und Art. 8 Abs. 1 EMRK). Im Zuge der Privatisierung der Telekommunikation ab ca. 1995 ist das Telekommunikationsgeheimnis auf die Privatunternehmen ausgedehnt worden, die als Anbieter elektronischer Kommunikationsdienste bzw. Netzbetreibern an die Stelle der staatlichen Behörden traten. Um eine Absenkung des Schutzstandards zu vermeiden, wurden auch die privaten Anbieter zur Wahrung der Vertraulichkeit der Kommunikation verpflichtet. Die Begründung für diese (rechtsdogmatisch sehr seltene) unmittelbare Ausdehnung des Schutzanspruchs eines Grundrechts auf den Privatrechtsverkehr ist, dass private Unternehmen bei der Gewährleistung des Telekommunikationsgeheimnisses eine dem Staat vergleichbare Funktion und Verantwortung übernehmen. Das Telekommunikationsgeheimnis soll vermeiden, dass Bürger von der Nutzung von Fernkommunikationsmitteln abgeschreckt werden, weil sie bei Fernkommunikation ihre Äußerungen „aus den Augen verlieren“ und zwangsläufig in fremde Hände geben. Um einen Chilling Effect auf die Kommunikation zu vermeiden, wird die strukturell höhere Bedrohung von Kommunkationsinhalten auf dem Transportweg durch eine zusätzliche Pflicht zur Wahrung der Vertraulichkeit kompensiert.

Aus diesem Grund ist das Telekommunikationsgeheimnis historisch immer auf einen bestimmten Personen- und Anbieterkreis beschränkt gewesen, nämlich auf den Anbieterkreis, der die Inhalte transportiert und dabei teils auch zur Kenntnis nimmt (z.B. zur Gewährleistung der Netzsicherheit). Das Telekommunikationsgeheimnis gleicht insofern anderen Geheimhaltungspflichten, die sich auf bestimmte Personengruppen richten, z.B. dem anwaltlichen oder ärztlichen Berufsgeheimnis. Die besondere Bedeutung dieser Vorschriften ergibt sich aus ihrer Bekanntheit und Verkehrsgeltung. Jeder Anbieter dieser Personen- bzw. Anbietergruppe und auch jeder Betroffene kennt diese Arten von Geheimhaltungspflichten als eine Verpflichtung besonderer Art. Die

Inhalte der Geheimhaltungspflicht sind leicht erfassbar und verständlich und werden von den jeweils Verpflichteten deshalb nicht nur als allgemeines Compliance-Thema, sondern als grundlegende Frage des Berufsethos behandelt. Umgekehrt genießen personengebundene Geheimhaltungsverpflichteten wie das Telekommunikationsgeheimnis ein erhöhtes Vertrauen in der Verkehrsanschauung.

Eine Beschränkung auf einen bestimmten Personenkreis scheint Art. 5 aber zu fehlen. Vielmehr scheint Art. 5 die Verpflichtung zur Wahrung der Vertraulichkeit der Kommunikation auf „Jedermann“ zu beziehen.

„Nachrichten“ werden nach dem bisherigen Art. 5 Abs. 1 der ePrivacy-RL bereits geschützt gegen das „Mitlauschen“ („Mithören, Abhören“), gegen das „Abfangen“ sowie das „Überwachen“ sowie gegen das „Speichern“. Art. 5 der ePrivacy-VO soll den Umfang des Verbotes nun noch erweitern: Nun soll generell jedes „Verarbeiten“ von „Kommunikationsdaten“ pauschal unter ein Verbot mit Erlaubnisvorbehalt gestellt werden. Art. 5 ePrivacy-VO scheint somit die gesamte Verarbeitung von Telekommunikationsdaten unter Erlaubnisvorbehalt zu stellen, *und zwar auch nach Ende des Telekommunikationsvorgangs*.

Dies würde einerseits dem TK-Geheimnis seine Fokussierung auf einen bestimmten Personenkreis nehmen und dadurch mit der historischen Tradition als Abwehrrecht gegen den Staat und staatsähnliche Anbieter brechen.

Andererseits würde eine Ausdehnung des Anwendungsbereichs des Art. 5 auf Nicht-Diensteanbieter auch zu konkreten praktischen Anwendungsproblemen führen. Denn Kommunikationsdaten sind für Personen, die nicht Anbieter von elektronischen Kommunikationsdiensten oder elektronischen Kommunikationsnetzen sind, *überhaupt keine Kommunikationsdaten.* In der bisherigen Ausprägung des Telekommunikationsgeheimnisses sind Kommunikationsdaten nicht mehr gesondert geschützt, nachdem die Kommunikation zugegangen ist (mit der Ausnahme von Kommunikationsmetadaten, die als Schutzreflex des Telekommunikationsgeheimnisses gegen staatliche Erhebung dauerhaft geschützt sind).

Aus der Sicht von Personen, die nicht selbst Anbieter von Kommunikationsdiensten oder –Netzen sind, fehlt für bereits zugegangene Daten somit der spezielle Bezug zum Transportvorgang, und folglich auch der besondere Schutzanspruch dieser Daten. Gleichwohl würde Art. 5, dem Wortlaut nach ausgelegt, besagen dass auch Nicht-Diensteanbieter an das Telekommunikationsgeheimnis gebunden sind, und zwar auch für Daten, die nicht mehr transportiert werden, sondern bereits zugegangen sind.

Eine solche Ausdehnung des Telekommunikationsgeheimnisses auch auf „sonstige Dritte“ ist nicht nur mit dessen spezifischem Schutzanspruch unvereinbar, es macht auch der Sache nach keinen Sinn. Eine Bindung von Nicht-Diensteanbietern an das Telekommunikationsgeheimnis hätte unverhältnismäßige Folgen. Denn dann wäre für Jedermann der Zugriff auf jeglichen Art von Telekommunikationsdaten, untersagt bzw. an äußerst enge Voraussetzungen gekoppelt. Das würde auch für Daten gelten, die gar nicht mehr transportiert werden, sondern bereits zugegangen sind. Es wäre beispielsweise untersagt, bereits zugegangene E-Mails für einen Dritten abzuspeichern oder Daten über vergangene Telefonanrufe aus einem Gerätespeicher auszulesen (z.B. zum Anlegen eines Gerätebackups).

Erlaubnisregelungen in Art. 6

Vorschlag:

- Art. 6 sollte grundlegend strukturell überarbeitet werden. Eine neue Struktur der Norm (ggf. durch Aufteilung auf mehrere Artikel) sollte klar stellen, in welchem Verhältnis die Verbots- und Erlaubnistatbestände zueinander stehen.
- Das Recht der Endnutzer, eine Verarbeitung der sie betreffenden Daten durch eine Einwilligung erlauben zu können, sollte nicht eingeschränkt werden. Das Recht auf informationelle Selbstbestimmung beinhaltet das Recht, gerade auch Datenverarbeitungen zu autorisieren, die aus Sicht des restriktiven Datenschutzes „unvernünftig“ sind.

Begründung:

Art. 6 enthält eine Reihe von Erlaubnisregelungen, die sich an die Anbieter von elektronischen Kommunikationsdiensten und die Betreiber von elektronischen Kommunikationsnetzen richten. Die Vorschrift ist leider in ganz zentralen Punkten systematisch unklar.

- Zunächst wird von vornherein nicht klar, in welchem Verhältnis diese Erlaubnisvorschriften zu den Erlaubnisvorschriften der DSGVO stehen sollen (insb. zu Art. 6 und Art. 9 DSGVO). Es würde dem traditionellen Verständnis des Telekommunikationsdatenschutzes entsprechen, wenn Art. 6 als *abschließend* gemeint ist, d.h. dem speziellen Anbieterkreis der Anbieter elektronischer Kommunikation und Betreiber elektronischer Kommunikationsnetze jede Verarbeitung von elektronischen Kommunikationsdaten verbietet, die nicht in Art. 6 der ePrivacy-VO erlaubt wird. Eine solche Klarstellung fehlt in Art. 6 aber. Vielmehr suggeriert der aktuelle Wortlaut lediglich in Abs. 3 ein solches Verbot mit Erlaubnisvorbehalt („nur“ bzw. „only“), während dieser Zusatz in Abs. 1 und Abs. 2 fehlt.

- Unklar ist außerdem das Verhältnis der Erlaubnisregelung in Abs. 1 zu den Erlaubnisregelungen in Abs. 2 und 3. Abs. 1 bezieht sich auf alle Kommunikationsdaten, während Abs. 2 und Abs. 3 jeweils nur Metadaten bzw. Inhaltsdaten erfassen. Abs. 1 erfasst zudem neben den Anbietern elektronischer Kommunikationsdienste auch Betreiber elektronischer Kommunikationsnetze, während Abs. 2 und Abs. 3 jeweils nur die Diensteanbieter erfassen.
- Aus dem gesamten Kontext des Art. 6 wird nicht deutlich, ob diese Erlaubnisvorschriften im gegenseitigen Verhältnis exklusiv sind, oder ob sie kumulativ nebeneinander gelten sollen.
- Die Vorschrift sollte vor diesem Hintergrund grundlegend überarbeitet werden. Dabei sollte darauf geachtet werden, dass Verbote („du darfst nicht“) und Erlaubnisse („du darfst“) systematisch voneinander getrennt werden. Der jeweilige Anwendungsbereich der jeweiligen Verbots- oder Erlaubnisvorschriften sollte unzweifelhaft klar werden. Außerdem sollte klargestellt werden, in welchem Verhältnis die Verbots- und Erlaubnisvorschriften zueinander stehen, insbesondere welches Verbot durch welche Erlaubnisvorschriften durchbrochen werden kann, und durch welche nicht.

- Auch innerhalb der jeweiligen Absätze ist unklar, in welchem Verhältnis die jeweiligen dort genannten Erlaubnistatbestände stehen. Insbesondere in Art. 6 Abs. 3 sind zwei unterschiedliche Rechtfertigungstatbestände geregelt, die beide eine Einwilligung der Nutzer voraussetzen. Es wird nicht hinreichend deutlich, in welchen Fällen welche der beiden Ziffern Anwendung finden soll.

- Abzulehnen ist in jedem Fall der in vielen Erlaubnisvorschriften des Art. 6 eingefügte Vorbehalt, laut dem Einwilligungen der Nutzer in bestimmten Fällen unwirksam sein sollen. So soll eine Einwilligung der Nutzer von vornherein unwirksam sein, wenn „*die betreffenden Zwecke durch eine Verarbeitung anonymisierter Informationen […] erreicht werden können*“ (Art. 6 Abs. 2 lit. c), wenn *„die Dienstleistung ohne Verarbeitung dieser Inhalte […] erbracht werden kann“* (Art. 6 Abs. 3 lit. a) oder wenn die *„Zwecke […] durch eine Verarbeitung anonymisierter Informationen […] erreicht werden können“ (Art. 6 Abs. 3 lit. b~~)~~.* In diesen Punkten würde der Entwurf der ePrivacy-VO den Nutzern die Dispositionsfreiheit über ihre Daten nehmen: Eine informationelle Selbstbestimmung des Nutzers durch Erteilung einer Einwilligung soll laut dem Entwurf von vornherein unmöglich sein, wenn die Datenverarbeitung – in den Augen des Gesetzgebers – „unvernünftig“ ist, weil eine datenschutzfreundlichere Lösung möglich wäre. Mit dieser Regelung stellt sich der Gesetzgeber an die Stelle der Betroffenen – er will an ihrer Stelle eine Einwilligung verweigern dürfen. Es fehlt aber die Rechtfertigung für Eingriffe in das Selbstbestimmungsrecht der Betroffenen. Denn die Ausnahme von der Einwilligungsmöglichkeit nimmt den betroffenen Nutzern die Möglichkeit, Nachteile bei der Privatheit gegen Vorteile in anderen Bereichen abzuwägen und auf Basis der Gesamtbetrachtung der Vor- und Nachteile eine Einwilligung abzugeben. Mit anderen Worten: Bürger sollen auch solche Datenverarbeitungen nicht autorisieren können, die sie als insgesamt vorteilhaft bewerten – bloß weil dabei ein Verlust an Privatheit entsteht. Die Einschränkungen des Einwilligungsrechts der Nutzer sollten gestrichen werden. Die *grundsätzliche* Verpflichtung zur Datenminimierung (Art. 5 Abs. 1 lit. c DSGVO) bleibt hiervon selbstverständlich unberührt.

<u>Keine Verpflichtung von Dienstleistern, die in der Sphäre des Empfängers agieren, auf das Fernmeldegeheimnis</u>

Vorschlag:

- Die ePrivacy-VO sollte klarstellen, dass Anbieter von elektronischen Kommunikationsdiensten, die im Auftrag eines Teilnehmers Kommunikationsinhalte in Empfang nehmen und *nach* Inempfangnahme verarbeiten, nicht mehr als Anbieter von elektronischen Kommunikationsdiensten, sondern als Dritte i.S.v. Art. 7 Abs. 1 Satz 2 ePrivacy-VO zu behandeln sind.

Begründung:

Innovative Kommunikationsdienste, insbesondere (aber nicht nur) im OTT-Bereich verbinden häufig Funktionen der Übermittlung von Nachrichten mit Funktionen, die eher zur Sphäre der Endnutzer der Kommunikation gehören. Weil diese Dienste aber technisch nicht mehr lokal beim Endnutzer stattfinden, sondern innerhalb der Cloud, ist eine Grauzone entstanden, in der solche Funktionen nur schwer vom Angebot elektronischer Kommunikationsdienste abgrenzbar sind.

In die vorgenannte Kategorie fallen z.B. „Telefonanlagen in der Cloud“. Diese verbinden die Verbindung von Telefonanrufen in das Sprachtelefonienetz (PSTN) mit Funktionselementen von klassischen Telefonanlagen (z.B. Weiterschalten oder Übernehmen von Anrufen oder die Speicherung, Verarbeitung und Übermittlung von Anrufdaten, teils auch Aufzeichnung von Gesprächen). Diese Funktionen finden gerade nicht lokal in den Räumen des Teilnehmers statt (wie bei einer klassischen Telefonanlage), sondern „in der Cloud“. Der Nutzer greift auf diese Funktionen über vernetzte Endgeräte oder ein Web-Portal zu. Die Funktionen einer „Telefonanlage in Cloud“ und erfolgen damit technisch gesehen u.U. zu einem Zeitpunkt, zu dem die Kommunikation dem Endnutzer noch nicht zugegangen ist. Damit ergeben sich schwierige Abgrenzungsfragen über die Frage, ob die Vorschriften zum Schutz des Fernmeldegeheimnisses bereits Anwendung finden (was wesentliche Features dieser Dienste rechtlich untersagen würde).

Dasselbe Problem stellt sich bei E-Mail-Diensten (insb. Webmail-Diensten), die zusätzliche Funktionen wie das Vorsortieren von Nachrichten (insb. zur Spamabwehr) oder die automatischen Ausfilterung von Nachrichten mit schädlichem Inhalt (Viren,

Trojaner) anbieten. Einige E-Mail-Dienste finanzieren sich auch über kontextbasierte Werbung, was ebenfalls ein Scannen der E-Mails notwendig macht. Denn laut dem neu formulierten Wortlaut von Art. 5 ePrivacy-VO soll auch das Scannen von Kommunikationsinhalten als Eingriff in das Fernmeldegeheimnis gelten – offenbar auch dann, wenn es vollautomatisch und ohne menschliche Kenntnisnahme erfolgt. Zu Ende gedacht bedeutet dies, dass ein Scannen von E-Mails (z.B. zum Erkennen von Virenbefall) nicht möglich ist, es sei denn es liegt eine Einwilligung aller betroffenen Endnutzer vor – insbesondere also auch eine Einwilligung des *Absenders* der Schadsoftware oder der Spamnachricht (vgl. insbesondere den Wortlaut von Art. 6 Abs. 3 lit. b e-Privacy-VO und von Erwägungsgrund 19 Satz 4 bis 7 e-Privacy-VO). Spam-Filter sind eine nützliche Technologie, die E-Mails systematisch scannt und nach typischen Merkmalen unerwünschter Nachrichten durchsucht. Für derartige Filter nicht nur das Einverständnis des Empfängers der Nachricht zu verlangen, sondern auch das Einverständnis des Absenders (Spammers), führt dazu, dass Spam-Mails ungehindert ihren Weg zum Empfänger finden können.

Die ePrivacy-Verordnung sollte nicht versuchen, die Spamfilterung oder Cloud-Telefonanlagen als Ausnahme vom Fernmeldegeheimnis zu definieren, sondern von vornherein als das behandeln, was sie sind: Als eine Verarbeitung von Kommunikationsinhalten, die bereits in der Sphäre des Empfängers angekommen sind. Diese Daten müssen deshalb nicht mehr den besonderen Regelungen zum Schutz von Kommunikation auf dem Transportweg unterfallen, sondern das normale Datenschutzrecht reicht aus.

Die ePrivacy-RL sollte für das dargestellte Problem eine strukturell saubere Lösung anbieten, indem sie klare Kriterien dafür zur Verfügung stellt, welche Dienste *in die Sphäre des Teilnehmers* fallen, d.h. nicht mehr an die Vorschriften zur Vertraulichkeit der Kommunikation gebunden sind. Sind die Inhalte in der Sphäre des Empfängers angekommen, sollten sie gem. Erwägungsgrund 19, Satz 8 und 9 ePrivacy-VO nur noch dem „normalen“ Datenschutzrecht gemäß der DSGVO unterfallen.

Um diese Klarstellung vorzunehmen, kann eine Weiterentwicklung des aktuellen Entwurfs an Art. 7 Abs. 1 Satz 2 anknüpfen. Diese Bestimmt nimmt bereits (offenbar deklaratorisch) „Dritte“ vom Anwendungsbereich der Vertraulichkeitsvorschriften aus,

wenn diese im Auftrag des Endnutzers Kommunikationsdaten aufzeichnen oder speichern. In Art. 7 (oder im Definitionsteil der ePrivacy-VO oder des EECC) sollte klargestellt werden, dass auch Anbieter von elektronischen Kommunikationsdiensten als Dritte i.S.v. Art. 7 Abs. 1 Satz 2 ePrivacy-VO zu behandeln sind, wenn sie im Auftrag eines Teilnehmers Kommunikationsinhalte in Empfang nehmen und diese Kommunikationsinhalte *nach* Inempfangnahme verarbeiten.

Diese Lösung würde dazu führen, dass Dienste wie die Spamfilterung von E-Mails oder Cloud-Telefonanlagen zulässig bleiben, denn sie fallen von vornherein nicht mehr unter das Angebot von elektronischen Kommunikationsdiensten und damit nicht dem Fernmeldegeheimnis. Diese Dienste würden somit nicht mehr den speziellen Vorschriften der Art. 5 ff. ePrivacy-RL unterfallen, sondern (nur) der DSGVO. Eine Schutzlücke steht nicht zu befürchten, da auf diese Dienste weiterhin die DSGVO anwendbar bleibt.

Fragwürdige Regelung zu Endgeräteinformationen in Art. 8 Abs. 2

Vorschlag:

- Die Vorschrift sollte gestrichen werden. Der Schutzgedanke von Art. 8 Abs. 2 bleibt unklar. Es ist nicht nachvollziehbar, wieso Endgeräte-Informationen gegenüber anderen Daten zusätzlichen Schutz benötigen. Ganz im Gegenteil haben solche Daten nur geringen Privatsphärenbezug. Sie sind aber für eine Vielzahl von Internet-Anwendung und auch für die Rechtsdurchsetzung im Internet wichtig.
- Falls die Norm beibehalten bleibt, sollte zumindest klargestellt werden, welchen personellen Anwendungsbereich sie hat. Eine Anwendung auf Anbieter elektronischer Kommunikationsdienste oder Netzbetreiber ist nicht sinnvoll, da dieser Anbieterkreis betreffend Kommunikationsmetadaten bereits Spezialvorschriften unterworfen ist.

Art. 8 Abs. 2 untersagt „*die Erhebung von Informationen, die von Endeinrichtungen ausgesendet werden, um sich mit anderen Geräten oder mit Netzanlagen verbinden zu können*“. Wie auch bei vielen anderen Vorschriften der ePrivacy-VO wird hier nicht klargestellt, wer in den personellen Anwendungsbereich der Norm fällt. Die Norm

scheint sich an Jedermann zu richten, auch wenn die EU-Kommission offenbar spezifische Anwendungsfälle im Auge hatte.

Im aktuellen Stadium scheint der Wortlaut von Art. 8 Abs. 2 etliche unterschiedliche Anwendungsfälle zu betreffen, z.B. das Auslesen von WLAN-Kennungen durch Anbieter von Navigations-Datenbanken, oder das Speichern von kommunikationsbezogenen Gerätedaten (z.B. MAC-Adresse, IMSI) durch Anbieter elektronischer Kommunikationsdienste oder Netzbetreiber.

Der Schutzgedanke der Norm wird nicht klar.

- Auf die Anbieter von elektronischen Kommunikationsdiensten und die Betreiber elektronischer Kommunikationsnetze lässt sich die Vorschrift nicht sinnvoll anwenden. Es ist nicht nachvollziehbar, wieso für diesen Anbieterkreis Endeinrichtungs-Informationen einen anderen Schutz benötigen als andere Kommunikationsmetadaten. Ganz im Gegenteil spricht viel dafür, für diese Informationen exakt denselben Schutz vorzusehen wie für andere Kommunikationsmetadaten.
- Für alle anderen potenziellen Normadressaten (Art. 8 ist als „Jedermannspflicht“ formuliert) erscheint der Schutzanspruch des Art. 8 Abs. 2 überzogen. Für diesen Anbieterkreis sind derartige Daten von vornherein keine Kommunikationsdaten (zur unklaren Begriffsdefinition siehe aber oben, Abschnitte „Fehlende Struktur beim personalen Anwendungsbereich“ und „Präzisierung des Anwendungsbereichs des Telekommunikationsgeheimnisses in Art. 5“).
- Zudem ist fragwürdig, wieso ausgerechnet die Daten, die von den Endgeräten ausgesendet werden, besonders geschützt werden sollten. Derartige Daten sind zwar Identifikatoren, aber sie sind grundsätzlich für eine unbestimmte Öffentlichkeit bestimmt, vergleichbar einer Telefonnummer. Es sind somit gerade keine Daten, die der jeweils Betroffene als besonders vertraulich betrachtet, sondern – ganz im Gegenteil – Daten ohne besonderen Privatsphärenbezug.
- Eventuell hat die Kommission bei Art. 6 Abs. 2 – ohne dies deutlich zu machen – einen ganz konkreten Anbieterkreis im Auge gehabt, nämlich die Anbieter von Diensten der Informationsgesellschaft, die als Betreiber von Webseiten oder von darauf enthaltenen Werbeflächen Endgerätedaten verwenden, um Informationen

über ihre Nutzer zusammenzutragen. Sollte diese Vermutung zutreffend sein, ist immer noch fragwürdig, wieso die ePrivacy-Verordnung die Verwendung der ausgesendeten Gerätedaten einschränkt. Das Abspeichern von nutzerbezogenen Daten in „Server-Logs“ und vergleichbaren Daten ist eine eingeübte Praxis, die etlichen legitimen Zwecken dient; hierzu zählt die Abwehr von Hacking- und DDoS-Angriffen oder die Vermeidung von Spam (beispielsweise in Kommentarspalten von Weblogs). Auch die Rechtsverfolgung im Internet, beispielsweise nach strafrechtlich relevanten Äußerungen in Social Networks, setzt zu einem gewissen Maß voraus, dass Diensteanbieter nutzerbezogene Daten speichern. Und soweit es grundsätzlich um die Speicherung von Nutzerprofilen geht, so ist das Profiling in der DSGVO bereits geregelt. Es ist nicht nachvollziehbar, wieso gerätebezogenes Profiling anders reguliert werden sollte als „normales“ Profiling.

Klarstellung des Normadressaten in Art. 9 Abs. 3

Vorschlag:

In Art. 9 Abs. 3 sollte präzisiert werden, wer die Pflicht hat, die Erinnerung vorzunehmen bzw. zu gewährleisten, dass die Erinnerung vorgenommen wird.

Begründung:

Art. 9 Abs. 3 wählt eine undeutliche Passiv-Formulierung, so dass nicht deutlich wird, wer eigentlich Normadressat der Vorschrift sein soll (siehe auch oben, Abschnitt „Personeller Anwendungsbereich“). Es sollte klargestellt werden, wer diese Pflicht konkret zu erfüllen hat.

Hinsichtlich einer möglichen Präzisierung zum Kopplungsverbot verweisen wir auf den Abschnitt „Ausweitung auf OTT-Anbieter“; betreffend des Verhältnisses von Art. 9 Abs. 2 zu Art. Art. 21 Abs. 5 DSGVO verweisen wir auf den Abschnitt „Verhältnis zur DSGVO“.

Fragwürdige Regulierung von Browser-Software in Art. 10

Vorschlag:

- Art. 10 sollte präzise und verkehrsübliche Begriffe verwenden. Statt von „in Verkehr gebrachte Software, die eine elektronische Kommunikation erlaubt, darunter auch das Abrufen und Darstellen von Informationen aus dem Internet“ sollte von „Browsern“ die Rede sein. Statt von „Informationen in der Endeinrichtung“ sollte von „Cookies“ gesprochen werden.
- In Art. 10 Abs. 3 sollte klargestellt werden, dass eine Pflicht zur Anzeige der Informationen nur insoweit besteht, als Nutzer ein Softwareupdate heruntergeladen und installiert haben.

Begründung:

Die Regelung in Art. 10 des Entwurfs betrifft Produkteigenschaften von Software, die elektronische Kommunikation ermöglicht. Sie trifft damit keine Regelungen, die den Vorgang der Telekommunikation selbst betreffen. Inhaltlich sieht sie vor, dass eine solche Software dazu geeignet sein muss, zu verhindern, dass andere als der Nutzer der Software selbst Informationen auf seinem Rechner speichert oder schon gespeicherte Informationen verarbeitet. Es geht darum, dem Nutzer Mittel zur Verfügung zu stellen, damit er die Nutzung von Cookies oder anderer Tracking-Verfahren verhindern kann, die sein Verhalten im Internet nachzeichnen. Die Software soll darüber hinaus den Nutzer über ihre Datenschutzeinstellungen bei der Installation informieren und seine Zustimmung zu Ihnen verlangen, bevor die Installation beendet wird.

Die Vorschrift soll erreichen, dass Browser und vergleichbare Software den Nutzer befähigen, seine Datenschutzeinstellungen bewusst zu wählen. Sie schreibt auch keinesfalls vor, dass die Standardeinstellungen datenschutzgünstig so gewählt werden, dass die Verwendung gängiger Verfahren verhindert wird. Das Ziel der Vorschrift ist zu begrüßen. Zu begrüßen ist auch, dass nicht zwingend vorgeschrieben wird, dass besonders datenschutzbegünstigende Voreinstellungen gewählt werden. Eine solche Vorgabe könnte die Nutzung des Internet massiv behindern, weil die dann vorgeschriebenen Voreinstellungen die Nutzung zahlreiche Internetauftritte behindert oder sogar unmöglich macht.

Der Wortlaut der Vorschrift verwendet zudem die sehr umständliche Beschreibung von *„Software, die eine elektronische Kommunikation erlaubt, darunter auch das Abrufen und Darstellen von Informationen aus dem Internet“.* Anders als offenbar intendiert würde diese sehr breite Definition nicht nur Browser erfassen, sondern annähernd alle Arten von Software, die im weitesten Sinn Bezug zum Internet haben. Unter anderem würde eine rein wortlautbezogene Auslegung auch annähernd jede App auf Mobilgeräten erfassen, sowie sonstige Software auf Routern, Modems und sonstigen Kommunikationskomponenten – bis hin zu den Betriebssystemen von Telefonanlagen und Handys.

Fraglich ist außerdem was unter einer „Information“ zu verstehen ist, die *„Dritte […] in der Endeinrichtung eines Endnutzers speichern“* bzw. in der Endeinrichtung verarbeiten. Der Fachausschuss weist darauf hin, dass das vermeintlich flüchtige Nutzen von Webseiten beim „Browsing“ in technischer Hinsicht immer einen Download darstellt, und dass viele der Web-Inhalte auch für längere Zeit im Gerät des Nutzers gespeichert bleiben (z.B. in den Download-Dateien oder im Cache-Speicher). Sowohl das „Ob“ des Downloads als auch die Dauer der Speicherung steht dabei aber immer im Ermessen des Nutzers und kann von ihm konfiguriert werden. Auch der externe Zugriff auf Dateien und Kapazitäten, die im Endgerät des Nutzers vorgehalten werden, ist technisch gesehen ein Standard-Vorgang beim Angebot von Web-Inhalten (z.B. bei der Nutzung von Javascript oder von Apps). Er unterliegt aber bereits jetzt der vollen Kontrolle der Nutzer (durch Konfigurationsmöglichkeiten).

Ob die Verortung der Vorschrift in einer speziell auf Telekommunikation gerichteten Verordnung zweckmäßig ist, erscheint außerdem zweifelhaft (siehe dazu auch oben, Abschnitt „Personeller Anwendungsbereich“). Art. 10 bezieht sich auch keinesfalls nur auf Daten der Telekommunikation. Vielmehr geht es auch um Daten, die bei einem elektronischen Bestellvorgang anfallen und sogar um Daten, die überhaupt nichts mit Telekommunikation zu tun haben. Insoweit fällt die Vorschrift aus dem Rahmen der sonst in der ePrivacy-VO enthaltenen Regelungen.

Unterstellt, es bleibt bei dem Ansatz, die Konfigurationsmöglichkeiten von Browsersoftware zu regulieren, wird angeregt, dass die Software auch so gestaltet

werden muss, dass der Nutzer die Datenschutzeinstellungen leicht ändern kann. Er muss nicht nur informiert, sondern auch in die Lage versetzt werden, die ihm passenden Sicherheitseinstellungen auszuwählen und sie nach seinen (sich möglicherweise ändernden) Bedürfnissen einzurichten und abzuändern. Ohne eine solche Möglichkeit ist die Vorschrift unvollständig. Eine nur auf komplizierten Wegen änderbare Software macht den Nutzer nicht autonom.

Zuletzt ist anzumerken, dass die in Art. 10 Abs. 3 geregelte Pflicht, auf die Konfigurationsmöglichkeit des Browsers spätestens zum 25. August hinzuweisen, nur erfüllt werden kann, wenn die Nutzer ein Update für die Software herunterladen und installieren. Hierauf haben die Anbieter von Browsersoftware keinen abschließenden Einfluss. Es sollte deshalb präzisiert werden, dass die Pflicht unter dem Vorbehalt steht, dass die Nutzer ein bereitgestelltes Update herunterladen und installieren.

Fehlende grundrechtsschützende Formulierungen in Art. 11

Vorschlag:

- Art. 11 sollte die zuletzt ergangenen Urteile des EuGH für eine einschränkende Präzisierung der Eingriffsvoraussetzungen nutzen, anstatt den Tatbestand noch schwammiger zu machen. Hilfsweise sollte es zumindest beim Wortlaut von Art. 15 der ePrivacy-RL bleiben.
- Der Wegfall der Regelung zur Vorratsdatenspeicherung ist nicht nachvollziehbar. An der Rechtslage kann der Wegfall nichts ändern, da die Einschränkungen zur Zulässigkeit einer Vorratsdatenspeicherung sich unmittelbar aus der EU-Grundrechtecharta ergeben. Der Wegfall der Vorschrift beeinträchtigt aber die Transparenz und Klarheit der Norm.
- Art. 11 Abs. 2 ist viel zu unpräzise formuliert und ist in einer „ePrivacy-Verordnung“ zudem deplatziert. Die Vorschrift sollte nicht übernommen, sondern allenfalls (präziser) in den EECC eingefügt werden.

Begründung:

Art. 11 des Entwurfs der VO enthält Regelungen, die es den einzelnen Staaten erlauben, für bestimmte, in Art. 23 (1) (a) bis (e) DSGVO genannte öffentliche Interessen das Telekommunikationsgeheimnis einzuschränken. Die Ergänzung der Eingriffsgründe erklärt sich durch eine Übernahme von Regelungen aus der Datenschutzgrundverordnung (VO (EU) 2016/679 v. 27.4.2016). Sie beachtet aber die besondere Schutzwürdigkeit der Telekommunikationsdaten nicht (dazu oben, Abschnitt „Einleitung“).

Eine ähnliche Regelung enthielt bislang Art. 15 Abs. 1 Richtlinie 2002/58/EG (E-Privacy-Richtlinie). Die neue Regelung scheint dabei die Eingriffsmöglichkeiten zu erweitern. Zu den öffentlichen Interessen, die Eingriffe rechtfertigen, gehören jetzt neben der Landesverteidigung und der Verhütung, Aufdeckung und Verfolgung von Straftaten auch die nationaler Sicherheit und sonstige wichtige Ziele des allgemeinen öffentlichen Interesses der Union oder ihrer Mitgliedsstaaten. Gemeint sind damit auch wirtschaftliche und finanzielle Interessen der Union und ihrer Mitgliedsstaaten. Zudem entfällt die Regelung des bisherigen Art. 15 Abs. 1 S. 2 Richtlinie 2002/58/EG, die eine Vorratsdatenspeicherung ausdrücklich erlaubte, dabei jedoch an enge Bedingungen knüpfte.

Die Vorschrift enthält im Unterschied zu Art. 15 Abs. 1 der Richtlinie 2002/58/EG keine näheren Regeln, unter welchen Voraussetzungen Eingriffe möglich sind. Sie verlangt nur, dass die Eingriffe den Kern der Grundrechte erhalten und notwendig, angemessen und verhältnismäßig sind. Die Struktur der Regelung entspricht der von Art. 15 Abs. 1 Richtlinie 2002/58/EG. Der Normcharakter entspricht dem einer Richtlinie, nicht dem einer Verordnung.

Darüber hinaus bleibt bereits das Ziel der beabsichtigten Regelungen unklar: Während es in der Vorbemerkung des Entwurfs heißt, es sei beabsichtigt, *„ein hohes Schutzniveau der Privatsphäre der Nutzer elektronischer Kommunikationsdienste“* zu gewährleisten, ist in Erwägung 42 des Entwurfs zu lesen, die geplante Verordnung ziele auf die *„Gewährleistung eines gleichwertigen Datenschutzniveaus“*, was die Frage aufwirft, welches Maß an nationalem Datenschutz den Orientierungspunkt bilden soll.

Die Erweiterung der möglichen Gründe für einen Eingriff in das Telekommunikationsgeheimnis ist schon inhaltlich bedenklich. Was eine Gefährdung der nationalen Sicherheit ist, die weder mit der Verteidigung noch mit der Bekämpfung von Straftaten in Zusammenhang steht, ist nicht erkennbar. Es bleibt damit völlig unklar, warum dieser zusätzliche Rechtfertigungsgrund in den Gesetzestext aufgenommen worden ist. Noch stärker gilt dies für den weiteren Rechtfertigungsgrund der Gefährdung allgemeiner Interessen. Dazu gehören schon nach dem Verordnungstext auch finanzielle Interessen des Staates. Insgesamt werden die Eingriffsmöglichkeiten deutlich erweitert.

Die Erweiterung der Möglichkeiten der Einschränkung des Grundsatzes der Vertraulichkeit bei der Nutzung elektronischer Kommunikationsdienste ist bei Zugrundelegung der wesentlichen Maßgaben des Urteils des EuGH vom 21. Dezember 2016 (C-203/15 und C-698/15) außerdem mit dem EU-Recht unvereinbar. Die Luxemburger Richter hatten in dem Urteil betont, dass Art. 15 Abs. 1 S. 1 der E-Privacy-RL als Ausnahme im Lichte der Art. 7, 8 und 11 der GrCH eng auszulegen, abschließend sei und eine Vorratsdatenspeicherung nur zum Zwecke der Kriminalitätsbekämpfung zulässig sei. Diese Grenze, die auch für andere Eingriffe in die betroffenen Grundrechte gilt, beachtet der Entwurf nicht.

Fragwürdig ist, dass Art. Art. 15 Abs. 1 Satz 2 Richtlinie 2002/58/EG nicht übernommen und durch keine andere Regelung ersetzt wird. Die Vorratsdatenspeicherung wird dadurch nicht verboten, sie wird nur nicht mehr ausdrücklich erwähnt. Der Verordnungsentwurf vermeidet so die nähere Auseinandersetzung mit den Grundsätzen des EuGH, der sich mit der Regelung in Art. 15 S. 2 Richtlinie 2002/58/EG in seiner Entscheidung vom 21.12.2016 (C-203/15 und C 698/15) befasst und sie stark einschränkend ausgelegt hat. Der EuGH hat in dem genannten Urteil betont, dass selbst zur Bekämpfung von organisierter Kriminalität und Terrorismus keine *„allgemeine und unterschiedslose Vorratsdatenspeicherung sämtlicher Verkehrs- und Standortdaten“* zulässig sei, weil auch in diesem Fall der Ausnahmecharakter der Vorratsdatenspeicherung verloren ginge. Eine entsprechende Einschränkung sucht man in dem Vorschlag vergebens.

Angesichts dieser Rechtsprechung verwundert die Erweiterung der Eingriffsmöglichkeiten noch mehr. Der EuGH hat nicht zum ersten Mal (vgl. Urt. v. 8.4.2014 C-293/12 und C 594-12) den hohen Rang insbesondere des Schutzes der Vertraulichkeit der Telekommunikation betont und sich dabei auf die Art. 7, 8 und 11 der Charta der Grundrechte der Europäischen Union (GrCH) berufen. Diese Grundrechte sind nicht nur bei Regelungen zur Vorratsdatenspeicherung, sondern auch jedem sonstigen Eingriff in die von der ePrivacy-VO geschützten Grundrechte zu beachten. Dies gilt in besonderem Maße für das „Mithören“ bzw. „Mitlesen“ von Telekommunikation. Dies ist nur zulässig, wenn es zur Bekämpfung schwerster Formen der Kriminalität zwingend erforderlich ist. Nur dann ist ja auch der Zugriff auf Daten möglich, die auf Grund von Regelungen zur Vorratsdatenspeicherung gespeichert sind (so EuGH, Urt. v. 21.12.2016, C-203/15 und C698/15). Aber auch die bloße Speicherung bzw. Kenntnisnahme von Metadaten der Telekommunikation kann leicht zu umfangreichen Persönlichkeitsprofilen und damit zu massiven Eingriffen in das Privatleben und auch der Meinungsfreiheit führen. Gerade deshalb sind Eingriffe nur in seltenen Fällen zulässig (EuGH, Urt. v. 21.12.2016, C-203/15 und C698/15).

Art. 11 Abs. 1 des Entwurfs greift dies nicht explizit auf. Vielmehr ergeben sich diese Beschränkungen nur durch eine entsprechende Auslegung der Normvorschrift, die Eingriffe nur zulässt, wenn sie in einer demokratischen Gesellschaft notwendig, angemessen und verhältnismäßig sind und die Grundrechte gewahrt sind. All diese Voraussetzungen werden die Staaten bei ihren Regelungen zu beachten haben (zu den sich daraus für den deutschen Gesetzgeber ergebenden Grenzen vgl. schon DAV-Stellungnahme 50/16).

Der Verordnungsgeber sollte die vom EuGH gezogenen Grenzen nicht zum Anlass nehmen, einen ohnehin schon unpräzisen Tatbestand noch weiter aufzuweichen, sondern zu einer Präzisierung von Art. 11 Abs. 1 gegenüber Art. 15 Abs. 1 Richtlinie 202/58/EG. Dies wäre schon deswegen angezeigt, weil es jetzt um eine Verordnung und nicht nur um eine Richtlinie geht. Hier ist der EU-Gesetzgeber aufgerufen, die sich aus dem EU-Primärrecht ergebenden Grenzen der Eingriffsmöglichkeiten auch selbst zu bestimmen und dies nicht dem einzelstaatlichen Gesetzgeber zu überlassen. Die geplante Erweiterung der Eingriffsmöglichkeiten ist damit nicht zu vereinbaren. Sie sollte daher entfallen.

Noch stärkere Bedenken ergeben sich hinsichtlich von Art. 11 Abs. 2 des Entwurfs. Diese Norm verpflichtet die Anbieter von Telekommunikation dazu, interne Prozeduren einzurichten, um Anforderungen der Behörden auf Zugang zu Telekommunikationsdaten zu genügen. Betroffen sind sowohl der Inhalt von Telekommunikation als auch bei der Kommunikation entstehende Metadaten. Auf Anforderung müssen die Anbieter auch die Aufsichtsbehörden über diese Prozeduren unterrichten. Auch hier fehlen nähere Detaillierungen der Regelung, obwohl diese Norm im Gegensatz zu Art. 11 Abs. 1 des Entwurfs die Anbieter unmittelbar verpflichtet und nicht nur die Einzelstaaten zu Regelungen ermächtigt. Die Verpflichtung bezieht sich dabei auf Eingriffsbefugnisse staatlicher Behörden, die der Entwurf selbst gar nicht regelt. Die Entwurfsverfasser können daher gar nicht wissen, welchen Umfang die Maßnahmen haben und welche Kosten entstehen. Die Vorschrift ist schon allein deshalb unverhältnismäßig. Sie ist darüber hinaus extrem unbestimmt. Sie zeigt noch nicht einmal im Ansatz auf, um welche Maßnahmen es eigentlich geht.

Die Vorschrift sollte daher darauf beschränkt werden, den Staaten zu erlauben, den Telekommunikationsanbietern solche Pflichten im Zusammenhang mit Eingriffsbefugnissen aufzuerlegen, die sie auf Grund von Art. 11 Abs. 1 angeordnet haben.

Unverhältnismäßig ist die Vorschrift zusätzlich dadurch, dass die Pflichten in keiner Weise beschränkt sind. Jedenfalls ist der Vorschrift nicht zu entnehmen, dass die Maßnahmen nur dann ergriffen werden müssen, wenn sie ihrerseits angemessen und verhältnismäßig sind. Der EuGH hatte in dem Urteil vom 21. Dezember 2016 darauf hingewiesen, dass präzise Regelungen des „Wie“ der Vorratsdatenspeicherung und des damit verbundenen Abrufprocedere („2. Stufe“ = Abruf der gespeicherten Daten bei den Unternehmen durch die Behörden) bereits deswegen erforderlich seien, weil nur auf diese Weise eine echte Kontrolle der Behörden ermöglicht werde.

Dem genügt der beabsichtigte Art. 11 Abs. 2 nicht einmal im Ansatz: Weder findet sich im Gesetzestext etwas zu der vom EuGH für grundsätzlich notwendig erachteten vorigen Kontrolle der Einhaltung der Voraussetzungen für den Abruf durch ein Gericht oder eine unabhängige Stelle, noch dazu, dass die von dem Datenabruf betroffenen

Personen im Nachhinein regelmäßig über die Maßnahme informiert werden müssen. Schließlich fehlen Regelungen zu dem vom EuGH betonten *„besonders hohen Schutz- und Sicherheitsniveau“* und zur Sicherstellung der unwiderruflichen Löschung der Daten bei den Betreibern nach Ablauf der Speicherfrist.

Auch der Aufwand für den Diensteanbieter spielt dem Text der Vorschrift nach für den Umfang der Pflichten keine Rolle. Der Aufwand für solche Maßnahmen kann aber (insbesondere bei kleineren Anbietern und Anbietern von OTT-Diensten) Geschäftsmodelle unwirtschaftlich machen. Dies muss der Gesetzgeber durch entsprechende Regelungen berücksichtigen, da auch die Anbieter durch Art. 16 GrCH in ihrer unternehmerischen Freiheit geschützt sind. Möglich wäre eine Übernahme der Kosten für solche Maßnahmen durch den anordnenden Staat oder eine Begrenzung der gebotenen Maßnahmen auf wirtschaftlich, im Hinblick auf die Schwere der zu bekämpfenden Gefahren, vertretbare Maßnahmen. Ohne solche Regelungen ist die Norm selbst dann nicht akzeptabel, wenn sie lediglich eine Regelungsbefugnis für die Einzelstaaten enthält.

Insgesamt sollte Art. 11 Abs. 2 des Entwurfs daher in gleicher Weise wie Art. 11 Abs. 1 des Entwurfs lediglich die Befugnis für die Einzelstaaten vorsehen, die Diensteanbieter zu den jeweiligen Anlässen auch unter Berücksichtigung der Interessen der Anbieter angemessenen Maßnahmen zu verpflichten, die es den Behörden ermöglichen, ihre Eingriffsbefugnisse auszuüben. Kosten wären ggfs. von den Einzelstaaten zu tragen.

Zusammenarbeit der Aufsichtsbehörden in Art. 18

Vorschlag:

- In Art. 18 sollte klargestellt werden, dass die Datenschutzaufsichtsbehörden bei der Wahrnehmung ihrer Kontrollfunktion nach der ePrivacy-VO die Regelungen des Telekommunikationsrechts berücksichtigen müssen, insbesondere die Regulierungsprinzipien (Art. 8 der Rahmenrichtlinie, 2002/21/EG).
- Der Satz „Die Aufgaben und Befugnisse der Aufsichtsbehörden werden in Bezug auf die Endnutzer wahrgenommen“ sollte gestrichen werden. Die Aufsichtsbefugnis

sollte sich nicht auf eine bestimmte Betroffenengruppe beziehen, sondern neutral auf die Vorschriften der ePrivacy-VO.

- Die Ausnahme „wenn dies zweckmäßig ist“ in Art. 18 Abs. 2 sollte gestrichen werden.

Begründung:

Grundsätzlich begrüßenswert ist, dass die ePrivacy-VO die Zuständigkeit für den Telekommunikationsdatenschutz von den nationalen sektorspezifischen Regulierungsbehörden auf die jeweiligen Datenschutzbehörden verlagert. Dies entspricht dem Schutzbedarf dieser Daten und der weitreichenden Schnittmenge zwischen dem Datenschutz und dem Schutz von Telekommunikationsdaten (als Ausprägung des Fernmeldegeheimnisses).

Die ePrivacy-Verordnung sollte allerdings sicherstellen, dass weiterhin auch die Kompetenzen der telekommunikations-spezifischen Regulierungsbehörden genutzt werden. Zum einen sind diese Behörden aufgrund ihrer Zuständigkeit für die übrigen Vorschriften der Telekommunikationsregulierung mit den Besonderheiten der Telekommunikationsregulierung besser vertraut. Zum anderen sieht die ePrivacy-Verordnung Regelungen vor, die ausschließlich telekommunikationsrechtlicher Natur sind, ohne einen Bezug zu personenbezogenen Daten zu haben. In solchen Bereichen lassen sich datenschutzrechtliche Gedanken nicht übertragen (zur Sonderverpflichtung von Anbietern im Telekommunikationsbereich siehe auch oben, Abschnitt „Präzisierung des Anwendungsbereichs des Telekommunikationsgeheimnisses in Art. 5“). Nur eine gegenseitige Konsultationspflicht bei Sachverhalten im Schnittmengenbereich kann sicherstellen, dass Datenschutzbehörden die Besonderheiten des Telekommunikations-Datenschutzrechts (als Ausprägung des Fernmeldegeheimnisses) im Blick behalten.

Vor diesem Hintergrund ist insbesondere der letzte Satz in Art. 18 Abs. 1 abzulehnen und sollte herausgenommen werden. Wenn die Datenschutzbehörden Teil der sektorspezifischen Regulierung des TK-Sektors werden sollen, dann darf sich diese Befugnis nicht auf „Endnutzer“ beschränken; vielmehr müssen die Behörden dann eine neutrale Regulierung gewährleisten, die nicht primär eine bestimmte Gruppe schützen soll, sondern gleichermaßen auch die Perspektiven der anderen Beteiligten in den Blick

nimmt und sich primär an den Regulierungsprinzipien des Telekommunikationsrechts orientiert (vgl. dazu bislang noch Art. 8 der Rahmenrichtlinie 2002/21/EG). Dies sollte in der ePrivacy-VO so auch klargestellt werden.

Auch die Einschränkung der Konsultationspflicht der Nationalen Regulierungsbehörden in Art. 18 Abs. 2 („wenn dies zweckmäßig ist“) ist aus diesem Grund falsch und zurückzuweisen. Die Pflicht zur Zusammenarbeit mit den Nationalen Regulierungsbehörden sollte für alle Regelungen der ePrivacy-VO grundsätzlich und ohne Vorbehalt festgeschrieben werden.