Stellungnahme des Europäischen Wirtschafts- und Sozialausschusses 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)“

(COM(2017) 10 final — 2017/0003 (COD))

(2017/C 345/23)

Berichterstatterin: **Laure BATUT**

Befassung	Europäisches Parlament, 16.2.2017
	Rat, 9.3.2017
Rechtsgrundlage	Artikel 16 und Artikel 114 AEUV
Zuständige Fachgruppe	Verkehr, Energie, Infrastrukturen, Informationsgesellschaft
Annahme in der Fachgruppe	14.6.2017
Verabschiedung auf der Plenartagung	5.7.2017
Plenartagung Nr.	527
Abstimmungsergebnis (Ja-Stimmen/Nein-Stimmen/Enthaltungen)	155/0/5

1. **Schlussfolgerungen und Empfehlungen**

1.1. Der Europäische Wirtschafts- und Sozialausschuss bedauert lebhaft, dass es angesichts der Überschneidung, des Umfangs und der Verflechtung der Rechtsvorlagen zum Datenschutz sowie des für ihr Verständnis notwendigen Hin- und Herblätterns unwahrscheinlich ist, dass sie, von Insidern abgesehen, wirklich gelesen und umgesetzt werden, und ihr Mehrwert für Bürger nicht ersichtlich ist, wobei dieser Aspekt in dem Verordnungsvorschlag ohnehin nicht berücksichtigt wird. Er empfiehlt, eine zusammenfassende Broschüre online zu stellen, in der sie für die Allgemeinheit verständlich erläutert und zugänglich gemacht werden.

1.2. Der EWSA hebt hervor, dass die Europäische Kommission unter den im Rahmen der Folgenabschätzung geprüften Politikoptionen diejenige ausgewählt hat, die auf eine „maßvolle Stärkung der Privatsphäre“ abhebt. Steht dahinter das Bemühen um einen Ausgleich mit den Interessen der Industrie? Die Europäische Kommission legt nicht dar, inwiefern eine „weitreichende Stärkung der Privatsphäre“ die Interessen der Industrie beeinträchtigt hätte. Durch diese Haltung wird der Text von Anfang an geschwächt.

1.3. Der EWSA empfiehlt, dass die Europäische Kommission

1. berücksichtigt, dass mittlerweile aus jeder Information Daten generiert und auf elektronischem Weg weitergegeben werden können, was sich auf die Privatsphäre von juristischen und natürlichen Personen auswirkt;

2. verdeutlicht, dass sich der Vorschlag (Artikel 5, 8 und 11) auf die Charta der Grundrechte der Europäischen Union und die Menschenrechtscharta stützt und inwiefern mittels nationaler Rechtsvorschriften Beschränkungen möglich sind (Erwägungsgrund 26);

3. die Artikel 5 und 6 des Vorschlags überprüft. Internet und Mobiltelefonie, die elektronische Kommunikation ermöglichen, sind zu Dienstleistungen von allgemeinem Interesse geworden, die universell zugänglich, verfügbar und erschwinglich sein müssen, ohne dass die Verbraucher gezwungen sind, dafür der Verarbeitung ihrer Daten durch den Provider oder Betreiber zuzustimmen. Es muss daher die Verpflichtung vorgesehen werden, dass den Nutzern systematisch anhand verständlicher Informationen die Möglichkeit gegeben werden muss, Cookies, Webtracking usw. abzulehnen;

4. klar ansagt, dass die zur Ergänzung der Datenschutz-Grundverordnung (DS-GVO) vorgeschlagene *Lex specialis* auch im Einklang mit deren Grundsätzen steht und nicht den dadurch gewährleisteten Schutz aushöhlt und dass jede Form der Verarbeitung, auch statistische Auswertungen (*web audience measuring*), auf der Grundlage der DS-GVO (Artikel 8) erfolgen müssen;

5. dafür sorgt, dass der Wortlaut der Verordnung und der Inhalt der Durchführungsmaßnahmen verständlich formuliert sind, damit ein Zuviel an delegierten Rechtsakten vermieden und den Bürgern und Unternehmen Regulierungssicherheit geboten wird;

6. eine Strategie entwickelt, aus der für alle Verbraucher klar hervorgeht, dass die EU weiterhin an der Wahrung der Menschenrechte festhält und dass es ihr ein Anliegen ist, den Schutz der Privatsphäre nicht nur seitens der Betreiber von elektronischen Kommunikationsdiensten, sondern auch seitens der „Over-the-top" (OTT)-Anbieter sicherzustellen;

7. verhindert, dass Datenschutzlücken im Gesundheitsbereich Einbrüche in die Privatsphäre und die Nutzung personenbezogener Daten zu gewerblichen Zwecken im Wege elektronischer Kommunikation ermöglichen;

8. sich mit der kollaborativen Wirtschaft und der Übermittlung und Nutzung von Daten über elektronische Kommunikation auf digitalen Plattformen, die häufig außerhalb der EU angesiedelt sind, befasst;

9. dem Internet der Dinge Rechnung trägt, das sehr invasiv ist und im Zuge der elektronischen Übermittlung von Daten Beeinträchtigungen des Privatlebens Tür und Tor öffnet;

10. beachtet, was nach dem Datentransfer geschieht, und die von den Anwendern gespeicherten, zumeist privaten Daten schützt (schnittstellenunabhängig und einschließlich Cloud Computing);

11. den Schutz automatisierter (Maschine-Maschine, M2M) Datenübertragung klärt und in einem Artikel, nicht nur in einem Erwägungsgrund (12), festlegt;

12. ein (bei der GD Justiz angesiedeltes) allgemein zugängliches und verständliches europäisches Portal errichtet, über das die Bürger Zugang zu europäischen und nationalen Schriften, zu Rechtsmitteln und zu Gerichtsentscheidungen haben und das ihnen dabei hilft, sich im Dschungel der Schriften zurechtzufinden und ihre Rechte wahrzunehmen (beispielsweise zum Verständnis des Erwägungsgrunds 25 und der Artikel 12 und 13);

13. den Überwachungsbehörden Mittel an die Hand gibt, ihre Aufgaben zu erfüllen (Europäischer Datenschutzbeauftragter, nationale Behörden);

14. den Verbrauchern im Wege einer neuen Richtlinie, die über die Empfehlung C(2013) 3539 hinausgeht, die Möglichkeit gibt, europäische Sammelklagen einzureichen, um ihre Rechte geltend zu machen ([1]).

2. **Legislativer Hintergrund**

2.1. Seit dem Inkrafttreten der **Richtlinien** 95/46/EG und **2002/58/EG** ([2]) über den Schutz der Privatsphäre in der elektronischen Kommunikation haben sich die elektronischen Kommunikationsnetze erheblich weiterentwickelt.

2.2. **2016 wurde die Datenschutz-Grundverordnung (DS-GVO) angenommen** (Verordnung (EU) Nr. 2016/679), die Grundlage für die einschlägigen Maßnahmen ist und die grundlegenden Verfahrensweisen, auch für justizielle Daten, festlegt. Dieser Verordnung zufolge dürfen personenbezogene Daten nur unter Einhaltung strengster Regeln, für legitime Zwecke und unter Wahrung der Vertraulichkeit erhoben werden (Artikel 5 der DS-GVO).

2.2.1. Die Europäische Kommission hat im **Oktober 2016** einen 300 Seiten starken Vorschlag für eine Richtlinie über den europäischen Kodex für die elektronische Kommunikation ([3]) vorgelegt, der noch nicht angenommen worden ist, auf den sie sich jedoch für einige Definitionen stützt, die weder in der DS-GVO noch in der vorliegenden Richtlinie vorkommen.

2.2.2. Im **Januar 2017** legte die Europäische Kommission **zwei Verordnungsvorschläge** zu Datenschutzaspekten vor, in denen sie sich auf die DS-GVO stützt: zum einen den Vorschlag für eine Verordnung zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe, Einrichtungen und sonstigen Stellen der Union (**COM(2017) 8 final**, Berichterstatter Jorge Pegado Liz) und zum anderen den Vorschlag für eine Verordnung über die Achtung des Privatlebens und den Schutz personenbezogener Daten (**COM(2017) 10 final**), der Gegenstand dieser Stellungnahme ist.

2.3. Diese drei Rechtsinstrumente sollen **ab dem gleichen Zeitpunkt, dem 25. Mai 2018, gelten**. Sie haben zum Ziel, die Rechte und die Überwachungsverfahren zu harmonisieren.

2.4. Zur Erleichterung dieses Vorhabens wurde als Rechtsinstrument zur Sicherstellung des Schutzes der Privatsphäre eine Verordnung anstatt einer Richtlinie gewählt.

([1]) Generaldirektion Justiz, IP/13/525 und Memo13/531 vom 11.6.2013.

([2]) In Artikel 13 der Richtlinie 2002/58/EG werden unerbetene Nachrichten (Spam) untersagt, und in der Änderungsrichtlinie von 2009 wird der Opt-in-Grundsatz eingeführt, demzufolge „Nachrichten zum Zwecke der Direktwerbung" nur mit Einwilligung der betreffenden Teilnehmer oder Nutzer versandt werden dürfen.

([3]) COM(2016) 590 final vom 12.10.2016, Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über den europäischen Kodex für die elektronische Kommunikation, S. 2 (ABl. C 125 vom 21.4.2017, S. 56).

3. **Einleitung**

3.1. Die Zivilgesellschaft möchte wissen, ob die EU in der sich abzeichnenden digitalen Welt einen Mehrwert bringt und Freiräume für eine unbehelligte persönliche Entfaltung sicherstellt.

3.2. Durch die laufende Erzeugung von Daten werden alle Nutzer überall erfassbar und identifizierbar. Die Datenverarbeitung, die zumeist in Zentren außerhalb Europas stattfindet, gibt Anlass zu Sorge.

3.3. Big Data (Massendaten) sind zu einer Währung geworden; ihre intelligente Verarbeitung ermöglicht Data-Profiling und die gewinnbringende Vermarktung von Informationen über natürliche und juristische Personen, häufig ohne Wissen der Betroffenen.

3.4. Vor allem aber macht das Auftreten neuer Akteure im Bereich der Datenverarbeitung, bei denen es sich nicht um Internet-Provider handelt, eine Überarbeitung der einschlägigen Rechtstexte erforderlich.

4. **Zusammenfassung des Vorschlags**

4.1. Mit diesem Verordnungsvorschlag möchte die Europäische Kommission einen Ausgleich der Verbraucher- und Industrieinteressen erreichen:

— sie erlaubt die Weiterverwendung der Daten durch die Betreiber, überlässt die Kontrolle darüber aber dem Endnutzer, der ausdrücklich seine Einwilligung erteilen muss;

— sie fordert von den Betreibern Auskunft über den Verwendungszweck;

— sie wählt mit der Politikoption 3 eine „maßvolle Stärkung der Privatsphäre“ anstatt der in Politikoption 4 vorgesehenen „weitreichenden Stärkung der Privatsphäre“.

4.2. Ziel des Vorschlags ist die Anwendung der Datenschutz-Grundverordnung (DS-GVO), die ebenso wie die Vertraulichkeit der personenbezogenen Daten und das Recht auf Vergessenwerden allgemeine Geltung hat, auf die Achtung des Privatlebens und den Schutz personenbezogener Daten im Rahmen der Telekommunikation; es wird die Einführung von strengeren Vorschriften zum Schutz des Privatlebens, von koordinierten Aufsichtsmaßnahmen und von Sanktionen vorgeschlagen.

4.3. Es werden keine spezifischen Maßnahmen für von den Nutzern selbst verursachte Datenschutzverletzungen vorgesehen, doch wird von Anfang an (Artikel 5) der Grundsatz der Vertraulichkeit elektronischer Kommunikationsdaten bekräftigt.

4.4. Provider können elektronische Kommunikationsinhalte verarbeiten,

— um einen Dienst für einen Endnutzer zu erbringen, der seine Einwilligung gegeben hat;

— wenn die betreffenden Endnutzer ihre Einwilligung gegeben haben (Artikel 6 Absatz 3 Buchstabe a und b).

4.5. Nach Eingang bei den Empfängern müssen die Inhalte gelöscht oder anonymisiert werden.

4.6. Gemäß Artikel 4 Absatz 11 der DS-GVO bedeutet die „‘Einwilligung“ der betroffenen Person jede freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist“.

4.7. In dem Entwurf wird die Anforderung einer in der DS-GVO definierten **ausdrücklichen Einwilligung** aufrechterhalten, wobei der Nachweis von den Verantwortlichen zu erbringen ist.

4.8. Die Verarbeitung beruht auf dieser Einwilligung. Der Verantwortliche muss „nachweisen können, dass die betroffene Person in die Verarbeitung ihrer personenbezogenen Daten eingewilligt hat“ (Artikel 7 Absatz 1 DS-GVO).

4.9. Durch Gesetzgebungsmaßnahmen der EU oder der Mitgliedstaaten können bestimmte Beschränkungen der (Rechte und Pflichten zur Gewährleistung der) Vertraulichkeit vorgenommen werden, um öffentliche Interessen zu wahren oder Überwachungsaufgaben wahrzunehmen.

4.10. Natürliche Personen müssen vor Aufnahme in ein öffentlich zugängliches Verzeichnis ihre Einwilligung geben und die Möglichkeit haben, die sie betreffenden Daten zu überprüfen und zu berichtigen (Artikel 15).

4.11. Ein Widerspruchsrecht wird jedem Nutzer die Möglichkeit geben, die Nutzung seiner einem Dritten (beispielsweise einem Händler) anvertrauten Daten zu unterbinden, auch bei jedem Versand einer Nachricht (Artikel 16). Die neuen Bestimmungen erleichtern den Nutzern die Kontrolle über ihre Einstellungen (Cookies, Kennungen) und unerbetene Kommunikation (Spams, Nachrichten, SMS, Anrufe) kann abgestellt werden, wenn der Nutzer keine Einwilligung gibt.

4.12. Das Recht auf Anzeige der Rufnummer und die Sperrung unerwünschter eingehender Anrufe (Artikel 12 und 14) gilt auch für juristische Personen.

4.13. Die Struktur des Aufsichtssystems steht im Einklang mit der DS-GVO (Kapitel VI über unabhängige Aufsichtsbehörden und Kapitel VII über deren Zusammenarbeit und Kohärenz).

4.13.1. Die Mitgliedstaaten und ihre nationalen Datenschutzbehörden sind dafür zuständig, die Einhaltung der Vertraulichkeitsregeln zu überwachen. Die anderen Aufsichtsbehörden können im Rahmen einer gegenseitigen Amtshilfe Einwände formulieren, die dann nationalen Aufsichtsbehörden vorgelegt werden. Die Aufsichtsbehörden arbeiten im Rahmen eines Kohärenzverfahrens untereinander und mit der Europäischen Kommission zusammen (Artikel 63 DS-GVO).

4.13.2. Der Europäische Datenschutzbeauftragte stellt die einheitliche Anwendung der erörterten Verordnung sicher (Artikel 68 und 70 DS-GVO).

Er kann Leitlinien, Empfehlungen und bewährte Verfahren bereitstellen, um die Anwendung der Verordnung zu erleichtern.

4.14. Jede natürliche und juristische Person, die Endnutzer ist, kann Rechtsbehelfe nutzen, wenn ihre Interessen durch Verstöße beeinträchtigt werden; sie haben Recht auf Schadenersatz.

4.15. Die vorgesehenen Geldbußen sollen der Abschreckung dienen. Bei Verstößen können sie sich auf bis zu 10 Mio. EUR bzw. für ein Unternehmen auf bis zu 2 % seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs belaufen, je nachdem, welche der Beträge höher ist (Artikel 23); für Verstöße, die keiner Geldbuße unterliegen, legen die Mitgliedstaaten die Sanktionen fest und informieren die Europäische Kommission.

4.16. Der neue Rechtstext über die Achtung des Privatlebens und den Schutz personenbezogener Daten soll **ab dem 25. Mai 2018 gelten**, genau wie die Datenschutz-Grundverordnung aus dem Jahr 2016, die Verordnung zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe, Einrichtungen und sonstigen Stellen der Union und die vorgeschlagene Richtlinie über die Neufassung des europäischen Kodex für die elektronische Kommunikation (COM(2016) 590 final), sofern sie angenommen werden.

4.17. Geltungsbereich der *Lex specialis* zur Umsetzung der DS-GVO:

— ***ratione jure*: Rechtsgrundlage**

Rechtsgrundlagen sind Artikel 16 (Datenschutz) und Artikel 114 (Binnenmarkt) AEUV sowie Artikel 7 und 8 der Grundrechtscharta. Mit der Verordnung soll die DS-GVO im Hinblick auf Daten, die als personenbezogene Daten einzustufen sind, ergänzt werden.

— ***ratione personae*: Interessenträger**

Interessenträger sind auf der einen Seite die Endnutzer, bei denen es sich gemäß dem europäischen Kodex für die elektronische Kommunikation um natürliche oder juristische Personen handelt, und auf der anderen Seite sämtliche Provider von Kommunikationsdiensten, und zwar nicht nur die herkömmlichen Anbieter, sondern vor allem die neuen Akteure, deren neue Dienste den Nutzern keine Garantien bieten. Die sogenannten Over-the-Top-Kommunikationsdienste („OTT-Dienste" — Sofortnachrichtenübermittlung, VoIP, multiple Schnittstellen usw.) werden vom geltenden Rechtsrahmen nicht erfasst.

— ***ratione materiae*: Daten**

Der Vorschlag enthält keine Bestimmung zur Vorratsdatenspeicherung in der Cloud und überlässt es den Mitgliedstaaten, im Einklang mit Artikel 23 DS-GVO über Beschränkungen des Widerspruchsrechts und der Rechtsprechung des Gerichtshofs der EU tätig zu werden (siehe Punkt 1.3 der Begründung).

Die Endnutzer müssen in die Speicherung der von den Systemen generierten Daten und Metadaten (Datum, Uhrzeit, Ort usw.) einwilligen, ansonsten sind diese Daten zu anonymisieren oder zu löschen.

— ***ratione loci*: wo?**

Die in den Mitgliedstaaten niedergelassenen, mit der Datenverarbeitung befassten Unternehmen oder einer ihrer in einem Mitgliedstaat niedergelassenen Vertreter müssen Auskünfte erteilen, die nationalen Aufsichtsbehörden kommen ihrer Aufgabe nach und der Europäische Datenschutzbeauftragte (EDSB) überwacht den gesamten Prozess.

4.18. Die Ziele der EU mit Blick auf den digitalen Binnenmarkt:

— Ein mit dem digitalen Binnenmarkt verfolgtes Ziel ist es, die Voraussetzungen für sichere digitale Dienste zu schaffen und das Vertrauen der Verbraucher zu stärken, um u. a. den Internethandel, Innovationen und dadurch wiederum Beschäftigung und Wachstum zu fördern (Begründung Punkt 1.1).

— Mit dem Verordnungsvorschlag wird auch eine Angleichung der Rechtstexte untereinander und Kohärenz zwischen den Mitgliedstaaten angestrebt.

— Alle drei Jahre führt die Europäische Kommission eine Bewertung der Durchführung der Verordnung durch und legt sie dem Europäischen Parlament, dem Rat und dem EWSA vor (Artikel 28).

5. **Allgemeine Bemerkungen**

5.1. Der EWSA begrüßt die gleichzeitige und unionsweite Einführung eines kohärenten Gesamtregelwerks, das den Schutz der Rechte natürlicher und juristischer Personen bei der Nutzung digitaler Daten mittels elektronischer Kommunikation zum Ziel hat.

5.1.1. Er ist erfreut, dass die EU sich für den Schutz der Bürger- und Verbraucherrechte einsetzt.

5.1.2. Der EWSA gibt zu bedenken, dass ungeachtet der angestrebten Harmonisierung die Auslegung zahlreicher Bestimmungen den Mitgliedstaaten überlassen bleibt, was der Verordnung Orientierungscharakter verleiht und einen großen Spielraum für die Vermarktung personenbezogener Daten lässt. Insbesondere im Gesundheitsbereich stehen Tür und Tor offen für die Erhebung ungeheurer Mengen an personenbezogenen Daten.

5.1.3. In Artikel 11 Absatz 1, Artikel 13 Absatz 2, Artikel 16 Absatz 4 und 5 sowie Artikel 24 entsprechen eher der Art Durchführungsbestimmungen, die einer Richtlinie, nicht aber einer Verordnung angemessen sind. Den Betreibern wird in dem Bemühen, die Dienstqualität zu verbessern, zu viel Flexibilität gelassen (Artikel 5 und 6). Diese Verordnung sollte integraler Bestandteil des Richtlinienvorschlags über den europäischen Kodex für die elektronische Kommunikation (COM (2016) 590 final) sein.

5.1.4. Der EWSA bedauert lebhaft, dass es angesichts der Überschneidung, des Umfangs und der Verflechtung dieser Rechtsvorlagen unwahrscheinlich ist, dass sie, von wenigen Insidern abgesehen, gelesen werden, zumal ständig dazwischen hin- und hergeblättert werden muss und ihr Mehrwert für Bürger nicht ersichtlich ist. Die Unlesbarkeit und Kompliziertheit des Vorschlags stehen im Widerspruch zum Leitgedanken des Programms zur Gewährleistung der Effizienz und Leistungsfähigkeit der Rechtsetzung (REFIT) und zum Ziel der besseren Rechtsetzung, erschweren die Auslegung und eröffnen Datenschutzlücken.

5.1.5. Beispielsweise enthält der Verordnungsvorschlag keine Definition von „Betreiber". Diese Definition ist im noch nicht in Kraft getretenen Entwurf für einen europäischen Kodex für die elektronische Kommunikation ([4]) festgelegt, durch den im Rahmen der Strategie für den digitalen Binnenmarkt die geltenden Vorschriften geändert werden, als da wären: die Rahmenrichtlinie 2002/21/EG, die Genehmigungsrichtlinie 2002/20/EG, die Universaldienstrichtlinie 2002/22/EG und die Zugangsrichtlinie 2002/19/EG in ihren geänderten Fassungen, die Verordnung (EG) Nr. 1211/2009 zur Einrichtung des GEREK, die Frequenzentscheidung 676/2002/EG, der Beschluss 2002/622/EG zur Einrichtung einer Gruppe für Frequenzpolitik und der Beschluss Nr. 243/2012/EU über ein Mehrjahresprogramm für die Funkfrequenzpolitik (RSPP). Das Basisreferenzdokument ist selbstredend die Datenschutz-Grundverordnung (siehe Ziffer 2.2), die der vorliegende Verordnungsvorschlag ergänzen soll und der er daher untergeordnet ist.

5.2. Der EWSA verweist insbesondere auf Artikel 8 über den Schutz der in Endeinrichtungen gespeicherten Daten und potenzielle Ausnahmefälle, der von grundlegender Bedeutung ist, da er der Informationsgesellschaft Zugriffsmöglichkeiten auf personenbezogene Daten einräumt, sowie auf den die für Laien kaum verständlichen Artikel 12 über die Rufnummernunterdückung.

5.2.1. Im Sinne von Artikel 2 der Richtlinie 95/46/EG bezeichnet der Ausdruck „‚personenbezogene Daten' alle Informationen über eine bestimmte oder bestimmbare natürliche Person (‚betroffene Person')". Im neuen Verordnungsvorschlag wird der Datenschutz auf Massendaten (Big Data) ausgeweitet, und er bezieht sich künftig auf natürliche und juristische Personen. Es ist einmal mehr hervorzuheben, dass mit dem Verordnungsvorschlag zwei Ziele verfolgt werden: der Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und die Gewährleistung des freier Verkehrs elektronischer Kommunikationsdaten und elektronischer Kommunikationsdienste in der EU (Artikel 1).

([4]) COM(2016) 590 und Anhänge 1 bis 11 vom 12.10.2016 (ABl. C 125 vom 21.4.2017, S. 56).

5.2.2. Der EWSA gibt zu bedenken, dass das Bestreben, die Daten juristischer Personen zu schützen (Artikel 1 Absatz 2) zu Konflikten mit anderen Rechtstexten führen wird, wo dies nicht vorgesehen ist bzw. wo kein klarer Bezug zu juristischen Personen hergestellt wird (siehe die DS-GVO, der Datenschutz in den europäischen Institutionen).

5.3. Der EWSA fragt sich, ob das eigentliche Ziel dieses Vorschlags nicht eher darin besteht, vor allem Artikel 1 Absatz 2 umzusetzen und „den freien Verkehr elektronischer Kommunikationsdaten und elektronischer Kommunikationsdienste in der Union" zu gewährleisten, der aus Gründen der Achtung des Privatlebens und der Kommunikation natürlicher Personen weder beschränkt noch untersagt werden darf, und nicht in der in Artikel 1 Absatz 1 angekündigten Wahrung der „Rechte auf Achtung des Privatlebens und der Kommunikation und den Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten".

5.4. Zentraler Grundsatz ist die Einwilligung der natürlichen oder juristischen Person. Nach Meinung des EWSA müssen die Nutzer deshalb informiert und geschult werden und Umsicht walten lassen, denn wenn sie einmal ihre Einwilligung gegeben haben, kann der Provider die Inhalte und Metadaten weiterverarbeiten, um möglichst viel Wirkung und Gewinn zu erzielen. Wie viele Nutzer sind sich vor ihrer Einwilligung wirklich darüber im Klaren, dass es sich bei einem Cookie um eine Verfolgungstechnik handelt? Der Befähigung der Nutzer, ihre Rechte wahrzunehmen, sowie der Anonymisierung bzw. Verschlüsselung der Daten sollten in dieser Verordnung Vorrang eingeräumt werden.

6. **Besondere Bemerkungen**

6.1. Personenbezogene Daten sollten nur von Einrichtungen erhoben werden, die sehr strenge Regeln einhalten und bekannte und legitime Ziele verfolgen (DS-GVO).

6.2. Der EWSA bedauert erneut „die allzu zahlreichen Ausnahmen und Einschränkungen, die sich auf die aufgeführten Grundsätze des Rechts auf Schutz personenbezogener Daten auswirken" ([5]). Markenzeichen der Europäischen Union sollte auch weiterhin die Ausgewogenheit von Freiheit und Sicherheit sein und nicht der Ausgleich von Grundrechten der Personen und Industrieinteressen. Die Artikel-29-Datenschutzgruppe hat in ihrer Stellungnahme zu dem Verordnungsvorschlag (WP247 vom 4.4.2017, Stellungnahme 1/2017, Ziffer17) kritisiert, dass das Schutzniveau der DS-GVO, insbesondere hinsichtlich der Lokalisierung der Endeinrichtungen und des uneingeschränkten Umfangs der Datenerhebung, ausgehöhlt wird und keine datenschutzfreundlichen Voreinstellungen (Ziffer 19) vorgesehen sind.

6.3. Daten bilden eine Persönlichkeit ab und werden zur Schattenidentität. Einer Person gehören die Daten, die sie generiert, sie hat aber keinen Einfluss auf das, was nach ihrer Verarbeitung damit geschieht. Die Zuständigkeit für die Regelung der Datenspeicherung und der Datenübermittlung liegt bei den Mitgliedstaaten und aufgrund der in dem Verordnungsvorschlag vorgesehenen möglichen Beschränkungen der Rechte findet keine Harmonisierung statt. Dadurch, dass die Beschränkung der Rechte in das Ermessen der Mitgliedstaaten gestellt wird, können Unstimmigkeiten entstehen.

6.4. Eine Frage stellt sich insbesondere in Bezug auf die Beschäftigten in Unternehmen: Wem gehören die Daten, die sie durch ihre Arbeit generieren? Wie sind sie geschützt?

6.5. Die Kontrollstrukturen sind nicht besonders übersichtlich ([6]); trotz der Überwachung durch den Europäischen Datenschutzausschuss ist Willkür ist nicht hinreichend ausgeschlossen, und es liegt keine Einschätzung des erforderlichen Zeitaufwands bis zur Verhängung von Sanktionen vor.

6.6. **Der EWSA plädiert für die Errichtung eines europäischen Portals,** auf dem alle europäischen und nationalen Schriften, alle Rechte, Rechtsmittel, Gerichtsentscheidungen und Verfahrensweisen zusammengetragen und aktualisiert werden, und das den Bürgern und Verbrauchern dabei hilft, sich im Dschungel der Schriften und Durchführungsvorschriften zurechtzufinden und ihre Rechte wahrzunehmen. Dieses Portal sollte sich zumindest an den Bestimmungen der Richtlinie (EU) 2016/2102 vom 26. Oktober 2016 über den barrierefreien Zugang zu den Websites und mobilen Anwendungen öffentlicher Stellen und den Erwägungsgründen 12, 15 und 21 des Vorschlags für einen *Europäischen Rechtsakt zur Barrierefreiheit* (COM(2015) 615 final — 2015/0278 (COD)) orientieren und allen Endnutzern leicht zugängliche und verständliche Inhalte bieten. Der EWSA ist bereit, an der Konzeption dieses Portals mitzuarbeiten.

6.7. In Artikel 22 fehlt ein Verweis auf „Sammelklagen", was der EWSA bereits in seiner Stellungnahme zum europäischen Kodex für die elektronische Kommunikation angemahnt hat.

([5]) ABl. C 125 vom 21.4.2017, S. 56 sowie ABl. C 110 vom 9.5.2006, S. 83.

([6]) Kapitel IV Artikel 19 und 21 des erörterten Verordnungsvorschlags stützt sich seinerseits wiederum auf Kapitel VIII, insbesondere Artikel 68 der DS-GVO.

6.8. Die Begrenzung des sachlichen Anwendungsbereichs (Artikel 2 Absatz 2), die Ausweitung der erlaubten Verarbeitung von Daten ohne Einwilligung des betroffenen Nutzers (Artikel 6 Absatz 1 und 2), der unwahrscheinliche Fall, dass ALLE betroffenen Endnutzer ihre Einwilligung geben (Artikel 6 Absatz 3 Buchstabe b und Artikel 8 Absatz 1, 2 und 3), die möglichen Beschränkungen der Rechte seitens der Mitgliedstaaten, wenn sie dies als „notwendige, geeignete und verhältnismäßige Maßnahme" erachten, lassen allesamt so unterschiedliche Auslegungen zu, dass dies einen echten Schutz der Privatsphäre unmöglich macht. Besonderes Augenmerk sollte dem Datenschutz in Verbindung mit Minderjährigen gelten.

6.9. Der EWSA begrüßt das in Artikel 12 vorgesehene Kontrollrecht, wobei aber die ausgesprochen kryptische Formulierung den Schwerpunkt auf Rufnummernunterdrückung zu legen scheint, als wäre Anonymität zu empfehlen, obwohl vom Prinzip der Rufnummernanzeige ausgegangen werden sollte.

6.10. Unerbetene Kommunikation (Artikel 16) und Direktwerbung sind bereits Gegenstand der Richtlinie über unlautere Geschäftspraktiken ([7]). Als Standardregelung sollte die Einwilligung und nicht der Widerspruch zugrunde gelegt werden.

6.11. Es ist vorgesehen, dass die Europäische Kommission alle drei Jahre eine Bewertung durchführt. Im digitalen Zeitalter ist diese Frist zu lang. Nach zwei Bewertungen wird sich die digitale Welt komplett verändert haben. Indes sollte die Befugnisübertragung (Artikel 25) zeitlich begrenzt werden und eventuell verlängerbar sein.

6.12. Rechtsvorschriften müssen die Wahrung der Nutzerrechte (Artikel 3 EUV) und gleichzeitig Rechtssicherheit für die wirtschaftlichen Tätigkeiten gewährleisten. Der EWSA bedauert, dass die Datenübertragung zwischen Maschinen (M2M) in dem Vorschlag nicht berücksichtigt wird, sondern dass dafür der europäische Kodex für elektronische Kommunikation herangezogen werden muss (Richtlinienvorschlag, Artikel 2 und 4).

6.12.1. Durch das Internet der Dinge ([8]) wird aus Big Data erst Huge Data und dann All Data. Sie sind der Schlüssel für die künftigen Innovationsschübe. Und damit kommunizieren kleine wie auch große Maschinen untereinander und leiten personenbezogene Daten weiter (bspw. messen intelligente Uhren die Herzfrequenz des Trägers und schicken sie an den jeweiligen Hausarzt u. dgl.). Zahlreiche digitale Akteure haben eine eigene Plattform für vernetzte Objekte errichtet: Amazon, Microsoft, Intel und in Frankreich Orange und La Poste.

6.12.2. Im Alltag kann das Internet der Dinge leicht zum Ziel bösartiger Angriffe werden, zumal die Menge an fernablesbaren persönlichen Informationen (Geopositionierung, Gesundheitsdaten, Video- und Audiostreaming) wächst. Die Datenschutzlücken sind u. a. von Interesse für Versicherungsunternehmen, die anfangen, ihre Kunden für Vernetzung und Eigenverantwortung zu sensibilisieren.

6.13. Diverse Internetgiganten versuchen, ihre ursprünglichen Anwendungen zu Plattformen zu machen. So ist zwischen der Facebook-App und der Facebook-Plattform zu unterscheiden, einer Entwicklerplattform für Anwendungen auf der Grundlage von Nutzerprofilen. Amazon begann als Online-Buchversand. Heute ist Amazon eine Plattform, die es Drittanbietern, von Einzelhändlern bis Großunternehmen, ermöglicht, ihre Produkte zu vermarkten und dafür die Amazon-Ressourcen wie Reputation, Logistik usw. zu nutzen. Grundlage für all das ist die Übertragung personengebundener Daten.

6.14. In der kollaborativen Wirtschaft entstehen immer mehr Plattformen: „eine Plattform, normalerweise eine Online-Plattform, um eine breite Palette von Anbietern von Waren oder Dienstleistungen mit einer breiten Palette von Nutzern zu verbinden" ([9]). Auch wenn sie positiv gesehen werden, weil sie Wirtschaftstätigkeit und Beschäftigung fördern, fragt sich der EWSA, wie die Übertragung der dort generierten Daten mittels der DS-GVO und der vorliegenden Verordnung kontrolliert werden kann.

Brüssel, den 5. Juli 2017

Der Präsident
des Europäischen Wirtschafts- und Sozialausschusses
Georges DASSIS

([7]) Richtlinie 2005/29/EG vom 11.5.2005, Artikel 8 und 9 (ABl. L 149 vom 11.6.2005, S. 22).
([8]) WP247/17-Stellungnahme vom 1.4.2017, Ziffer 19 (ABl. C 12 vom 15.1.2015, S. 1).
([9]) ABl. C 125 vom 21.4.2017, S. 56.