Stellungnahme

zum Kommissionsentwurf der e-Privacy Verordnung (COM (2017) 10 final)

27. April 2017

Bitkom vertritt mehr als 2.400 Unternehmen der digitalen Wirtschaft, davon gut 1.600 Direktmitglieder. Sie erzielen mit 700.000 Beschäftigten jährlich Inlands-umsätze von 140 Milliarden Euro und stehen für Exporte von weiteren 50 Milliarden Euro. Zu den Mitgliedern zählen 1.000 Mittelständler, 300 Start-ups und nahezu alle Global Player. Sie bieten Software, IT-Services, Telekommunikations- oder Internetdienste an, stellen Hardware oder Consumer Electronics her, sind im Bereich der digitalen Medien oder der Netzwirtschaft tätig oder in anderer Weise Teil der digitalen Wirtschaft. 78 Prozent der Unternehmen haben ihren Hauptsitz in Deutschland, 9 Prozent kommen aus Europa, 9 Prozent aus den USA und 4 Prozent aus anderen Regionen. Bitkom setzt sich insbesondere für eine innovative Wirtschaftspolitik, eine Modernisierung des Bildungssystems und eine zukunftsorientierte Netzpolitik ein.

Bundesverband
Informationswirtschaft,
Telekommunikation
und Neue Medien e.V.

Susanne Dehmel
Mitglied der Geschäftsleitung
Vertrauen & Sicherheit
T +49 30 27576-223
s.dehmel@bitkom.org

Albrechtstraße 10
10117 Berlin

Präsident
Thorsten Dirks

Hauptgeschäftsführer
Dr. Bernhard Rohleder

Zusammenfassung

Mit der Datenschutz-Grundverordnung (DS-GVO) wurden bereits EU-weit einheitliche strenge datenschutzrechtliche Vorschriften für alle Sektoren festgelegt, die ein flächendeckend hohes Datenschutzniveau garantieren. Der Gesetzentwurf der EU-Kommission zur e-Privacy Verordnung (eP-VO) droht jedoch die im langjährigen und mühsamen Prozess gefundene Balance zwischen dem Schutz der Privatsphäre und neuen Technologien wieder zu zerschlagen, indem in weiten Bereichen Datenverarbeitungen, die unter der DS-GVO zulässig wären, entweder unter den Vorbehalt einer strengeren Form der Einwilligung gestellt oder gänzlich untersagt werden.

Zudem werden durch den Entwurf auch Vorgänge erfasst, bei denen keine personenbezogenen Daten verarbeitet werden, indem er strenge Regeln für die Kommunikation zwischen Unternehmen und Maschinen vorsieht, die heute gängige Abläufe in der europäischen Wirtschaft in Frage stellen und Spielräume für Innovationen im Bereich Industrie 4.0 und dem Internet der Dinge sowie in anderen neuen Geschäftsfeldern stark verengt. Die Wettbewerbsfähigkeit der Wirtschaft in Europa wird damit über alle Wirtschaftszweige hinweg bedroht.

Bitkom hat daher schwerwiegende Bedenken bezüglich des eP-Vorschlages und lehnt diesen in der aktuellen Form ab. Das angestrebte Ziel der EU-Kommission einer 'besseren Rechtsetzung' spiegelt sich nicht in dem Vorschlag wieder. Auch erschwert der Vorschlag den Aufbau einer europäischen digitalen Datenwirtschaft und läuft damit der Strategie zum digitalen Binnenmarkt zuwider.

Bewertung der einzelnen Vorschläge der e-Privacy Verordnung:

1. Art. 1 -4, Art.27: Anwendungsbereich, Definitionen und Inkrafttreten

Der Anwendungsbereich der eP-VO ist nur schwer zu fassen, was sowohl bei der Auslegung als auch der Anwendung der Vorschriften zu grundsätzlichen Problemen führt:

- **Zu viele unterschiedliche Anknüpfungspunkt bei einzelnen Vorschriften:** Zum einen bereitet es große Verständnisschwierigkeiten, dass die Vorschriften zur eP-VO an unterschiedliche Bezugspunkte anknüpfen. Einmal formulieren sie Pflichten für Anbieter von „elektronischen Kommunikationsdiensten" bzw. „Betreiber von Kommunikationsnetzen", einmal gehen Sie vom „Endgerät" aus, einmal von der „Endeinrichtung" und dann wiederum vom „Endnutzer". Auch ist an vielen Stellen unklar, wer der Kreis an geschützten Personen ist, so wird z.B. bei der Einwilligung in Art. 9 auf den „Endnutzer" abgestellt, in der DS-GVO dagegen auf die „betroffene Person". Dies sind aber zwei verschiedene Normadressatenkreise.

- **Zu viele Querverweise auf andere Vorschriften:** Die vielen Bezugspunkte werden nicht in der eP-VO definiert, sondern es wird lediglich auf andere EU-Gesetze verwiesen z.B. auf die Rl. 2008/63, auf die Rl. 2016/0288 , auf die VO. 2016/679 und auf die Rl. 2014/53. Diese Verweise finden sich an unterschiedlichen Stellen im Vorschlag.

- **Unklarheit bei Definitionen:** Darüber hinaus stehen viele der Def. auch noch nicht fest. Die eP-VO verweist z.B. in Art. 4 auf die Def. der Richtlinie über den europäischen Kodex für die elektronische Kommunikation („Kodex"), die derzeit noch auf EU-Ebene verhandelt wird. Die Auswirkungen der einzelnen eP-Vorschriften auf verschiedene Geschäftsmodelle hängen jedoch unmittelbar vom Inhalt und dem Umfang dieser Def. ab. So wird z.B. derzeit noch diskutiert, welche Dienste als „elektronische Kommunikationsdienste" verstanden werden und wie die „Übertragung von Signalen" auszulegen ist. Bevor diese Diskussion nicht abgeschlossen ist, ist schlecht zu beurteilen, wie sich die Ausweitung der eP-VO auf M2M-Kommunikation auswirkt.

- **Unklarheit bei den Ausnahmen des Anwendungsbereichs:** In **Art. 2 Abs.2 lit. c)** wird festgestellt, dass die eP-VO nicht für elektronische Kommunikationsdienste gilt, die nicht öffentlich zugänglich sind. Dabei wird der in Deutschland bestehende Meinungsstreit, ob ein Arbeitgeber bei der erlaubten Privatnutzung Telekommunikationsdienste anbietet, entschieden, in dem klarstellend in **Erw.13** ausgeführt wird, dass die eP-VO keine Anwendung auf „geschlossene Nutzergruppen", wie Unternehmensnetzwerke findet. Dieses Ergebnis sollte aus Sicht der deutschen Unternehmen noch klarer herausgearbeitet werden. Im Verhältnis Arbeitnehmer zu Arbeitgeber sollten einheitlich die Normen der DS-GVO Anwendung finden. Eine Differenzierung in Abhängigkeit davon, ob die IT-Ressourcen des Arbeitgebers geschäftlich oder privat genutzt werden ist kaum

praktikabel. Auch sollte die Schwelle näher definiert werden, unter welchen Voraussetzungen ein elektronischer Kommunikationsdienst nicht öffentlich zugänglich ist. Dies ist in der Praxis schwierig zu bestimmen, wie beispielsweise bei einem WLAN-Hotspot, der in einem Unternehmen betrieben wird. Es wäre daher hilfreich, wenn generelle Kriterien zur Abgrenzung von öffentlichen und geschlossenen Nutzergruppen formuliert werden würden, z.B. Mindestvoraussetzungen für den Beitritt eines Endnutzers zu einer geschlossenen Gruppe.

- **Unklarheiten bei Auswirkungen auf M2M-Kommunikation:** Gem. **Erw.12** eP-VO soll der Anwendungsbereich auch auf elektronische Kommunikation Anwendung finden, die nicht nur zwischen natürlichen Personen stattfindet, sondern auch zwischen jur. Personen und Maschinen erfolgt, was verstärktes Bedrohungspotenzial für neue Geschäftsmodelle haben könnte.

  Durch die Unklarheiten in den Definitionen und im Anwendungsbereich können neg. Auswirkungen für Unternehmen entstehen, die die Signalübertragung im Rahmen von M2M-Kommunikation in ihre Produkte einbinden, wie z.B. im Rahmen von vernetzten Fahrzeugen, automatisierten Lieferketten oder Fuhrparklösungen u.a. in der Automobilindustrie und Logistikbranche. Auch sehr viele andere Themenfelder aus beispielsweise Verkehr, Handel (z.B. die Kommunikation eines Kühlschranks mit einem Lebensmittelgeschäft oder andere Smart Home-Lösungen), Energie (z.B. der Ladevorgang in der Elektromobilität) könnten durch den Vorschlag tangiert werden.

  Beispiel: *Unternehmen (A) bietet Maschinensteuerungssoftware als Industrie 4.0-Anwendung an. Diese wird von Unternehmen (B) für seine Maschine genutzt, die vernetzt zusammenarbeiten. Eine Funktion dieser Software ist die automatische Übertragung bestimmter Sensordaten an vernetzte Maschinen an anderen Standorten. Dies verhindert, dass z.B. der Druck zu hoch wird und bestimmte Maschinen ausfallen (Predictive Maintenance). Die Maschinen sind über Festnetz mit dem Internet von Internetanbieter (C) verbunden.*

  Bei solchen kombinierten Diensten ist es schwierig abzugrenzen, wo die reine Kommunikationsübertragung endet und wo die Datenverarbeitung nach der DS-GVO anfängt; Was ist mit Unternehmen, die unterschiedliche Dienstleistungen gebündelt anbieten z.B. bei Smart Home? Welcher Teilnehmer hat welche Vertraulichkeits-/Datenschutz- sowie Sicherheitspflichten nach welcher Rechtsvorschrift in der eP-VO sowie nach anderen Parallel-Rechtsakten?

  Verschiedene Vorschriften der eP-VO führen in diesem Kontext zu Auslegungsschwierigkeiten:

- In **Art. 6** wird ein Verbot der Datenverarbeitung von z.B. **Standortdaten** festgeschrieben. Für diese Datenkategorie sollen strengere und zur DS-GVO parallele Vorschriften gelten, jedoch nur für „elektronische Kommunikationsdienste“. Auch die Verarbeitung von **Kommunikationsinhalten zwischen Maschinen** wird unter Erlaubnisvorbehalt sowie enge Ausnahmen gestellt. Was eine Maschine bzw. M2M-Kommunikation ist und wer im oben genannten Beispiel Betreiber des Kommunikationsdienstes-/Netzes ist, ist nicht abschließend geklärt. Auch ist im M2M-Kontext oftmals unklar, welcher „Endnutzer“ eine Einwilligung geben könnte. Die fast ausschließliche Abstellung auf die Einwilligung in Art. 6 ist für viele Anwendungsfälle schwierig handhabbar.

- Nach **Art. 8 Abs.2** ist eine **weitere Datenerarbeitung untersagt**, nämlich die „Erhebung von Informationen" die von „Endeinrichtungen" ausgesendet werden, um sich mit anderen Geräten oder mit „Netzanlagen" zu verbinden. Die „Erhebung" darf ausschließlich „zum Zwecke der Herstellung einer Verbindung für die dazu erforderliche Dauer" erfolgen (lit. a) oder wenn ein deutlicher Hinweis erfolgt (lit. b) z.B. in Form von Icons (Abs.3). Auch wenn die EU-Kommission möglicherweise ganz bestimmte Sachverhalte mit dieser Vorschrift adressieren wollte, **könnte der mögliche Anwendungsbereich wesentlich größer sein und sich negativ auf viele Geschäftsmodelle auswirken.**[1]

  So werden beispielsweise auch bei dem oben genannten Industrie 4.0-Beispiel Signale wie die Gerätekennung der Maschine (A) ausgesendet, dass sich Maschine (B) sich mit ihr verbinden kann. Maschine (B) speichert die Information, dass sie angefunkt und dass ihr Sensordaten übermittelt wurden und protokolliert, was sie als Reaktion darauf gemacht hat. Dabei stellt sich die Frage, ob das erforderliche Protokoll auch über die erforderliche Dauer der Kommunikation hinaus gespeichert und zu weiteren Zwecken auf Basis der DS-GVO verarbeitet werden darf z.B. zu Zwecken der Qualitätssicherung der Produktion oder Analyse zur Effizienzsteigerung durch beispielsweise Big Data. Eine „Erhebung von Informationen" kann zu unterschiedlichen Zwecken verarbeitet werden. Die Abgrenzung zwischen eP-VO und DS-GVO ist hier schwierig.

Ergebnis: Durch die unterschiedlichen Anknüpfungspunkte, die vielen Querverweise auf teilweise noch nicht feststehende Definitionen sowie sehr generellen Formulierungen ist der Kommissionsvorschlag unübersichtlich und selbst für den qualifizierten Leser nicht zu verstehen. Diese Komplexität, die sich nicht nur aus dem unklaren Anwendungsbereich und den Def. ergibt, sondern auch aus den vielen Parallelanforderungen zur DS-GVO und der Richtlinie für Netzwerk- und Informationssicherheit, wird zu großer Rechtsunsicherheit bei Unternehmen führen. Parallel laufen auch die Verhandlungen um das Anpassungs- und Umsetzungsgesetz in Deutschland sowie anderen EU-Mitgliedsstaaten. **Insbesondere für klein- und mittelständische Unternehmen ist eine solch komplizierte Gesetzgebung nicht handhabbar.**

Darüber hinaus passen Unternehmen ihre Datenschutzprozesse mit erheblichem Aufwand und Zeitdruck an die DS-GVO an, um fristgerecht bis Mai 2018 die Vorgaben umzusetzen. **Die Parallelanforderungen zur DS-GVO werden die Umsetzung erheblich verzögern.** Sollten sich Europäisches Parlament und Rat unerwarteter Weise schon dieses Jahr auf einen Text einigen, blieben Unternehmen **nicht mal fünf Monate Zeit für die Umsetzung der eP-VO.** Dies kann in so kurzer Zeit nicht bewerkstelligt werden. Ebenfalls scheint es schlicht unzumutbar, dass Unternehmen ihre Datenschutzprozesse und Geschäftsmodelle, die sie derzeit mit erheblichen Aufwand und Kosten auf die strengen Vorschriften der DS-GVO umstellen kurz nach deren Inkrafttreten wieder an die teilweise ganz anderen und in weiten Bereichen noch strengeren Vorschriften der ep-VO anpassen.

[1] Siehe auch aktuelle Diskussion z.B. http://swd-rechtsanwaelte.de/blog/e-privacy-verordnung-cookies-nur-mit-einwilligung/.

Allgemeine Handlungsempfehlungen: Der Gesetzgeber sollte sich daher bei den Verhandlungen zur eP-VO im Sinne der weiteren Harmonisierung für eine inhaltlich schlanke, an der DS-GVO orientierte Verordnung einsetzen, in der neue unbestimmte Rechtsbegriffe sowie zusätzliche Öffnungsklauseln vermieden werden:

- **Es sollte so schnell wie möglich Klarheit über die Definitionen im Kodex für die elektronische Kommunikation geschaffen werden.**

- **Alle Begrifflichkeiten, die in der eP-VO benutzt werden, sollten anwenderfreundlicher in den Begriffsbestimmungen zu finden sein**.

- **Der Anwendungsbereich der eP-VO sollte so beschränkt sein, dass er M2M-Kommunikationsdienste nicht berührt.**

- **Es sollte näher definiert werden, unter welchen Voraussetzungen ein elektronischer Kommunikationsdienst nicht öffentlich zugänglich ist.**

- **Es sollte eine klare Abgrenzung zwischen der Vertraulichkeit der Kommunikation (Telekommunikations-/Fernmeldegeheimnis) und der Verarbeitung von Daten (Datenschutz) geben**. Regelungsbereiche, die bereits von der DS-GVO oder anderen Rechtsakten abgedeckt sind, sollten nicht parallel in der eP-VO wieder aufgegriffen werden.

- **Vorschriften zu Co- und Selbstregulierung sollten auch auf die eP-VO Anwendung finden.** Mit Art. 40 ff. der DS-GVO wurde bereits ein wirksames Mittel zur effektiven Um-und Durchsetzung von datenschutzrechtlichen Bestimmungen geschaffen. Dagegen greift der Vorschlag der EU-Kommission zur eP-VO diese Vorschriften nicht auf, obwohl sich an zahlreichen Stellen selbstregulative Ansätze anbieten würden. Neben den bereits bestehenden Modellen zum Einsatz von Cookies könnten z.B. auch Löschfristen für Metadaten (sofern keine gesetzlichen Vorschriften bestehen) oder Anforderungen an Webbrowseranbieter durch Co- und Selbstregulierung näher spezifiziert werden. Da es unklar ist, ob die in Art. 40 ff. DS-GVO niedergelegten Vorschriften auch gleichzeitig Anwendung auf rekurrierende Rechtsakte wie die eP-VO finden, sollte es eine explizite Klarstellung im Entwurf der Verordnung geben.

Sollte der Gesetzgeber diesem generellen Ansatz der EU-Kommission jedoch folgen, sollten sich die Vorschriften zu Verarbeitung zumindest an der Regelungstechnik der DS-GVO, wie in den folgenden Punkten beschrieben, orientieren.

2. Art. 5 und 6: Vertraulichkeit elektronischer Kommunikationsdaten und erlaubte Verarbeitung elektronischer Kommunikationsdaten

Im Gegensatz zur DS-GVO weist der Vorschlag der eP-VO keine flexiblen Tatbestände auf, auch nicht unter der Prämisse, dass konkrete datenschutzfreundliche Technologien verwendet werden. Darüber hinaus wird das bisher im TKG niedergelegte Fernmeldegeheimnis ausgedehnt und zweckentfremdet, indem selbst das zwingend erforderliche automatisierte Verarbeiten von Kommunikationsdaten zum Zwecke der Kommunikation als ein Eingriff in die Vertraulichkeit der Kommunikation deklariert wird und Kerndienstleistungen von Dienstanbietern und selbstverständliche Vorgänge wie das Speichern einer E-Mail in Zukunft eine Einwilligung voraussetzen.

1. **Verarbeitung von elektronischen Kommunikationsmetadaten:** Laut eP-VO sollen elektronische Kommunikationsmetadaten z.B. Standortdaten (Art. 6 Abs.1, 2) nur für gesetzlich definierte Zwecke verarbeitet werden dürfen, z.B. für die Gewährleistung der Sicherheit eines Dienstes (Art. 6 Abs.1 lit. b) oder für Abrechnungen (Art. 6 Abs.2 lit. b). Für andere Zwecke ist die Einwilligung der Nutzer erforderlich (Art.6 Abs.2 lit. c), der eine weitere rechtliche Hürde, ein Anonymisierungstest vorangestellt wird. Diese hohen Anforderungen erschweren die Datenverarbeitung in vielen Fällen oder machen sie nahezu unmöglich.

   Beispiele: Dadurch können die Vorteile, die sich durch die Verarbeitung für den Verbraucher und die gesamte Gesellschaft ergeben, nicht ausgeschöpft werden, wie beispielsweise:

- **Kaufmännische Analysen:** *Identifikation von Nutzungstrends von Diensten, Entwicklung eines tieferen Verständnisses der Einflüsse der Veränderung von Angeboten, insbesondere Preisen sowie die Optimierung des Produktangebots auf Grundlage der vorbenannten Erkenntnisse.*

- **Verbesserung des Kundenservice:** *Identifikation schlechter Netzqualität, Verbesserung der Netzinfrastruktur, Möglichkeit zur gezielteren Lösung von Kundenanliegen.*

- **Big Data Analysen:** *Verbesserung des Transportwesens, insbesondere im öffentlichen Personennahverkehr*

Handlungsempfehlungen: Um europäischen Unternehmen zu ermöglichen, digitale Technologien einzusetzen und innovative Datenverarbeitungen zu entwickeln, sollten folgende Punkte bei der Ausgestaltung der Verarbeitungsgrundlagen in der eP-VO berücksichtigt werden:

- **Interessenabwägung im Einzelfall:** Hierzu hat die Art. 29 Datenschutzgruppe für das Verhältnis der RL 2002/58/EU zur RL 95/46/EG vertreten, dass es nicht Sinn der RL 2002/58/EU gewesen ist, Datenverarbeitungen zu verhindern, welche im Hinblick auf die Interessen der Betroffenen akzeptabel sind.

- **Privilegierung pseudonymer Datenverarbeitung:** Bei der Verarbeitung großer Datenmengen, oftmals in Echtzeit, wird es künftig nur schwer möglich sein, mit rein einwilligungsbasierten Lösungen belastbare und damit verwertbare Ergebnisse zu erhalten – zumal sich der Zweck einer Datenverarbeitung gerade bei Big Data

Analytics ständig im Hinblick auf neue Korrelationen und Erkenntnisse ändert. Umso wichtiger werden deshalb Pseudonymisierungslösungen, die eine geeignete Grundlage und Flexibilität für kommerzielle Datenweiterverarbeitungen schaffen können und gleichzeitig die Interessen der Einzelnen angemessen schützen.

Daher ist es wichtig, Ausnahmen vom Einwilligungserfordernis bei der Datenweiterverarbeitung zu schaffen, solange der Schutz der Daten des Einzelnen garantiert ist. **Art. 6 sollte daher an Art. 6 Abs.4 DS-GVO angepasst werden**: demnach besteht die Möglichkeit der Weiterverarbeitung ohne erneuten Erlaubnistatbestand, soweit der neue Verarbeitungszweck „kompatibel" und damit mit dem urspr. erhobenen Zweck vereinbar ist. Dabei spielen insbesondere Schutzmechanismen wie Pseudonymisierung und Verschlüsselung zum Schutz der Daten eine hervorgehobene Rolle (Art. 6 Abs.4 lit. e DS-GVO).

Die Pseudonymisierung als anerkannte Schutzmaßnahme in der DS-GVO hat insofern den Vorteil gegenüber anonymisierten Daten, als der für Big Data Anwendungen so wichtige „identifier", erhalten bleibt, unter gleichzeitiger Wahrung des Schutzes personenbezogener Daten.

Beispiel: *Innovative Geschäftsmodelle wie etwa für Infrastrukturoptimierung oder Verkehrsmanagement benötigen „identifier", um verwertbare Ergebnisse mithilfe der Auswertung von Entwicklungsverläufen zu erzielen. Dabei kommt es nicht auf die Identifizierung einzelner Personen an, sondern lediglich auf Merkmale, die eine Verkettung der Daten erlauben.*

Eine Anpassung an Art. 6 Abs. 4 DS-GVO würde den Anbietern die nötige Flexibilität geben, Metadaten zu anderen Zwecken nach Maßgabe der bereits in der DS-GVO festgelegten Kriterien zu verarbeiten. Damit würde ein gangbarer Weg für die Praxis aufgezeigt, der neben der Gewährleistung eines angemessenen Datenschutzniveaus dennoch Raum für Innovation lässt.

Darüber hinaus sollten berücksichtigt werden:

- **Sicherheit und Verfügbarkeit der Netze und Dienste:** Kommunikationsmetadaten und -inhalte sollten zu Zwecken der Betrugs- und Spamerkennung sowie der Erkennung von Spyware oder Datenabflüssen und damit zum Schutze der eigenen Kommunikationsdienste und im Netzwerk verbundenen Parteien verarbeitet werden dürfen. Netzwerk-/dienstbasierte Sicherheit, die ihrerseits nicht von der Einwilligung abhängen kann, ist zur Erreichung dieser Ziele essentiell.[2] Um Bedrohungen oder Angriffe zu identifizieren, ist die Verarbeitung von Metadaten, einschließlich der Protokollinformationen erforderlich. Dies gilt umso mehr, als die Verantwortlichkeit der Netzbetreiber innerhalb des Netzes – etwa als kritische Infrastruktur – stetig steigt. Ziel muss es sein, die Anforderungen für diese Zwecke möglichst unternehmerfreundlich auszugestalten:

[2] Erw. 49 DS-GVO stellt dies in Rechnung. So stelle die Datenverarbeitung i.R.d. strengen Zweckbindung ein legitimes Interesse dar, wenn sie für Netzbetreiber, Dienstanbieter und Sicherheitsdienstleister erforderlich und angemessen ist, um Netzwerk- und Informationssicherheit zu gewährleisten. Das schließe unbefugte Netzwerkzugriffe, die Verteilung von Schadsoftware und die Abwehr von DDoS-Angriffen und damit verbundene Schädigungen von Computern und anderen elektronischen Kommunikationssystemen ein.

➔ **Definition von Metadaten um Protokollinformationen erweitern:** Für die oben genannte Zwecke sind zur zuverlässigen Erkennung von Mustern auch Protokollinformationen erforderlich. Diese stellen ihrerseits nicht den eigentlichen Inhalt der Telekommunikation dar. Gleichwohl wird diskutiert, wo die Grenzen zwischen dem Inhalt der Telekommunikation und Protokollinformationen als Bestandteil des Telekommunikationsvorgangs zu ziehen sind. **Vor diesem Hintergrund wäre eine entsprechende Klarstellung in Art. 4 Abs. 3 c) hilfreich, dass zu den „Metadaten" sämtliche technischen Informationen gehören, die im Rahmen der Netzwerkkommunikation erforderlich sind, um dem Empfänger die übertragenen und unter lit. b) genannten Inhalte zu präsentieren (Protokollinformationen).**

➔ **Verfügbarkeit von elektronischen Kommunikationsdiensten und Netzwerken mitaufnehmen:** Die zunehmenden Sicherheitsbedrohungen zeigen, dass Angriffe häufig nicht nur die Sicherheit sondern auch die Verfügbarkeit von elektronischen Kommunikationsdiensten und Netzwerken zum Ziel haben können. Dies ist insbesondere dann problematisch, wenn sich Angriffe nicht unmittelbar gegen das Netzwerk, sondern gegen die an das Netz angeschlossenen Geräte der Nutzer wie z.B. Router richten, die nicht Teil des elektronischen Kommunikationsnetzes sind. **Das Recht zur Datenverarbeitung zu Zwecken der Sicherheit nach Art. 6 Abs. 1 lit. b) müsste folglich auch zur Sicherstellung der generellen Verfügbarkeit des Netzes ausgeweitet und entsprechend ergänzt werden.**[3]

Abrechnung gegenüber Service Providern: Art. 6 Abs. 2 lit. b) erlaubt ausdrücklich die Verarbeitung von Metadaten zur Rechnungsstellung und zur Berechnung von Zusammenschaltungsentgelten. Es ist unklar, ob von diesen beiden Erlaubnistatbeständen neben der Abrechnung gegenüber Endnutzern auch die Abrechnung gegenüber Service Providern erfasst ist. **Insofern wäre auch hier eine Klarstellung wünschenswert.**

2. **Verarbeitung von elektronischen Kommunikationsinhalten:** Auch dürfen Anbieter von elektronischen Kommunikationsdiensten **elektronische Kommunikationsinhalte (Art. 6 Abs. 3)** nur unter strengen rechtlichen Voraussetzungen verarbeiten, da selbst das zwingend erforderliche automatisierte Verarbeiten von Kommunikationsinhalten zum Zwecke der Kommunikation schon als ein Eingriff in die Vertraulichkeit der Kommunikation deklariert wird und Kerndienstleistungen von Dienstanbietern und selbstverständliche Vorgänge wie das Speichern einer E-Mail in Zukunft eine Einwilligung voraussetzen. Folgende Punkte sollten aus Sicht des Bitkom beachtet werden:

- **Schutzziel der Vertraulichkeit überdehnt:** Das eigentliche Schutzziel „Vertraulichkeit der Kommunikation", wie man es derzeit aus dem Telekommunikations-/Fernmeldegeheimnis kennt, wird in dem Kommissionsvorschlag ausgedehnt und zweckentfremdet, indem die gesamte Kommunikation, die auf der Verarbeitung von Kommunikationsdaten basiert, unter ein Verbot mit Erlaubnisvorbehalt gestellt wird.

[3] **Beispiel**: Hacker-Angriff auf Kunden-Router, der zur Beeinträchtigung oder zur Nicht-Verfügbarkeit des Dienstes führt. Die Verarbeitung von Kommunikationsdaten zur Verhinderung von Störungen von an die Telekommunikationsanlage angeschlossenen Telekommunikations- und Datenverarbeitungssystemen der Nutzer sollte daher möglich sein.

- **Standardvorgänge der Dienstleistungserbringung grundsätzlich verboten:** Nach Art**. 6 Abs. 3 lit. a**) soll die Verarbeitung elektronischer Kommunikationsinhalte erlaubt sein „zum alleinigen Zweck der Bereitstellung eines bestimmten Dienstes für einen „Endnutzer'", wenn der „betreffende Endnutzer" seine Einwilligung gegeben hat und die „Dienstleistung ohne Verarbeitung dieser Inhalte nicht erbracht werden kann".

  Beispiel: *Geht ein Nutzer beispielsweise einen Vertrag mit einem E-Mail-Dienstanbieter ein, ist unverständlich, warum darüber hinaus noch eine Einwilligung erforderlich sein soll für eine Leistung, die von ihm erwartet wird:*
  - *Die Darstellung einer Email zur Betrachtung durch den Nutzer in einer gewöhnlichen Web-Ansicht ist bereits Verarbeitung (ohne diese sähen die Nutzer nur unverständliche Zeichen und Zahlen im "Roh-Code").*
  - *Das Ausdrucken einer Email bedeutet bereits Verarbeitung von Kommunikationsinhalten.*
  - *Die Indexierung von Emails, damit die Nutzer sie in ihrem Postfach nach Inhalten, Schlagwörtern durchsuchen können (Standard-Funktion in jedem Email-Service) bedeutet Verarbeitung von Kommunikationsinhalten und –metadaten*
  - *Die Organisation und Sortierung von Emails nach Absendern oder Betreffzeilen ist Verarbeitung von Kommunikationsmeta- und Inhaltsdaten*
  - *Spam-Erkennung, Rechtschreib- und Grammatikprüfung oder etwa Auto-Vervollständigung sind Vorgänge der Verarbeitung von Inhalten und Metadaten.*
  - *Kollaborative Software zur Textverarbeitung mit mehreren Bearbeitern stünde aufgrund der Möglichkeit zur "Kommunikation" der Nutzer potenziell unter einem Verbot mit Erlaubnisvorbehalt.*

  Wird „Endnutzer" als derjenige interpretiert, der am Ende einer Kommunikation steht, würde dies bedeuten, dass beispielsweise für die Übermittlung einer E-Mail von einer Einwilligung sowohl des Versenders auch des Empfängers erforderlich wäre. Eine solche Regelung wäre praxisfern.

  Beispiel neue Kommunikationsfeatures: Auch bei anderen modernen Dienstleistungen muss teileweise bereits bei der Übertragung der Kommunikation auf den Inhalt zugegriffen werden:
  - *Bei Live-Übersetzungen für Voice/Massengerdienste,*
  - *Voice-To-Text Features für behindere Benutzer, Reaktion auf Sprechbefehle und neue Formen der Interaktion.*

- **Einwilligung vom Endnutzer bzw. Endnutzern unklar:** Es ist auch unklar, worauf der Begriff „Endnutzer" in dieser Vorschrift abzielt und von wem der Betreiber elektronischer Kommunikationsdienste eine Einwilligung einholen muss.

  Beispiel Plattform: *Hat ein elektronischer Kommunikationsdienst einen Unternehmenskunden, ist unklar, ob der Kommunikationsdienst die Einwilligung von diesem Kunden einholen muss oder anderen Personen wie den Arbeitnehmern des Kunden oder externen Besuchern bei beispielsweise einer Plattform. Sollte letzteres der Fall sein, ist wiederum unklar, ob die Pflicht den Dienstanbieter oder dessen Kunden trifft.*

  Auch die Vorschrift in **Art. 6 Abs. 3 lit. b)** weist eine ähnliche Problematik auf:

  Beispiel: *So würde ein Verbot mit Einwilligungsvorbehalt „aller betreffender Endnutzer" bedeuten, dass ein Dienstleister, der die Nachricht zur Spambekämpfung scannen möchte eine Einwilligung des Senders und*

Empfängers der Kommunikation bräuchte. Dies würde bedeuten, dass Software, die Spam filtert, nur eingesetzt werden kann, wenn der Spammer sein Einverständnis gegeben hat. Eine solche Regelung wäre praxisfern.

3. Art. 7: Speicherung und Löschung elektronischer Kommunikationsdaten

Art 6 Abs. 2 lit. b) regelt neben der Verarbeitung von Metadaten zur Abrechnung auch die Verarbeitung von Metadaten zur Erkennung und Beendigung betrügerischer und missbräuchlicher Nutzung elektronischer Kommunikationsdienste. Art. 7 Abs. 2 legt fest, dass Metadaten zu löschen oder zu anonymisieren sind, sobald sie für die Übermittlung der Kommunikation nicht mehr benötigt werden. Ausnahmen sind für die Verarbeitung gem. Art. 6 Abs. 1 lit. b) und Art. 6 Abs. 2 lit. a) und c) vorgesehen. Art. 7 Abs. 3 regelt eine Ausnahme für die Abrechnung gem. Art. 6 Abs. 2 lit. b). **Eine Ausnahme von der sofortigen Löschverpflichtung zugunsten der Missbrauchserkennung und –beendigung gem. Art. 6 Abs. 2 lit. b) fehlt hingegen. Die Daten wären also unverzüglich nach Beendigung der Kommunikation zu löschen, was eine Missbrauchserkennung nahezu unmöglich machen würde. Art. 7 sollte daher entsprechend ergänzt werden.**

4. Art. 8: Schutz der in der Endeinrichtung der Endnutzer oder sich auf diese beziehenden Informationen

Art. 8 Abs.1 verbietet jede vom Endnutzer nicht selbst vorgenommen Nutzung der Verarbeitungs- und Speicherfunktion und jede Erhebung von Informationen aus Endeinrichtungen der Endnutzer. **Ausnahmen** sind nur in sehr engen Fällen vorgesehen.

- **Nicht jede Nutzung von Verarbeitungs- und Speicherfunktion ist grundsätzlich schlecht:** In **Erw. 20** wird keine Unterscheidung zwischen nützlichen und schädlichen Cookies gemacht, sondern „Spyware und Webbugs" werden neben anderen Cookie-Technologien als „Verfolgungstechniken" deklariert. Dabei wird neben dem, was für die reine Diensterbringung notwendig ist, lediglich eine Ausnahme als nicht die Privatsphäre gefährdend angesehen, nämlich die Messung des Webdatenverkehrs. Die technische Nutzung der Verarbeitung und Speicherfunktion sowie die Erhebung von Informationen aus Endeinrichtungen können sich in vielen Fällen positiv auf den Endnutzer auswirken:

  Beispiel: *Cookies werden beispielsweise als technisches Mittel eingesetzt, um Werbung effizienter einzusetzen. Durch den sogenannten Frequency Cap (dt. Deckelung der Frequenz) wird beispielsweise die Häufigkeit einer Werbeeinblendung für einen Nutzer reguliert (z.B. maximal 10-mal angezeigt, dann wird anderes Werbemittel benutzt). Auch muss derjenige, der die Werbung selbst schaltet zu Abrechnungszwecken mit dem Vermarkter wissen, wie viele Besucher die Werbung gesehen haben.*

- **Alleiniges Abstellen auf Einwilligung nicht praktikabel:** Anders wird als in Deutschland nur noch auf die Einwilligung abgestellt, was die Nutzung von pseudonymisierten Daten weder berücksichtig, noch privilegiert (siehe §15 Abs.3 TMG). Auch andere Tatbestände aus der DS-GVO, wie das berechtigte Interesse, sollen keine

Anwendung finden. Gerade in der digitalen Welt, in der laufend neue Anwendungen und Geschäftsmodelle entstehen, sind flexiblere Regelungen dringend erforderlich.

- **Gängige Verfahren nicht mehr zulässig:** Auch sind gängige Verfahren nur dann erlaubt, wenn der Anbieter sie selbst durchführt (Art. 8 Abs.2 i.V.m Art. 10). In den meisten Fällen wird aber bereits die Reichweitenmessung und insbesondere weitergehende Webanalytics von Dritten durchgeführt.

  Beispiel: *So ist sogenannte **Third-Party-Webanalytics**, das weit überwiegend genutzte Verfahren. In Zukunft soll die Webanalyse jedoch nur noch zulässig sein, wenn der Anbieter sie selbst vornimmt. Damit muss der weit überwiegende Teil der europäischen Wirtschaft seine Verfahren beim Bereitstellen von Webseiten und Internetdiensten umstellen. Während finanzstarke Unternehmen das erforderliche Know-How, die Technik und die personellen Ressourcen hierfür möglicherweise in ihren eigenen Häusern aufbauen können, werden viele kleine und mittelständische Unternehmen nicht in der Lage sein dies zu tun und daher auf die Analyse ihrer Webangebot verzichten müssen und im Wettbewerb abgeschlagen.*

- **Einzelfallregelungen ohne Ausdifferenzierung:** In **Erw. 21** ist geregelt, dass „Konfigurationsprüfungen, die Anbieter von Diensten der Informationsgesellschaft vornehmen, um ihre Dienste entsprechend den Einstellung des Endnutzers bereitstellen zu können, wie auch das bloße Feststellen der Tatsache, dass das Gerät des Endnutzers die vom Endnutzer geforderten Inhalte nicht empfangen kann“ nicht als Zugriff auf ein Gerät oder die Nutzung der Verarbeitungsfunktion des Geräts betrachtet werden sollen. Die Kommission versucht hier Einzelfälle zu regeln, ohne sie zu benennen, was immer das Risiko von Kollateralschäden mit sich bringt.

  Beispiel: *Diese Regelung erfasst auch jedes Tracking von Browser style sheets, wie beispielsweise „Textise“, „Color Transform” und „Tools für Farbblinde“. Der Webseitenbetreiber kann also dadurch direkt herausfinden, ob der Nutzer eine Sehbehinderung hat oder nicht. Auch wenn das noch nicht direkt ein besonderes Datum ist, so lässt es aber Rückschlüsse auf besondere Daten zu.*

  Das dürfte für die meisten Datenschützer durchaus eine erhebliche Beeinträchtigung des Rechts auf informationelle Selbstbestimmung sein, ganz zu schweigen von etwaigen Diskriminierungsmöglichkeiten, und damit dem Erw. 21 einleitenden Satz 1 widersprechen. In dieser Form ist die Ausnahme daher nicht angemessen und daher zu überarbeiten.

Handlungsempfehlungen: Art. 8 muss ausdifferenzierter gestaltet werden. Es bedarf einer flexiblen und technologieneutralen Vorschrift, die unterschiedliche Fallbeispiele abdecken kann. Die Tatbestände sollten sich wie schon oben beschrieben an der Regelungstechnik der DS-GVO orientieren.

5. Art. 9: Einwilligung

Die im Kommissionvorschlag parallelen und von der DS-GVO abweichenden Regeln wie in **Art. 9** sind aus Sicht der Digitalwirtschaft weder schlüssig noch notwendig und führen zu neuen Rechtsunsicherheiten bei der derzeitigen Auslegung und Umsetzung der DS-GVO:

- **Unterschiedliche Normadressaten führen zu Unklarheiten:** So führt u.a. die Abstellung auf **unterschiedliche Kreise geschützter Personen** zu Rechtsunsicherheit. In der DS-GVO wird das „Datensubjekt" geschützt, wohingegen die eP-VO auf den „Endnutzer" abstellt. Dabei ist insbesondere bei komplexen Sachverhalten unklar, wer von wem eine Einwilligung einholen muss.

- **Verfallszeit von Einwilligungen nicht angemessen**: Auch die avisierte Verfallszeit von Einwilligungen nach **Art. 9 Abs. 3 eP-VO** bedeutet einen vollständigen Systembruch gegenüber den Regelungen der DS-GVO dar und stellt die Netzbetreiber ohne naheliegende Gründe schlechter als andere Unternehmen im digitalen Sektor, deren Datenverarbeitungen bzw. die dazu erforderlichen Einwilligungen „nur" den allgemeinen Anforderungen unterliegen Die DS-GVO hat mit **Art. 7 Abs. 3** bereits die Vorgaben zum Widerruf der Einwilligung im Datenschutzrecht verschärft, indem diese „jederzeit und ohne Grund" erfolgen kann und „so einfach wie die Erteilung" ausgestaltet werden muss. In Verbindung mit den sehr umfangreichen Transparenzpflichten der DS-GVO ist der Verbraucher ausreichend geschützt. Die weiter verschärften Anforderungen an die Einwilligung, wie jene in **Art. 9 Abs.3** werden dazu führen, dass der Verbraucher regelmäßig mit Anfragen konfrontiert wird, die ihm eine Vielzahl von Einwilligungen für von ihm für selbstverständlich erachtete Vorgänge abverlangen. Und es bleibt für den Verbraucher nicht bei einer Einwilligung, denn nach Art 9 Abs. 3 muss er von allen Anbietern **alle sechs Monate** im Hinblick auf alle erteilten Einwilligungen darauf hingewiesen werden, dass er diese Einwilligungen jederzeit widerrufen kann.

Handlungsempfehlung: Um die möglichst zügige Auslegungs- und Umsetzungsprozess der EU-Datenschutzregeln nicht zu konterkarieren, s**chlägt der Bitkom daher die Streichung des Art. 9 eP-VO vor.**

6. Art. 10: Bereitzustellende Informationen und Einstellungsmöglichkeiten zur Privatsphäre

Art. 10 Abs. 1 verbietet Unternehmen auf Dritte zurückgreifen, was gängige Verfahren zur Erfassung von Nutzungsdaten zur bedarfsgerechten Gestaltung von Internetdiensten unterbindet. **Art. 10 Abs. 2** schreibt vor, dass bei der Installation die „Software" den „Endnutzer" über die Einstellungsmöglichkeiten zur Privatsphäre informieren und zur Fortsetzung der Installation die Einwilligung vom „Endnutzer" verlangen muss.

- **Zu weiter Anwendungsbereich:** Die Vorschriften in **Art. 10** betreffen generell „**Software, die eine elektronische Kommunikation erlaubt**", einschließlich des Abrufs und der Anzeige von Internetinhalten. Dazu zählen nicht nur herkömmliche Browser, sondern unter anderem auch eine Großzahl von Apps auf Smartphones, Tablets, Smartwatches und sonstigen Endgeräten (einschließlich PCs). Die Regelungen machen für alle Hersteller

derartiger Software konkrete Vorgaben dazu, wie diese anzubieten sind.

Beispiele: *Nach diesen Vorgaben müsste der **Hersteller einer Email-App** eine Einstellung implementieren, welche es dem Nutzer ermöglicht, den Empfang von Emails zu verhindern. **Anbieter von Nachrichten-Apps,** die zum Beispiel von Verlagen angeboten werden, müssten eine Einstellung anbieten, mit der Drittinhalte, wie Werbung, Videos, Online-Karten, Börse- Sport- oder Wetternachrichten geblockt werden können. Und **Hersteller von Browsern** müssen eine Einstellung anbieten, mit der verhindert werden kann, dass mit dem Browser Webseiten auf das Endgerät des Nutzers geladen werden können. Überdies müssten die Hersteller den Verbraucher im Rahmen von Installationsprozessen auf diese Einstellungen hinweisen und ihn dazu drängen, in die Einstellung einzuwilligen. Aufgrund der Vielzahl von Software und Apps, die die Verbraucher heutzutage parallel auf mehreren Endgeräten nutzen, sähen sich Verbraucher ständig mit einer Vielzahl von Anfragen hinsichtlich dieser Einstellungen konfrontiert.*

- **Abhängigkeit verschiedener Parteien unklar:** Dabei stellen sich auch Fragen bezüglich der Abhängigkeit verschiedener Parteien wie dem Browseranbieter, dem Webseitenbetreiber und Dritter, die beispielsweise Werbung auf der Webseite des Webseitenbetreibers schalten. So kann es nicht sein, dass ein Webseitenbetreiber keine Möglichkeit mehr hat, eine Einwilligung für Cookies einzuholen und gänzlich von den Einstellungen eines Webbrowsers abhängig ist. Dabei würden dem Nutzer eine Reihe an gewollten Einwilligungen vorgehalten werden, weil dieser die Komplexität nicht durchschaut, sprich dass er parallel seinen Browser umstellen muss, um an das gewünschte Cookies zu kommen. Auch könnte es sein, dass der Browser kein entsprechendes Verfahren oder eine Schnittstelle bereitstellt und damit eine ganze Kette an Akteuren abschneidet. Dem Webseitenbetreiber muss nach wie vor die Möglichkeit gegeben sein, eine Einwilligung von den Nutzern seiner Webseite einzuholen sowie Werbung von Dritten auf seiner Webseite zu schalten. **Hier sollte es Klarstellungen geben insbesondere zur Abgrenzung derzeitiger Do-not-Track Standards.**

- **Gefährdung der IT-Sicherheit und der Funktionalität von Endgeräten:** Der Entwurf erschwert oder unterbindet mit **Artikel 10 Abs. 2** auch Vorgänge, die für eine Aufrechterhaltung der IT-Sicherheit bei Unternehmen und Behörden essentiell sind.

Beispiel: *So steht die Zulässigkeit der Erhebung technischer Rahmendaten, welche von zugreifenden Systemen durch die Firewall eines Hostsystems erfasst werden, unter der Voraussetzung, dass eine Benachrichtigung an das zugreifende System erfolgt. Da jedoch Firewallsysteme in der Regel keinen Output an die zugreifenden Systeme abgeben und viele zugreifenden Systeme ohnehin keine Benachrichtigung darstellen können, müssten viele Datenerhebungen unterbleiben, die für das Betreiben einer Firewall zum Schutz vor Angriffen essentiell. Daneben hat die Regelung auch zur Folge, dass die Funktionalität von Endgeräten erheblich eingeschränkt wird. So wird es in Zukunft für europäische Verbraucher wohl nicht mehr möglich sein, die Zugriffsdaten für Internetzugangspunkte auf ihren Endgeräten zu speichern ("Remember this Wifi"), da eine solche Speicherung über den Zeitraum der Verbindung hinaus nur dann zulässig wäre, wenn der Nutzer eine Benachrichtigung an den Zugangspunkt sendet, die dieser ohnehin nicht darstellen kann. Nutzer müssten sich daher in Zukunft stets erneut mit manueller Eingabe des Passwortes bei von Ihnen häufig verwendeten Internetzugangspunkten anmelden.*

7. Art. 11: Beschränkungen

Der Bitkom befürwortet die Harmonisierung des europäischen Datenschutzrechtsahmens, der durch zu viele Spielräume der EU-Mitgliedstaaten für abweichende Regeln konterkariert wird. Für international agierende Unternehmen ist es für eine effiziente Umsetzung der Verordnung im gesamten Unternehmen oder der gesamten Unternehmensgruppe wichtig, dass es nicht zu viele nationale Sonderregeln gibt. Auch zur Erleichterung des Abschlusses von Verträgen über die Landesgrenzen hinweg ist die Einheitlichkeit des Rechts entscheidend. **Die Öffnungsklauseln sollten daher gründlich geprüft werden.**

8. Art. 12: Anzeige der Rufnummer des Anrufers und des Angerufenen und deren Unterdrückung

Die in **Art. 12 Abs.1 lit. c)** niedergelegte Pflicht zur Etablierung einer netzseitigen Funktion der Abweisung von Anrufen mit unterdrückter Rufnummer (ACR) im Hinblick auf (1) das Volumen der so initiierten Anrufe und (2) den Umfang der damit verbundenen Rechtsgutsverletzung ist nicht verhältnismäßig. Hinzu kommt, dass auf der Seite des Endgeräts ohne weiteres entsprechende Funktionalitäten aktiviert werden können. Vor diesem Hintergrund erscheint es angemessen, nicht nur den eigentlichen Verursacher auszublenden, sondern darüber auch die Möglichkeit außer Betracht zu lassen, sich effektiv gegen diese Anrufe zu wehren. Schließlich ist es auch im Einzelfall faktisch und rechtlich möglich, über die Auswertung von Verkehrsdaten die Urheber derartiger Praktiken zu identifizieren und zur Rechenschaft zu ziehen.

Für den angerufenen Endnutzer sollte die Möglichkeit bestehen, seine Rufnummer auf die Sammelrufnummer zu beschränken (*beispielsweise die Zentrale eines Unternehmens*) und insbesondere die Nebenstellen beim anzurufenden Endnutzer nicht anzuzeigen. **Diese Ergänzung sollte in einem zusätzlichen Absatz lit. e) mitaufgenommen werden.**

9. Art. 15 Teilnehmerverzeichnisse

Mit der vorgeschlagenen Formulierung des Art. 15 sind Problemstellungen verbunden, die ein weiteres Erscheinen von sog. „weißen" Seiten, also namensalphabetischer, die Kommunikationsdaten privater Personen enthaltenden Verzeichnissen in allen medialen Ausprägungen, sowie Auskunftsdienste mit den Kommunikationsdaten Privater in der Zukunft praktisch unmöglich machen. In Deutschland würden so rund 80 % der in diesem Markt tätigen Unternehmen mit mehreren 1000 Mitarbeitern die Geschäftsgrundlage entzogen, mindestens 500 Millionen Euro Marktvolumen würden vernichtet.

- **Der Markt für Betreiber elektronischer Kommunikationsdienste und der Markt für Verzeichnis- und Auskunftsdienste sind bis auf wenige Ausnahmen voneinander unabhängig und getrennt.** Art. 15 konkretisiert, dass die Betreiber öffentlich zugänglicher Verzeichnisse, also in Deutschland rund 200 meist mittelständische

Unternehmen, das Einverständnis der dort eingetragenen und veröffentlichten natürlichen Personen einholen und sie über die weiteren Einzelheiten, die mit einer Eintragung verbunden sind, informieren müssen. Die Verzeichnis-Anbieter in Deutschland und anderen EU-Mitgliedsstaaten verfügen über keinerlei Kontakt zu „Subscribern" (Def. alter Art. 12) oder „Endnutzern", ja dürfen aufgrund der bereits geltenden datenschutzrechtlichen Bestimmungen gar keinen Kontakt zu diesen aufnehmen, da zwischen beiden kein Rechtsverhältnis besteht. Ein Einholen des Einverständnisses durch jeden einzelnen der über 200 Auskunfts- und Verzeichnisanbieter würde zudem von den Endnutzern nicht akzeptiert, ein freier Wettbewerb dementsprechend gegenüber anbietereigenen Verzeichnis- und Auskunftsdiensten massiv behindert bzw. sogar verhindert. **Betreiber von Verzeichnisdiensten sind nicht in der Lage, den in Art. 15 des Entwurfs festgelegten Verpflichtungen nachzukommen. Die seit Jahrzehnten bewährte Systematik, dass die Kommunikationsdaten vom Anbieter der elektronischen Kommunikationsdienste aufgenommen werden, muss daher zwingend beibehalten werden.**

- **Einwilligung bzw. Widerspruchsrecht:** Die Erfahrungen mit dem derzeit gem. § 104 TKG in Deutschland geltenden Antrags-Erfordernis haben eindeutig belegt, dass die Anwendung einer Antrags- oder Einwilligungsregelung für die Veröffentlichung von Kommunikationsdaten von den Betroffenen aufgrund des von ihnen selbst als eher gering eingeschätzten Schutzbedürfnisses nicht erwartet wird. Die negativen Folgen einer schon aus Unkenntnis über die Regelung und deren Folgen nicht abgegebenen Einwilligung werden vielfach erst nach Monaten wahrgenommen und sind dann kaum noch zu heilen. Ein klares, einfach und unkompliziert auszusprechendes Widerspruchsrecht wird gerade in dieser Hinsicht auch auf Seiten der überwiegenden Mehrheit der Endnutzer als vollkommen ausreichend angesehen und trägt dem Schutzbedürfnis – wie auch die weitestgehend kritiklose Nutzung von OTT-Diensten wie WhatsApp etc. deutlich belegt – vollkommen und umfassend Rechnung. OTTs verfügen bereits heute über Kommunikationsadressen auch privater Nutzer und sind zudem in der Lage, private Netzwerke und Beziehungsgeflechte auszulesen. Hier muss eine größtmögliche Gleichbehandlung mit den Verzeichnisanbietern in Deutschland bzw. der EU sichergestellt werden.

- **Natürliche Personen, die wirtschaftlich agieren:** Art.15 in der Entwurfsfassung differenziert nicht zwischen natürlichen Personen und z.B. Einzelkaufleuten, Selbstständigen, Kleingewerbetreibenden und Freelancern, also Einzelpersonen, die wirtschaftlich tätig sind. Um diesen eine möglichst breite Erfassung in Verzeichnissen und damit eine Gleichbehandlung mit ihren Wettbewerbern anderer Rechtsformen zu ermöglichen, sollten wirtschaftlich agierende Einzelpersonen juristischen Personen gleichgestellt werden. Gleiches sollte für Daten gelten, die in anderen öffentlich zugänglichen Quellen bereits veröffentlicht wurden sowie Daten, die die Endnutzer selbst z. B. über Selbsteintragungstools bereitgestellt haben.

10. Art. 16: Unerbetene Kommunikation

Das mit **Art. 6 Abs. 1 lit. f i.V.m. Art. 21 Abs. 2 DS-GVO gefundene Ansatz** erkennt die Verarbeitung personenbezogenen Daten zum Zwecke des Direktmarketings grundsätzlich als legitimes Interesse an und gibt dem Betroffenen ein jederzeitiges Widerspruchsrecht. Dieses Konzept wird durch die Regelung in **Art. 16 Abs. 1** konterkariert. Lediglich im gegenüber der DS-GVO deutlich beschränkten Umfang der (Rück-)Ausnahme in Art. 16 Abs. 2 wird dieses Konzept wieder aktiviert. Für welche Arten des Direktmarketings in Zeiten der Digitalisierung von Geschäftsprozessen damit ein Anwendungsbereich für Art. 6 Abs. 1 lit. f verbleibt, ist unklar.

Darüber hinaus sollte aus deutscher Perspektive das Verhältnis der Vorschriften zum telefonischen Marketing, insbes. Art. 1, zu den geltenden UWG-Bestimmungen geklärt werden. **Es sollte dann an dieser Stelle die Gelegenheit genutzt werden, bestehende Unklarheiten des § 7 Abs. 3 UWG zu beseitigen**, die sich derzeit auch in Art. 16 wiederfinden. Dies ist etwa die Frage, was „ähnliche Produkte oder Dienstleistungen" sind, und ob die Annahme von „Geschäftsbeziehungen" („context of a sale") voraussetzt, dass es tatsächlich zum Geschäftsabschluss gekommen ist oder die Anbahnung eines Geschäfts ausreicht; ferner die Frage, zu welchem Zeitpunkt der Hinweis auf das Widerspruchsrecht zu erfolgen hat.

11. Art. 17: Information über erkannte Sicherheitsrisiken

Art. 17 legt Informationspflichten für Betreiber „elektronischer Kommunikationsdienste" fest, die den „Endnutzer" darüber informieren müssen, wenn ein „besonderes Risiko" besteht, dass die Sicherheit von Netzen „beeinträchtigt werden könnte".

- **Mehrfachregulierung sollte vermieden werden:** Auch nach anderen Gesetzen wie dem IT-Sicherheitsgesetz oder dem Kodex bestehen bereits Meldepflichten. Eine Mehrfachregulierung sollte vermieden werden. So sollte nicht nur die RL 2002/58/EU, sondern auch die VO 611/2013/EU aufgehoben werden; dieses Ergebnis hat der Verordnungsgeber in den Erw. 19 ff. der VO 611/2013/EU bereits im Blick gehabt. **Auf Grund der Mehrfachregulierung könnte Art.17 gestrichen werden.**

- **Unbestimmte Vorschrift wird zu Auslegungsproblemen in der Praxis führen:** Sollte, die Vorschrift nicht gestrichen werden, sollte zumindest im Rahmen des **Art. 17** klarer formuliert werden, welche Erheblichkeits- und welche Wahrscheinlichkeitsschwelle erreicht sein muss, um die Pflicht zur Information des Nutzers nach sich zu ziehen. Die Vorschrift und insbesondere Formulierung „beeinträchtigt werden könnte" ist zu unbestimmt und in der Praxis so nicht handhabbar. Auch müssen Sicherheitsrisiken für das Netz insgesamt nicht zwangsläufig zu Risiken für die Rechte und Freiheiten der Endnutzer führen. Zudem bringt bereits der Betrieb des Netzes an sich und die Nutzung des Netzes durch die Endnutzer abstrakte Risiken mit sich, die einzugehen sich der Endnutzer zwangsläufig entscheidet. Das gilt umso mehr, als die vorgeschlagenen Anforderungen deutlich über die i.R.d. Verordnung 611/2013/EU festgelegten hinausgehen

- **Hinweise auf anerkannte Informationen zu Sicherheitsrisiken sollten ausreichend sein:** Sicherheitsbehörden wie das BSI weisen bereits auf eine allgemeine Gefährdungslage hin. Es sollte in der eP-VO klargestellt werden, das man der Informationspflicht auch nachkommen kann, indem man durch einen Link solche anerkannten Informationen bereitstellt. Dies wäre insbesondere für kleine und mittelständische Unternehmen besser handhabbar.

12. Art. 18 ff.: Unabhängige Aufsichtsbehörden und Durchsetzung

Generell begrüßt der Bitkom, dass die eP-VO an dieser Stelle auf die Vorschriften der DS-GVO zurückgreift:

- **Klare Abgrenzung der Kompetenzen der Behörden:** Es sollte klar in Deutschland abgegrenzt werden, welche Behörden (BNetzA, BfDI, Landesdatenschutzbehörden, telekommunikations-spezifische Regulierungsbehörden) für welche Sachverhalte zuständig sind. Die teilweise überlappenden Kompetenzen führen insbesondere in Deutschland, wo es allein 17 Datenschutzbehörden gibt, zu Rechtsunsicherheit.

- **Abgrenzung bezüglich Sanktionen zur DS-GVO und anderen Rechtsakten:** Es sollte klargestellt werden, dass Sachverhalte, welche neben der Verletzung von Bestimmungen der eP-VO auch eine Verletzung der DS-GVO darstellen können, nur auf Grund einer Vorschrift und eines Verwaltungsverfahrens sanktioniert werden. Darüber hinaus drohen Marktverzerrungen, da die EU-Mitgliedsstaaten nach Art.24 das Strafmaß selbst festlegen können. Diese sollten sich daher bereits bei der derzeitigen Umsetzung der DS-GVO eng abstimmen.