VERBAND DER INTERNETWIRTSCHAFT E.V.

Stellungnahme zum Entwurf der Europäischen Kommission über den 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 (COM(2017)10 final)

Berlin, 28. Februar 2017

Am 10. Januar 2017 stellte die Europäische Kommission ihren Entwurf für den 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 (COM(2017)10 final) (ePrivacyVO) vor. Die Verordnung soll nach dem Wunsch der Kommission die Vertraulichkeit der elektronischen Kommunikation regeln und darüber hinaus Regeln für die Übermittlung von Daten und deren Speicherung festschreiben. Die ePrivacyVO soll laut Aussage der EU-Kommissarin Věra Jourová ein Lex Specialis zur EU Datenschutz-Grundverordnung (DS-GVO) sein. Die hier getroffenen Regelungen würden also demzufolge Vorrang vor denen aus der DS-GVO haben.

In ihrer Strategie für den digitalen Binnenmarkt im Jahr 2015 hat die Kommission festgesetzt, dass die bis jetzt gültige ePrivacy-RL (Richtlinie 2002/58/EU) einer Überprüfung unterzogen werden solle, um sicherzustellen, dass ihre Vorgaben mit denen der Datenschutzgrundverordnung in Einklang stehen. Das Ergebnis, eine neue ePrivacyVO, geht weit über dieses formulierte Ziel hinaus. eco hat sich in der Vergangenheit dafür eingesetzt, dass ein möglichst einheitlicher und sektorenübergreifender Regulierungsrahmen für den Datenschutz geschaffen wird.

Allgemeine Anmerkungen:

Datenschutz soll im europäischen Binnenmarkt grundsätzlich einheitlichen universellen Maßstäben unterworfen sein. Sektorspezifische Regelungen – wie beispielsweise für den Bereich der elektronischen Kommunikation – sollten sich auf einen klar umrissenen Bereich konzentrieren. Ein so präzisiertes regulatorisches Umfeld bietet allen Teilhabern der digitalen Gesellschaft – vom Anbieter elektronischer Kommunikationsdienste bis hin zu Webseitenbetreibern und Internetnutzern – Rechts- und Planungssicherheit. Mit der neu vorgelegten ePrivacyVO geht die Kommission weit über das gesteckte Ziel einer Überprüfung der bestehenden Richtlinie hinaus. Die ePrivacyVO schränkt digitale Geschäftsmodelle ein und erschwert den Aufbau einer europäischen Datenwirtschaft durch restriktive Vorschriften und eine übermäßige Ausweitung des Regulierungsfelds.

Der Umstand, dass die Verordnung direkt gültiges Recht in allen Mitgliedsstaaten wird, sorgt zusätzlich für Anpassungs- und Umsetzungsbedarf in der deutschen Telekommunikations- und Telemedienregulierung im Bereich des

TKG und des TMG. Gleichzeitig bestehen aber sowohl durch den Umstand, dass die Kommission den Weg einer Verordnung gewählt hat, als auch durch die Inhalte der Verordnung Probleme, die speziell die Internetwirtschaft vor Herausforderungen stellt.

- **Ausweitung der Regulierung durch die ePrivacyVO**

Die ePrivcayVO bezieht sich auf die beiden für die Internetwirtschaft zentralen Verordnungen des europäischen Kodex für die elektronische Kommunikation (EECC) und der EU-DS-GVO. Gleichzeitig führt die ePrivacyVO neue Definitionen in Bezug auf die DS-GVO ein und erweitert bestehende Definitionen des EECC.

So wird zum einen der Anwendungsbereich der Regulierung von Diensten eröffnet, die in den EECC ausdrücklich nicht mit einbezogen sind. Die zusätzlichen Definitionen im Bereich des Datenschutzes erweitern die Regeln der EU-DS-GVO auf jegliche elektronische Kommunikation – auch auf solche, die nicht zwischen Personen stattfindet. Diese Ausweitung steht den Zielen der EU-Kommission aus der Strategie für den digitalen Binnenmarkt entgegen, eine europäische Datenwirtschaft (Building a European Data Economy) aufzubauen und die Rahmenbedingungen für Big Data Angebote und den freien Verkehr von Daten in Europa zu ermöglichen. Hier haben sich gerade in den vergangenen Jahren Akteure, die spezialisierte Dienstleistungen – auch für klassische Industrieunternehmen – zur Verfügung stellen und in einem stark spezialisieren Wettbewerbsumfeld agieren, am Markt etabliert.

- **Fragmentierung der Datenschutzregulierung**

Problematisch ist, dass einzelne Aspekte der ePrivacyVO in einem unklaren Verhältnis insbesondere zur EU-DS-GVO stehen. Dies ist beispielsweise in Artikel 6 der ePrivacyVO der Fall, der keine Aussage zur Weiterverarbeitung von Daten trifft. Die DS-GVO ermöglicht hier in begrenztem Rahmen die Weiterverarbeitung. Inwieweit dieser Rahmen aber ausgeschöpft werden kann, wird aus dem Verordnungsentwurf nicht ersichtlich, da diese lediglich die Verarbeitung selbst restriktiv handhabt. Auch ist die Bezugnahme auf mehrere Artikel aus der EU-DS-GVO (Artikel 18ff) problematisch, da diese im Zuge des weiteren Gesetzgebungsverfahren stärker abgewandelt werden können, so dass die Datenschutzregulierung durch die ePrivacyVO noch stärker fragmentiert wird.

Erschwerend kommt hinzu, dass für die EU-DS-GVO Delegierte und Durchführungsrechtsakte entwickelt werden können, die die Umsetzungsregeln für die DS-GVO näher bestimmen und die in einem Spannungsverhältnis mit der ePrivacyVO stehen, für die ebenfalls Delegierte und Durchführungsrechtsakte entwickelt werden könnten.

Der vorliegende Verordnungsentwurf sorgt nicht für Rechtssicherheit, sondern für Unklarheit. Eine weitere Fragmentierung der Regulierung durch national unterschiedlich ausgelegte Statuten könnte die oben beschriebenen Probleme verstärken.

- **Die Regelungssystematik zwischen EECC, EU-DS-GVO und ePrivacyVO wird inkonsistent**

Zwar wird immer wieder betont, dass die ePrivacyVO ausschließlich für einen bestimmten Bereich als Lex Specialis zur EU-DS-GVO gilt. Doch bereits die aufgeworfenen Aspekte zeigen, dass diese Abgrenzung nicht gelungen ist.

Unklar ist zudem, wie das Verhältnis zum EECC an dieser Stelle ist. Der ursprüngliche Ansatz der EU-Kommission, eine klare EU-DS-GVO vorzulegen, die für alle Marktteilnehmer ein einheitliches und hohes Maß an Datenschutz vorschreibt, und mit dem EECC einen Rahmen für den Telekommunikationsmarkt und diesem entsprechenden Regeln zu definieren, ist verloren gegangen. Mit der ePrivacyVO wird so ein neuer, separater Geltungsbereich abgesteckt, der die Maßstäbe der maßgeblichen europäischen Rechtsakte verzerrt und damit inkonsistent.

- **Die ePrivacyVO bedarf einer grundsätzlichen Überarbeitung**

Der Entwurf der ePrivacyVO wirft zahlreiche, grundsätzliche regulatorische Fragen auf – in Bezug auf das Regulierungsgefüge und auch in Bezug auf die Vereinbarkeit von bestehenden Regulierungen bspw. durch die EU-DS-GVO. Diese Fragen müssen beantwortet werden. Die ePrivacyVO muss mit der EU-DS-GVO harmonisiert werden, überflüssige Regelungen gestrichen werden. Die EU-Kommission hat wiederholt bekräftigt, dass die ePrivacyVO gleichzeitig mit der EU-DS-GVO in Kraft treten soll. Der Zieltermin wäre damit der 25. Mai 2018. Dieser Umstand ist in zweierlei Hinsicht äußerst unglücklich. Zum einen wird sich der Gesetzgebungsprozess der ePrivacyVO aller Voraussicht nach noch bis zum Ende des Jahres hinziehen. Zum anderen zeigt sich in Bezug auf die Inhalte der Verordnung grundsätzlicher, intensiver Prüfungs- und Erörterungsbedarf.

Stellt man die schon jetzt greifbaren inhaltlichen Wechselwirkungen von ePrivacyVO und EU-DS-GVO heraus, wird klar, dass eine Umsetzung der beiden Rechtsakte in der gegebenen Zeit von den Unternehmen der Internetwirtschaft nicht erfolgen kann. Eine Verlängerung der Frist ist daher unumgänglich. Erschwerend kommt auch hinzu, dass der EECC als zweiter Bezugspunkt noch nicht verabschiedet ist. Auch die Annexe des EECC und die GEREK Verordnung können hier zusammen mit dem EECC eine Wechselwirkung mit der ePrivacyVO entfalten. Eine vorschnelle Verabschiedung der ePrivacyVO mit Bezug zu diesen Regelungen sollte daher unterbleiben.

Hinzu kommt der dringende Bedarf nach einer grundsätzlichen Überprüfung der einzelnen Artikel auf Notwendigkeit, Geltungsbereich und Wechselwirkungen mit bereits bestehenden Regulierungen und den daraus resultierenden Umfassenden Beratungen mit Internetwirtschaft, Zivilgesellschaft und politischen Akteuren. Dieser sollte ausgeschöpft werden, um eventuell noch bestehende Regelungslücken gemeinsam zu identifizieren und sinnvoll zu adressieren.

Anmerkungen zu den einzelnen Regelungen:

- **Zu Artikel 1 „Gegenstand“**

Artikel 1 entspricht einer modifizierten Form des Artikel 1 der EU-DS-GVO. Er erweitert aber den Kreis der Betroffenen im Vergleich zur DS-GVO um juristische Personen (Art. 1 lit. 1). De facto weitet dieser Aspekt den Datenschutz auf Daten jenseits der personenbezogenen Daten aus. Dies hat entsprechende Auswirkungen auf weitere Wirtschaftsbereiche, in denen Daten elektronisch übermittelt und verarbeitet werden. Gerade im Bereich der M2M Kommunikation ist dies problematisch, da bspw. im Bereich der Produktion von Gütern, der Warenwirtschaft und der Logistik u.U. persönliche Daten gar nicht berührt sind. In der weiteren Diskussion wäre es daher sinnvoll, genau zu überprüfen, inwieweit diese materielle Ausweitung des Geltungsbereichs der ePrivacyVO tatsächlich sinnvoll ist, oder ob dadurch nicht bereits bestehende bewährte Praktiken infrage gestellt und Innovationen gehemmt werden.

- **Zu Artikel 4 „Begriffsbestimmungen“**

Artikel 4 der Verordnung greift die beiden maßgeblichen benachbarten Regulierungen der EU-KOM auf – den EECC und die EU-DS-GVO. Positiv hervorzuheben bleibt hier, dass der Gesetzgeber erkennbar diesen Regulierungen und den dort festgesetzten Begriffen Rechnung getragen hat. Gleichzeitig stellt sich aber in Bezug auf die Übernahme der Definitionen aus dem E-ECC (Art. 4 lit. 1b, Art. 4 lit. 2) eine zentrale Problematik der ePrivacyVO. Die Erweiterung des Begriffes der „interpersonellen Kommunikationsdienste“ auch um solche Dienste, die auch die interpersonelle Kommunikation als „Nebenprodukt“ ermöglichen (vgl. Erwägungsgrund 11). Die Abgrenzung ist dadurch schwierig. Die EU-Kommission selbst hat dies in Bezug auf soziale Netzwerke bei der Präsentation am 10. Januar 2017 dahingehend konkretisiert, dass lediglich die Nachrichtenfunktion der Plattformen bzw. Dienstleistungen unter die Regulierung falle. Dies wiederum führte zu weiteren Nachfragen von Bürgerrechtsorganisationen, die die Verordnung anders ausgelegt hatten. Offensichtlich wurde dadurch, dass die vorliegende Definition sehr problematisch ist und überprüft werden muss.

Mit Blick auf diese Debatte kann festgehalten werden, dass die in der ePrivacyVO getroffenen Regeln unklar sind – bspw. bei der Frage, ob bei größeren Plattformen lediglich der Anteil der persönlichen Kommunikation geschützt ist, oder ob auch weitere Aspekte dieser Plattformen berührt sind.

Auch die in Art. 4 lit. 3 eingeführten Begriffe „elektronische Kommunikationsdaten“ bzw. deren Unterscheidungen von „elektronische Kommunikationsmetadaten“ (Art. 4 lit 3c) und „elektronische Kommunikationsinhalte“, sind unscharf, was zu Debatten darüber geführt hat, in welchen Fällen bspw. Standortdaten von wem verarbeitet werden dürfen. Die von der EU intendierte technologieneutrale und offene Definition sorgt hier für Unklarheit (vgl. Erwägungsgrund 14). Darüber hinaus besteht durch die Definition das massive Problem, dass der Schutzgegenstand aus der EU-DS-GVO – die personenbezogenen Daten – ausgeweitet wird auf jegliche Form des elektronischen Austauschs von Daten. Die Kommunikation zwischen zwei Geräten in den Schutz der Privatsphäre mit einzuschließen, ist nicht hilfreich.

Die Folgen sind Unklarheiten bei der Gestaltung, insbesondere von elektronischer Kommunikation im Geschäfts- und im technischen Bereich – also zwischen verschiedenen Endgeräten, die gemäß Erwägungsgrund 12 der ePrivacyVO ausdrücklich eingeschlossen sein sollen.

Die Regelung sollte dringend überprüft werden und in Bezug auf Reichweite korrigiert werden.

- **Zu Artikel 5 „Vertraulichkeit elektronischer Kommunikationsdaten”**

Artikel 5 stellt klar, dass die in Artikel 4 definierten „elektronische Kommunikationsdaten“ vertraulich zu behandeln sind. Er schränkt die Verarbeitung aller elektronischen Kommunikationsdaten erheblich ein, sofern nicht die vorliegende Verordnung die Verarbeitung zulässt. Die Regelung soll dazu dienen, die in Artikel 4 definierten „elektronischen Kommunikationsdaten“ umfassend vor Zugriff durch andere Personen oder Organisationen als die Teilnehmer der Kommunikation schützen. Eine solche Herangehensweise ist problematisch. Neue, innovative Wege zur Datenverarbeitung werden damit unterbunden und für Unternehmen und Marktteilnehmer eingeschränkt, bzw. sind schwerer zu realisieren, da Einwilligungen eingeholt werden müssen.

eco empfiehlt, die vorliegende Regelung im Einklang mit der EU-DS-GVO offener zu gestalten und zu prüfen, inwieweit überhaupt Bedarf besteht für eine spezielle Regel zur Vertraulichkeit im Umgang mit elektronischen Kommunikationsdaten.

- **Zu Artikel 6 „Erlaubte Verarbeitung elektronischer Kommunikationsdaten“**

Artikel 6 soll die für Artikel 5 benannten Ausnahmen formulieren, in denen die Verarbeitung von elektronischen Kommunikationsdaten zulässig ist. Das hier aufgezeigte verbleibende Spektrum für die Datenverarbeitung ist problematisch. Die Vorgaben zur Verarbeitung von Metadaten (Artikel 6 lit. 2a) sind

zu streng. Sie könnten sich auch auf die Anbieter anderer Dienste wie der Überprüfung der Quality of Service erstrecken.

Auch ist die Regelung der ausdrücklichen Zustimmung zur Verarbeitung von Daten zu konkreten Zwecken (Art. 6 lit. 2 und Art. 6 lit. 3b) problematisch, da sie zu enge Vorgaben macht. Für zusätzliche Formen der Verarbeitung im Rahmen von Kommunikationsdiensten müsste dieser Regelung zu Folge eine neue Einwilligung vom Nutzer erfragt werden.

Die in Art. 6 lit. 3b formulierte Anforderung zur Anonymisierung geht de facto über die EU-DS-GVO hinaus, da diese besagt, dass Daten zu pseudonymisieren seien. In der EU-DS-GVO und in der ePrivacyVO ist der Begriff der Anonymisierung selbst nicht definiert, an dieser Stelle somit ein unbestimmter Rechtsbegriff.

eco fordert, bei Artikel 6 zu prüfen, inwieweit die Einwilligungsregeln mit den Prinzipien der EU-DS-GVO harmonisierbar sind und inwieweit die Auflagen für die Pseudonymisierung aus der EU-DS-GVO einer Anonymisierung gerecht werden. Vor diesem Hintergrund wäre dann auch zu prüfen, ob der Artikel 6 nicht grundsätzlich anders gefasst werden müsste und i.V.m. Artikel 5 die Systematik der Regelung – ein pauschales Verbot mit einzelnen Ausnahmetatbeständen – geändert werden müsste. In ihrer jetzigen Form stellen diese wenigen und eng gefassten Ausnahmeregeln mit unklaren Formulierungen ein Hemmnis für die europäische Datenwirtschaft dar.

- **Zu Artikel 7 „Speicherung und Löschung elektronischer Kommunikationsdaten“**

Artikel 7 schreibt vor, dass elektronische Kommunikationsinhalte grundsätzlich durch den Betreiber zu löschen oder zu anonymisieren sind, wenn die Empfänger sie erhalten haben (Art. 7 lit. 1). Dies gilt darüber hinaus auch für die bei einer Kommunikation anfallenden Metadaten (Art. 7 lit. 2). Beide Aspekte sind problematisch zu sehen. Löschung und Anonymisierung von Kommunikationsinhalten korrespondieren mit den zu Artikel 6 aufgeworfenen Kritikpunkten, dass der Begriff der Anonymisierung nicht eindeutig definiert ist (im Gegensatz zur Pseudonymisierung). Auch wurden vereinzelt Bedenken geäußert, dass mit der vorliegenden Auflage zur Anonymisierung bzw. Löschung von Kommunikationsmetadaten derzeit angebotene Dienste von Telekommunikationsdiensteanbietern wie bspw. die Erstellung von Heatmaps zur Überprüfung der Netzauslastung oder dem Auftreten von Störungen deutlich erschwert würden. Der Erwägungsgrund 17 sieht aber genau die Erstellung dieser Heatmaps als relevant an und führt dazu aus, dass Positionsdaten an dieser Stelle nicht als Metadaten zu verstehen seien.

Diese Debatte zeigt, dass die Regeln der ePrivacyVO zu weit gefasst, zu unspezifisch sind, und nicht geeignet, um eine europäische Datenwirtschaft aufzubauen. Sie birgt sogar die Gefahr, bestehende Praktiken zu unterminieren, die sich für den Breitbandausbau und ggfs. auch später für die Verkehrsplanung als nützlich erweisen könnten. Der Artikel 7 sollte für die Speicherung und Verarbeitung von elektronischen Kommunikationsdaten als

Maßstab die Artikel 5 bis 11 der EU-DS GVO nehmen und den Datenschutz ausdrücklich auf personenbezogene Daten beschränken und die Verarbeitung und ggfs. Weiterverarbeitung von Daten in dem von der DS-GVO gesetzten Rahmen ermöglichen.

- **Zu Artikel 8 "Schutz der in Endeinrichtungen der Endnutzer gespeicherten oder sich auf diese beziehenden Informationen"**

Artikel 8 soll den Umgang der Kommunikation mit Nutzerendgeräten regeln. Auch hier besteht das Problem, dass der Schutz vertraulicher Kommunikation auf Bereiche ausgeweitet wird, die über den Schutz der personenbezogenen Daten weit hinausgehen (vgl. dazu Erwägungsgrund 20).

Positiv hervorzuheben ist, dass der Artikel selbst so formuliert ist, dass er Geschäftsmodelle zur Refinanzierung entgeltfreier Dienste nicht grundsätzlich ausschließt und z.B. der Einsatz von Cookies zur Verbesserung des Angebotes weiterhin möglich ist. Gleichzeitig sind die Formulierungen jedoch unscharf, so dass Unklarheit über den Einsatz bestimmter Analysetools besteht (Art. 8 lit. 1d). So bleibt der Einsatz von Analysetools dritter Anbieter durch den Verordnungstext unklar. Die Kommission hat bei der Präsentation der ePrivacyVO zwar erklärt, dass die Messung des Publikums auf Internetauftritten grundsätzlich möglich bleiben sollte. Dies spiegelt sich jedoch in der derzeit vorliegenden Formulierung nicht wieder. Die Regelung zur Einwilligungspflicht bei 3rd-Party Cookies birgt ebenfalls Risiken in sich, da sie Einwilligungen der Nutzer erfordert. Unternehmen, die mit solchen Produkten auf die Nutzer zugehen, werden zunächst eine Vielzahl an Einwilligungen einholen müssen. Anbieter von Diensten und Produkten, die sich ausdrücklich auf die Messung von Webseitenpublikum oder auf das Ausrollen von Werbung fokussieren, läuft dies zuwider. Schwierig ist im Kontext der Cookies vor allem auch die Frage nach der Wechselwirkung mit der EU-DS-GVO, welche in Erwägungsgrund 30 explizit Cookies aufführt und auf die Artikel 4ff der DS-GVO verweist. Um Doppelregulierung zu vermeiden, sollte der Umgang mit Cookies und Endgeräten über die EU-DS-GVO und deren Delegierten und Durchführungsrechtsakten erfolgen, anstatt über eine zusätzliche Regulierung in der ePrivacyVO.

- **Zu Artikel 9 „Einwilligung"**

Die Einwilligung ist im europäischen Datenschutz zentraler Aspekt. Daher ist zu begrüßen, dass sich die ePrivacyVO auch an den in der EU-DS-GVO vorgelegten Definitionen orientiert. Unklar bleibt indes, ob die in Artikel 9 lit. 2 formulierten Regelungen tatsächlich den Anforderungen der Artikel 7 und 8 der DS-GVO gerecht werden und inwieweit aus diesen Artikeln weitere Delegierte und Durchführungsrechtsakte entstehen, bzw. wie sich diese zur ePrivacyVO verhalten.

Auch die Wechselwirkung zu lit. 3 des Artikels 9 ist an dieser Stelle fehl am Platz. Die Erinnerungsverpflichtung alle 6 Monate wird dazu führen, dass

Nutzerinnen und Nutzer von einer wahren Flut an Anfragen überhäuft werden. Ob eine solche Form der Erinnerung überhaupt im Nutzerinteresse sein kann, darf somit stark bezweifelt werden.

- **Zu Artikel 10 „Bereitzustellende Informationen und Einstellungsmöglichkeiten zur Privatsphäre"**

Artikel 10 regelt, wie die Privatsphäreeinstellungen von Software, die dem Markt zur Verfügung gestellt wird, zu gestalten sind. Positiv hervorzuheben ist an dieser Stelle, dass für die Umsetzung dieser Regelung die Möglichkeit besteht, dies im Rahmen eines Updatezyklus durchzuführen und so die Belastungen für die Umstellung möglichst gering zu halten. Ist der Anpassungsbedarf bei den zahlreichen Computerprogrammen und Apps, die voraussichtlich betroffen sein werden, doch enorm.

Dennoch ist die Notwendigkeit dieses Artikels vor dem Hintergrund des Artikels 25 der EU-DS-GVO, der Privacy by Design vorschreibt, fragwürdig. Die Umsetzung, insbesondere bei alter und obsoleter Software, die nicht mehr am Markt angeboten wird, ist nicht möglich. Der Artikel 10 der ePrivacyVO trägt damit weder den Anforderungen an Software noch der Realität vernetzter Systeme Rechnung. Der Artikel 25 EU-DS-GVO ist ausreichend. Der vorliegende Artikel sollte gestrichen werden.

- **Zu Artikel 11 „Beschränkungen"**

Artikel 11 gibt Beschränkungen für die Artikel 5 bis 8 auf gesetzlicher Grundlage durch Mitgliedsstaaten oder der EU aus.

Hier besteht das Risiko, dass solche Zugriffswünsche unter dem Aspekt der Einrichtung interner Verfahren zur Beantwortung von Anfragen auf Zugang zu elektronischen Kommunikationsdaten von Endnutzern (Art. 11 lit. 2) zu einer Doppelregulierung durch die EU einerseits und durch nationale Gesetze im Bereich der Sicherheit andererseits führen. Dem Subsidiaritätsprinzip folgend sollten solche Anforderungen durch nationale Gesetzgeber im Rahmen der Sicherheitsgesetzgebung erfolgen. Eine Doppelregulierung in diesem sensiblen Bereich ist nicht hilfreich.

Auch besteht begründeter Anlass zur Sorge, dass die in Art. 11 lit. 2 formulierten „internen Verfahren" Vorgaben zu Übergabeschnittstellen für das Auslesen auch von verschlüsselter Kommunikation beinhalten soll.

Vor diesem Hintergrund sollte geprüft werden, ob ein solcher Artikel überhaupt mit dem Ziel eines hohen Datenschutzes und einer sinnvollen vertraulichen Kommunikation vereinbar ist. Es sollte auf jeden Fall klargestellt werden, dass die hier aufgestellte Regelung Regierungsinstitutionen nicht dazu ermächtigt, standardisiert Daten auslesen zu können.

- **Zu Artikel 12 „Anzeige der Rufnummer des Anrufers und des Angerufenen und deren Unterdrückung“**

Artikel 12 der ePrivacyVO regelt die Anzeige der Identifikation von Kommunikationsteilnehmern auf Grundlage des Artikels 107 des EECC. Unklar bleibt an dieser Stelle, wieso die vorliegende Regelung nicht in den EECC Eingang gefunden hat, und inwieweit diese Regelung nicht den Artikel 107 konterkariert, der diese Aufgabe den nationalen Behörden zuweist. Im Zuge der Beratungen des EECC wäre es sinnvoll, über eine Übernahme des vorliegenden Artikels nachzudenken und zu prüfen, ob der hier formulierte Text nicht bereits durch den Vorschlag für den Artikel 107 abgedeckt ist.

- **Zu Artikel 14 „Sperrung eingehender Anrufe“**

Der Artikel regelt die Bereitstellung einer Möglichkeit zur Verweigerung der Annahme von Anrufen bei nummernbasierten interpersonellen Kommunikationsdiensten. Erwägungsgrund 30 führt an, dass hier vor allem Telefonanbieter ihre Kunden auf die Möglichkeit, sich vor unerwünschten Anrufen zu schützen, hinweisen sollen und ihnen dies entgeltfrei anbieten sollten. Zwar kann aus einer solchen Regelung der Bezug zum Schutz der Privatsphäre hergeleitet werden, dieser ist jedoch aufgrund des gewählten Weges über die Technologie nicht in einer ePrivacyVO zu regeln. Es könnte entweder eine Regelung über den EECC oder über einen Durchführungsrechtsakt zur EU-DS-GVO erfolgen. Inwieweit die Vorgabe der EU-DS-GVO zur Privacy by Design aus Artikel 25 mit der Annahme entsprechender Anrufe in Wechselwirkung steht, sollte erörtert werden.

- **Zu Artikel 15 „Öffentlich zugängliche Verzeichnisse“**

Der Artikel regelt Maßgaben für die Veröffentlichung in öffentlich zugänglichen Teilnehmerverzeichnissen. An dieser Stelle sei hervorzuheben, dass im EECC bereits Regelungen zu Auskunftsmedien getroffen worden sind. Im Sinne einer stringenten und kohärenten Regulierung wäre es begrüßenswert, wenn die Regelungen für Auskunftsmedien einheitlich gestaltet würden. Die Maßgaben der EU-DS-GVO zur Einwilligung in die Verwendung personenbezogener Daten müssen ebenfalls berücksichtigt werden.

- **Zu Artikel 17 „Information über erkannte Sicherheitsrisiken“**

Der Artikel 17 regelt, dass Betreiber von elektronischen Kommunikationsdiensten dazu verpflichtet sind, ihre Nutzer im Fall von „bestimmten Risiken, die die Sicherheit von Kommunikationsnetzen oder Diensten gefährden könnten“ darüber zu informieren und ihnen Wege zur Abhilfe unter Angabe der dafür möglicherweise anfallenden Kosten aufzuzeigen. Hier besteht die Frage, inwieweit diese Regelung überhaupt notwendig ist. Einerseits bestehen in der EU-DS-GVO Regelungen zum Umgang bei risikobehafteter Datenverarbeitung (Artikel 9 i.V.m. Artikel 35) und zur Meldepflicht (Artikel 33

DS-GVO). Andererseits beinhaltet die NIS-RL (Richtlinie 2016/1148/EU) Auflagen für die Meldung von Vorfällen beim Abfluss personenbezogener Daten (Art. 14 und 16 NIS-RL). Die durch die NIS-RL aufgestellte Systematik der Zusammenarbeit von Anbietern „digitaler Dienste“ wird durch den Verordnungsentwurf durcheinandergebracht. Die fakultative Formulierung „beeinträchtigt werden könnte“ ist an dieser Stelle nicht hilfreich, da sie die Zahl der Fälle, in denen Informationspflicht ausgelöst wird, deutlich erhöht und gerade bei Kommunikationsdiensten oftmals nicht klar ist, ob tatsächlich Daten abfließen.

- **Zu Artikel 29 „Inkrafttreten und Anwendung“**

Der Artikel stellt klar, dass die Verordnung am 25. Mai 2018 wirksam wird, bis dahin alle aufgestellten Regelungen umgesetzt sein müssen. Dieses Zeitfenster ist zu kurz bemessen. Wenn man bedenkt, dass zahlreiche IT-Produkte umgestellt werden müssen und neue Meldewege eröffnet werden sollen und Unternehmensprozesse neugestaltet werden müssen, wird dies offensichtlich. Die wenigen Monate, die zwischen der tatsächlichen Verabschiedung der Verordnung und ihrem Wirksamwerden vorhanden sein werden, sind für IT-Unternehmen nicht ausreichend, um den Anforderungen der ePrivacyVO adäquat gerecht zu werden.

Erschwerend kommt hinzu, dass auch der EECC, auf den sich verschiedene Artikel der ePrivacyVO beziehen, noch verabschiedet werden muss und Delegierte und Durchführungsrechtsakte der EU-DS-GVO derzeit in Abstimmung sind. Vor diesem Hintergrund ist es zwingend erforderlich zu prüfen, ob die Verabschiedung dieser Rechtsakte nicht abgewartet werden müsste, bevor mit der Arbeit an der ePrivacyVO fortgefahren werden kann und inwieweit die hier aufgestellten spezialgesetzlichen Regelungen dann überhaupt noch Sinn ergeben.