verbraucherzentrale
Bundesverband

# GEWÄHRLEISTUNG DER PRIVATSPHÄRE UND VERTRAULICHKEIT IN DER ELEKTRONISCHEN KOMMUNIKATION

Stellungnahme des Verbraucherzentrale Bundesverbands e.V. zum Vorschlag der EU-Kommission für eine Verordnung über Privatsphäre und elektronische Kommunikation

15. März 2017


**Impressum**

*Verbraucherzentrale*
*Bundesverband e.V.*

*Team*
*Digitales und Medien*

*Markgrafenstraße 66*
*10969 Berlin*

*digitales@vzbv.de*



Bundesverband der Verbraucherzentralen und Verbraucherverbände

Verbraucherzentrale Bundesverband e.V.

# INHALT

# I. EINLEITUNG

Die Datenschutzrichtlinie für elektronische Kommunikation[1] (folgend ePrivacy-Richtlinie / ePRL) spezifizierte und ergänzte die bisherige europäische Datenschutzrichtlinie[2], die ab Mai 2018 durch die europäische Datenschutz-Grundverordnung[3] (folgend DSGVO) abgelöst wird. In der Mitteilung „Strategie für einen digitalen Binnenmarkt für Europa“ (COM(2015) 192 final) vom 6. Mai 2015 legte die EU-Kommission fest, dass die ePRL überprüft werden sollte, sobald die DSGVO beschlossen wurde. In Folge dieser Überprüfung hat die EU-Kommission am 10. Januar 2017 einen Vorschlag für eine Verordnung über Privatsphäre und elektronische Kommunikation[4] (folgend ePrivacy-Verordnung / ePVO) vorgelegt.

Doch nicht nur die Änderungen des europäischen Rechtsrahmens macht eine Überarbeitung der ePRL notwendig, auch die schnell voranschreitenden technischen Entwicklungen im Bereich der elektronischen Kommunikation machen eine Novelle erforderlich. Eine Modernisierung ist dringend notwendig, um den Schutz der persönlichen Daten und die Privatsphäre der Verbraucherinnen und Verbraucher[5] auch in Zukunft zu gewährleisten und gleichzeitig die Rechtssicherheit und Wettbewerbsfähigkeit der europäischen Unternehmen zu stärken.

*Der Verbraucherzentrale Bundesverband (vzbv) begrüßt daher grundsätzlich die Vorschläge der EU-Kommission*. Aus Sicht der Verbraucher ist eine sektorspezifische Regelung für den Bereich der elektronischen Kommunikation auch weiterhin dringend geboten. Ziel der ePVO sollte es sein, eine europaweite Harmonisierung und eine hohe Konsistenz mit der DSGVO zu erreichen. Außerdem sollte der sachliche Anwendungsbereich der ePVO ausgeweitet werden, um auch Over-the-Top-Kommunikationsanbieter (folgend OTTs[6]) und Telemedien zu erfassen, wenn diese klassische Telekommunikationsdienste substituieren. In keinem Fall dürfen jedoch die neuen und überarbeiteten Vorschriften hinter den Prinzipien und Vorgaben der DSGVO zurück bleiben, sondern müssen sich an dieser messen lassen. Gleichzeitig darf auch der bisherige Schutzstandard der ePRL durch die ePVO nicht unterschritten werden.

---

[1] Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation) in der Fassung der Richtlinie 2009/136/EG vom 25. November 2009

[2] Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr

[3] Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG.

[4] Vorschlag für eine Verordnung über die Achtung des Privatlebens und den Schutz personenbezogener Daten in der elektronischen Kommunikation und zur Aufhebung der Richtlinie 2002/58/EG. Alle Artikel und Erwägungsgründe ohne Gesetzesangaben beziehen sich auf die ePVO.

[5] Die gewählte männliche Form bezieht sich stets auf weibliche und männliche Personen. Wir bitten um Verständnis für den weiteren Verzicht auf Doppelbezeichnungen zugunsten einer besseren Lesbarkeit des Textes.

[6] OTTs sind Dienste, die über einen Internetzugangsdienst angeboten werden, ohne dafür eine eigene Telekommunikationsinfrastruktur zu verwenden. Das Gremium Europäischer Regulierungsstellen für elektronische Kommunikation unterscheidet zwischen OTT-0-Diensten, die eine Verbindung zu klassischen Telekommunikationsdiensten herstellen können und der sektorspezifischen Telekommunikationsregulierung unterliegen, wie beispielsweise Skype-Out. OTT-1 bezeichnet Dienste, die sich unter anderem wegen ihrer eingeschränkten Konnektivität nicht als Telekommunikationsdienste qualifizieren, diese jedoch substituieren können, wie zum Beispiel Voice-Over-IP-Telefonate oder Instant Messaging. OTT-2, umfasst Dienste, die keine Telekommunikationsdienste substituieren, sondern komplementäre Leistungen anbieten, wie beispielsweise Social Media Plattformen oder Streaming-Portale. In dieser Stellungnahme werden unter dem Begriff „OTTs“ lediglich OTT-1-Dienste gefasst.

Der Verbraucherzentrale Bundesverband fordert die Institutionen der Europäischen Union sowie die Bundesregierung auf, die Rechte der einzelnen Verbraucher und Bürger konsequent ins Zentrum der Ausgestaltung der ePVO zu stellen. Ausgangspunkt der Betrachtungen und Ausgestaltung muss zwingend das Individuum und sein Recht auf Privatsphäre und Vertraulichkeit im Bereich der elektronischen Kommunikation sein.

Vor diesem Hintergrund begrüßt der vzbv, dass die Bundesregierung frühzeitig das Gespräch mit den verschiedenen Interessengruppen sucht und bedankt sich beim Bundesministerium für Wirtschaft und Energie für die Gelegenheit zur Stellungnahme.

# II. DIE KERNFORDERUNGEN IM ÜBERBLICK

### SEKTORSPEZIFISCHE REGELUNG

> Es ist weiterhin ein sektorspezifisches Gesetz im Bereich der elektronischen Kommunikation dringend geboten, das die DSGVO detailliert und ergänzt, um das Recht auf Privatsphäre und Vertraulichkeit im Bereich der elektronischen Kommunikation sicherzustellen.

### VERORDNUNGSCHARAKTER UND MARKTORTPRINZIP

> Ziel der ePVO ist es, eine europaweite Harmonisierung und eine hohe Konsistenz mit der DSGVO zu erreichen. Der vzbv bewertet es daher als positiv, dass die Form einer Verordnung gewählt und das Marktortprinzip festgelegt wurde. In keinem Fall dürfen die neuen und überarbeiteten Vorschriften hinter den Prinzipien und Vorgaben der DSGVO zurück bleiben, sondern müssen sich an dieser messen lassen. Gleichzeitig darf der bisherige Schutzstandard der ePRL durch die ePVO nicht unterschritten werden.

### EINBEZIEHUNG VON OTTS IN DEN ANWENDUNGSBEREICH

> Der sachliche Anwendungsbereich der ePVO muss ausgeweitet werden auf alle elektronischen Kommunikationsdienste, die funktional äquivalent zu klassischen Telekommunikationsdiensten sind und diese substituieren sowie auf interpersonelle Kommunikationsdienste, die nur eine untergeordnete Nebenfunktion eines anderen Dienstes darstellen.

### VERARBEITUNG VON ELEKTRONISCHEN KOMMUNIKATIONSMETADATEN

> Die in der ePVO vorgesehene Trennung von Kommunikationsinhalten und Kommunikationsmetadaten ist in der Praxis oftmals nicht möglich. Es muss daher klargestellt werden, dass immer von elektronischen Kommunikationsinhalten auszugehen ist, wenn aus den elektronischen Kommunikationsmetadaten Rückschlüsse auf die Inhalte der Kommunikation gezogen werden können.

## VERARBEITUNG VON ELEKTRONISCHEN KOMMUNIKATIONSINHALTEN

Da Inhalte der elektronischen Kommunikation hochsensible Informationen über die daran beteiligten natürlichen Personen offenlegen können, was zu schweren Folgen im persönlichen und gesellschaftlichen Leben führen kann, sollte für die Verarbeitung von elektronischen Kommunikationsinhalten stets eine ausdrückliche Einwilligung der Endnutzer erforderlich sein, soweit die Verarbeitung nicht erforderlich ist, um einen von den Endnutzern gewünschten Dienst zu erbringen.

## SCHUTZ DER IN DEN ENDEINRICHTUNGEN DER ENDNUTZER GESPEICHERTEN ODER SICH AUF DIESE BEZIEHENDEN INFORMATIONEN

Aufgrund der hohen Relevanz der mit den Endgeräten verbundenen Informationen für die Persönlichkeit und Privatsphäre der Endnutzer und den damit gleichzeitig einhergehenden hohen Gefahren, ergibt sich ein besonderes Schutzbedürfnis. Daher müssen die in Endeinrichtungen der Endnutzer gespeicherten oder sich auf diese beziehenden Informationen einem besonderen Schutz unterliegen.

## VERARBEITUNG VON IN DEN ENDEINRICHTUNGEN DER ENDNUTZER GESPEICHERTEN ODER SICH AUF DIESE BEZIEHENDEN INFORMATIONEN

Hinsichtlich der Verarbeitung von Informationen, die auf den Endgeräten der Endnutzer gespeichert sind oder sich auf diese beziehen, zum Zweck Messung des Webpublikums durch den Betreiber des vom Endnutzer gewünschten Dienstes, fehlen weitere dringend notwendige Schutzvorgaben. Die Endnutzer müssen der Verarbeitung widersprechen können. Außerdem müssen das Prinzip der Datenminimierung sowie die Vorgaben der DSGVO zur Auftragsverarbeitung Anwendung finden.

## ERHEBUNG VON INFORMATIONEN, DIE VON DEN ENDEINRICHTUNGEN AUSGESENDET WERDEN

Für die Erhebung von Informationen, die von Endeinrichtungen ausgesendet werden, sollte stets eine Datenschutzfolgeabschätzung durchgeführt werden müssen. Sollte diese zu dem Ergebnis kommen, dass ein hohes Risiko für den Betroffenen besteht, darf eine solche Erhebung nur mit Einwilligung des Endnutzers möglich sein.

Darüber hinaus muss klargestellt werden, dass die Grundprinzipien und Vorgaben der DSGVO zu den Anforderungen des Verordnungsentwurfs hinzutreten.

## EINWILLIGUNG DER ENDNUTZER

Das Verhältnis von Einwilligungen, die über Softwareeinstellungen vorgenommen wurden und Einwilligungen, die unabhängig davon abgegeben wurden, muss geklärt werden. Wenn der Endnutzer eine Einwilligung abgeben soll, die seiner Softwareeinstellung widerspricht, sollte diese neue Einwilligung immer ausdrücklich abgegeben werden müssen. Es muss außerdem klargestellt werden, dass der Endnutzer alle Einwilligungen stets widerrufen kann.

### (VOR)EINSTELLUNGEN ZUR PRIVATSPHÄRE

> Grundsätzlich sollten auch für Anbieter von Hardware und Software, die eine elektronische Kommunikation erlaubt, die Verpflichtungen des Privacy-by-Design und -Default gelten. Nur so können die Rechte der Endnutzer wirksam und praktikabel geschützt werden. Dies würde die DSGVO in sinnvoller und notwendiger Weise ergänzen.

### UNERBETENE KOMMUNIKATION PER E-MAIL

> Einer Ausweitung der Möglichkeiten für Direktwerbung im Vergleich zur derzeitigen Rechtslage ist inakzeptabel. Die Kontaktangaben des Endnutzers sollten ohne seine Einwilligung lediglich zu Zwecken der E-Mail-Werbung für eigene ähnliche Produkte oder Dienstleistungen verarbeitet werden dürfen.

### VERTRETUNG DER BETROFFENEN PERSON

> Es muss sichergestellt werden, dass die Vorgaben des Art. 80 DSGVO auch im Telekommunikationsbereich Anwendung finden. Alles andere würde hinter der DSGVO zurück bleiben und damit gegen EWG 5 des Entwurfs verstoßen.

# III. GRUNDSÄTZLICHE ERWÄGUNGEN

### 1. SEKTORSPEZIFISCHE REGELUNG

Ziel der ePVO ist, das Recht auf Privatsphäre und der Vertraulichkeit im Zusammenhang mit der elektronischen Kommunikation sicherzustellen. Um dieses Ziel erreichen zu können, ist weiterhin eine sektorspezifische Regelung dringend geboten. Die ab Mai 2018 geltende DSGVO ist dafür alleine nicht ausreichend. Durch die spezifischen Risiken im Bereich der elektronischen Kommunikation besteht weiterhin die Notwendigkeit, die abstrakten Vorschriften der DSGVO für diesen spezifischen Bereich zu konkretisieren – was auch durch Art. 95 DSGVO anerkannt wird. Insofern detailliert und ergänzt die ePVO notwendiger Weise die DSGVO.

Die DSGVO bildet ferner lediglich Art. 8 der EU-Grundrechtecharta (Schutz personenbezogener Daten) ab, während die ePVO darüber hinaus Art. 7 der EU-Grundrechtecharta (Achtung des Privat- und Familienlebens) ausgestaltet, der unter anderem das Recht auf vertrauliche Kommunikation festschreibt. Die Möglichkeit der vertraulichen Kommunikation ist nicht nur unerlässlich, um die Persönlichkeitsrechte des Einzelnen zu schützen, sondern auch um die Funktionsfähigkeit demokratischer Gesellschaften sicherzustellen. Allerdings steht diese Vertraulichkeit in Zeiten der Digitalisierung durch die Fortschritte und neuen Möglichkeiten bei der Datenverarbeitung unter starkem Beschuss. Daher sind weiterhin klare und strikte Regelungen notwendig, um die Vertraulichkeit der Kommunikation zu schützen. Vor diesem Hintergrund begrüßt es der vzbv, dass auf Basis der ePVO eine Verarbeitung von Daten der elektronischen Kommunikation nur auf Grundlage eines gesetzlichen Erlaubnistatbestands oder mit

Einwilligung der Nutzer möglich sein soll und eine Verarbeitung auf Basis einer Interessenabwägung für diesen besonders sensitiven Bereich ausgeschlossen wird.

Darüber hinaus werden wesentliche verbraucherschützende Vorschriften der ePVO durch die DSGVO nicht abgedeckt. Dazu gehören beispielsweise Regelungen zum Schutz der in Endeinrichtungen der Endnutzer gespeicherten oder sich auf diese beziehenden Informationen oder Vorschriften zu unerbetener Kommunikation über elektronische Kommunikationsdienste.

Der vzbv betont, dass eine klare sektorspezifische Regelung nicht nur den Grundrechtsschutz der Endnutzer stärkt, sondern zugleich Rechtssicherheit für Unternehmen schafft. Darüber hinaus ist eine solche Regelung geeignet, das verlorene Vertrauen der Menschen in die digitale Wirtschaft zu verbessern. Im Jahr 2015 vertrauten lediglich 32 Prozent der Deutschen Internet- und Telefonanbietern. Nur 19 Prozent vertrauten der Internetwirtschaft.[7] 70 Prozent der Deutschen zeigten sich besorgt, dass ihre Daten zu anderen Zwecken verwendet werden, als sie ursprünglich erhoben wurden (wie Direktmarketing, Profilbildung oder interessensbezogener Werbung).[8] 42 Prozent der deutschen Internetnutzer vermeiden sogar bestimmte Webseiten, weil sie befürchten, dass ihre online-Aktivitäten beobachtet werden.[9] Auch in einer breit angelegten Umfrage des Vodafone Instituts für Gesellschaft und Kommunikation vom Januar 2016 spiegelt sich das geringe Vertrauen der Verbraucher in datenverarbeitende Dienste wieder. Beispielsweise vermeiden es 56 Prozent der deutschen Befragten, in E-Mails oder Textnachrichten über sehr persönliche Dinge zu schreiben, da sie befürchten, dass Dritte auf diese zugreifen könnten.[10] Außerdem gaben 36 Prozent der deutschen Befragten an gänzlich auf soziale Netzwerke zu verzichten, um ihre Daten zu schützen.[11]

Durch das mangelnde Vertrauen kann sogar die Gefahr entstehen, dass die Erfolgschancen vorbildlicher oder datenschutzfreundlicher Dienste in Mitleidenschaft gezogen werden. Im Gegensatz dazu wirkt Privatsphäre und Vertraulichkeit in der Kommunikation vertrauensbildend, da sie Risiken für die Endnutzer verringern. Das Vertrauen der Verbraucher wird mittelfristig eine Grundbedingung für den Erfolg datenintensiver Geschäftsmodelle in Europa sein.

> Es ist daher weiterhin ein sektorspezifisches Gesetz im Bereich der elektronischen Kommunikation dringend geboten, das die DSGVO detailliert und ergänzt, um das Recht auf Privatsphäre und Vertraulichkeit im Bereich der elektronischen Kommunikation sicherzustellen.

---

[7] Europäische Kommission: Special Eurobarometer 431; 2015; Seite 66; http://ec.europa.eu/public_opinion/archives/ebs/ebs_431_en.pdf; 06.03.2017

[8] Europäische Kommission: Special Eurobarometer 431; 2015; Seite 69 http://ec.europa.eu/public_opinion/archives/ebs/ebs_431_en.pdf; 06.03.2017

[9] Europäische Kommission: Flash Eurobarometer 443; 2016; Seite 39; https://data.europa.eu/euodp/en/data/dataset/S2124_443_ENG; 06.03.2017

[10] Vodafone Instituts für Gesellschaft und Kommunikation: Big Data – A European Survey on the Opportunities and Risks of Data Analytics; Seite 53; 2016 http://www.vodafone-institut.de/wp-content/uploads/2016/01/VodafoneInstitute-Survey-BigData-en.pdf; 06.03.2017

[11] Vodafone Instituts für Gesellschaft und Kommunikation: Big Data – A European Survey on the Opportunities and Risks of Data Analytics; Seite 76; 2016 http://www.vodafone-institut.de/wp-content/uploads/2016/01/VodafoneInstitute-Survey-BigData-en.pdf; 06.03.2017

## 2. VERORDNUNGSCHARAKTER UND MARKTORTPRINZIP

Ein weiteres Ziel der ePVO ist es, eine europaweite Harmonisierung des Rechts auf Privatsphäre und der Vertraulichkeit im Zusammenhang mit der elektronischen Kommunikation auf einem hohen Niveau sicherzustellen. Dieses Ziel wurde zwar schon bisher durch die ePRL verfolgt, konnte in der Vergangenheit jedoch nicht ausreichend erreicht werden. Die Mitgliedsstaaten nutzten nicht nur die ihnen eingeräumten Spielräume, sondern setzten auch andere Vorschriften höchst unterschiedlich um, wie beispielsweise die Regelungen zu Cookies und ähnlichen Technologien.[12] In Folge dessen konnten zum Beispiel deutsche Verbraucher in der Vergangenheit ihre europarechtlich vorgesehenen Rechte zum Schutz ihrer Privatsphäre nur unzureichend wahrnehmen.[13]

Vor diesen Hintergrund bewertet es der vzbv positiv, dass die EU-Kommission in ihrem Vorschlag die Form einer Verordnung gewählt und in diesem entsprechend der DSGVO das Marktortprinzip festgelegt hat. So kann eine europaweite Harmonisierung und eine hohe Konsistenz zur DSGVO erreicht werden.

> Ziel der ePVO ist es, eine europaweite Harmonisierung und eine hohe Konsistenz mit der DSGVO zu erreichen. Dieses Ziel ist am einfachsten mit der Rechtsform einer Verordnung und der Einführung des Marktortprinzips zu erreichen.

In dem Verordnungsentwurf der ePVO bleiben viele Fragen hinsichtlich des Zusammenspiels der beiden Verordnungen jedoch ungeklärt. Dies gilt insbesondere für Stellen, an denen die Vorgaben der ePVO hinter denen der DSGVO zurück bleiben (wie das Recht der Endnutzer ihre Einwilligung in eine Datenverarbeitung jederzeit zu widerrufen) oder für Stellen, an denen explizit auf bestimmte Artikel der DSGVO verwiesen wird (wie das Recht auf wirksamen gerichtlichen Rechtsbehelf), aber nicht auf andere damit in Zusammenhang stehende Artikel (wie die Möglichkeiten der Vertretung von betroffenen Personen).

> In keinem Fall dürfen die neuen und überarbeiteten Vorschriften hinter den Prinzipien und Vorgaben der DSGVO zurück bleiben, sondern müssen sich an dieser messen lassen. Gleichzeitig darf der bisherige Schutzstandard der ePRL durch die ePVO nicht unterschritten werden.

Dies gilt insbesondere für Fälle, in denen die bisherige ePRL spezifischere Schutzmaßnahmen vorsieht, die über die Vorgaben der Datenschutzrichtlinie beziehungsweise der DSGVO hinaus gehen, beispielsweise wenn für bestimmte Verarbeitungen nicht jede nach der DSGVO mögliche Rechtsgrundlage zugelassen, sondern alleine auf die Rechtsgrundlage der Einwilligung des Betroffenen abgestellt wird.

---

[12] DLA Piper: EU Law on Cookies; 2014, https://www.dlapiper.com/~/media/Files/Insights/Publications/2014/09/EU_Cookies_Update_September_2014.pdf; 06.03.2017

[13] Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder zur Verfolgung des Nutzungsverhaltens im Internet; 2015; https://www.bfdi.bund.de/SharedDocs/Publikationen/Entschliessungssammlung/DSBundLaender/Entschliessung_Cookies.html; 06.03.2017

## 3. EINBEZIEHUNG VON OTTS IN DEN ANWENDUNGSBEREICH

Zwar war die ePRL schon bisher ein wichtiges Instrument, um das Recht auf Privatsphäre und Vertraulichkeit im Bereich der elektronischen Kommunikation sicherzustellen, jedoch konnte ein umfassender Schutz aufgrund des eingeschränkten Anwendungsbereichs der Richtlinie nicht erreicht werden. Ein Grund ist der ökonomische, soziale und politische Bedeutungszuwachs von OTTs, dem die ePRL bisher nicht ausreichend gerecht wird.

Während noch vor wenigen Jahren der Großteil der elektronischen Kommunikation über traditionelle Telekommunikationsanbieter geführt wurde, kommunizieren Verbraucher heute in erster Linie über Dienste der Informationsgesellschaft beziehungsweise über OTTs. Beispielsweise sendeten die deutschen Verbraucher im Jahr 2012 – als die ePRL in Deutschland implementiert wurde – noch über 160 Millionen SMS-Nachrichten und 20 Millionen WhatsApp-Nachrichten am Tag. Im Jahr 2015 hatten sich diese Zahlen umgekehrt: die Deutschen sendeten weniger als 40 Millionen SMS-Nachrichten pro Tag, aber über 660 Millionen WhatsApp-Nachrichten.[14] Diese Nachrichten stehen jedoch nicht unter einem vergleichbaren Schutz wie klassische SMS-Nachrichten.

Diese Unterscheidung ist für viele Verbraucher im höchsten Maße irritierend. So glauben 62 Prozent der Deutschen fälschlicher Weise, dass per Gesetz Instant-Messaging- und VoIP-Telefoniekonversationen vertraulich seien und niemand auf diese ohne ihre Einwilligung zugreifen dürfe.[15] Für sie ist nicht verständlich, weshalb eine Nachricht die per SMS versendet wird, einen höheren Schutz genießt als eine Nachricht, die sie – teilweise über dieselbe Smartphone-Applikation – über das Internet versenden.

Damit einhergehend ist auch aus grundrechtlicher Perspektive die bisherige Unterscheidung heutzutage nicht mehr nachvollziehbar. Denn würde das Schutzniveau nicht an die heutigen Kommunikationsgegebenheiten angepasst werden, würde sich das allgemeine Schutzniveau durch die Verlagerung der Kommunikation massiv verringern.

Der vzbv begrüßt daher, dass der Anwendungsbereich der ePVO auf alle Kommunikationsdienste ausgeweitet werden soll, wenn diese funktional äquivalent zu klassischen Telekommunikationsdiensten sind und diese substituieren, einschließlich interpersonelle Kommunikationsdienste, die nur eine untergeordnete Nebenfunktion eines anderen Dienstes darstellen. Dies betrifft insbesondere die Regelungen zur Vertraulichkeit der Kommunikation, die Regelungen zu Meta- und Inhaltsdaten, die Regelungen zum Schutz von Informationen der Endgeräte der Nutzer, zu datenschutzfreundlichen Einstellungen sowie die Regelungen zu unerwünschten Nachrichten.

> Der sachliche Anwendungsbereich der ePVO muss ausgeweitet werden, um alle Kommunikationsdienste zu erfassen, wenn diese funktional äquivalent zu klassischen Telekommunikationsdiensten sind und diese substituieren sowie interpersonelle Kommunikationsdienste, die nur eine untergeordnete Nebenfunktion eines anderen Dienstes darstellen.

---

[14] Statista: Anzahl gesendeter SMS-Nachrichten pro Tag in Deutschland bis 2015; 2015; http://de.statista.com/statistik/daten/studie/3624/umfrage/entwicklung-der-anzahl-gesendeter-sms--mms-nachrichten-seit-1999/; 06.03.2017

[15] Europäische Kommission: Flash Eurobarometer 443; 2016; Seite 27; https://data.europa.eu/euodp/en/data/dataset/S2124_443_ENG; 06.03.2017

# IV. DIE EINZELNEN REGELUNGEN

## 1. ARTIKEL 2 – SACHLICHER ANWENDUNGSBEREICH

### Artikel 2 Absatz 1

In Art. 2 Abs. 1 werden nicht alle Adressaten der Verordnung entsprechend des EWG 8 genannt. Im Sinne der Regelungsklarheit ist dies besonders hinsichtlich der in Art. 10 und Art. 16 genannten Adressaten wichtig, die bisher in Art. 2 direkt nicht genannt sind.

> Auch die Anbieter von Software, die elektronische Kommunikation ermöglicht, sowie natürliche und juristische Personen, die mithilfe elektronischer Kommunikationsdienste an Endnutzer gerichtete gewerbliche Direktwerbung betreiben, sollten als Adressaten der ePVO in Art. 2 Abs. 1 benannt werden.

## 2. ARTIKEL 4 – BEGRIFFSBESTIMMUNGEN

### Artikel 4 Absatz 2

Der vzbv begrüßt, dass die Definition für „interpersoneller Kommunikationsdienst“ auch Dienste einschließt, die eine interpersonelle und interaktive Kommunikation lediglich als untrennbar mit einem anderen Dienst verbundene untergeordnete Nebenfunktion ermöglichen (wie der Service-Chat eines Onlinehändlers). Die Vertraulichkeit der Kommunikation wird nicht weniger schutzwürdig, nur weil es sich bei der genutzten Technologie um eine „untergeordnete Nebenfunktion“ eines Dienstes handelt.

### Artikel 4 Absatz 3 Buchstabe b) und Buchstabe c)

Es ist grundsätzlich zu begrüßen, dass mit der ePVO künftig sowohl elektronische Kommunikationsinhalte, als auch elektronische Kommunikationsmetadaten geschützt werden sollen. *Jedoch ist die in der ePVO vorgesehene Trennung von Kommunikationsinhalten und Kommunikationsmetadaten in der Praxis oftmals nicht möglich*. So ist beispielsweise bei SMS-Nachrichten die Trennung der Daten technisch unmöglich.[16] Gleiches gilt beispielsweise für die Header von E-Mails, die neben Kommunikationsmetadaten auch den Betreff der E-Mail enthalten und damit Rückschlüsse auf die Inhalte der Nachricht zulassen können.

> Es muss daher klargestellt werden, dass immer von elektronischen Kommunikationsinhalten auszugehen ist, wenn aus den elektronischen Kommunikationsmetadaten Rückschlüsse auf die Inhalte der Kommunikation gezogen werden können.

### Artikel 4 Absatz 3 Buchstabe e)

Der englische Begriff der „electronic mail“ in Art. 4 Abs. 3 lit. e) wird in der deutschen Fassung des Verordnungsvorschlags als „„E-Mail“ (elektronische Post)“ übersetzt. *Dies*

[16] Sueddeutsche.de: Vorratsdatenspeicherung erfasst auch den Text von SMS; 2015; http://www.sueddeutsche.de/politik/vorratsdatenspeicherung-sms-inhalte-werden-gespeichert-1.2693495; 06.03.2017

*ergibt keinen Sinn.* Denn laut des Inhaltes der Definition soll dieser Begriff „jede über ein elektronisches Kommunikationsnetz verschickte elektronische Nachricht, die Informationen in Text-, *Sprach-, Video-, Ton- oder Bildform enthält*“ erfassen. Das Format einer E-Mail wird jedoch durch den Internetstandard RFC 5322 festgelegt, wonach E-Mails nur aus Textzeichen bestehen. Demnach ist „E-Mail“ lediglich eine Teilmenge der „elektronischen Post“, wie sie in der englischen Fassung des Verordnungsvorschlags definiert ist.

> Die Definition von „electronic mail“ der deutschen Fassung des Verordnungsvorschlags sollte als „elektronische Post“ übersetzt werden und darf nicht „E-Mail“ lauten.

## 3. ARTIKEL 5 – VERTRAULICHKEIT ELEKTRONISCHER KOMMUNIKATION

Der vzbv begrüßt, dass alle elektronischen Kommunikationsdaten künftig vertraulich behandelt werden müssen und Eingriffe in die Übermittlung, wie Mithören, Abhören, Speichern, Beobachten, Scannen oder andere Arten des Abfangens (einschließlich des Beobachtens, welche Webseiten ein Endnutzer besucht, den Zeitpunkt der Besuche, die Interaktion mit anderen usw.) oder Überwachens oder Verarbeitens elektronischer Kommunikationsdaten, untersagt sind, außer wenn der betroffene Nutzer eingewilligt hat oder es dafür eine gesetzliche Ermächtigung gibt.

> Der Wortlaut des Art. 5 sollte jedoch dahingehend angepasst werden, dass klar ist, dass nicht lediglich „Eingriffe in elektronische Kommunikations*daten*“ untersagt sind, sondern jegliche Eingriffe in elektronische Kommunikation. Außerdem ist der Begriff der „Personen“ irreführend, da sowohl natürliche als auch juristische Personen, aber auch mittelbare Eingriffe durch eine automatische Verarbeitung durch Maschinen eingeschlossen sein müssen. Daher sollten die entsprechenden Formulierungen des EWG 15 in Art. 5 übernommen werden.

## 4. ARTIKEL 6 – ERLAUBTE VERARBEITUNG ELEKTRONISCHER KOMMUNIKATIONSDATEN

### Artikel 6 Absatz 1

Es ist unklar, warum Art. 6 Abs. 1 auf die „Betreiber elektronischer Kommunikationsnetze und -dienste“ Bezug nimmt, während an allen anderen Stellen der Verordnung lediglich „Betreiber elektronischer Kommunikationsdienste“ aufgeführt werden.

### Artikel 6 Absatz 1 Buchstabe b)

Art. 6 Abs. 1 lit. b) lässt Fragen hinsichtlich des Zusammenspiels der ePVO und der DSGVO offen. *Im derzeitigen Wortlaut ist Art. 6 Abs. 1 lit. b) zu weit gefasst*. Während EWG 45 DSGVO die Verarbeitung von personenbezogenen Daten durch Betreiber von elektronischen Kommunikationsnetzen und –diensten nur in dem Maße zulässt, wie es

dies für die Gewährleistung der Netz- und Informationssicherheit *unbedingt notwendig und verhältnismäßig ist*, muss die Verarbeitung elektronischer Kommunikationsdaten nach Art. 6 Abs. 1 lit. b) lediglich zur Aufrechterhaltung oder Wiederherstellung der Sicherheit elektronischer Kommunikationsnetze und dienste oder zur Erkennung von technischen Defekten und Fehlern bei der Übermittlung der elektronischen Kommunikation *nötig sein*.

> Art. 6 Abs. 1 lit. b) muss an EWG 49 DSGVO angepasst werden und darf nicht hinter der DSGVO zurück bleiben. Dies würde gegen EWG 5 verstoßen.

**Artikel 6 Absatz 2 Buchstabe c)**

*Der vzbv betrachtet es als kritisch, dass die Möglichkeiten der Verarbeitung von Kommunikationsmetadaten durch die Betreiber elektronischer Kommunikationsdienste ausgeweitet werden sollen*. Diese war bisher auf Dienste beschränkt, die einen Mehrwert für die Betroffenen geboten haben. Nun ist die Verarbeitung zu jedem Zweck möglich, zu dem der Betroffene einwilligt. Gleichzeitig begrüßt der vzbv, dass nun auch andere Anbieter von elektronischen Kommunikationsdiensten die Kommunikationsmetadaten der Endnutzer nur mit deren Einwilligung verarbeiten dürfen. Jedoch sollten an die Verarbeitung von Kommunikationsmetadaten hohe Anforderungen gestellt werden:

> Da Kommunikationsmetadaten eine besondere Aussagekraft haben und auf Grund der Breite und der Komplexität der Nutzungsmöglichkeiten müssen besonders hohe Anforderungen an die Informiertheit Einwilligung gestellt werden. Es muss den Betroffenen stets klar sein, wofür ihre Daten verwendet werden.

> Da Kommunikationsmetadaten eine besondere Aussagekraft haben, sollte für deren Verbreitung stets eine Datenschutzfolgeabschätzung (Art. 35 DSGVO) vorgenommen und gegebenenfalls die Aufsichtsbehörde konsultiert (Art. 36 DSGVO) werden müssen. Diese Anforderungen sollten in die Regelung des Art. 6 aufgenommen werden.

Grundsätzlich ist es vorstellbar, dass Kommunikationsmetadaten anonymisiert verarbeitet werden können. Der vzbv möchte jedoch darauf hinweisen, dass gerade die Anonymisierung von Standortdaten äußerst anspruchsvoll ist, da eine Analyse und Kombination dieser Daten leicht zu einer Identifizierung der Betroffenen führen kann.[17] Im Jahr 2013 zeigten beispielsweise Forscher des MIT und der Harvard University, wie einfach es ist, einzelne Individuen auf Basis ihrer Mobiltelefon-Standortdaten zu identifizieren.[18] In einer anderen Studie zeigten Forscher der Columbia University und Google Research im Jahr 2016, dass geogetaggte Beiträge von lediglich zwei Social-Media-

[17] Vgl. Artikel-29-Datenschutzgruppe: Stellungnahme 13/2011 zu den Geolokalisierungsdiensten von intelligenten mobilen Endgeräten; 2011; http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp185_de.pdf; 06.03.2017

[18] Scientific Reports, Article 1376: Unique in the Crowd - The privacy bounds of human mobility; 2013; http://www.nature.com/articles/srep01376; 06.03.2017

Anwendungen einer Person ausreichend sind, um die entsprechenden Konten zu verknüpfen.[19] Entsprechend hoch müssen die Anforderungen an eine wirksame Anonymisierung sein.

> Darüber hinaus sollte aus dem Wortlaut des Art. 6 Abs. 2 lit. c) hervor gehen, dass das Prinzip der Datenminimierung auch dann greift, wenn die betreffenden Zwecke durch eine Verarbeitung anonymisierter Informationen nicht erreicht werden können. Beispielsweise sollte in diesen Fällen die Granularität von Kommunikationsmetadaten auf das Maß reduziert werden, das für den Zweck notwendig ist, für den sie erhoben wurden.

### Artikel 6 Absatz 3

*Der vzbv erachtet es als äußerst kritisch, dass mit Einwilligung der Nutzer künftig auch elektronischen Kommunikationsinhalten verarbeitet werden können*. Dabei können, „Inhalte der elektronischen Kommunikation […] hochsensible Informationen über die daran beteiligten natürlichen Personen offenlegen, von persönlichen Erlebnissen und Gefühlen oder Erkrankungen bis hin zu sexuellen Vorlieben und politischen Überzeugungen, was zu schweren Folgen im persönlichen und gesellschaftlichen Leben, zu wirtschaftlichen Einbußen oder Schamgefühl führen kann“, wie in EWG 2 korrekt dargelegt. Außerdem fällt „der Inhalt elektronischer Kommunikation […] in den Wesensgehalt des nach Artikel 7 der Charta geschützten Grundrechts auf Achtung des Privat- und Familienlebens, der Wohnung und der Kommunikation“ (EWG 19).

> Daher sollte – entsprechend der Anforderungen des Art. 9 DSGVO zur Verarbeitung besonderer Kategorien personenbezogener Daten – stets eine ausdrückliche Einwilligung aller beteiligten Endnutzer für die Verarbeitung von elektronischen Kommunikationsinhalten erforderlich sein, soweit die Verarbeitung nicht erforderlich ist, um einen von den Endnutzern gewünschten Dienst zu erbringen.

> Aufgrund des hohen Risikos der Verarbeitung von elektronischen Kommunikationsinhalten, sollte außerdem vor der Verbreitung stets die Aufsichtsbehörde konsultiert werden müssen (Art. 36 DSGVO), selbst wenn es sich um einen vom Endnutzer gewünschten Dienst handelt. Diese Anforderung sollte in die Regelung aufgenommen werden.

## 5. ARTIKEL 7 – SPEICHERUNG UND LÖSCHUNG ELEKTRONISCHER KOMMUNIKATIONSDATEN

Laut Art. 7 sollen Betreiber elektronischer Kommunikationsdienste elektronische Kommunikationsdaten löschen oder anonymisieren, sobald der Zweck ihrer Verarbeitung erfüllt wurde. *Während die wirksame Anonymisierung von elektronischen Kommunikationsmetadaten – wie bereits oben angeführt – eine äußerst anspruchsvolle Aufgabe*

[19] Columbia University: Linking Users Across Domains with Location Data; 2016; www.cs.columbia.edu/~mani/pub/RiedererWWW2016.pdf; 06.03.2017

*darstellt, ist absolut unklar, wie eine wirksame Anonymisierung von elektronischen Kommunikationsinhalten erreicht werden soll*.

> Vor diesem Hintergrund – und da es sich bei elektronischen Kommunikationsinhalten um besonders schutzwürdige Informationen handelt – sollten diese Daten stets gelöscht werden müssen, sobald der beziehungsweise die vorgesehenen Empfänger die elektronischen Kommunikationsinhalte erhalten haben und die Endnutzer ihre weitere Aufzeichnung, Speicherung oder anderweitigen Verarbeitung im Einklang mit der DSGVO nicht ausdrücklich wünschen.

## 6. ARTIKEL 8 – SCHUTZ DER IN ENDEINRICHTUNGEN DER ENDNUTZER GESPEICHERTEN ODER SICH AUF DIESE BEZIEHENDEN INFORMATIONEN

Der vzbv begrüßt den Ansatz der EU-Kommission, die in Endeinrichtungen der Endnutzer gespeicherten oder sich auf diese beziehenden Informationen künftig einem besonderen Schutz zu unterstellen. Wie in EWG 20 richtig ausgeführt, sind diese Endeinrichtungen und die mit ihnen in Zusammenhang stehenden Informationen Teil der Privatsphäre der Endnutzer, da diese Informationen „einen tiefen Einblick in komplexe emotionale, politische und soziale Aspekte der Persönlichkeit einer Person geben können“. Dementsprechend ist es auch für 95 Prozent der deutschen Internetnutzer wichtig, dass nur mit ihrer Erlaubnis auf Informationen auf ihren Endgeräten zugegriffen wird.[20]

Jedoch ist es gleichzeitig wegen der hohen technischen Komplexität der Endeinrichtungen für den durchschnittlichen Endnutzer problematisch, umfassende und wirksame Maßnahmen zum Selbstschutz zu treffen. *Aus dieser hohen Relevanz der Endgeräte für die Persönlichkeit und Privatsphäre der Endnutzer, ergibt sich in Verbindung mit den damit gleichzeitig einhergehenden hohen Gefahren, ein besonderes Schutzbedürfnis*. Es ist somit richtig, dass sich dieser Schutz auf jegliche Informationen in diesem Zusammenhang erstrecken und technikneutral alle Technologien erfassen soll, die diesen Schutz gefährden.

Nichtsdestotrotz ist das Recht der Endnutzer, selbst Schutzmaßnahmen gegen *unrechtmäßige* Angriffe auf Ihre IT-Systeme vorzunehmen (vor denen dementsprechend auch Art. 8 der Verordnung nicht schützt), eine zentrale Voraussetzung für den Schutz der in Endeinrichtungen gespeicherten oder sich auf diese beziehenden Informationen und damit für eine vertrauliche Kommunikation. So sollten Endnutzer beispielweise das Recht haben, ihre Kommunikation zu verschlüsseln beziehungsweise ihre Netzwerke und ihre Endgeräte nach dem Stand der Technik absichern oder Schutzmaßnahmen vornehmen zu können, um ihre Kommunikation, Netzwerke und Endgeräte vor „malvertising“ oder „mobile cramming“ zu schützen.[21]

---

[20] Europäische Kommission: Flash Eurobarometer 443; 2016; Seite 30; https://data.europa.eu/euodp/en/data/dataset/S2124_443_ENG; 06.03.2017

[21] Vgl.: eco - Verband der Internetwirtschaft e.V.: Malvertising - Werbung als Einfallstor für Malware; 2016; https://www.it-trends-sicherheit.de/vortraege/vortragdetail/malvertising-werbung-als-einfallstor-fuer-malware/; 06.03.2017

> Endnutzer sollten das Recht haben, Schutzmaßnahmen gegen unrechtmäßige Angriffe auf Ihre IT-Systeme vorzunehmen. Es sollte verboten sein, IT-Sicherheitsmaßnahmen der Endnutzer zu umgehen oder zu schwächen.

### Artikel 8 Absatz 1 Buchstabe b)

Grundsätzlich begrüßt der vzbv, dass nach Art. 8 Abs. 1 lit. b) künftig die Nutzung der Verarbeitungs- und Speicherfunktionen von Endeinrichtungen und jede Erhebung von Informationen aus Endeinrichtungen der Endnutzer nur gestattet sein soll, wenn der Endnutzer seine Einwilligung gegeben hat. So erachten es beispielsweise 87 Prozent der deutschen Internetnutzer als wichtig, dass ihr online-Verhalten nur mit ihrer Einwilligung überwacht wird.[22]

> Es muss jedoch klargestellt sein, dass diese Verarbeitungen den Vorgaben der DSGVO entsprechen müssen, insbesondere hinsichtlich der Prinzipien der Zweckbindung und der Datenminimierung. Außerdem sollte die Erhebung von sensitiven Informationen aus Endeinrichtungen der Endnutzer entsprechend der DSGVO nur mit deren ausdrücklicher Einwilligung erlaubt sein.

> Darüber hinaus sollten außergewöhnlich aufdringliche Technologien verboten werden, insbesondere solche, die den kompletten von den Endgeräten ausgehenden Datenverkehr erfassen sollen oder solche, mit denen versucht wird, Entscheidungen der Endnutzer zu umgehen.

Beispielsweise sollten Technologien, wie das in Europa verbreitete Tracking durch Telekomunikationsunternehmen über Unique Identifier Header (UIDH)[23] – so genannte Super-Cookies – oder Cookies, die nach dem Löschen durch den Nutzer automatisch neu erstellt werden und somit die Wahl der Benutzer umgehen – so genannte Zombie-Cookies – verboten sein.

Darüber hinaus sollten dem besonderen Schutzbedürfnis von Minderjährigen Rechnung getragen werden, da Kinder sich der betreffenden Risiken, Folgen und ihrer Rechte möglicherweise weniger bewusst sind.

> Dementsprechend sollten die Bedingungen für die Einwilligung eines Kindes in Bezug auf Verarbeitung von Informationen, die auf seinen Endeinrichtungen gespeichert sind oder sich auf diese beziehenden, den Bedingungen des Art. 8 DSGVO entsprechen.

### Artikel 8 Absatz 1 Buchstabe d)

Entsprechend des Verordnungsvorschlags soll künftig eine Nutzung der Verarbeitungs- und Speicherfunktionen von Endeinrichtungen und die Erhebung von Informationen

---

[22] Europäische Kommission: Flash Eurobarometer 443; 2016; Seite 34; https://data.europa.eu/euodp/en/data/dataset/S2124_443_ENG; 06.03.2017

[23] Access Now: The Rise of Mobile Tracking Headers; 2015; https://www.accessnow.org/cms/assets/uploads/archive/AIBT-Report.pdf; 06.03.2017

aus Endeinrichtungen der Endnutzer erlaubt sein, wenn sie für die Messung des Webpublikums nötig ist, sofern der Betreiber des vom Endnutzer gewünschten Dienstes der Informationsgesellschaft diese Messung durchführt. *Jedoch fehlen weitere dringend notwendige Schutzvorgaben.*

> Den Endnutzern muss eine transparente, einfache und wirksame Möglichkeit zum Widerspruch gegen die Erfassung der Informationen eingeräumt werden.
>
> Es muss klargestellt werden, dass stets das Prinzip der Datenminimierung zu beachten ist. So sollten die Daten anonymisiert werden müssen, wenn der Zweck der Verarbeitung dennoch erreicht werden kann, beispielsweise indem das letzte Oktett der IP-Adressen der Endnutzer vor jeglicher Speicherung gelöscht wird.
>
> Außerdem müssen die Vorgaben der Artikel 28 und 29 DSGVO beachtet werden, wenn der Betreiber des vom Endnutzer gewünschten Dienstes für die Messung des Webpublikums die Dienste von Auftragsverarbeitern in Anspruch nimmt.

**Artikel 8 Absatz 2 Buchstabe b)**

*Der vzbv erachtet die vorgeschlagenen Regelungen des Art. 8 Abs. 2 lit. b) als überaus kritisch*. Smartphones und andere Geräte versenden eindeutig wiedererkennbare Signale, um eine Telefon-, Internet-, WLAN- oder Bluetooth-Verbindung zu ermöglichen. Entsprechend EWG 25 fallen darunter unter anderem die MAC-ID, IMEI (internationale Mobilfunkgerätekennung) oder die IMSI (internationale Mobilfunk-Teilnehmerkennung).

Diese Signale können von Unternehmen, wie beispielsweise dem Einzelhandel, verwendet werden, um die Endnutzer auch in der Offline-Welt zu tracken. So können sie einen Endnutzer wiedererkennen, wenn er zum wiederholten Male ein Geschäft betritt oder seine Bewegungen innerhalb des Geschäftes nachverfolgen. Je nach eingesetzter Technik (wie Tracking der IMSI) ist es möglich, die Bewegungen einzelner Personen über einen längeren Zeitraum und über eine Entfernung von mehreren hundert Metern zu verfolgen. Darüber hinaus können diese Daten mit weiteren Informationen verknüpft und somit die Identifikation der betroffenen Endnutzer erleichtert werden. Daher muss bei solchen Systemen stets von einer Erhebung und Verarbeitung personenbezogener Daten ausgegangen werden.[24]

Die Erhebung solcher Informationen soll nach den Vorschlägen der EU-Kommission künftig ohne die Einwilligung der Verbraucher erlaubt sein. Darüber hinaus ist fraglich, ob nach den derzeitigen Plänen eine Widerspruchsmöglichkeit bestehen soll. Verbraucher sollen lediglich Hinweise erhalten, wenn sie einen derart überwachten Bereich betreten. Es ist aber fraglich, inwieweit der öffentliche Raum Möglichkeiten bietet, solche Informationen in angemessenem Umfang und für Verbraucher wahrnehmbar darzustellen. Oftmals dürfte auch die klare Abgrenzung eines solchen Bereichs technisch nur schwer möglich sein, so dass auch die Daten von Personen erfasst werden können, die beispielsweise über/neben einem Geschäft wohnen, das diese Techniken einsetzt. Darüber hinaus ist oftmals die einzige Möglichkeit der Endnutzer, sich vor einer solchen Erhebung zu schützen, ihre Endgeräte zu deaktivieren (wie beim Tracking der IMSI). *Die vorgeschlagenen Regelungen sind daher absolut inakzeptabel.*

---

[24] Vgl. Artikel-29-Datenschutzgruppe: Stellungnahme 13/2011 zu den Geolokalisierungsdiensten von intelligenten mobilen Endgeräten; 2011; Seite 11; http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp185_de.pdf; 06.03.2017

Die Betreiber solcher Techniken sollten daher stets eine Datenschutzfolgeabschätzung durchführen und die Aufsichtsbehörden kontaktieren müssen, entsprechend der Art. 35 und 36 DSGVO.

Sollte die Datenschutzfolgeabschätzung zu dem Ergebnis kommen, dass ein hohes Risiko für den Betroffenen besteht und sollte sich dieses Risiko nicht durch technische und organisatorische Maßnahmen verringern lassen (zum Beispiel Pseudonymisierung der MAC-Adressen durch Bildung eines Hashwerts), darf eine solche Erhebung nur mit Einwilligung des Endnutzers möglich sein.

Sollte die Datenschutzfolgeabschätzung zu dem Ergebnis kommen, dass ein geringes Risiko für den Betroffenen besteht, muss ihm ein einfaches und wirksames Widerspruchsrecht zugestanden werden.

Darüber hinaus muss klargestellt werden, dass auch hier die Grundprinzipien und Vorgaben der DSGVO zu den Anforderungen des Verordnungsentwurfs hinzutreten, insbesondere die Prinzipien der rechtmäßigen Verarbeitung, nach Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Weise, der Zweckbindung sowie der Datenminimierung.

## 7. ARTIKEL 9 – EINWILLIGUNG

### Artikel 9 Absatz 1

Der vzbv begrüßt, dass für die Verordnung grundsätzlich die Erfordernisse an eine Einwilligung nach Art. 7 DSGVO gelten sollen. *Jedoch sind EWG 18 Satz 3 und Satz 4 missverständlich formuliert*. Die Freiwilligkeit der Einwilligung darf nicht auf „grundlegende breitbandige Internetzugangs- und Sprachkommunikationsdienste“ begrenzt sein. Dies würde hinter den Anforderungen der DSGVO zurück bleiben und damit EWG 5 widersprechen.

EWG 18 Satz 3 und Satz 4 müssen klarer formuliert werden, so dass deutlich wird, dass die Freiwilligkeit der Einwilligung nicht auf „grundlegende breitbandige Internetzugangs- und Sprachkommunikationsdienste“ begrenzt ist.

### Artikel 9 Absatz 2

Der vzbv begrüßt, dass Endnutzer ihre Einwilligung für die Zwecke des Art. 8 Abs. 1 lit b) benutzerfreundlich und transparent in den passenden technischen Einstellungen einer Software geben können sollen. Bereits heute drücken 33% der deutschen Internetnutzer ihren Widerspruch gegen die Nachverfolgung ihrer Interessen im Internet durch den Einsatz von Anti-Tracking-Tools aus.[25]

Es muss jedoch klargestellt werden, dass der Begriff der „Software“, weit auszulegen ist und auch Browser-Plugins, Do-Not-Track-Header, Anti-Tracking-Tools und ähnliche Software erfasst und nicht nur „Software, die den Zugang zum Internet ermöglicht“.

[25] Europäische Kommission: Flash Eurobarometer 443; 2016; Seite 41; https://data.europa.eu/euodp/en/data/dataset/S2124_443_ENG; 06.03.2017

*Problematisch erachtet der vzbv jedoch, dass (nach Punkt 3.4 der Begründung zur Verordnung) Web-site-Betreiber weiterhin die Möglichkeit haben sollen, die Einwilligung zur Datenverarbeitung unabhängig von der Softwareeinstellung mit einer individuellen Anfrage beim Endnutzer einzuholen*.[26] Dies bedeutet, dass gerade die Endnutzer, die sich beim Installationsprozess einer Software bewusst dafür entschieden haben, keine Einwilligung abzugeben, künftig weiterhin unverändert Cookie-Bannern und –Hinweisen begegnen werden.

*Darüber hinaus muss dringend geklärt werden, wie das Verhältnis von Einwilligungen zu betrachten ist, die über Softwareeinstellungen vorgenommen wurden und Einwilligungen, die unabhängig davon abgegeben wurden*. Sprich: Was passiert, wenn der Endnutzer keine Einwilligung durch seine Software-Einstellung abgibt, diese aber vermeintlich auf anderem Wege erteilt? Hierbei muss sichergestellt werden, dass der tatsächliche Wunsch des Verbrauchers respektiert und nicht umgangen wird.

> Wenn der Endnutzer eine Einwilligung abgeben soll, die seiner Softwareeinstellung widerspricht, sollte diese neue Einwilligung immer ausdrücklich abgegeben werden müssen

### Artikel 9 Absatz 3

Art. 9 Abs. 3 gesteht den Endnutzern zu, ihre Einwilligung in Bezug auf Art. 6 Abs. 2 lit. c) und Art. 6 Abs. 3 lit. a) und b) zu widerrufen. *Es ist jedoch unverständlich, warum hier Art. 8 Abs. 1 lit. b) nicht aufgeführt wird*. Sollte hinsichtlich Art. 8 Abs. 1 lit. b) kein Widerruf möglich sein, würde dies hinter der DSGVO zurückbleiben und EWG 5 widersprechen.

> Es muss klargestellt werden, dass der Endnutzer seine Einwilligung, die er zu Zwecken des Art. 8 Abs. 1 lit. b) abgegeben hat, stets widerrufen kann.

## 8. ARTIKEL 10 – BEREITZUSTELLENDE INFORMATIONEN UND EINSTELLUNGSMÖGLICHKEITEN ZUR PRIVATSHÄRE

### Artikel 10 Absatz 1

Der vzbv begrüßt, dass künftig Software, die eine elektronische Kommunikation erlaubt, die Möglichkeit bieten muss, zu verhindern, dass Dritte Informationen in der Endeinrichtung eines Endnutzers speichern oder bereits in der Endeinrichtung gespeicherte Informationen verarbeiten.

> Es muss jedoch klar sein, dass durch die Formulierung „in Verkehr gebrachte Software“ jegliche Software eingeschlossen ist, die Kommunikation ermöglicht, also

[26] An dieser Stelle muss auch die Frage hinsichtlich der geteilten Verantwortung zwischen den Anbietern gezielter Online-Werbung und den Website-Betreibern gestellt werden. Üblicherweise willigt der Endnutzer der Datenverwendung gegenüber dem Website-Betreiber ein. Die Datenverarbeitung selbst, auf die der Website-Betreiber kaum einen Einfluss hat, wird aber durch einen Dritten – dem Anbieter gezielter Online-Werbung – vorgenommen.

auch Betriebssysteme oder Software, die nicht alleine sondern nur mit einer entsprechenden Hardware vertrieben wird.

Auch sollten EWG 23 und EWG 24 sprachlich angepasst werden, um klarzustellen, dass diese Regelung nicht auf „Software, die das Abrufen und Darstellen von Informationen aus dem Internet erlaubt“ begrenzt ist.

Darüber hinaus sollte Software, die eine elektronische Kommunikation erlaubt, Einstellungsmöglichkeiten bieten, eine Einwilligung für die Zwecke des Art. 8 Abs. 1 lit. b) abzugeben, um beispielsweise eine Einwilligung in das Fingerprinting über die Einstellungen zu ermöglichen oder dieses zu untersagen, zum Beispiel durch generelle Do-Not-Track-Einstellungen. Dementsprechend sollte auch EWG 23 nicht nur auf Cookies bezogen sein.

Denn sollte es solche Einstellungsmöglichkeiten für die Einwilligung für die Zwecke des Art. 8 Abs. 1 lit. b) nicht geben, würden dies die Vorschriften des Art. 9 Abs. 2 konterkarieren.

### Artikel 10 Absatz 2

*Der vzbv bedauert, dass sich die EU-Kommission nicht dazu durchringen konnte, zu regeln, dass Software, die eine elektronische Kommunikation erlaubt, stets datenschutzfreundlich voreingestellt sein muss*. Zwar müssen die Nutzer künftig bei der Installation aktiv eine der Einstellungen auswählen, das Flash Eurobarometer 443 der EU-Kommission zeigt jedoch eindeutig, dass sich die Verbraucher datenschutzfreundliche Voreinstellungen wünschen. In dieser Studie hatten sich 90 Prozent der deutschen Internetnutzer für solche Voreinstellungen in ihren Webbrowsern ausgesprochen.[27] Gleichzeitig zeigt die Studie auch, dass besonders ältere Menschen, Menschen mit niedriger Bildung sowie Menschen, die das Internet wenig verwenden, seltener Änderungen in den Datenschutzeinstellungen ihrer Software vornehmen.[28] Datenschutzfreundliche Voreinstellungen schützen also in erster Linie diese besonders vulnerablen Verbrauchergruppen.

Darüber hinaus ist die Formulierung „Bei der Installation“ unklar. Soll hier nur Software erfasst sein, die durch den Endnutzer installiert wird und auf Endgeräten vorinstallierte Software ausgeschlossen sein? Dies wäre deutlich zu kurz gegriffen.

*Insgesamt erscheint der von der EU-Kommission gewählte Ansatz – im Gegensatz zu einem echten Privacy-by-Default – sowohl für die Endnutzer, als auch für die Anbieter von Software – impraktikabel*. Auf der einen Seite werden viele Endnutzer damit überfordert sein, entsprechende Einstellungen auf ihren Endgeräten vorzunehmen (siehe oben). Oftmals werden sie bei der Installation der Applikation nicht einschätzen können, welche der Einstellungen für sie vorteilhaft oder tatsächlich notwendig sind. Und diese schwere Entscheidung müssten sie bei einer Vielzahl von Applikationen treffen.

---

[27] Europäische Kommission: Flash Eurobarometer 443; 2016; Seite 46; https://data.europa.eu/euodp/en/data/dataset/S2124_443_ENG; 06.03.2017

[28] Europäische Kommission: Flash Eurobarometer 443; 2016; Seite 37; https://data.europa.eu/euodp/en/data/dataset/S2124_443_ENG

Auf der anderen Seite müsste, nach den derzeitigen Formulierungen, auch solche Software von den Endnutzern zur Fortsetzung der Installation die Einwilligung zu einer Einstellung verlangen, die einen Zugriff durch Dritte überhaupt gar nicht vorsieht. So müsste zukünftig beispielsweise auch bei der Installation einer Router-Firmware (elektronische Kommunikation erlaubt) der Endnutzer eine Einwilligung zu einer Einstellung abgeben. All diese Probleme ließen sich mit jedoch dem Gebot von datenschutzfreundlichen Voreinstellungen umgehen.

> Grundsätzlich sollten auch für Anbieter von Hardware und Software, die eine elektronische Kommunikation erlaubt, die Verpflichtungen des Privacy-by-Design und -Default gelten. Nur so können die Rechte der Endnutzer wirksam und praktikabel geschützt werden. Dies würde die DSGVO in sinnvoller und notwendiger Weise ergänzen.

## 9. ARTIKEL 16 – UNERBETENE KOMMUNIKATION

### Artikel 16 Absatz 1

Der vzbv begrüßt, dass künftig grundsätzlich eine Einwilligung notwendig sein soll, wenn natürliche oder juristische Personen Direktwerbung über elektronische Kommunikationsdienste an Endnutzer richten, die natürliche Personen sind. Positiv ist auch, dass diese Vorschrift technikneutral formuliert wurde, denn für den Endnutzer macht es keinen praktischen Unterschied, auf welche Weise ihn die Nachricht erreicht - die mögliche Belästigung ist identisch.

### Artikel 16 Absatz 2

Der vzbv bedauert jedoch, dass Verbraucher lediglich eine Widerspruchsmöglichkeit haben sollen, wenn Unternehmen von diesen Kunden elektronische Kontaktangaben für E-Mail im Zusammenhang mit dem Verkauf eines Produkts oder einer Dienstleistung erhalten haben und diese Kontaktdaten anschließend zur Direktwerbung für eigene ähnliche Produkte oder Dienstleistungen verwenden. Der vzbv erkennt jedoch an, dass dies der geltenden Rechtslage entspricht.

> Es muss jedoch klargestellt werden, dass es nicht zu einer Ausweitung der Möglichkeiten für Direktwerbung im Vergleich zur derzeitigen Rechtslage kommt. Akzeptabel ist unter den oben genannten Bedingungen lediglich eine Nutzung von Kontaktangaben für Werbung per E-Mail (im Sinne des Internetstandards RFC 5322). Eine Ausweitung über die Definition von E-Mail auf „jede über ein elektronisches Kommunikationsnetz verschickte elektronische Nachricht, die Informationen in Text-, Sprach-, Video-, Ton- oder Bildform enthält“ ist inaktzeptabel. Dementsprechend muss sowohl die deutsche Definition von „elektronischer Post“ in Art. 4 Abs. 3 lit. e), als auch der Wortlaut des Art. 16 Abs. 2 der englischen Fassung der Verordnung angepasst werden, so dass dieser sich nicht auf „electronic mail“, sondern lediglich auf „e-mail“ bezieht.

### Artikel 16 Absatz 4

Besonders persönliche Direktwerbeanrufe werden von Verbrauchern als sehr belästigend wahrgenommen. In diesen Situationen sind Verbraucher oftmals überrumpelt, stehen unter Druck und sind verwundbar für missbräuchliche Praktiken wie untergeschobene Verkäufe oder Verträge – besonders wenn es sich um sehr junge oder alte Verbraucher handelt. [29] Im Vergleich zu unerbetenen elektronischen Nachrichten, denen Verbraucher in Ruhe begegnen können, handelt es sich daher bei persönlichen Anrufen um einen weitaus größeren Eingriff.

Obgleich unerbetene Anrufe in Deutschland einem Einwilligungsvorbehalt unterliegen, gibt es noch eine Vielzahl von Beschwerden. In den Jahren 2013 bis 2016 erhielt die Bundesnetzagentur 113.126 schriftliche Beschwerden in Bezug auf unerlaubte Telefonwerbung.[30] Die Verbraucherzentralen verzeichneten allein zwischen Juli 2014 und November 2015 über 19.500 Beschwerden zu unerlaubten Werbeanrufen und am Telefon untergeschobenen Verträgen.[31]

Darüber hinaus können auch bei persönlichen Direktwerbeanrufen finanzielle Kosten für Endnutzer entstehen, beispielsweise wenn diese eine kostenpflichtige Anrufweiterleitung eingerichtet haben, oder sich im Ausland befinden, wo sie für den Empfang von Anrufen ein Entgelt entrichten müssen.

*Vor diesen Hintergründen erachtet es der vzbv als kritisch, dass Art. 16 Abs. 4 eine Öffnungsklausel für die Mitgliedsstaaten enthält, persönliche Direktwerbeanrufe natürliche Personen zuzulassen, wenn diese dem Erhalt solcher Kommunikation nicht widersprochen haben*. So könnten nationale Vorgaben durch Unternehmen aus Mitgliedsstaaten unterlaufen werden, in denen ein geringeres Schutzniveau festgeschrieben ist

> Eine europaweite Einwilligungslösung ist daher dringend geboten, Alternativ sollte klargestellt werden, dass auch innerhalb Europas ein "Marktortprinzip" gilt. Sprich: Wenn in Deutschland eine Einwilligung notwendig ist, sollten sich dann auch Unternehmen aus anderen EU-Mitgliedsstaaten danach richten müssen, wenn diese deutsche Verbraucher anrufen.

## 10. ARTIKEL 21 – RECHTSBEHELFE

### Artikel 21 Absatz 1

Auch in Art. 21 Abs. 1 bleiben wichtige Fragen hinsichtlich des Zusammenwirkens der ePVO und der DSGVO offen. So ist unklar, warum zwar auf die Rechte der Endnutzer in den Artikeln 77, 78 und 79 der DSGVO verwiesen wird, jedoch nicht auf Art. 80 DSGVO (Vertretung von betroffenen Personen). *Eine Ausklammerung von Art. 80 DSGVO wäre jedoch inakzeptabel, da die Rechte der Verbraucher hinter den guten Vorgaben der DSGVO zurückbleiben würden*. Denn nach dieser können betroffene

[29] Verbraucherzentrale.de: Unerlaubte Telefonwerbung - Belästigung hält an; 2015; https://www.verbraucherzentrale.de/unerlaubte-telefonwerbung-nervt-weiterhin

[30] Antwort der Bundesregierung auf schriftliche Frage des Abgeordneten Markus Tressel im Monat Februar 2017, Frage Nr. 137; 2017; http://docs.dpaq.de/11978-antwort_unerlaubte_telefonwerbung.pdf

[31] Verbraucherzentrale.de: Unerlaubte Telefonwerbung - Belästigung hält an; 2015; https://www.verbraucherzentrale.de/unerlaubte-telefonwerbung-nervt-weiterhin

Personen Verbraucherverbände oder andere Organisationen ohne Gewinnerzielungsabsicht damit beauftragen, in ihrem Namen gegen ein Unternehmen zu klagen, wenn dieses gegen den Schutz ihrer persönlichen Daten verstößt. Verbraucherverbände könnten also in allen Branchen die Datenschutzinteressen der Verbraucher durchsetzen, außer im besonders sensiblen Telekommunikationsbereich.

> Es muss sichergestellt werden, dass die Vorgaben des Art. 80 DSGVO auch im Telekommunikationsbereich Anwendung finden. Alles andere würde hinter der DSVO zurückbleiben und damit gegen EWG 5 verstoßen.

### 11. ARTIKEL 23 – ALLGEMEINE VORAUSSETZUNGEN FÜR DIE VERHÄNGUNG VON GELDBUßEN

**Artikel 23 Absatz 2 Buchstabe a)**

Aufgrund der hohen Relevanz der Endgeräte für die Persönlichkeit und Privatsphäre der Endnutzer in Zusammenhang mit den damit gleichzeitig verbundenen hohen Gefahren, ergibt sich ein besonderes Schutzbedürfnis. Daher müssen die in Endeinrichtungen der Endnutzer gespeicherten oder sich auf diese beziehenden Informationen einen besonderen Schutz unterliegen. *Dementsprechend sollten auch mögliche Sanktionen dem Rahmen entsprechen, den die Verordnung für Verstößen gegen Grundsätze der Vertraulichkeit der Kommunikation vorsieht*.

> Verstöße gegen die Verpflichtungen einer juristischen oder natürlichen Person, die elektronische Kommunikationsdaten nach Art. 8 verarbeitet, sollten in den Bußgeldrahmen des Art. 23 Abs. 2 aufgenommen werden.

# V. WEITERE ANMERKUNGEN

### 1. BESCHRÄNKUNGEN DURCH DIE MITGLIEDSSTAATEN

Der vzbv weist darauf hin, dass der Europäische Gerichtshof mit seinem Urteil in den Rechtssachen C-293/12 und C-594/12 die Richtlinie zur Vorratsdatenspeicherung 2006/24/EC für ungültig erklärt hat. Daher bedauert der vzbv, dass die ePVO die Mitgliedsstaaten nicht daran hindert, Regelungen zur Vorratsdatenspeicherung beizubehalten oder einzuführen.

*Auf keinen Fall aber darf die ePVO keine neue Verpflichtung zur Vorratsdatenspeicherung von Telekommunikationsverbindungsdaten enthalten*. Vielmehr müssen sich alle nationalen Gesetze auf Basis des Art. 11 an den Vorgaben der Europäischen Grundrechtecharta und der Europäische Menschenrechtskonvention sowie den Rechtsprechungen des Europäischen Gerichtshofs und des Europäischer Gerichtshof für Menschenrechte messen lassen.

Den Mitgliedsstaaten muss es ferner untersagt werden, bestehende Regelungen zur Vorratsdatenspeicherung auch auf die nun durch die ePVO erfassten OTT-Dienste auszuweiten.

## 2. ABSICHERUNG DER KOMMUNIKATION

Die Prinzipien des Datenschutzes durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen – als Umsetzung der Zweckbindung und Datenminimierung – sind wichtige Instrumente, um Verbraucher zu schützen, insbesondere jene, die nur über wenig Wissen über Internet-Technologien verfügen. Diese Grundsätze sind ein Kern der DSGVO und sollten in der ePVO als sektorspezifische Rechtsvorschrift detailliert umgesetzt werden. Um das Prinzip der Datenminimierung weiter zu stärken sollten Unternehmen unter anderem ihren Kunden grundsätzlich die Nutzung elektronischer Kommunikationsdienste und ihre Bezahlung anonym oder unter Pseudonym zu ermöglichen, soweit dies technisch möglich und zumutbar ist.

*Die Möglichkeit der sicheren Verschlüsselung der Kommunikation ist nicht nur essentiell für die Sicherheit der Bürger und das Vertrauen der Verbraucher, sondern auch für die gesamte europäische Wirtschaft*.[32]

Die Anbieter elektronischer Kommunikation sollten dazu verpflichtet werden, die Vertraulichkeit der Kommunikation standardmäßig unter Verwendung des aktuellen Stands der Technik abzusichern. Insbesondere sollte es daher explizit verboten sein, Hintertüren in Soft- und Hardware einzubauen, die eine Überwachung der elektronischen Kommunikation erlaubt.

[32] Information Technologie & Innovation Foundation: Report „Unlocking Encryption: Information Security and the Rule of Law“; 2016; https://itif.org/publications/2016/03/14/unlocking-encryption-information-security-and-rule-law; 06.03.2017