Deutsche Vereinigung für Datenschutz e.V.
Reuterstraße 157
53113 Bonn
www.datenschutzverein.de

Bonn, 31.05.2017

Stellungnahme der Deutschen Vereinigung für Datenschutz (DVD) zum

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

vom 10.01.2017 (Dokument: COM(2017) 10 final 2017/0003(COD))

Inhalt

A Allgemeine Erwägung

Angesichts der technischen Entwicklung der elektronischen Kommunikation und der damit verbundenen ökonomischen, sozialen und kulturellen Konsequenzen und den teilweise exzessiv genutzten Möglichkeiten zur Überwachung von Menschen über Kommunikationsmittel und angesichts der damit verbundenen Eingriffe in die Grundrechte auf Datenschutz (Artikel 8 Grundrechtecharta - GRCh) sowie auf Vertraulichkeit der Kommunikation (Artikel 7 GRCh) ist die Entwicklung eines einheitlichen rechtlichen Rahmens für den Schutz der digitalen Freiheitsrechte in Europa von zentraler Bedeutung. Daher begrüßt die Deutsche Vereinigung für Datenschutz (DVD) die Bestrebungen der Ge-

setzgebungsorgane der Europäischen Union (EU), eine direkt anwendbare und umfassende „Verordnung über Privatsphäre und elektronische Kommunikation“ (ePrivacy-Verordnung) zu erarbeiten und zu verabschieden. Eine solche ist auch nach der Verabschiedung der Europäischen Datenschutz-Grundverordnung (EU) 2016/679 vom 27.04.2016 (DS-GVO) aus Sicht der DVD dringend erforderlich.

Zu begrüßen sind dabei insbesondere folgende mit diesem Projekt verbundenen Ziele:

- die Regulierung in einer verbindlichen Verordnung anstelle der bisher national umzusetzenden Richtlinie,
- die Einbeziehung aller modernen Kommunikationsformen, insbesondere auch der sog. Over-the-Top-Kommunikationsdienste („OTT-Dienste“) und damit sämtlicher von Artikel 7 GRCh geschützten elektronischen Kommunikationsformen (u. a. Messaging-Dienste, soziale Netzwerke) in die Regulierung,
- die Einbeziehung von juristischen Personen in den Kommunikationsschutz (Erwägungsgrund (EG) 3),
- die Einbeziehung von Maschine-Maschine-Kommunikation (EG 12),
- die Einbeziehung von Daten über die Metadaten sowie Kommunikationsinhalte (EG 14),
- die spezifische Berücksichtigung von modernen Formen der Mobilkommunikation (Artikel 8),
- die enge rechtliche Verknüpfung zwischen der ePrivacy-Verordnung und der DS-GVO.

B Einzelstellungnahme zum Entwurf der ePrivacy-Verordnung

Es werden folgende Verbesserungsvorschläge gemacht:

Zu Artikel 1 Gegenstand

In Artikel 1 Abs. 3 sollte, um das **Verhältnis zwischen der ePrivacy-Verordnung und der DSGVO** zu präzisieren, eine Regelung aufgenommen werden, wonach die DSGVO vollständig anwendbar bleibt, soweit die ePrivacy-Verordnung keine verdrängenden Regelungen enthält. Dies ist ausschließlich in Bezug auf die gesetzlichen Erlaubnisregelungen zur Verarbeitung von Kommunikationsdaten der Fall. Dadurch wird klargestellt, dass z. B. sämtliche Regelungen der DSGVO zu den Betroffenenrechten, zur Einwilligung, zu technisch-organisatorischen Maßnahmen oder zum Rechtsschutz bei der Kommunikation personenbezogener Daten anwendbar bleiben.

Zu Artikel 2 Sachlicher Anwendungsbereich

Es ist unklar, was im Sinne von Abs. 2 lit. c unter „elektronische Kommunikationsdienste, die nicht öffentlich zugänglich sind“ zu verstehen ist, für welche die ePrivacy-Verordnung nicht gelten soll (vgl. EG 16: Anwendung bei „unbestimmter Gruppe von Endnutzern“). Im Interesse einer Präzisierung und zugleich einer Abstimmung mit Artikel 2 Abs. 2 lit. c DSGVO sollte klargestellt werden, dass mit der Ausnahme solche Dienste

erfasst werden, die „zu Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten“ (**Haushaltausnahme**) dienen. Damit wird zugleich signalisiert, dass Dienste mit geschlossenen Benutzergruppen, bei denen ein Anbieter-Verbraucher-Verhältnis besteht, z. B. bei Betreibern von WLAN-Hotspots eines Cafés oder Flughafens oder bei zahlenmäßig nicht eingeschränkten Internet-Kommunikationsangeboten, von der Verordnung erfasst werden. Zumindest in der Begründung (in den Erwägungsgründen) sollte präzisiert werden, dass die Kommunikation über eine Internet-Plattform wie z. B. Facebook oder Twitter unter den Schutz von Artikel 7 GRCh und den Anwendungsbereich der ePrivacy-Verordnung fällt.

Zu Artikel 3 Räumlicher Anwendungsbereich und Vertreter

Ein Mangel der DSGVO besteht darin, dass die **Hersteller von Hardware und Software**, mit der personenbezogene Daten verarbeitet werden, nur indirekt (z. B. über Zertifizierungskriterien gem. Artikel 42 Abs. 5 DSGVO) angesprochen werden. Dieses normative Defizit wird bisher in der ePrivacy-Verordnung für den besonders relevanten Kommunikationsbereich nicht behoben. Dies hat zur Folge, dass z. B. die Angebote von Browser-Technologie oder von WLAN-Routern nur indirekt über den Markt reguliert werden, obwohl diese für die Vertraulichkeit der Kommunikation höchst relevant sind. Diesem Defizit kann durch eine spezifische Regelung für diese Adressatengruppe und eine entsprechende Ausweitung des Anwendungsbereichs abgeholfen werden.

Zu Artikel 4 Begriffsbestimmungen

Bei der Definition des zentralen Begriffs des **elektronischen Kommunikationsdienstes** wird in Abs. 1 lit. b auf die Definition in der „Richtlinie über den europäischen Kodex für die elektronische Kommunikation“ verwiesen. Dieser Kodex verfolgt eine teilweise andere Zielrichtung als die ePrivacy-Verordnung und ist für den einfachen Nutzer nicht direkt zugänglich. Daher wird vorgeschlagen, diese Definition ausdrücklich in Artikel 4 aufzunehmen.

In Abs. 3 lit. c wird erstmals der Begriff der „elektronische Kommunikationsmetadaten“ (**Metadaten**) eingeführt. Dies ist grundsätzlich zu begrüßen. In Erwägungsgrund 2 wird zurecht dargestellt, dass diesen Metadaten in vielen Fällen eine besondere Sensitivität zugewiesen werden muss. Dem sollte – über Artikel 6 Abs. 2 hinausgehend – Rechnung getragen werden, z. B. indem die Zulässigkeit der Verarbeitung von Metadaten grundsätzlich von einer Datenschutz-Folgenabschätzung (gemäß Artikel 35 DS-GVO) abhängig gemacht wird.

Eine besondere Form von Metadaten sind die Daten zum **Standort des Geräts**. Von dieser Regelung nicht erfasst sind Standortdaten, die nicht zur Erbringung des Kommunikationsdienstes, sondern zur Erbringung eines Telemediendienstes, also zur Vermittlung von Medieninhalten genutzt werden (EG 17 Satz 4). Hierfür wird i. d. R. die gesonderte GPS-Ortung verwendet, die sich hinsichtlich ihrer Sensitivität nicht von Kommunikations-Standortdaten unterscheidet. Für diese Daten sollte in der Verordnung ein vergleichbarer Schutz vorgesehen werden.

In Abs. 3 lit. e wird der englische Begriff „**electronic mail**“ im Deutschen mit „E-Mail“ übersetzt. Dieser „deutsche“ Begriff ist für eine spezifische Form der Internet-Kommunikation im deutschen Sprachgebrauch belegt. Deshalb sollte eine andere Bezeichnung verwendet werden, z. B. „elektronische Post“, wie er bereits in der ePrivacy-Richtlinie (Richtlinie 2002/58/EG) verwendet wird.

Datenschutz-Folgenabschätzung und vorherige Konsultation, weitergehende Veröffentlichung

Es wird vorgeschlagen, eine eigenständige Regelung aufzunehmen, in der sämtliche Formen der kommunikativen Datenverarbeitung zusammengefasst werden, in denen gemäß dieser Verordnung eine **Datenschutz-Folgenabschätzung** oder eine vorherige Konsultation (Artikel 35, 36 DSGVO) zur Pflicht gemacht wird (vgl. zu Artikel 4 – Metadaten, Artikel 6 – Inhaltsdaten, Artikel 8 Endeinrichtungsdaten).

Wird in der vorliegenden Verordnung eine Pseudonymisierung oder Anonymisierung zur Pflicht gemacht, so sollte eine gesonderte Regelung die Betreiber verpflichten, die Art und Weise der **Datenminimierung** den Nutzern oder allgemein öffentlich bekannt zu machen.

Insofern ist die Festlegung möglichst europaweit geltender **Standards** wünschenswert, so wie dies in der DSGVO angelegt ist (Artikel 35, 40, 42 Abs. 2, 5). Die Erarbeitung von Standards könnte spezifisch und verbindlich geregelt werden.

Zu Artikel 6 Erlaubte Verarbeitung elektronischer Kommunikationsdaten

In Abs. 2 lit. c wird die Verarbeitung von Metadaten erlaubt, wenn der Endnutzer seine Einwilligung erteilt hat. Da ein Endgerät in vielen Fällen von mehr als einem Nutzer genutzt wird, sollte klargestellt werden, dass die **Einwilligung „aller“ Endnutzer** erforderlich ist.

In Abs. 3 lit. a und b wird die Verarbeitung von Kommunikationsinhalten von der Einwilligung der jeweiligen Nutzer abhängig gemacht. Es ist allgemein anerkannt, dass es sich bei diesen Daten um sensitive Daten handelt. Für die Einwilligung solcher Daten bedarf es eines gesteigerten Warneffekts. Dieser wird bzgl. sensitiver Daten in Artikel 9 Abs. 2 lit. a DSGVO dadurch hergestellt, dass eine „**ausdrückliche“ Einwilligung** gefordert wird. Diese spezifische Anforderung sollte auch hier vorgesehen werden.

Wegen der Sensitivität der Verarbeitung von Kommunikationsinhalten sollte in Abs. 3 lit. a zusätzlich zum Einwilligungserfordernis verpflichtend eine **Datenschutz-Folgenabschätzung** nach Artikel 35 DSGVO, evtl. gar eine vorherige Konsultation der Aufsichtsbehörde nach Artikel 36 DSGVO vorgesehen werden.

Für die Verarbeitung von Inhaltsdaten für weitere Zwecke ist nach Abs. 3 lit. b eine obligatorische Prüfung vorgesehen, ob diese „durch eine Verarbeitung anonymisierter Informationen nicht erreicht werden können“. Im Interesse der Klarstellung sollte auch die Möglichkeit der **Pseudonymisierung** explizit erwähnt werden, so wie dies auch derzeit

in § 13 Abs. 6 TMG schon in Bezug auf die Erbringung eines Telemediendienstes der Fall ist.

Zu Artikel 8 Schutz der in der Endeinrichtung der Endnutzer gespeicherten oder sich auf diese beziehenden Informationen

In Abs. 1 lit. b wird als Erlaubnistatbestand für die Verarbeitung von Endgeräteinformationen die Einwilligung genannt. Wegen der Sensitivität der Verarbeitung dieser Daten und im Interesse der Klarstellung sollte geregelt werden, dass eine „**explizite Einwilligung für den konkreten Zweck**“ erteilt werden muss.

Nicht akzeptabel ist, dass dem Betreiber gem. Abs. 1 lit. d „für die **Messung des Webpublikums**“ diese uneingeschränkt erlaubt wird. „Messung des Webpublikums“ ist die Beschreibung einer Verarbeitungsmaßnahme und nicht eines Verarbeitungszweckes. Die Regelung erteilt somit einen Freibrief für eine Weiterverarbeitung der Endgerätedaten. Zur Behebung dieses Defizits kann auf die bewährten Schutzmechanismen des § 15 Abs. 3 TMG verwiesen werden, der als erlaubte Zwecke die Werbung, die Marktforschung sowie die bedarfsgerechte Gestaltung des Dienstes nennt, zu einer Information des Nutzers verpflichtet und diesem die Möglichkeit eines die Verarbeitung ausschließenden Widerspruchs eröffnet. Als weitere Einschränkung ist eine zeitliche Begrenzung der Verarbeitung sinnvoll.

In Abs. 2 lit. b soll unter bestimmten Voraussetzungen der **Offline-Tracking** erlaubt werden, wobei sowohl eine hinreichende Information und eine Abschaltmöglichkeit für die Betroffenen vorgesehen ist. Damit bleibt die Verantwortung für die Datenminimierung vollständig in der Hand der Nutzer, welche die mit dem Tracking verbundenen Risiken oft nicht hinreichend abschätzen können. Daher sollte vorgesehen werden, dass in jedem Fall eine vorherige Konsultation der Aufsichtsbehörde nach Artikel 36 DSGVO zur Verpflichtung gemacht wird. Nur dadurch kann sichergestellt werden, dass, wie schon bisher vorgesehen, die Anforderungen des Artikel 32 DSGVO, etwa im Hinblick auf eine Pseudonymisierung, eingehalten werden oder dass als angemessene Garantie eine Einwilligung der Nutzer eingeholt werden muss. Auch insofern ist eine zeitliche Begrenzung der Verarbeitung sinnvoll.

In der Regelung des Abs. 2 lit. b sollte es für den Betroffenen nicht nur möglich sein, die Datenerhebung zu „beenden“, ihm sollte es auch möglich sein, diese **vollständig auszuschließen**.

Zu Artikel 9 Einwilligung

In Abs. 2 ist vorgesehen, dass die Einwilligung in Form einer Software-Einstellung erteilt werden kann. Es sollte klargestellt werden, dass dies auch für die Ausübung von **Widerspruchsrechten** gilt, so dass technische Vorgaben zum Tracking (z. B. Browsereinstellungen, „do not track“) verpflichtend beachtet werden müssen.

Zumindest in den Erwägungsgründen sollte klargestellt werden, dass bei den Softwareeinstellungen die **Anforderungen an Einwilligungen gemäß der DSGVO** (spezifisch, informiert, nachweisbar, in klarer einfacher Sprache) zu beachten sind.

Kommt es zu einem Widerspruch zwischen Softwareeinstellung und Einwilligungsanforderung eines Betreibers, so sollte in jedem Fall die Eröffnung der Möglichkeit einer spezifischen **ausdrücklichen Einwilligung im Einzelfall** zur Pflicht gemacht werden. Das von vielen OTT-Anbietern praktizierte „Friss-oder-stirb-Prinzip“ (take it or leave it) muss wirksam ausgeschlossen werden.

Zu Artikel 10 Bereitzustellende Informationen und Einstellungsmöglichkeiten zur Privatsphäre

Zumindest in den Erwägungsgründen zu Abs. 1 sollte klargestellt werden, dass mit den Einstellungsmöglichkeiten **sämtliche Formen der Zuordnung**, einschließlich dem Fingerprinting, verhindert werden können müssen.

Die Formulierung von Abs. 2 greift inhaltlich zu kurz, da sie vorinstallierte Software nicht mit abdeckt. Es muss klargestellt werden, dass Artikel 25 DSGVO mit der Verpflichtung zum **Privacy by Design und by Default** sowohl im Hinblick auf die Kommunikationsdienste wie auch auf die Endeinrichtungsgestaltung anwendbar ist und dass hierüber hinreichend informiert werden muss.

Zu Artikel 11 Beschränkungen

Die Regelung sieht vor, dass die Union oder Mitgliedstaaten Ausnahmen von den in Artikel 5 und 8 ePrivacy-Verordnung vorgesehenen Rechten und Pflichten regeln dürfen (Wahrung der Vertraulichkeit und Schutz der Endeinrichtungsinformationen), soweit dies dem Schutz „wichtiger Interessen der Union oder eines Mitgliedstaats, insbesondere eines wichtigen wirtschaftlichen oder finanziellen Interesses“ dient (Verweis auf Artikel 23 Abs. 1 lit. a-e DSGVO). Diese Öffnungsklausel geht über das hinaus, was an Eingriffen in der Vorgängerregelung des Artikel 15 Abs. 1 Richtlinie 2002/58/EG sowie in der DSGVO vorgesehen ist, sie schließt die Bereiche Währung, Haushalt, Steuer und Gesundheit mit ein und lädt zum Erlass von unverhältnismäßigen Regelungen zur Überwachung bzw. zur Vorratsdatenspeicherung ein. Auch der EuGH hat hierzu engere Rahmenbedingungen definiert (EuGH U. v. 21.12.2016, C-203/15 u. C-698/15, DVBl 2017, 177 ff. = K&R 2017, 105 ff.).

Zu Artikel 15 Öffentlich zugängliche Verzeichnisse

Es ist zu begrüßen, dass eine Eintragung von Daten von „Endnutzern, die natürliche Personen sind“ in öffentliche Verzeichnisse nur mit deren Einwilligung erfolgen darf. Allerdings ist die vorgeschlagene Regelung, dass der jeweilige Anbieter des Verzeichnisses diese Einwilligung beim Endnutzer einholen muss, weder praxistauglich noch Endnutzerfreundlich. Vielmehr sollte die zumindest in Deutschland bewährte Regelung beibehalten werden, nach der es ausreichend ist, dass diese Einwilligung vom Endnutzer gegenüber

dem jeweiligen Betreiber des Kommunikationsdienstes erklärt wird, so dass der Endnutzer nicht von Anfragen der alleine in Deutschland über 60 vorhandenen Verzeichnisanbieter überhäuft wird.

Zu Artikel 16 Unerbetene Kommunikation

In den Erwägungsgründen sollte klargestellt werden, dass die Regelungen zur unerbetenen Kommunikation nicht nur für die Zusendung, sondern auch für die **Anzeige von (personalisierter) Direktwerbung** anzuwenden ist.

Anders als im Offline-Bereich erfolgt bei Telekommunikationsdiensten eine massenhafte Nutzung von Kommunikationsdaten zur Platzierung, Versendung von unerwünschter Werbung oder Durchführung von Direktwerbeanrufen. Daher ist – anders als bei Artikel 21 Abs. 2 DSGVO – die Einräumung eines Widerspruchsrechts nicht ausreichend, um z. B. unerwünschte Spam zu verhindern. Deshalb sollte, entgegen Abs. 2 und 4, für diese Fälle eine **Einwilligung** europaweit zwingend erforderlich sein.

Es sollte präzisiert werden, dass der Widerruf einer Einwilligung bzw. der **Widerspruch** gegen Direktmarketing nicht nur „in einfacher Weise“ (Abs. 6) möglich sein muss, sondern auch nicht technisch oder anderweitig, z. B. durch Kosten, behindert werden darf (so nur bei Erhalt von E-Mail-Werbung gem. Abs. 2). Der Widerruf einer Einwilligungserklärung muss bzgl. Form und technischem Mittel der Erklärung selbst entsprechen können (ebenso Artikel 7 Abs. 3 DSGVO).

Es sollte klargestellt werden, dass – über Abs. 3 hinausgehend – **Werbung unter falscher Identität** „und“ mit falschen Erreichbarkeitsdaten unzulässig ist. Verstöße hiergegen sollten sanktioniert werden.

Zu Artikel 17 Information über erkannte Sicherheitsrisiken

Die Pflicht für Betreiber, die Endnutzer über erkannte Sicherheitsrisiken zu informieren, sollte auf Anbieter von Kommunikations-**Hard- und -Software** ausgeweitet werden. Es sollte präziser festgelegt werden, unter welchen Voraussetzungen und mit welchen Inhalten die über Artikel 34 DSGVO hinausgehende Informationspflicht umzusetzen ist.

Für die DVD:

- Dr. Thilo Weichert (Vorstandsmitglied der Deutschen Vereinigung für Datenschutz e.V.) – E-Mail: weichert@datenschutzverein.de
- Frank Spaeing (Vorsitzender der Deutschen Vereinigung für Datenschutz e.V.) E-Mail: spaeing@datenschutzverein.de
- Werner Hülsmann (stellv. Vorsitzender der Deutschen Vereinigung für Datenschutz e.V.) – E-Mail: huelsmann@datenschutzverein.de