Digitale Gesellschaft e. V.
Singerstraße 109
10179 Berlin

+49 30 97894230

info@digitalegesellschaft.de
www.digitalegesellschaft.de
@digiges

Berlin, den 21. März 2017

Stellungnahme des Digitale Gesellschaft e.V. zum Vorschlag der Europäischen Kommission für eine Verordnung über die Achtung des Privatlebens und den Schutz personenbezogener Daten in der elektronischen Kommunikation

Zu dem vorliegenden Vorschlag nehmen wir wie folgt Stellung:

A. Vorbemerkungen

Der Digitale Gesellschaft e.V. begrüßt den Vorschlag der EU-Kommission für eine Verordnung über die Achtung des Privatlebens und den Schutz personenbezogener Daten in der elektronischen Kommunikation (ePVO).

Besonders erfreulich ist aus unserer Sicht die Entscheidung, die spezifischen Datenschutzanforderungen beim Betrieb und bei der Nutzung von elektronischen Kommunikationsdiensten im Wege einer Verordnung und damit grundsätzlich EU-weit einheitlich zu regeln.

Des Weiteren freuen wir uns darüber, dass die Regelung auch für die bisher kaum reglementierten OTT-Anbieter gelten soll. Auf diese Weise wird gewährleistet, dass die Endnutzer unabhängig von dem jeweils konkret verwendeten elektronischen Kommunikationsmittel stets das gleiche Schutzniveau genießen.

Schließlich halten wir eine Neuregelung auch mit Blick auf die rasant fortschreitende Entwicklung beim Tracking der Endnutzer und der von ihnen verwendeten Endeinrichtungen für dringend geboten.

Die Verordnung enthält zahlreiche gute Ansätze für einen zeitgemäßen Schutz der elektronischen Kommunikation. An einigen Stellen sind aus unserer Sicht jedoch Nachbesserungen und Änderungen erforderlich, die wir im Nachfolgenden näher ausführen.

B. Die Vorschriften im Einzelnen

1. Artikel 1

Die Regelungen der ePVO sollen ein EU-weit einheitliches Niveau für den Schutz von Grundrechten und Grundfreiheiten bei der Nutzung und der Bereitstellung elektronischer Kommunikationsdienste gewährleisten. Darüber hinaus sollte es den Mitgliedstaaten jedoch stets möglich sein, durch Vorschriften auf nationaler Ebene höhere Schutzstandards für das Recht auf Achtung des Privatlebens und der Kommunikation sowie für das Recht auf den Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten festzulegen. Wir halten es deshalb für geboten, Artikel 1 um eine entsprechende Öffnungsklausel zu erweitern.

2. Artikel 4

Die Begriffsbestimmungen in Artikel 4 lassen eine Definition des Kernbegriffs der „elektronischen Kommunikation" vermissen. Zur besseren Verständlichkeit und Begriffsklarheit sollte eine solche Definition in die Verordnung aufgenommen werden.

Wir begrüßen, dass der Begriff des „interpersonellen Kommunikationsdienstes" gemäß Artikel 4 Abs. 2 auch solche Dienste einschließt, „die eine interpersonelle und interaktive Kommunikation lediglich als untrennbar mit einem anderen Dienst verbundene Nebenfunktion ermöglichen". Für die Schutzbedürftigkeit der Kommunikation von Endnutzerinnen und Endnutzern kommt es nicht darauf an, ob der im Einzelfall verwendete Kommunikationsdienst als Haupt- oder Nebenfunktion ausgestaltet ist.

3. Artikel 6

3.1. Allgemeines

Artikel 6 normiert bestimmte Ausnahmen von dem in Artikel 5 geregelten grundsätzlichen Verbot von Eingriffen in elektronische Kommunikationsdaten. Um einer unbeabsichtigten Aufweichung des Verbotes vorzubeugen und den Grundsatz des Artikel 5 zu stärken, müssen die Ausnahmen strikt auf das im jeweiligen Einzelfall notwendige Maß beschränkt werden.

In der gegenwärtigen Fassung erlauben die Tatbestände des Artikel 6 jedoch gerade keine graduellen Abweichungen von dem grundsätzlichen Verbot. Aufgrund der Verwendung des Wortes „wenn" gehorchen die Ausnahmen bislang dem „Alles oder nichts"-Prinzip: Sobald ein Ausnahmefall eingreift, ist die Verarbeitung von Kommunikationsdaten zulässig, ohne dass der Umfang der Verarbeitung auf das für die jeweilige Ausnahme nötige Maß beschränkt wird. Wir halten es deshalb für geboten, im Rahmen des Artikel 6 anstelle des Wortes „wenn" das Wort „soweit" zu verwenden.

3.2. Artikel 6 Abs. 2 lit c) und Artikel 6 Abs. 3 lit b)

Artikel 6 Abs. 2 lit c) sowie Artikel 6 Abs. 3 lit b) sehen Ausnahmen vom grundsätzlichen Verbot des Artikels 5 vor, wenn eine Einwilligung in die Verarbeitung von Kommunikationsdaten vorliegt. Unverständlich ist, warum Artikel 6 Abs. 2 lit c) die Verarbeitung von Kommunikationsmetadaten bereits dann erlaubt, wenn „der betreffende Endnutzer" seine Einwilligung erteilt hat, während eine Verarbeitung der Kommunikationsinhalte gemäß Artikel 6 Abs. 3 lit b) nur dann zulässig ist, wenn „alle betreffenden Endnutzer" eingewilligt haben. Die Verarbeitung von Kommunikationsmetadaten betrifft mindestens in dem gleichen Maße wie die Kommunikationsinhalte stets sämtliche Kommunikationsteilnehmer. Deshalb sollte auch die Verarbeitung von Kommunikationsmetadaten der Einwilligung aller betreffenden Endnutzer bedürfen.

Des Weiteren werden die Verarbeitungszwecke, in die eine Einwilligung möglich ist, weder in Artikel 6 Abs. 2 lit c) noch in Artikel 6 Abs. 3 lit b) in irgendeiner Weise beschränkt oder bedingt. Sowohl im Hinblick auf besonders schutzbedürfige Personengruppen wie Kinder und Jugendliche als auch im Hinblick auf besonders sensible Datenarten wie Gesundheitsdaten oder

Informationen aus dem innersten Kreis der persönlichen Lebensgestaltung bedarf Artikel 6 daher dringend der Ergänzung.

Gerade in den vorgenannten Konstellationen muss sichergestellt sein, dass sich die Betroffenen der Bedeutung, der Risiken, der Konsequenzen und der Reichweite ihrer Einwilligungen bewusst sind. Dies gilt für die Verarbeitung sowohl von Kommunikationsmetadaten als auch von Kommunikationsinhalten. Eine Verarbeitung darf in diesen Fällen daher nur dann zulässig sein, wenn durch technische Maßnahmen oder in anderer Weise gewährleistet ist, dass die Betroffenen umfassende Informationen über die Verarbeitung erhalten und diese auch tatsächlich wahrgenommen und verstanden haben. Ist die Verarbeitung nicht erforderlich, um einen Dienst für Endnutzer bereitzustellen, sollte darüber hinaus speziell im Fall von Kommunikationsinhalten stets eine ausdrückliche Einwilligung erforderlich sein.

4. Artikel 7

Artikel 7 normiert Lösch- und Anonymisierungspflichten ausdrücklich nur für die Betreiber elektronischer Kommunikationsdienste. Zugleich nimmt Artikel 7 Abs. 1 und Abs. 2 jedoch Bezug auf Artikel 6 Abs. 1, der wiederum die Verarbeitung von Kommunikationsdaten auch für die Betreiber von Kommunikationsnetzen erlaubt. Um Unklarheiten zu vermeiden, sollte in Artikel 7 klargestellt werden, dass die dort geregelten Pflichten auch für Betreiber von Kommunikationsnetzen gelten.

Des Weiteren halten wir es nicht für sinnvoll, die Anonymisierung von Kommunikationsdaten als Alternative zu ihrer Löschung vorzusehen. Durch die Zusammenführung mit weiteren Daten können insbesondere anonymisierte Metadaten leicht einer bestimmten natürlichen Person zugeordnet und der mit der Anonymisierung bezweckte Schutz der Privatsphäre auf diese Weise ausgehebelt werden. Dies gilt umso mehr, als dass die Verordnung keine besondere Zweckbindung und keine Höchstspeicherfristen für die anonymisierten Daten vorschreibt.

5. Artikel 8

5.1. Allgemeines

Wir begrüßen die Zielsetzung des Artikels 8, die in Endeinrichtungen der Endnutzer gespeicherten Informationen besonders zu schützen. Um dieses Ziel effektiv zu erreichen, sind nach unserer Auffassungen jedoch verschiedene Nachbesserungen nötig.

Viele Endnutzer ergreifen bereits heute selbst Maßnahmen, um sich aktiv gegen die Ausspähung ihrer Endgeräte und die Verfolgung im Netz zu schützen (z.B. durch die Verwendung von Ad- oder Skriptblockern). Im Gegenzug sind immer mehr Online-Anbieter bestrebt, solche Maßnahmen zu umgehen oder die Verwendung ihrer Dienste nur dann zu ermöglichen, wenn Endnutzer diese Maßnahmen unterlassen. Artikel 8 sollte es daher verbieten, von Endnutzern selbst getroffene Vorkehrungen zum Schutz ihrer Endeinrichtungen vor Ausspähung und zum Schutz vor Verfolgung im Netz zu umgehen. Ebenso sollte es verboten werden, die Benutzung von Kommunikationsdiensten nur zu ermöglichen, wenn solche Schutzvorkehrungen zuvor deaktiviert werden.

5.2. Art. 8 Abs. 1 lit b)

Artikel 8 Abs. 1 lit b) ermöglicht Dritten die Nutzung der Verarbeitungs- und Speicherfunktionen von Endeinrichtungen sowie die Erhebung von Informationen aus Endeinrichtungen, wenn der Endnutzer eine entsprechende Einwilligung abgegeben hat. Wie Artikel 9 Abs. 2 klarstellt, kann diese Einwilligung auch in den Einstellungen einer Software, die den Zugang zum Internet ermöglicht, gegeben werden. Des Weiteren lässt Artikel 10 es zu, die Browsereinstellungen zum Schutz der Privatsphäre schon bei Auslieferung der Software so zu konfigurieren, dass die Einwilligung erteilt wird.

Im Zusammenspiel ermöglichen es die drei genannten Vorschriften daher, den Schutz der Endeinrichtungen gezielt zu unterlaufen. Um diese Gefahr zu minimieren, sollte Artikel 9 Abs. 2 gestrichen und in Artikel 8 Abs. 1 lit b) das Erfordernis einer ausdrücklichen Einwilligung aufgenommen werden. Alternativ könnte in Artikel 10 die Verpflichtung aufgenommen werden, Browser und andere Software, die den Zugang zum Internet ermöglicht, nur mit besonders strikten Voreinstellungen zum Schutz der Privatsphäre auszuliefern (Privacy by default) und

eine Änderung dieser Voreinstellungen durch Endnutzer nur zuzulassen, wenn zuvor ein entsprechender ausdrücklicher Warnhinweis angezeigt wurde.

5.3. Artikel 8 Abs. 2 lit b)

Artikel 8 Abs. 2 lit b) ermöglicht die Erhebung von Informationen, die von Endeinrichtungen ausgesendet werden, um sich mit anderen Geräten oder Netzanlagen zu verbinden. Darunter sind eindeutige Kennungen der Endeinrichtungen wie MAC-Adresse, IMEI und IMSI zu verstehen. Diese Informationen ermöglichen es, einzelne Endgeräte zu identifizieren und in der analogen Welt zu verfolgen. Beispielsweise könnten die Informationen dazu verwendet werden, um die Bewegungen eines Endnutzers in einem bestimmten Ladenlokal nachzuzeichnen oder festzuhalten, wann, wie häufig und wie lange er bestimmte Filialen einer Handelskette betritt.

Verschärft wird diese Problematik noch durch den Umstand, dass es technisch kaum möglich ist, den räumlichen Bereich, in dem die Erhebung der Informationen stattfindet, hinreichend klar und trennscharf zu begrenzen. Es besteht daher die Gefahr, dass Informationen aus den Endeinrichtungen selbst von Endnutzern erhoben werden, die das betreffende Ladenlokal gar nicht betreten haben, sondern sich lediglich in seiner Nähe aufhalten.

Vor diesem Hintergrund greift die Regelung des Artikels 8 Abs. 2 lit b), die lediglich eine Information über die Datenerhebung vorschreibt, deutlich zu kurz. Um sicherzustellen, dass keine Daten aus den Endgeräten von Personen erhoben werden, die sich lediglich im Nahbereich des jeweiligen Ladenlokals aufhalten, darf die Erhebung nur nach ausdrücklicher Einwilligung der Betroffenen erfolgen. Des Weiteren darf das Betreten eines Ladenlokals nicht davon abhängig gemacht werden, dass die Betroffenen zunächst in die Datenerhebung eingewilligt haben. Ansonsten könnten die Betroffenen schnell in eine Lage geraten, in der sie sich faktisch gezwungen sehen, die Einwilligung zu erteilen.

6. Artikel 9 und Artikel 10

Zu den notwendigen Nachbesserungen bei den Artikeln 9 und 10 wird auf die Ausführungen unter 5.2. verwiesen.

7. Artikel 11

Die Öffnungsklausel des Artikel 11 Abs. 1 ist viel zu weit gefasst und erlaubt eine nahezu vollständige Aushöhlung der Verordnung durch nationale Sonderregelungen. Die dort genannten Beschränkungen für Abweichungen auf der Ebene der Mitgliedstaaten - wie die Wesensgehaltsgarantie oder der Verhältnismäßigkeitsgrundsatz - stellen lediglich rechtsstaatliche Selbstverständlichkeiten dar. Im Ergebnis werden die zahlreichen erfreulichen Ansätze zum Schutz der Privatsphäre damit zur Disposition der nationalen Gesetzgeber gestellt. Dies läuft dem umfassenden Harmonisierungsziel einer EU-Verordnung klar zuwider.

Des Weiteren stellt Artikel 11 Abs. 1 in der gegenwärtigen Fassung eine Hintertür für die Einführung einer Vorratsdatenspeicherung bei OTT-Anbietern dar. Nicht zuletzt vor dem Hintergrund der Entscheidungen des Europäischen Gerichtshofs zu anlasslosen Speicherpflichten für Telekommunikationsanbieter (C-293/12 und C-203/15, C-698/15) sollte Artikel 11 aber vielmehr ausdrücklich klarstellen, dass auch die Betreiber von Kommunikationsdiensten nicht durch mitgliedstaatliche Rechtsnormen zu einer anlasslosen und verdachtsunabhängigen Speicherung von Kommunikationsdaten verpflichtet werden dürfen.

Artikel 11 Abs. 2 sollte des Weiteren ausdrücklich regeln, dass Betreiber elektronischer Kommunikationsdienste nicht im Wege mitgliedstaatlicher Rechtsnormen dazu verpflichtet werden dürfen, staatlichen Stellen einen Direktzugriff auf die Kommunikationsdaten von Endnutzern zu gewähren. Es muss gewährleistet sein, dass einer Anfrage auf Zugang zu elektronischen Kommunikationsdaten erst nach einer entsprechenden Prüfung durch den Betreiber entsprochen werden kann. In der gegenwärtigen Fassung hingegen werden staatliche Direktzugriffe auf die bei einem Betreiber gespeicherten Kommunikationsdaten nicht mit der gebotenen Deutlichkeit ausgeschlossen.