STELLUNGNAHME

BVDW
Wir sind das Netz

**Stellungnahme des Bundesverbandes Digitale Wirtschaft (BVDW) e.V.
zum Entwurf einer**

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)

Berlin, 03.März 201

Ansprechpartner:
RA Michael Neuber
Justiziar/ Leiter Recht und Regulierung
BVDW e.V.
T:+49 30 206218612
neuber@bvdw.org

Der BVDW ist die zentrale Interessenvertretung für Unternehmen, die digitale Geschäftsmodelle betreiben oder deren Wertschöpfung auf dem Einsatz digitaler Technologien beruht. Mit mehr als 600 Mitgliedsunternehmen aus unterschiedlichsten Segmenten der Internetindustrie ist der BVDW interdisziplinär verankert und hat damit einen ganzheitlichen Blick auf die Themen der Digitalen Wirtschaft. Wir bedanken uns für die Möglichkeit zur nachfolgenden Stellungnahme.

1. Allgemeines

Ziel der Neuregelungen soll die Angleichung der bisherigen Bestimmungen zum Persönlichkeitsschutz im Bereich der elektronischen Kommunikation an die Vorgaben der EU-Datenschutzgrundverordnung (EU-DSGVO) sein.

Ausweislich des Art. 2 ePV gilt die Verordnung für die Verarbeitung elektronischer Kommunikationsdaten, die in Verbindung mit der Bereitstellung und Nutzung elektronischer Kommunikationsdienste erfolgt, und für Informationen in Bezug auf die Endeinrichtungen der Endnutzer. Auf diesen Anwendungsbereich beschränkt sich die Verordnung jedoch nicht.

Nach den Erwägungsgründen sollen die neuen Bestimmungen als lex specialis zum europäischen Datenschutzrecht anzusehen sein. Aus unserer Sicht ergibt sich im Bereich des Datenschutzrechts weder eine Kompetenz der zuständigen Generaldirektion Connect zu entsprechender Regulierung noch können die im Entwurf vorgelegten Normen zur Regulierung im Bereich elektronische Kommunikation, Privatheit und Endgeräteschutz wegen des auf

sämtliche Informationssachverhalte erstreckten Anwendungsbereichs den spezifischen Datenschutzregeln der EU-DSGVO, insbesondere im Bereich der generellen Dienste der Informationsgesellschaft vorgehen.

Die Kernkritikpunkte im Überblick:

- Unzulässig erweiterter Anwendungsbereich
- Uneinheitliche und unklare Begriffsbestimmungen
- Kein level playing field zwischen den verschiedenen Anbietern digitaler Angebote im Internet
- Fehlende Kohärenz mit EU-DSGVO
- Überschießende Spezialnormen für den Online-Bereich
- Verbot von 3rd Party-Cookies bedroht Funktionsweise des Internets

2. Fehlerhaftes Schutzzweckverständnis

Der BVDW hält die Einführung zusätzlicher Datenschutzregeln für den Bereich der elektronischen Kommunikation für rechtlich falsch und elementar wirtschaftsgefährdend. Der immens verbreiterte Anwendungsbereich geht über den eigentlichen Schutzzweck der ehemaligen ePrivacy-Richtlinie, die allein den Schutz der Vertraulichkeit der Kommunikation zum Gegenstand hatte, unzulässig hinaus. Mit den Mitteln des Datenschutzrechts sollen nun telekommunikative Vorgänge sowie der – mit dem Datenschutzrecht nicht erreichbare – Endgeräteschutz sichergestellt werden. Da unter Kommunikation hier jeder datengestützte Informationsaustausch verstanden wird, ist hier praktisch die gesamte Online-Branche von neuen Datenschutzregeln betroffen.

Die Erstreckung des für den Datenschutz geltenden Verbots mit Erlaubnisvorbehalt auf sämtliche Vorgänge des digitalen Datenaustauschs bedeutet nichts weniger, als die Kommunikationsfreiheit zu beschränken. Nach Art. 1 Abs. 2 ePV soll der freie Verkehr elektronischer Kommunikationsdaten gewährleistet werden und darf nicht bei der Verarbeitung personenbezogener Daten weder beschränkt noch untersagt werden.

Art. 5 ePV statuiert indes ein Verbot der Verarbeitung von Kommunikationsdaten. Der Schutz des informationellen Selbstbestimmungsrechts und das Fernmeldegeheimnis haben unterschiedliche Schutzrichtungen.

Während bei ersterem Fragen der Datenverarbeitung in jedwedem Kontext (auch Kommunikationsdaten) eine Rolle spielen geht es bei letzterem um den Inhalt der Kommunikation. Der Begriff der

Verarbeitung muss – wenn es hier um eine lex specialis im Datenschutzbereich geht – in Ermangelung anderweitiger Definition aus Art. 4 EU-DSGVO stammen. Dort erfasst sind sowohl das Erheben als auch das Erfassen, die Organisation, die Speicherung die Verwendung oder Übermittlung etc. Eine Erstreckung des Verbots auf Verarbeitungen von Datenflüssen, die der Kommunikation zuzuordnen sind, ist nicht vom Schutzzweck gedeckt. Es wird umfassend ein Kommunikationsschutz etabliert.

3. Verhältnis zur EU-DSGVO

Der Verordnungsentwurf wirft erhebliche Wertungswidersprüche im Verhältnis zu den gesetzlichen Grundregeln über Datenverarbeitungserlaubnisse aus der EU-DSGVO auf.

Es ist absolut uneinsichtig, dass hier weitere, teilweise widersprechende Regelungen für den Bereich der Dienste der Informationsgesellschaft (Online-Services) geschaffen werden sollen. Im Verlaufe der Verhandlungen zur EU-DSGVO wurde über Jahre darum gerungen, praktikable Regelungen für sämtliche Datenverarbeitungen zu formulieren. Mit ihrem einseitigen und dazu noch extrem eingeschränkten Einwilligungsprimat wird diese Arbeit und deren Ergebnis beinahe vollständig konterkariert. Der Schutz des Endgerätes gegen illegitime Einwirkungen durch Dritte kann nicht als Grund herhalten, sämtliche, in der EU-DSGVO als legal definierte Datenverarbeitungsszenarien umzuschreiben.

Diese Art der nachträglichen Spezialregulierung hat bereits jetzt einen weiteren, gravierenden Nachteil für die digitale Wirtschaft. Es wird massive Rechtsunsicherheit geschaffen. Denn solange nicht klar ist, wie die neuen ePV-Regeln aussehen werden, ist auch eine Vorbereitung auf die kommende EU-DSGVO kaum zukunftsfest vorstellbar. Die Unternehmen der digitalen Wirtschaft haben derzeit noch ca. 500 Tage bis zur Geltung der neuen Regeln. Nun sollen weitere hinzukommen. Derzeit als legal erachtete Verarbeitungsmodelle können nach ePV-Grundsätzen künftig entweder unmöglich werden oder einem strikten Einwilligungserfordernis unterfallen.

4. Einwilligungen in notwendige Dienstleistungen

Art. 6 ePV skizziert die erlaubten Verarbeitungen im Bereich der elektronischen Kommunikation. Im Vergleich zur Referenzvorschrift des Art. 6 EU-DSGVO findet sich keine ausgleichende Balance zwischen den harten Einwilligungsvorbehalten und –schranken und

den Rechten der Unternehmen auf Betätigung auf Grundlage eines legitimen Interesses.

a) Art. 6 Abs. 3 a)

Eine Einwilligung soll erforderlich sein, soweit elektronische Kommunikationsinhalte verarbeitet werden und die Dienstleistung ohne diese Inhaltsverarbeitung nicht erbracht werden kann. Hier ist allerdings eher von einer vertraglichen Ebene der Bedingungen des Kommunikationsdienstes und seiner Funktionalitäten auszugehen.

Stattdessen sollen der bzw. die Endnutzer auch noch einwilligen. Warum erstens eine Einwilligung für den Versand beispielsweise einer Chat-Nachricht nebst Bild notwendig ist, wenn diese Datenverarbeitung ohnehin notwendig für die Erbringung der vertraglich geschuldeten Leistung ist und dem Versand dann auch (beide) Seiten zustimmen müssen, ist nicht klar.

Ohne Einwilligung wäre damit eine Vielzahl von Online-Diensten unmöglich. Es stellt sich dabei nämlich die Frage, ob hier dann eine Datenverarbeitung gegen Einwilligung und damit ungewollt ein Kopplungsverhältnis vorläge. So würde Kommunikation aus Gründen des Datenschutzrechts unterbunden. Das ist nicht hinnehmbar.

b) Art. 6 Abs. 3 b) ePV

Hiernach dürfen Betreiber elektronischer Kommunikationsdienste elektronische Kommunikationsdaten nur verarbeiten, wenn

„alle betreffenden Endnutzer ihre Einwilligung zur Verarbeitung ihrer elektronischen Kommunikationsinhalte für einen oder mehrere bestimmte Zwecke gegeben haben, die durch eine Verarbeitung anonymisierter Informationen nicht erreicht werden können, und wenn der Betreiber hierzu die Aufsichtsbehörde konsultiert hat".

Gemäß Erwägungsgrund 19 soll diese Vorschrift das Scannen von Textnachrichten zur Ausspielung relevanter Werbung im Kontext einer Nachricht unter einen Erlaubnisvorbehalt stellen. Allerdings nur, soweit eine Anonymisierung nicht möglich ist.

Diese Vorschrift wirft zweifach Fragen auf. Zunächst unterliegen Datenverarbeitungen, die nicht während des Übertragungsvorgangs stattfinden (Abhören) nicht telekommunikations- sondern datenschutzrechtlichen Vorgaben. E-Mail-Inhalte werden aber grundsätzlich nach der Übertragung gescanned, um darauffolgend Werbung einzublenden. Diese Verarbeitungen sind in der EU-DSGVO in Art. 6 niedergelegt. Eine Spezialregelung für das

Auslesen von übertragenen Kommunikationsinhalten kommt daher nicht in Frage.

Eine Einwilligung soll nur notwendig sein, wo anonyme Verarbeitungen nicht möglich sein sollen. Soweit die Verarbeitung auf Grundlage einer Einwilligung erfolgt, kann eine Aufsichtsbehörde allerdings wohl zum Schluss kommen, dass anonyme Verarbeitungen möglich gewesen wären. Die Norm klärt indes nicht, wie sich ein solches Ergebnis auf die Wirksamkeit einer Einwilligung auswirkt.

5. Inkongruente Regeln für Online-Datenverarbeitungen

Die weiteren, für die Dienste der Informationsgesellschaft (Webseiten und Apps) besonders relevanten wie verfehlten Bestimmungen finden sich in den Art. 8 bis 10 des Verordnungsentwurfs. Von engen Ausnahmen abgesehen, sollen die Nutzung von Rechen- und Speicherfähigkeiten eines Endgerätes sowie das Erheben jeglicher Informationen (einschließlich Informationen über die Beschaffenheit von Hard- oder Software) verboten sein. Hierzu soll allein der Besitzer des Gerätes in der Lage sein dürfen. Dies geht weit über das bisherige Anwendungsverständnis hinaus und erfasst damit auch Techniken wie z.B. das technische Fingerprinting, wie sich aus Erwägungsgrund 20 ergibt. Privacy und Endgeräteschutz sind nicht Schutzzweck des Datenschutzrechts.

a) Art. 8 ePV

Der neue Art. 8 ePV soll eine Neugestaltung der bisherigen „Cookie"-Regelung darstellen. Künftig sollen sämtliche Maßnahmen, welche Informationen über ein Endgerät generieren oder auslesen – unabhängig von der technischen Ausgestaltung - von der Regulierung erfasst und grundsätzlich einwilligungsbedürftig sein.
Die neuen Regeln lassen allerdings nur noch Cookies und Webmessungen zu, die der Webseitenbetreiber selbst setzt. Künftig sollen alle Dienste, die der Webseitenbetreiber üblicherweise von Dritten ausführen lässt, ausgesperrt bleiben. Darüber wachen soll dann die Zugangssoftware, in den meisten Fällen also der Browser.

Da das heutige Internet fast ausschließlich über Dienste von externen Anbietern funktioniert, werden die Browser künftig für jeden einzelnen Dienst eine neue Einwilligung einholen müssen. Dies führt zwangsläufig zu wesentlich mehr pop-up-Fenstern als früher. Die Einwilligung betrifft im Übrigen die Anbieter von Tracking-Diensten unabhängig von der individuellen Webseite. Ein Tracking erfolgt nicht pro Webseite sondern z.B. über AdServer und das

Targeting System eines Inhalteanbieters. Möchte man z.B. Werbung eines bestimmen Online-Angebotes sperren, wird so der technische Anbieter gesperrt. Damit werden automatisch aber auch alle anderen Verwender desselben technischen Systems gesperrt. Die Folge ist, dass ein auf anderen Webseiten ggf. erwünschtes oder für die Nutzung notwendiges Targeting ebenfalls nicht funktioniert.

Ein besserer Datenschutz oder aber eine bessere Nutzerfreundlichkeit sind damit nicht erreicht, im Gegenteil. Die vorgesehenen Ausnahmen sind zu eng und bedürfen der Überarbeitung.

- **Notwendige Webservices definieren**

Ausgehend von der Funktionsweise und Strukturen des werbefinanzierten Internets die Ausnahmen in Art. 8 Abs. 1 c) müssen Maßnahmen einschließen, die der Reichweitenmessung, Werbeblocker-Identifizierung, oder der Integritäts- und Sicherheitsüberprüfung auch durch Drittanbieter dienen. Die Erkennung der verwendeten Hardware und Software (insb. Browser) ist beispielsweise essentiell, da teilweise auf diese spezifischen Merkmale bei der Auslieferung von Webseiten eingegangen werden muss um eine fehlerfreie Darstellung gewährleisten zu können.
Diese Ausnahmen müssen vor allem vor dem Hintergrund der verfehlten Technikregelung des Art. 10 ePV funktionsfähig sein.

- **Fehlende Definition von Drittparteien, zu enge Legalausnahme für Webmessungen**

Mit Blick auf die fehlende Definition bzw. Unterscheidung zwischen Erst- und Drittparteien im Kontext der Bereitstellung eines Dienstes der Informationsgesellschaft (Webseitenaufruf) ist unklar, wer unter die Legalausnahme für Webmessungen des Art. 8 Abs. 1 d) fallen soll. Üblicherweise halten Webseitenbetreiber keine eigenen technischen Plattformen oder Lösungen für Webanalysen vor sondern lassen diese von Dritten ausführen. In technischer Hinsicht sind Dritte im Umfeld einer Datenverarbeitung auf einer Webseite alle Dienste, die nicht über die URL des Webseitenanbieters bereitgestellt werden. Soweit Drittparteien per Einstellung nach Art. 10 Abs. 2 ePV pauschal ausgeschlossen werden können sollen, wird die Ausnahme nur noch für Besucherzähler der Webseite funktionieren. Dies bedeutet einen Rückfall in das Internet der 90er Jahre. Hier ist dringend Klarstellung nötig, welche Dienste künftig erlaubt sein werden.

- **Fehlende Berücksichtigung von Verarbeitungen auf Grundlage eines berechtigten Interesses**

Während in Art. 8 Abs. 2 b), 3 für die Nutzung Sendedaten (WiFi) eine Information des Nutzers ausreichen soll, um Konnektionsdaten (z.B. IMEI, MAC-Adresse) zu verarbeiten, ist eine Ausnahme zugunsten eines ausbalancierten Ansatzes für die Verarbeitung von Daten gemäß Art. 8 Abs. 1 ePV nicht vorgesehen. Die rigide Fokussierung auf die Einwilligung abseits der zu engen und obendrein klarstellungsbedürftigen Legalausnahmen steht im klaren Widerspruch zu den Datenverarbeitungserlaubnissen in Art. 6 Abs. 1 f) EU-DSGVO. Ohne die Möglichkeit einer Verarbeitung auf Grundlage eines legitimen Interesses, wird es künftig vollständig unklar, in welchen Datenverarbeitungsumfeldern eine Einwilligung notwendig ist und wo nicht. Es ist daher erforderlich eine dem Art. 6 Abs. 1 f) EU-DSGVO entsprechende Regelung einzuführen, um Inkongruenzen auszuschließen.

b) Art. 9 ePV

In Art. 9 ePV finden sich Vorgaben für die Einwilligung, die sich nach den Grundsätzen der EU-Datenschutzgrundverordnung richten. Mit Blick auf Einwilligungen bezüglich des Setzens von Cookies wird in Absatz 2 klargestellt, dass für eine Erklärung der Einwilligung auch genügt, dass geeignete technische Einstellungen einer Internetverbindungssoftware ausreichen. Damit wird die Verbindung zu den in Art. 10 ePV geregelten technischen Vorgaben hergestellt. Für eine wirksame Einwilligung selbst gelten hingegen die umfangreichen Informationspflichten aus Art. 4 und 7 EU-Datenschutzgrundverordnung. Unklar und offenbar nicht bedacht ist die Frage, in welchem Verhältnis technische Einstellungen über den Browser (Software) zu wirksamen Erklärungen nach Maßgabe der EU-DSGVO stehen.

c) Art. 10 ePV

Am problematischsten ist die aus technischer und rechtlicher Sicht vollständig verfehlte Regelung des Art. 10 ePV. Gemäß Art. 10 Abs. 1 ePV muss jede Verbindungs-Software die Option bieten, Dritte (3rd-Parties) vom Zugriff auf das Endgerät auszuschließen. Der Nutzer muss sich hier für eine Option entscheiden. Bei Ausschluss sämtlicher Drittparteien können werbefinanzierte Webangebote nicht mehr funktionieren. Beispielhaft ist hier der komplette Geschäftszweig des Affilinet Marketings zu nennen. Hierbei ist es essentiell, dass nach Abschluss eines Online-Kaufes ermittelt werden kann, welche digitalen Affilinet-Marketingmaßnahmen der Endnutzer im Vorfeld bedient hat, um die entsprechenden Partner monetär berücksichtigen zu können.

Es ist unklar, wer Drittpartei im Sinne der Technikregelung des Art. 10 ePV sein soll. Mit Blick auf die Privilegierung von Maßnahmen in Art. 8 Abs. 1 c) und d) ePV wären davon alle Dienstleister als Dritte erfasst, welche nicht die URL des Webseitenanbieters beinhalten. Art. 10 ePV steht bereits hier in Widerspruch zu den gesetzlichen Erlaubnissen des Art.8 ePV.

Daneben führt die Regelung zu vollständiger Rechtsunsicherheit bezogen auf die Wirksamkeit einer erklärten Einwilligung bzw. steht dem entgegen. Die Auswahl eines Settings erfüllt zunächst nicht die Kriterien einer informierten Einwilligung der über Art. 9 ePV einbezogenen EU-DSGVO.

Der Nutzer muss die Freiheit haben, seine ggf. restriktiven Einstellungen auch wieder zu ändern. Wie und unter welchen Umständen diese Entscheidung ganz oder für einzelne Webseiten bezogen auf jegliche Art nicht privilegierter Cookies geändert werden kann, ist nicht geregelt. Web-Browser müssten dann auch nachgelagerte Informationsfenster steuern oder auf Änderungsoptionen in Abhängigkeit des Funktionierens einer Webseite hinweisen.

Bei jeder Änderung der Einstellungen, müsste der Nutzer seine informierte und spezifische Einwilligung gegenüber jeder anfragenden, verantwortlichen Stelle erklären. Verantwortlich für die Sicherstellung wäre hier aber der Browser (Software) als Gatekeeper. Er müsste für das Ändern von Einstellungen eine Granularität bezogen auf sämtliche benötigte Drittdienste bereitstellen.

Mit einem solchen Whitelisting würde der Browser nicht nur zum Super-Cookie, die von der EU-Kommission versprochene Nutzerfreundlichkeit würde wegen der notwendigen Informationsbereitstellungen nicht mehr gegeben. Angesichts der vollständig ungeklärten Haftungsfragen und der zugleich vorgesehenen Sanktionen zeigt sich, dass dieser Ansatz weder rechtlich noch technisch darstellbar ist. Art. 10 ePV ist daher zu streichen.