STELLUNGNAHME

BVDW
Wir sind das Netz

Stellungnahme des Bundesverbandes Digitale Wirtschaft (BVDW) e.V.
zum Fortschrittsbericht der bulgarischen Ratspräsidentschaft vom 11.01.2018 bezogen auf den Textentwurf 2017/0003 (COD)

zur

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 - ePV)

vom 05.12.2017

Berlin, 12.Januar 2018

Ansprechpartner:
RA Michael Neuber
Justiziar/ Leiter Recht un
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 630 Mitgliedsunternehmen aus unterschiedlichsten Segmenten der Internetindustrie ist der BVDW interdisziplinär verankert und hat damit einen ganzheitlichen Blick auf die Themen der Digitalen Wirtschaft.

Ergänzend zu unserer Stellungnahme vom 03. März 2017 auf den Entwurf der EU-Kommission vom 10. Januar 2017 nehmen wir auf den aktuellen Entwurfstext des EU-Rats vom 05. Dezember 2017 sowie den aktuellen Sachstandsbericht der bulgarischen Ratspräsidentschaft vom 11. Januar 2018 wie folgt weiter Stellung:

Zu den einzelnen Diskussionspunkten

1. Link to General Data Protection Regulation (GDPR) and clarification on where the e-PR complements and where particularizes it, with a focus on Articles 5, 6, 7, 8 and 10

Hier ist die **Option 1** einschlägig.

Die Verordnung kann keine Anwendung finden, wo es um Datenverarbeitungen geht, die – auch soweit sie webbasiert angeboten werden – keine elektronische Direktkommunikation sondern einen allgemeinen Dienst der Informationsgesellschaft betreffen (Webseiten). Es bedarf einer weitergehenden Abgrenzung und Festlegung auf Kommunikations(inhalts)daten in Transit.

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. Erfasst sein soll darüber hinaus auch reine „machine-to-machine"-Kommunikation. Auf diesen Anwendungsbereich beschränkt sich die Verordnung jedoch nicht.

Nach den Erwägungsgründen sollen die neuen Bestimmungen als lex specialis zum europäischen Datenschutzrecht anzusehen sein. Diese Ansicht geht in Bezug auf den gesamten Regelungsbereich der Verordnung geht bereits im Ansatz fehl. Die im Entwurf vorgelegten Normen zur Regulierung im Bereich elektronische Kommunikation, Privatheit und Endgeräteschutz können wegen des auf sämtliche Informationssachverhalte erstreckten Anwendungsbereichs nicht den spezifischen Datenschutzregeln der EU-DSGVO, insbesondere im Bereich der Dienste der Informationsgesellschaft generell vorgehen.

Wie bereits unserer ersten Stellungnahme vom 13. April 2017 kritisiert wird insbesondere nicht deutlich, welche Regelungen einer künftigen ePV der DSGVO nun vorgehen (sie ergänzen) bzw. diese präzisieren sollen. Wegen Ihres auf die elektronische Kommunikation fokussierten Anwendungsbereiches ergeben sich teilweise unklare Überschneidungen. Die Sicherung der Vertraulichkeit der Kommunikation (Art. 7 EU-Grundrechtecharta) hat eine grundsätzlich andere und erheblich weitere Schutzwirkung als das allgemeine Datenschutzrecht. Dies wird bereits dadurch deutlich, dass die Schutzwirkung des Datenschutzrechts auf natürliche Personen begrenzt ist während der Schutz der Vertraulichkeit der Kommunikation auch für juristische Personen gilt.

Die Frage, an welchen Stellen die ePV die EU-DSGVO ergänzt bzw. präzisiert, ist wegen der unvermeidbaren Überschneidung und beinahe unmöglichen Unterscheidung von personenbezogenen und nicht-personenbezogenen Kommunikationsdaten kaum eindeutig beantwortbar. Genau hier liegen aber die systemischen Defizite des Entwurfs.

Die Etablierung strenger Einwilligungserfordernisse bzw. die engen Erlaubnistatbestände mit Blick auf Vertraulichkeitsgesichtspunkte führen zu einer faktischen Entwertung der gesetzlichen Datenverarbeitungserlaubnisse aus der EU-DSGVO im Onlinebereich außerhalb webbasierter Kommunikationsdienste und gelten sogar dort, wo es entweder nicht um die Verarbeitung personenbezogener Daten oder elektronische Kommunikationsdaten geht (Art.8). Heutige wie zukünftige Geschäftsmodelle und Innovationen im Bereich digitaler Angebote, wie insbesondere im Bereich des Internets der Dinge (IOT) werden durch diese Regulierung unmöglich gemacht. Die zusätzlichen Verweise auf ein Kopplungsverbot und die gesetzliche Verpflichtung zur softwareseitigen Zugangskontrolle hätten erhebliche Marktverschiebungen und Wettbewerbsverzerrungen zur Folge. Das Datenschutzrecht wird so zum Wirtschaftsrecht.

- Art. 5 – Die bulgarische Ratspräsidentschaft versteht laut aktuellem Sachstandsbericht die Regelungen zum telekommunikationsrechtlichen Vertraulichkeitsschutz als Ergänzung der EU-DSGVO-Regeln im Hinblick auf elektronische Kommunikation. Nach herkömmlichen Verständnis schützt das Fernmeldegeheimnis die in Transit befindlichen Informationen. Die Aufnahme des datenschutzrechtlichen Begriffs der „Verarbeitung“ in Art. 5 ePV bewirkt allerdings die Unterstellung sämtlicher Kommunikationsregelungen auch unter das datenschutzrechtliche Regime des Verbots mit Erlaubnisvorbehalt. Für die elektronische Kommunikation gilt also nicht mehr nur das Verbot des „Abfangens“ (was für Transitdaten klar geregelt sein muss) sondern auch des Verarbeitens von Daten auf Endgeräten. Soweit hier personenbezogene Daten betroffen sind, soll dies nur noch mit Einwilligung möglich sein, obwohl die EU-DSGVO Zugriff und Datenverarbeitung gleichermaßen – und abgestuft – abbildet.
- Art. 6 – Die Verarbeitung auch nicht-personenbezogener Kommunikationsdaten unter ein Verbot zu stellen, stellt keine

Ergänzung der EU-DSGVO dar. Es handelt sich hier vielmehr um eine Spezialregelung des Telekommunikationsrechts.

- Art. 8 – Endgeräteschutz ist in der Tat kein Thema der EU-DSGVO, da dieser dem Schutz der Vertraulichkeit jedweder Daten sowohl natürlicher als auch juristischer Personen dienen soll. Die behauptete Ergänzung der EU-DSGVO in diesem Fall stellt sich als Aushöhlung der datenschutzrechtlichen Erlaubnisse im Bereich der Nutzungsdaten dar. Es geht hier nicht um Kommunikationsinhalte-Verarbeitung (Vertraulichkeit) sondern Nutzungsdatenverarbeitung (technologische Zugriffsnotwendigkeiten). Wenn diese aber unter die Definitionen des Personenbezugs fallen sollen, müssen Abwägungskriterien zugelassen werden, die Art. 8 nicht vorsieht. Es handelt sich daher nicht um eine Ergänzung der EU-DSGVO.

5. Article 8: Protection of information stored in terminal equipment of end-users and related to or processed or emitted by such equipment

Hier sind **Optionen 3 und ergänzend Option 4** einschlägig.

Gemäß Art. 1 (3) soll die ePV als speziellere Regelung der EU-DSGVO vorgehen, dies aber nur insoweit, wie tatbestandlich ein „processing of electronic communications data that qualify as personal data“ in Rede steht. Adressaten sind „providers of electronic communications services“ und ausdrücklich nicht Anbieter von Diensten der Informationsgesellschaft, für welche die Anforderungen dennoch gelten sollen. Unter elektronische Kommunikation wird hier also erweitert auch das Transportieren jeder digitalen Dateninformation im Rahmen eines Webseitenaufrufs verstanden, mit den entsprechenden Konsequenzen für deren Funktionalität.

Die Einwilligungsregelungen in Art. 8 ePV können im Zusammenspiel mit den Technikvorgaben des Art. 10 (siehe dort) nicht funktionieren. Aber auch ohne diese Besonderheit des Entwurfs muss Art. 8 völlig anders gestaltet werden, damit die Funktionalitäten heutiger Webservices erhalten bleiben können. Die neuen Regeln lassen allerdings nur noch Cookies und Webmessungen zu, die der Webseitenbetreiber selbst setzt. Künftig sollen alle Dienste, die Webseitenbetreiber üblicherweise von Dritten ausführen lassen, ausgesperrt bleiben. Darüber wachen soll dann die Zugangssoftware, in den meisten Fällen also der Browser.

Exkurs: Notwendige Datenverarbeitungen auf werbefinanzierten Webseiten

Heutige Webangebote wie kostenfreie journalistische Inhalte, kommunikations- und andere Spezialdienste können Nutzern heute nur deshalb kostenfrei angeboten werden, weil Werbetreibende die Angebote – wie beim privaten und öffentlich-rechtlichen Fernsehen - finanzieren. Journalistische Tätigkeiten sind nicht Medienunternehmen vorbehalten und können mit Gewinnerzielungsabsicht verbunden sein (vgl. EuGH, Urt. v. 16. 12. 2008 – C-73/07). Dafür muss aber auch das Funktionieren der verwendeten Technologie sichergestellt sein. Die über das zustandslose http-Protokoll versendeten Daten können ohne Nachverfolgung (Tracking) nicht geprüft werden. Bei Werbefinanzierten Webseiten haben sowohl Seitenbetreiber als auch Werbetreibender ein Interesse zu erfahren, ob die geldwerte Werbung ihr Ziel auch erreicht hat, ob und mit welcher Frequenz sie richtig dargestellt wurde oder ob Blocker oder Bots aktiv sind. Ebenso müssen Abrechnungsprüfungen und Zugriffslegitimitäten geprüft werden können. Dies alles ist schlicht **notwendig**, um ein kostenfreies Webseitenangebot heutzutage bereitstellen zu können (Selbst Bezahlschranken finanzieren vor dem Hintergrund der geringen Zahlungsbereitschaft keine Webseitenangebote vollständig. Auch hier wird weiter Werbung benötigt – analog öffentlich-rechtlichem Fernsehen) Die Legalerlaubnisse des Art. 8, welche sich auf die Notwendigkeit des Setzens on Cookies beziehen dürfen daher nicht rein technisch, sondern müssen wirtschaftlich verstanden und ausgelegt werden. Jedenfalls diese Trackings sind also notwendig, um einen Webseiten- oder App-Service überhaupt anbieten zu können. Anderenfalls werden diese Angebote vom Markt verschwinden.

Während Art. 6 ePV mittlerweile eine Reihe von Datenverarbeitungsbefugnissen textiert wurden, die für Art. 8 ebenfalls (bei grundrechtsorientierter Betrachtung: erst recht) geboten sind, insbesondere die Verarbeitungsbefugnis nach Art. 6 (2) b für elektronische Metadaten (u.a. zu vertraglichen Zwecken oder um die bedingungskonforme Nutzung eines Dienstes/Angebots sicherzustellen) sowie die Befugnis, elektronische Metadaten u.a. für statistische Zwecke in pseudonymisierter Form verarbeiten

zu dürfen, findet sich keine ausgleichende Balance zwischen den harten Einwilligungsvorbehalten und –schranken und den Rechten der Unternehmen auf Betätigung auf Grundlage eines legitimen Interesses. 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. 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

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 und nutzerfreundliches Anwendungserlebnis zu gewährleisten. Nur zusammen mit den Transparenzanforderungen und einem Widerspruchsrecht sowie einer Verpflichtung zur technischen Absicherung dieser Verarbeitungen durch Maßnahmen wie Pseudonymisierung oder Verschlüsselung/Verhashung kann das Ziel von datenschutzfreundlichem und sicherem „free-flow-of-data“ unter der Prämisse echten „Privacy-by-designs“ erreicht werden.

Mindestens erforderliche Ergänzungen:

- Art. 8 (1) c ist wie folgt zu ergänzen: *"it is necessary for providing an information society service requested by the enduser which shall include inter alia maintaining, operating and managing the integrity, access or security of the information society service, enhancing user experience or measures for preventing unauthorized access to or use of the information society service according to the terms of use for making available the service to the enduser;* or"

  Es handelt sich um essentielle Maßnahmen zur Bereitstellung von Internetangeboten, die einwilligungsbasiert logischerweise nicht durchführbar sind.
- Art. 8 (1) ist durch einen weiteren Erlaubnistatbestand (als Buchstabe g (Rat) oder als Buchstabe e nach Version KOM) zu ergänzen. Hierfür bestehen zwei Optionen:

  OPTION 1: *"a clear and prominent notice is displayed to the public informing of, at least, the modalities of the collection, its purpose, the person responsible for it and the other information required under Article 13 of Regulation 2016/679/EU where personal data are collected, as well as any measure the end-user of the terminal equipment can take to stop or minimize the collection. The collection of such information shall be conditional on the application of appropriate technical and organization measures to ensure that the collection and processing of information is limited to what is necessary in relation to the purposes of processing and to ensure a level of security appropriate to the risks, as set out in Article 32 of Regulation 2016/679/EU, have been applied, which may inter alia include pseudonymisation of the information collected as set out in Art. 4 (5) of Regulation (EU) 2016/679"*

  OPTION 2: *"it is necessary under the conditions as set out in point (f) of Regulation (EU) 2016/679, provided that the processing is limited in time and space to the extent necessary for this purpose and the data is made anonymous or erased as soon as it is no longer needed for this purpose. The conditions as set out in paragraph 2a and paragraph 2b shall apply accordingly"*

Der Zugriff auf Webseitenangebote oder die Nutzbarkeit mobiler Apps kann nicht einseitig vom Nutzer dort gefordert werden, wo der Anbieter technisch und wirtschaftlich notwendige Datenverarbeitungen vornehmen muss. Allein Nutzerbezogene Trackings auf Grundlage eines berechtigten Interesses können ein Widerspruchsrecht mit Blick auf die konkret nutzerbezogene Datenverarbeitung, nicht aber gegen jedwede Verarbeitung begründen. Es muss daher klar sein, dass die wirtschaftliche Betätigungsfreiheit der Unternehmen entsprechend gewährleistet ist durch die entsprechende Klarstellung im Gesetz:
"Access to specific website content may still be made conditional on the well -informed acceptance of a cookie or similar device, if it is used for a legitimate purpose."

Siehe dazu auch Punkt 7.

6. Article 10: software privacy settings

Hier ist allein Option 3 einschlägig.

Artikel 10 ist zu streichen. Die Regelung ist sowohl aus technischer und rechtlicher Sicht vollständig verfehlt. Auch der Text vom 05.12.2017 enthält keine brauchbaren Verbesserungen, und zwar sowohl für einwilligungsbasierte wie auch für legal erlaubte Datenverarbeitungen.

Die Einwilligungszentrierung in Art. 6 bzw. 8 führt bereits 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. 4a ePV einbezogenen EU-DSGVO (Siehe Kommentar des BVDW zu WP259 v. 17.11.2017).

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.

a) Selbst gesetzlich privilegierte Drittanbieter technisch ausgeschlossen.

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.

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. Auf der anderen Seite müssten anderweitig generierte Einwilligungen technisch respektiert werden.

Art. 10 (2a) versucht zwar die daten- und wettbewerbspolitische Fehlentscheidung des KOM-Vorschlags aus Art. 10 Abs. 2, Hs.2, wonach Browser/Softwareanbieter zum Gatekeeper für sämtliche Datenverarbeitungen im Internet erklärt werden sollen, für die einwilligungsbasierte Datenverarbeitung nach Art. 8 (1) b auszugleichen.

Er enthält hier aber keine unmittelbar rechtliche Verpflichtung zur automatischen Umsetzung von Einwilligungen, die im Zuge der Nutzung eines Internetangebots nach Art. 8 (1) erteilt werden. Nach wie vor existiert damit keine „counter-balance“ zwischen den Browser-/Softwareherstellern auf der einen und allen nachfolgenden Stufen der Wertschöpfung auf der anderen Seite. Verglichen mit dem Ansatz des EP bedeutet der Vorschlag des Rats sogar einen Rückschritt. Zugleich ist zu fragen, wer die Legitimität der anderweitig z.B. auf Ebene der Webseite eingeholten behaupteten Einwilligung verifiziert. Auch dies spricht vollständig gegen eine technisch und rechtlich tragbare Lösung in Art. 10.

Mit dem intendierten Whitelisting würde der Browser zuletzt 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.

Aus systematischen sowie aus daten- und wirtschafts- politischen Gründen ist Art. 10 zu streichen. Soweit dies nicht in Frage kommt, sind mindestens die nachfolgenden Änderungen notwendig:

Art. 10 (2): "*Upon installation, the software shall inform the end-user about the privacy settings options and, to continue with the installation, require the end-user to consent to a setting. After installation and insofar the privacy settings prevent other parties from transmitting to or storing information on the terminal equipment of a user and from processing information already stored on or collected from that equipment , the software shall ensure that an information society service requested by the end-user may prompt that end-user for his or her expression of consent in the sense of Art. 8 (1) point (b). Any consent given in this context by an end user shall prevail automatically overthe existing privacy settings for that particular information society service and be applied accordingly by the software, e. g., via offering an interface or plugin or by using procedures provided by the specific information society service.*"

Der auf der Installationsebene absehbar hauptsächlich zu uninformierten Entscheidungen führende Zwang zur Vornahme von Browsereinstellungen bzw. zur Zustimmung zu Browservoreinstellungen wird aufgegeben. Zudem wird der einwilligungsbasierten *Datenverarbeitung* auf der Nutzungsebene eine im Interesse gleicher Wettbewerbsbedingungen praxistaugliche „browser-obligation" zur Seite gestellt, die auf dem Ansatz des EP basiert, beim Wortlaut aber präziser ausfällt.

Art. 10 (3)(neu): *"The software shall not prevent any processing which is legally allowed according to Art. 8 (1) a), c) or d) or (2) a). The right to object to the processing of personal data pursuant to Article 21 of Regulation (EU) 2017/679 remains unaffected."*

Nur so wäre gesichert, dass erlaubte Drittparteien (z.B. Auftragsverarbeiter) Zugriff auf das Endgerät haben.

7. Artikel 4a und Einwilligungsvoraussetzungen

Für detaillierte Informationen hierzu, siehe den separaten BVDW-Kommentar zu den Guidelines der Artikel-29-Datenschutzgruppe für Einwilligungen (WP 259) vom 28. November 2017.

Kurzbemerkungen:
Der pauschale Verweis auf die Einwilliungsregelungen der EU-DSGVO führt ohne spezifische Klarstellungen für den hier geregelten Anwendungsbereich auf Technikebene in mehrfacher Hinsicht zu unlösbaren Problemen.

Hier zeigt sich am besten, dass die Fokussierung auf die Einwilligung nicht mehr sondern am Ende weniger Datenschutzgrundlagen wie „Privacy-by-design“ oder Datensparsamkeit respektiert. Ein weiteres Argument, die gesetzlichen Erlaubnistatbestände zu stärken (s.o. unter 1.)

a) Kopplungsverbot

Aufgrund des Pauschalverweises in Art. 4a (1) wird das Kopplungsverbot nach der EU-DSGVO zur Anwendung kommen. Die Formulierung des Rats ist zwar gegenüber dem jede wirtschaftliche Datenverarbeitung glatt ausschließenden Vorbringen des EP vorzugswürdig (Art. 8 (1b), Art. 9 (3b), ErwG 18), sie bedeutet aber keinen Fortschritt gegenüber der Version KOM. Bei werbefinanzierten Geschäftsmodellen besteht eine untrennbare Einheit zwischen dem Angebot/Inhalt und seiner Finanzierung durch Werbung. Die entsprechende Datenverarbeitung - nach DS-GVO muss diese ab Mai 2018 umfänglich transparent gemacht werden - ist weder überraschend noch unsachlich. Sie ist vielmehr notwendig, um das Angebot, das als entgeltloses immer zugleich Werbeträger ist, überhaupt realisieren zu können. Der europäische Gesetzgeber muss diesem (auch verfassungsrechtlich geschützten) Zusammenhang Rechnung tragen und ihn auf der Ebene des Normtextes absichern.

Der Rat muss eine eindeutige Formulierung gerichtet auf die Anerkennung eines Bedingungszusammenhangs zwischen der Diensterbringung auf der einen und einer legitimen werbewirtschaftlichen Datenverarbeitung auf der anderen Seite einfügen.

Neben der Etablierung gesetzlicher Verarbeitungsbefugnisse muss ein Art. 4a (1) S.2 neu eingefügt werden:
„The application of Regulation (EU) 2016/679/EU must not oblige providers of information society services to offer a service without data processing which the service provider means to provide together with the service like, e.g. data processing for the purpose of advertising".

Mindestens muss so wie in der derzeit geltenden ePrivacy-Richtlinie (Erw. 25) formuliert warden (Siehe Punkt 5):
„Access to specific website content may still be made conditional on the well-informed acceptance of a cookie or similar device, if it is used for a legitimate purpose".

Das Kopplungsverbot würde hierdurch nicht ausgehöhlt, sondern im Interesse der Rechtssicherheit auf diejenigen Fallgestaltungen bezogen, bei denen die Datenverarbeitung aus Sicht der betroffenen Person nicht zu rechtfertigen ist.

b) Anforderungen an den Nachweis erteilter Einwilligungen

Das Konzept der einwilligungsbasierten Datenverarbeitung bzw. der hierfür vorgenommene Verweis auf die EU-DSGVO füjrt zur Unmöglichkeit des Nachweises auf Cookie-Ebene.In seiner derzeitigen Form ist die Einwilligung im Sinne von Art. 8 (1) b) für die klare Mehrheit der Angebote rechtlich nicht belastbar.

(1) Soweit die ePV auch den Bereich juristischer Personen betrifft, was bei Art. 8 der Fall ist, stellt sich zwangsläufig die Frage, wer die Einwilligung rechtsverbindlich erteilen kann. Der Vorschlag des Rats in Art. 4a (1) („mutatis mutandis") und (2) ist in dieser Hinsicht unbrauchbar. Wenn eine nicht vertretungsberechtigte Person am Rechner sitzt, wird man nach allgemeinen Grundsätzen jedenfalls keine wirksame Einwilligung für die juristische Person erhalten können. Da der

Webseitenbetreiber aber keinesfalls erkennen bzw. unterscheiden kann, ob eine juristische oder natürliche Person auf ein Angebot zugreift, kann die verantwortliche Stelle durchweg nicht darauf bauen, dass sie eine wirksame Einwilligung im Rechtssinn erhalten hat. Die verantwortliche Stelle ist nach der DS-GVO hierfür aber nachweis- und beweispflichtig, Art. 7 (1), ErwG 42 DS-GVO.

(2) Die Einwilligung einer identfizierbaren natürlichen Person kann nicht nachgewiesen werden, jedenfalls soweit nicht Log-in basierte Angebote in Rede stehen.

Klicks bzw. Nutzungsaktionen auf Webseiten oder Brwoserebene können serverseitig zwar gespeichert werden (Aktion, Zeitpunkt, IP Adresse sowie ggf. Cookie-ID), hieraus resultiert aber keine belastbare Verbindung zu einer bestimmten oder auch nur bestimmbaren natürlichen Person. Die Anforderung an die Einwilligung im Sinne der DS-GVO (s. hierzu Art. 29 AG, WP 259, S. 19 ff) werden damit für den genuinen Anwendungsbereich der EPR nicht erfüllbar sein.

Die Art.29-Arbeitsgruppe geht in ihrem aktuellen Papier auf diesen Punkt nicht spezifisch ein, was jedoch keinesfalls als Dispens verstanden werden darf, denn sie betont die Verantwortlichkeit des Einwilligungsempfängers und seine Nachweisverpflichtung („*…the controller must be able to prove that a data subject in a given case has consented. As long as a data processing activity in question lasts, the obligation to demonstrate consent exists", .a.a.O., S.20)*

Auch die Einwilligungserklärung via Browsereinstellungen (Art. 4a (2)) muss konkret, d.h. personenbezogen, nachweisbar sein. Die erforderliche Verknüpfung dürfte den Produzenten der Software (Browser und Betriebssystem) gelingen: durch die diesen Anbietern massenweise verfügbaren Log-In Konten kann jede im Zusammenhang mit der Software erfolgende Nutzeraktion (z.B. „Cookies akzeptieren") mit den hinterlegten Daten der ausführenden Person zusammengeführt werden. Diese Möglichkeit besteht für freie Internetangebote jedoch nicht. Webseiten haben auf der technischen Ebene keinen Zugriff auf den Browser/die Software und dort vorgenommene Einstellungsänderungen.