17/DE

WP 247

Stellungnahme 01/2017 zum Vorschlag für eine Verordnung über die Privatsphäre

angenommen am 4. April 2017

DIE GRUPPE FÜR DEN SCHUTZ VON PERSONEN BEI DER VERARBEITUNG PERSONENBEZOGENER DATEN

eingesetzt durch die Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995,

gestützt auf Artikel 29 und Artikel 30 dieser Richtlinie,

gestützt auf ihre Geschäftsordnung,

HAT FOLGENDE STELLUNGNAHME ANGENOMMEN:

ZUSAMMENFASSUNG

Die Datenschutzgruppe begrüßt den Vorschlag der Europäischen Kommission vom 10. Januar 2017 für eine Verordnung über die Privatsphäre. Sie begrüßt auch die **Entscheidung für eine Verordnung** als Rechtsinstrument. Damit wird sichergestellt, dass die Vorschriften in der gesamten EU einheitlich sind, und zudem wird Aufsichtsbehörden und Organisationen auf diese Weise gleichermaßen Klarheit geboten. Außerdem hilft dies, die Kohärenz mit der Datenschutz-Grundverordnung sicherzustellen. Diese Kohärenz wird durch die Entscheidung unterstützt, dass **für die Überwachung der Einhaltung der Datenschutz-Grundverordnung dieselbe Behörde zuständig sein soll** wie für die Durchsetzung der Datenschutzbestimmungen für die elektronische Kommunikation.

Gleichzeitig ist die Entscheidung für ein **ergänzendes Rechtsinstrument (bzw. für dessen Beibehaltung)** positiv zu bewerten. Der Schutz vertraulicher Kommunikation und von Endeinrichtungen weist besondere Eigenschaften auf, auf die in der Datenschutz-Grundverordnung nicht eingegangen wird. Folglich werden ergänzende Bestimmungen in Bezug auf diese Art von Diensten benötigt, um einen angemessenen Schutz des Grundrechts auf Privatsphäre und Vertraulichkeit der Kommunikation, einschließlich der Vertraulichkeit von Endeinrichtungen, zu gewährleisten. In dieser Hinsicht befürwortet die Datenschutzgruppe nachdrücklich das in der vorgeschlagenen Verordnung gewählte **grundsatzorientierte Vorgehen** mit **umfassenden Verboten, eng gefassten Ausnahmen** und **der gezielten Anwendung des Begriffs „Einwilligung“**.

Die Datenschutzgruppe begrüßt die Ausweitung des Anwendungsbereichs der vorgeschlagenen Verordnung auf **Over-The-Top („OTT“)-Anbieter.** Diese Dienste sind funktional gleichwertig mit herkömmlichen Kommunikationsmitteln und haben folglich ein ähnliches Potenzial, sich auf das Recht der Menschen in der EU auf Privatsphäre und auf Vertraulichkeit der Kommunikation auszuwirken. Auch ist erfreulich, dass die vorgeschlagene Verordnung eindeutig **den Inhalt und die damit zusammenhängenden Metadaten abdeckt** und anerkennt, dass **Metadaten sehr sensible Daten offenlegen können.**

Die Datenschutzgruppe stellt jedoch auch vier **schwerwiegende Problembereiche** fest: In Bezug auf die **Verfolgung der Standorte von Endeinrichtungen, die Bedingungen, unter denen eine Analyse des Inhalts und der Metadaten erlaubt ist, die Standardeinstellung von Endeinrichtungen und „Tracking Walls“** würde die vorgeschlagene Verordnung das von der Datenschutz-Grundverordnung gebotene Schutzniveau senken. In der vorliegenden Stellungnahme unterbreitet die Datenschutzgruppe spezifische Vorschläge, durch deren Umsetzung sichergestellt werden könnte, dass die Verordnung über die Privatsphäre dasselbe oder ein höheres Schutzniveau bieten würde, das dem sensiblen Charakter von Kommunikationsdaten (und zwar sowohl des Inhalts als auch der Metadaten) angemessen wäre.

Wi-Fi-Tracking unterliegt gemäß der Datenschutz-Grundverordnung je nach den Umständen und dem Zweck der Erhebung personenbezogener Daten wahrscheinlich der Einwilligung oder darf nur durchgeführt werden, wenn die erhobenen personenbezogenen Daten anonymisiert werden. Dafür müssen die folgenden vier Bedingungen erfüllt sein: Der Zweck der Erhebung personenbezogener Daten von Endeinrichtungen ist auf rein statistische

Zählungen beschränkt, die Verfolgung wird zeitlich und räumlich auf das zu diesem Zweck unbedingt notwendige Maß beschränkt, die Daten werden unmittelbar danach gelöscht oder anonymisiert, und es bestehen wirksame Möglichkeiten zur Nichtteilnahme. Der Europäischen Kommission wird empfohlen, einen technischen Standard für mobile Endgeräte zu fördern, mit dem automatisch Widerspruch gegen eine solche Verfolgung signalisiert wird.

Ausgangspunkt für die **Analyse des Inhalts und der Metadaten** sollte sein, dass die Verarbeitung von Kommunikationsdaten ohne die Einwilligung aller Endnutzer (Absender und Empfänger) verboten ist. Damit Anbieter Dienste anbieten können, die der Nutzer ausdrücklich gefordert hat (beispielsweise die Such- und Indexierungsfunktion oder Text-to-Speech-Dienste), sollte eine „häusliche" Ausnahme für die Verarbeitung von Inhalt und Metadaten für rein persönliche Zwecke des Nutzers selbst möglich sein.

Im Hinblick auf die **Einwilligung in die Verfolgung** fordert die Datenschutzgruppe ein ausdrückliches Verbot von „Tracking-Walls", also von Entscheidungen des Typs „Alles oder nichts", die den Nutzer zwingen, in die Verfolgung einzuwilligen, da er sonst keinen Zugang zu dem Dienst erhält.

Schließlich empfiehlt die Datenschutzgruppe, dass Endeinrichtungen und Software **standardmäßig Datenschutzeinstellungen bieten** müssen und den Nutzern klare Möglichkeiten geben, diese Standardeinstellungen bei der Installation zu bestätigen oder zu ändern. Bei der Nutzung muss es einfach sein, auf diese Einstellungen zuzugreifen. Nutzer müssen die Möglichkeit haben, durch ihre Browser-Einstellungen eine konkrete Einwilligung zu signalisieren. Datenschutz-Präferenzen sollten nicht auf Eingriffe Dritter oder auf Cookies beschränkt sein. Die Datenschutzgruppe empfiehlt dringend, die Einhaltung des Standards „Do Not Track" („Nicht verfolgen") vorzuschreiben.

Die Datenschutzgruppe hat weitere bedenkliche Punkte ermittelt, die sich beispielsweise auf den Anwendungsbereich, den Schutz der Endeinrichtungen und die Direktwerbung beziehen. Schließlich hat die Datenschutzgruppe Fragen herausgearbeitet, die eine Klärung verdienen, damit die Endnutzer besser geschützt werden und allen betroffenen Interessenträgern mehr Rechtssicherheit geboten wird.

INHALTSVERZEICHNIS

1. EINLEITUNG

1. Die Artikel-29-Datenschutzgruppe (nachfolgend „Datenschutzgruppe“) begrüßt den Vorschlag der Europäischen Kommission für die Verordnung über die Privatsphäre („vorgeschlagene Verordnung“ oder „Verordnung über die Privatsphäre“) [1], welche die Datenschutzrichtlinie für elektronische Kommunikation[2] ersetzen soll.

2. Viele Aspekte der vorgeschlagenen Verordnung sind positiv, und die Europäische Kommission hat mit dieser Verordnung einen wichtigen Schritt unternommen. Die Verordnung kann jedoch weiter verbessert werden. Dies würde nicht nur dazu dienen, die Endnutzer besser zu schützen, sondern es würde auch allen betroffenen Interessenträgern mehr Rechtssicherheit bieten.

3. Die Datenschutzgruppe hat daher eine Reihe von Problempunkten thematisiert und Empfehlungen für Klarstellungen herausgearbeitet, die vom Europäischen Parlament und vom Ministerrat in ihrer Debatte über die vorgeschlagene Verordnung aufgegriffen werden könnten. In der vorliegenden Stellungnahme werden zuerst die positiven Aspekte der vorgeschlagenen Verordnung betrachtet und dann die Fragen und die zu klärenden Punkte herausgestellt.

2. POSITIVE ASPEKTE DER VORGESCHLAGENEN VERORDNUNG

EU-WEITE HARMONISIERUNG, ANGLEICHUNG VON GELDBUßEN UND AUSSCHLIEßLICHE DURCHSETZUNG DURCH DATENSCHUTZBEHÖRDEN

4. Die Datenschutzgruppe begrüßt die **Entscheidung für eine Verordnung als Rechtsinstrument**. Damit werden einheitliche Vorschriften in der gesamten EU (mit nachfolgend erörterten Ausnahmen) sichergestellt, und Aufsichtsbehörden und Organisationen wird gleichermaßen Klarheit geboten. Angesichts der Schlüsselrolle der Datenschutz-Grundverordnung („DS-GVO“)[3] für die vorgeschlagene Verordnung wird so die Übereinstimmung zwischen den beiden Rechtsinstrumenten unterstützt. Gleichzeitig ist **die Entscheidung für ein ergänzendes Rechtsinstrument (bzw. für dessen Beibehaltung)** positiv zu bewerten. Der Schutz vertraulicher Kommunikation

[1] Vorschlag 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), 2017/0003 (COD), URL: http://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:52017PC0010&from=DE.

[2] 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), ABl. L 201 vom 31.7.2002, S. 37-47, URL: http://eur-lex.europa.eu/legal-content/DE/TXT/?uri=celex:32002L0058.

[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 (Datenschutz-Grundverordnung), *ABl.* L 119 vom 4.5.2016, S. 1-88, URL: http://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A32016R0679.

und von Endeinrichtungen weist besondere Eigenschaften auf, auf die in der Datenschutz-Grundverordnung nicht eingegangen wird. Folglich werden ergänzende Bestimmungen in Bezug auf diese Art von Diensten benötigt, um einen angemessenen Schutz dieses Grundrechts zu gewährleisten. In diesem Zusammenhang **unterstützt** die Datenschutzgruppe auch **das in der vorgeschlagenen Verordnung gewählte grundsatzorientierte Vorgehen mit umfassenden Verboten und eng gefassten Ausnahmen** und vertritt die Ansicht, dass die Einführung unbegrenzter Ausnahmen im Sinne von Artikel 6 der DS-GVO und insbesondere von Artikel 6 Buchstabe f der DS-GVO (berechtigtes Interesse) vermieden werden sollte.

5. Die **Durchsetzung dieser Vorschriften durch dieselbe Behörde, die für die Überwachung der Einhaltung der DS-GVO zuständig ist,** unterstützt ebenfalls die Kohärenz zwischen den beiden Instrumenten. Angesichts des Zusammenhangs zwischen dem Schutz personenbezogener Daten und dem Schutz vertraulicher Kommunikation sowie der Endeinrichtungen ist es hilfreich, dass die Durchsetzung der Vorschriften der vorgeschlagenen Verordnung derselben Aufsichtsbehörde anvertraut wird, die die DS-GVO durchsetzt (Erwägungsgrund 38 und Artikel 18 der vorgeschlagenen Verordnung). Darüber hinaus bestätigt die Rechtsprechung des Gerichtshofs der Europäischen Union („EuGH“)[4], dass die in Artikel 7 der Charta vorgeschriebene Unabhängigkeit der Überwachungsbehörde wesentlich ist. Aus praktischer Sicht würde das jedoch zu einem beträchtlichen zusätzlichen Arbeitsaufwand für die Datenschutzbehörden führen, dessen Bewältigung ohne zusätzliche Haushaltsmittel nicht gewährleistet werden kann. Deshalb begrüßen die Datenschutzbehörden Erwägungsgrund 38 der vorgeschlagenen Verordnung, in dem betont wird, dass jede Aufsichtsbehörde zusätzlich mit Finanzmitteln, Personal, Räumlichkeiten und Infrastruktur ausgestattet werden sollte, die für die wirksame Wahrnehmung ihrer Aufgaben nach der neuen Verordnung notwendig sind. Es wird ebenfalls begrüßt, dass Artikel 18 Absatz 2 die Rechtsgrundlage für die Zusammenarbeit zwischen den Aufsichtsbehörden der vorgeschlagenen Verordnung und den nationalen Regulierungsbehörden der Richtlinie über den europäischen Kodex für die elektronische Kommunikation[5] schafft.

6. Angesichts der engen Beziehung zwischen der vorgeschlagenen Verordnung und der DS-GVO ist auch die **Angleichung der in der vorgeschlagenen Verordnung vorgesehenen Geldbußen mit der DS-GVO** zu begrüßen. Die in den Anwendungsbereich der vorgeschlagenen Verordnung fallenden Tätigkeiten sind recht sensibler Natur und umfassen unter anderem Eingriffe in vertrauliche Kommunikationen oder in Endeinrichtungen. Die Höhe der Geldbußen sollte dieser sensiblen Natur angemessen sein. Dies ist auch der Grund, aus dem eine

[4] Siehe beispielsweise die Urteile des Gerichtshofs vom 6. Oktober 2015 in der Rechtssache C-362/14 (Sicherer Hafen), Rdnr. 41 und vom 21. Dezember 2016 in den verbundenen Rechtssachen C-203/15 und C-698/15 (Tele2 gegen Watson), Rdnr. 123.

[5] Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über den europäischen Kodex für die elektronische Kommunikation (Neufassung), 2016/0288 (COD), 12.10.2016, URL: http://eur-lex.europa.eu/legal-content/DE/ALL/?uri=comnat:COM_2016_0590_FIN.

Harmonisierung in der gesamten EU wichtig ist, um in der ganzen Region das gleiche hohe Schutzniveau bieten zu können. Artikel 23 der vorgeschlagenen Verordnung sieht wirksame Geldbußen für Verstöße gegen die Verordnung vor, die mit einigen Ausnahmen (siehe Ziffer 38) der Höhe der Geldbußen entsprechen, die für Verstöße gegen die Vorschriften der DS-GVO vorgesehen sind.

7. Auch die **Streichung spezieller Vorschriften zur Meldung von Verletzungen des Schutzes personenbezogener Daten** aus diesen Rechtsvorschriften ist zu begrüßen, um eine unnötige Überschneidung mit den Vorschriften der DS-GVO zu Datenschutzverletzungen zu vermeiden.

8. Es ist auch **erfreulich, dass der Fokus jetzt auf einem gleichen Schutzniveau für alle Endnutzer liegt**, da die vorgeschlagene Verordnung auf die Unterscheidung zwischen „Teilnehmern" und anderen Nutzern elektronischer Kommunikationsdienste verzichtet.

AUSWEITUNG DES ANWENDUNGSBEREICHS VERGLICHEN MIT DER DATENSCHUTZRICHTLINIE FÜR ELEKTRONISCHE KOMMUNIKATION

9. Die Datenschutzgruppe begrüßt die **Ausweitung des Anwendungsbereichs der vorgeschlagenen Verordnung auf Over-The-Top („OTT")-Anbieter.** Diese Dienste sind funktional gleichwertig mit herkömmlicheren Kommunikationsmitteln und haben folglich ein ähnliches Potenzial, sich auf das Recht der Menschen in der EU auf Privatsphäre und auf Vertraulichkeit der Kommunikation auszuwirken. Die Datenschutzgruppe begrüßt insbesondere, dass jetzt alle OTT-Kategorien (OTT0, OTT1 und einige OTT2)[6] in den Anwendungsbereich der Verordnung fallen, da sie nicht nur herkömmliche Mittel zur Kommunikation (OTT0) abdeckt, sondern gemäß Artikel 8 Absatz 1 Buchstabe c der vorgeschlagenen Verordnung auch funktional gleichwertige Dienste (OTT1). Es ist auch als positiv zu vermerken, dass zusätzlich zu den Definitionen im Kodex einige OTT2 einbezogen werden, wenn sie eine interpersonelle und interaktive Kommunikation als untrennbar mit einem anderen Dienst verbundene Nebenfunktion ermöglichen, wie Spiele, Dating-Apps oder Bewertungsportale (Artikel 4 Absatz 2 der vorgeschlagenen Verordnung). Ebenso wird **die Erläuterung** begrüßt, **dass sich der Schutz auch auf die Maschine-Maschine-Kommunikation bezieht.** Erwägungsgrund 12 verdeutlicht, dass auch untereinander kommunizierende Geräte in den Anwendungsbereich des Schutzes fallen, der im Rahmen der vorgeschlagenen Verordnung gewährt wird. Das ist wünschenswert, da solche Kommunikationen häufig Informationen enthalten, die durch das Recht auf Privatsphäre geschützt sind. Die Anwendbarkeit sollte jedoch geklärt werden (siehe Ziffer 40h).

[6] Für eine weitere Erklärung dieser Begriffe siehe BEREC, *Report on OTT Services*, BoR (16) 35, 29. Januar 2016, S. 15 und 16, URL: http://berec.europa.eu/eng/document_register/subject_matter/berec/reports/5751-berec-report-on-ott-services. Beachten Sie bitte den Hinweis in dem Bericht, dass die Kategorien als Begriffe zu verstehen sind, die in der Debatte über die Überprüfung genutzt werden, nicht jedoch als Rechtsbegriffe.

10. Es ist auch positiv, dass **die vorgeschlagene Verordnung eindeutig den Inhalt und die damit zusammenhängenden Metadaten abdeckt**. Erwägungsgrund 14 verdeutlicht, dass die Begriffsbestimmung von „elektronische Kommunikationsdaten“ in Artikel 4 Absatz 3 Buchstabe a hinreichend breit gefasst sein sollte, damit sie *alle* Inhalte und die damit zusammenhängenden Metadaten abdeckt, und dies unabhängig beispielsweise vom Mittel für die Übertragung der Signale. In Ziffer 39 verweist die Datenschutzgruppe jedoch auf ihre Bedenken, weil nach wie vor über diese aktuelle Begriffsbestimmung von „elektronische Kommunikationsdaten“ debattiert wird. In Übereinstimmung mit dieser Ausweitung des Anwendungsbereichs hält die Datenschutzgruppe **die Anerkennung, dass Metadaten sehr sensible Daten offenlegen können** (siehe Absatz 2.2 der Begründung; Erwägungsgrund 2) für eine wesentliche Hinzufügung. Sie begrüßt die Tatsache, dass die Europäische Kommission damit die Erwägungen des EuGH in den Rechtssachen *Digital Rights Ireland* und *Tele2/Watson* übernommen hat. Die Datenschutzgruppe schätzt auch die **Anerkennung, dass die Analyse von Inhalten eine mit einem hohen Risiko verbundene Verarbeitung darstellt**. Erwägungsgrund 19 und Artikel 6 Absatz 3 Buchstabe b legen die logische Rechtsvermutung dar, dass das Scannen von Inhalten eine mit einem hohen Risiko verbundene Verarbeitung gemäß Artikel 35 der DS-GVO darstellt und unabhängig von dem Vorliegen eines hohen Restrisikos offensichtlich stets der vorherigen Konsultation der (federführenden) Aufsichtsbehörde bedarf. Gleichzeitig hat die Datenschutzgruppe Bedenken wegen des Anwendungsbereichs der Begriffsbestimmung „Metadaten“ und der Tatsache, dass die Analyse von Metadaten nicht denselben verbindlichen Anforderungen an eine Datenschutz-Folgenabschätzung unterliegt (siehe die Randnummern 33 und 46).

11. Zu begrüßen ist auch die fortgesetzte **Anerkennung der Bedeutung einer Anonymisierung**. Bereits in der Datenschutzrichtlinie für elektronische Kommunikation haben Maßnahmen zur Anonymisierung eine Rolle bei der Sicherstellung der Vereinbarkeit gespielt (beispielsweise Artikel 6 Absatz 1 der Datenschutzrichtlinie für elektronische Kommunikation, in dem festgestellt wird, dass Verkehrsdaten zu löschen oder zu anonymisieren sind, sobald sie für die Übertragung einer Nachricht nicht mehr benötigt werden). In Artikel 6 Absatz 2 Buchstabe c und in Artikel 6 Absatz 3 Buchstabe b der vorgeschlagenen Verordnung wird auf der Grundlage der Einwilligung eine Ausnahme vom Verbot der Verarbeitung von Metadaten und von Inhalt erlaubt, vorausgesetzt, es liegen Gründe (ein Grund) vor, *„die durch eine Verarbeitung anonymisierter Informationen nicht erreicht werden können“*. Das Erfordernis solcher Datenschutzmaßnahmen zusätzlich zum Einholen der Einwilligung der Nutzer schützt diese vor einer unberechtigten Verarbeitung. Die Datenschutzgruppe hat jedoch gleichzeitig schwerwiegende Bedenken, dass die Annahme solcher Anonymisierungstechniken bei der Verfolgung des Standortes der Nutzer durch ihre tragbaren Geräte nicht erforderlich wäre (siehe Ziffer 17). Darüber hinaus sollten die Anbieter stets eine Datenschutz-Folgenabschätzung durchführen, selbst wenn Maßnahmen zur Anonymisierung ergriffen werden (siehe Ziffern 33 und 46). Die Datenschutzgruppe fordert zusätzlich die Pflicht zur Veröffentlichung des Vorgehens zur Anonymisierung und Bündelung von Daten (siehe Ziffer 42b).

12. Ein weiterer positiver Punkt ist die **weit gefasste Formulierung des Schutzes der Endeinrichtungen**. Erwägungsgrund 20 und Artikel 8 legen fest, dass die für den Zugriff auf die Endeinrichtungen verwendeten Technologien nicht von Bedeutung sind: jeder Eingriff in die Endeinrichtungen der Endnutzer, einschließlich der Nutzung der Verarbeitungsfunktionen des Geräts, bedarf der Einwilligung des Endnutzers (mit bestimmten Ausnahmen). Hilfreich ist hier die Bestätigung der Europäischen Kommission, dass die Verfolgung von Gerätekennungen unter diese Bestimmung fällt. Darüber hinaus begrüßt es die Datenschutzgruppe, dass nach Erwägungsgrund 22 **Browser-Einstellungen** einer einzelnen Person **durchsetzbar sind,** wenn sich ein Dritter nicht an diese Einstellungen hält. Das ist in solchen Situationen hilfreich, in denen ein Dritter (z. B. ein Ad-Netzwerk) diese Einstellungen missachtet. Dies sollte jedoch auch in einer einschlägigen Vorschrift der vorgeschlagenen Verordnung niedergelegt werden.

13. Schließlich ist auch die fortgesetzte **Einbeziehung juristischer Personen in den Anwendungsbereich der vorgeschlagenen Verordnung** zu begrüßen (siehe Absatz 2.2 der Begründung; Erwägungsgründe 3, 33 und 42; Artikel 1, 15 und 16 Absatz 5). Dies ist auch schon in der Datenschutzrichtlinie für elektronische Kommunikation vorgesehen. Da die Datenschutzbehörden jedoch mit der Durchsetzung dieser neuen Vorschriften betraut werden, ist es hilfreich, dies besonders zu betonen. Das erlaubt es den Datenschutzbehörden, in Fällen Maßnahmen zu ergreifen, in denen juristische Personen Opfer eines Verstoßes sind, beispielsweise wenn Unternehmen Spam erhalten oder wenn ihre Kommunikationen heimlich überwacht werden. Die Datenschutzgruppe hat jedoch auch Bedenken, dass die Anwendung der Einwilligung auf juristische Personen nicht klar ist (siehe Ziffer 41a) und dass nicht eindeutig ist, was im Fall von Direktwerbung mit dem „berechtigten Interesse“ von juristischen Personen gemeint ist (siehe Ziffer 43c).

GEZIELTE ANWENDUNG DES BEGRIFFS DER EINWILLIGUNG

14. Die Datenschutzgruppe begrüßt eine andere Kategorie von Verbesserungen in Bezug auf die Anwendung und die Auslegung des Begriffs der Einwilligung. Zum einen ist **die Klarstellung** begrüßenswert, **dass der Internetzugang und die (mobile) Telefonie unverzichtbare Dienste sind und dass die Anbieter dieser Dienste ihre Kunden nicht „zwingen“ können, in eine Datenverarbeitung einzuwilligen, die für die Bereitstellung des unverzichtbaren Dienstes selbst nicht erforderlich ist.** Insbesondere in Erwägungsgrund 18 wird festgestellt, dass grundlegende breitbandige Internetzugangs- und Sprachkommunikationsdienste als unverzichtbare Dienste gelten. Angesichts der Abhängigkeit der Menschen vom Zugang zu solchen Diensten bedeutet dies, dass eine Einwilligung in die Verarbeitung ihrer Kommunikationsdaten für solche zusätzlichen Zwecke (z.B. die Verarbeitung für Werbe- oder Marketingzwecke) nicht wirksam sein kann. Gleichzeitig ist die Datenschutzgruppe besorgt, dass diese Erläuterung zu eingeschränkt ist. Auch die Dienste bestimmter OTT-Anbieter können als unverzichtbare Dienste gelten, und die Verordnung über die Privatsphäre sollte solche Alles-oder-Nichts-Entscheidungen auch unter anderen Umständen ausdrücklich verbieten (siehe Ziffer 20).

15. Darüber hinaus ist es erfreulich, dass **Pflicht zur Einwilligung in die Aufnahme von personenbezogenen Daten natürlicher Personen in Verzeichnisse harmonisiert wird**. Nach Artikel 15 der vorgeschlagenen Verordnung muss für die Verarbeitung von Daten in öffentlich zugänglichen Verzeichnissen die Einwilligung natürlicher Personen eingeholt und juristischen Personen eine Widerspruchsmöglichkeit eingeräumt werden. Das wird in Erwägungsgrund 31 weiter ausgearbeitet, in dem festgestellt wird, dass diese Einwilligung in Bezug auf die konkreten Kategorien personenbezogener Daten, die in das Verzeichnis aufgenommen werden, ausdrücklich erteilt werden muss. Die Datenschutzgruppe merkt jedoch an, dass in der vorgeschlagenen Verordnung klarer zum Ausdruck gebracht werden könnte, dass für Such- und Umkehrsuchfunktionen eine gesonderte ausdrückliche Einwilligung erforderlich ist (siehe Ziffer 37).

16. **Die neue zielgerichtete Ausnahme für nicht intrusive Eingriffe in Endeinrichtungen** wird ebenfalls anerkannt. Die Datenschutzgruppe findet die Klarstellung in der vorgeschlagenen Verordnung hilfreich, dass das Verbot nicht für die Messung des Webdatenverkehrs gilt (unter der eng gefassten Ausnahme, dass der Betreiber des vom Endnutzer gewünschten Dienstes der Informationsgesellschaft diese Messung durchführt, siehe Artikel 8 Absatz 1 Buchstabe d der vorgeschlagenen Verordnung). Siehe auch Erwägungsgrund 21. Die Datenschutzgruppe schlägt jedoch eine technologisch neutralere Definition vor, um die Anwendbarkeit dieser Ausnahme klarzustellen (siehe Ziffer 25).

3. SCHWERWIEGENDE PROBLEMBEREICHE

DER IM RAHMEN DER DS-GVO GEWÄHRTE SCHUTZ WIRD DURCH DIE VORGESCHLAGENE VERORDNUNG UNTERGRABEN

Wie oben dargestellt wurde, enthält die vorgeschlagene Verordnung eine Reihe sehr wichtiger Verbesserungen. Es gibt jedoch auch Bereiche, die mehr oder weniger große Bedenken hervorrufen. In diesem Abschnitt erläutert die Datenschutzgruppe die vier Themenbereiche, die bei ihr die **größten Bedenken** hervorrufen. Hierbei handelt es sich um Vorschriften, die **das von der DS-GVO gewährte Schutzniveau untergraben**:

17. **Die in der Verordnung niedergelegten Pflichten hinsichtlich der Verfolgung des Standortes von Endeinrichtungen sollten mit den Anforderungen der DS-GVO übereinstimmen**. In Artikel 8 Absatz 2 Buchstabe b der vorgeschlagenen Verordnung wird für die Erhebung von Informationen, die von Endeinrichtungen ausgesendet werden, lediglich ein Hinweis und die Durchführung von Sicherheitsmaßnahmen gefordert. In Artikel 8 Absatz 2 Buchstabe b wird weiter festgestellt, dass die für diese Erhebung verantwortliche Person auf Maßnahmen hinweisen muss, die der Endnutzer ergreifen kann, um die Erhebung zu beenden oder auf ein Minimum zu beschränken. Dabei vermittelt Artikel 8 Absatz 2 Buchstabe b den Eindruck, dass Organisationen die von der Endeinrichtung ausgesendeten Informationen ohne die Einwilligung der betroffenen Personen erheben dürften, um die Bewegungen von Einzelpersonen zu verfolgen (wie beispielsweise „Wi-Fi-Tracking“ oder „Bluetooth-Tracking“). Offensichtlich könne die diese Daten erhebende Partei den Anforderungen mit Hilfe eines Hinweises entsprechen, in dem

sie die Nutzer dazu auffordert, ihrer Geräte abzuschalten, wenn sie nicht verfolgt werden wollen. Ein solcher Ansatz würde dem grundlegenden Ziel der Telekommunikationspolitik der Europäischen Kommission zuwiderlaufen, allen Europäern grenzüberschreitend zu niedrigen Kosten einen mobilen Hochgeschwindigkeitsinternetzugang mit hohem Datenschutz zu bieten.

Darüber hinaus legt die vorgeschlagene Verordnung keine klaren Beschränkungen hinsichtlich des Umfangs der Datenerhebung oder der nachfolgenden Verarbeitungstätigkeiten fest. In diesem Zusammenhang sollte angemerkt werden, dass MAC-Adressen personenbezogene Daten sind, selbst nachdem Sicherheitsmaßnahmen wie Streuspeicherverfahren durchgeführt wurden. Dadurch dass keine weiteren Anforderungen oder Beschränkungen festgelegt werden, ist das Schutzniveau, das die vorgeschlagene Verordnung diesen personenbezogenen Daten bietet, signifikant niedriger als das von der DS-GVO gebotene Schutzniveau. In dieser Verordnung wird verlangt, dass eine solche Verfolgung rechtmäßig und nach Treu und Glauben erfolgen und transparent sein muss. In Erwägungsgrund 25 wird weiter wenig hilfreich festgestellt, dass einige der Funktionsmerkmale des Wi-Fi-Tracking keine große Gefahr für die Privatsphäre mit sich bringen, während andere dies tun, z. B. solche, die mit der Verfolgung einzelner Personen über einen längeren Zeitraum verbunden sind. Während die Datenschutzgruppe die Anerkennung begrüßt, dass mit dieser Verfolgung ein hohes Datenschutzrisiko einhergeht, ist es nicht sinnvoll, bereits im Vorfeld zu entscheiden, dass dies bei anderen Funktionsmerkmalen nicht der Fall ist, ohne die Umstände und die Verhältnismäßigkeit der Verarbeitung weiter zu bewerten. Bei der Durchführung einer solchen Bewertung sollten die folgenden Bedingungen in Bezug auf nicht anonymisiertes Wi-Fi-Tracking berücksichtigt werden.

Eine solche Verfolgung unterliegt gemäß der DS-GVO je nach den Umständen und dem Zweck der Erhebung personenbezogener Daten wahrscheinlich der Einwilligung oder sie darf nur durchgeführt werden, wenn die erhobenen personenbezogenen Daten anonymisiert werden. Diese Anonymisierung sollte vorzugsweise direkt nach der Erhebung erfolgen. Ist eine sofortige Anonymisierung aufgrund der Zwecke, für die die Daten erhoben werden, nicht möglich, dürfen diese Daten während des Zeitraums, in dem sie nicht anonymisiert sind, nur unter den folgenden Voraussetzungen verarbeitet werden: (i) der Zweck der Datenerhebung ist auf rein statistische Zählungen beschränkt (siehe die nachfolgenden Beispiele); (ii) die Verfolgung wird zeitlich und räumlich auf das zu diesem Zweck unbedingt nötige Ausmaß beschränkt; (iii) die Daten werden unmittelbar danach gelöscht oder anonymisiert und (iv) es müssen wirksame Möglichkeiten zur Nichtteilnahme bestehen. Die für die Datenverarbeitung Verantwortlichen müssen natürlich in jedem Fall die Anforderung erfüllen, angemessene Informationen bereitzustellen.

Die Datenschutzgruppe ist besorgt, dass es angesichts der steigenden Nutzung solcher Technologien zur Verfolgung durch private und öffentliche Organisationen ein inakzeptables Hindernis für die Bürger darstellen könnte, wenn eine mögliche Nichtteilnahme für jede diese Daten erhebende Organisation individuell zu erklären wäre. Deshalb ruft die Datenschutzgruppe den europäischen Gesetzgeber dazu auf, die Entwicklung technischer Standards zu fördern, mit denen Geräte automatisch die

Ablehnung einer solchen Verfolgung signalisieren, und sicherzustellen, dass die Einhaltung eines solchen Signals durchsetzbar ist.

Nach der DS-GVO wäre beispielsweise wahrscheinlich eine Einwilligung erforderlich, wenn ein für die Verarbeitung Verantwortlicher die indirekt bestimmbaren (Wi-Fi- oder Bluetooth-)MAC-Adressen von Geräten erhebt und speichert und den Standort der Nutzer berechnet, um diesen Standort über einen längeren Zeitraum zu verfolgen, beispielsweise durch mehrere Läden hindurch. Dies ist insbesondere dann der Fall, wenn eine solche Verfolgung in öffentlichen Räumen stattfindet, in denen die Nutzer die berechtigte Erwartung haben, nicht identifiziert oder verfolgt zu werden, in denen die MAC-Adressen Vorübergehender jedoch gesammelt werden. Eine solche Einwilligung könnte beispielsweise mit Hilfe einer App eingeholt werden, die die Nutzer dazu auffordert, die Verfolgung ihres Standortes in angegebenen Bereichen im Austausch für kommerzielle Angebote zu erlauben, oder indem an bestimmten Standorten Check-In-Möglichkeiten geboten werden oder durch einen Einwilligungsvordruck in Wi-Fi-Hotspots.

Den für die Verarbeitung Verantwortlichen könnte es nur in wenigen Ausnahmefällen gestattet werden, die von der Endeinrichtung ausgesendeten Informationen ohne die Einwilligung der betroffenen Personen zu verarbeiten, um die Bewegungen der betroffenen Person zu verfolgen. Das könnte beispielsweise der Fall sein, wenn die Zahl der Kunden ermittelt wird, die sich an einem bestimmten Ort befinden oder wenn die ausgesendeten Daten auf beiden Seiten einer Sicherheitskontrolle erhoben werden, um die Wartezeit anzugeben. Die Daten müssten jedoch in beiden Fällen gelöscht oder anonymisiert werden, sobald der statistische Zweck der Erhebung erfüllt werden kann. Das bedeutet, dass die MAC-Adressen der Geräte von Besuchern, die sich an einem bestimmten Ort aufhalten, wie beispielsweise in einem Laden, sofort nach Erhebung und ohne dauerhafte Speicherung anonymisiert werden müssen, und dies auf eine solche Weise, dass eine erneute Identifizierbarkeit technisch ausgeschlossen ist. Im Fall der Berechnung der Wartezeit müssten die MAC-Adressen gelöscht oder anonymisiert werden, sobald sie nicht mehr für die Berechnung der Wartezeit relevant sind (beispielsweise, da der Besucher auf der anderen Seite der Sicherheitskontrolle angelangt ist oder weil er die Schlange verlassen hat).
Zusätzlich müsste der für die Verarbeitung Verantwortliche Anforderungen zur Datenminimierung erfüllen (beispielsweise keine Verfolgung rund um die Uhr, wenn der Zweck auf die Ladenöffnungszeiten und/oder auf Stichproben in bestimmten Abständen beschränkt ist). Für die Verarbeitung Verantwortliche müssen auch andere Maßnahmen ergreifen, um sicherzustellen, dass es keine oder nur sehr geringe Auswirkungen auf das Recht auf Privatsphäre gibt, beispielsweise, indem die Privatsphäre der Menschen geschützt wird, die nahe bei einer Datenerhebungsstelle wohnen.

Die Entscheidung in Artikel 8 Absatz 2 der vorgeschlagenen Verordnung, dass nur ein einfacher Hinweis erforderlich ist, ist angesichts der Schlussfolgerung in Erwägungsgrund 20 umso bemerkenswerter, dass Informationen in Bezug auf das Gerät des Endnutzers auch im Fernzugang zu Identifizierungs- und Verfolgungszwecken erhoben werden können, was - nach der vorgeschlagenen

Verordnung - eine ernsthafte Verletzung der Privatsphäre dieser Endnutzer darstellen kann. Außerdem geht diese Pflicht nicht über die bereits in Artikel 13 und 14 DS-GVO vorgesehene Informationspflicht hinaus. Die ernsthafte Verletzung der Privatsphäre durch die Verfolgung wird durch den möglichen Zugriff anderer auf die erhobenen Daten noch verschärft, beispielsweise durch die Möglichkeit von Strafverfolgungsbehörden, Endnutzer basierend auf der/den gespeicherten MAC-Adresse(n) zu identifizieren, die die mobilen Geräte der Endnutzer senden.

18. **Die Bedingungen, unter denen eine Analyse des Inhalts und der Metadaten erlaubt ist, müssen ausgearbeitet werden.**

In Artikel 6 der vorgeschlagenen Verordnung werden unterschiedliche Schutzniveaus für Metadaten bzw. den Inhalt vorgesehen. Die Datenschutzgruppe unterstützt diese Unterscheidung nicht: Beide Datenkategorien sind hochsensibel. Folglich sollte für Metadaten und den Inhalt ein und dasselbe hohe Datenschutzniveau vorgesehen werden. Ausgangspunkt sollte also sein, dass die Verarbeitung von Metadaten und des Inhalts ohne die Einwilligung aller Endnutzer (Absender und Empfänger) verboten ist.

Abhängig vom jeweiligen Zweck können jedoch bestimmte Verarbeitungen ohne Einwilligung erlaubt werden, wenn sie für die folgenden Zwecke unbedingt erforderlich sind:

- Anbieter können elektronische Kommunikationsdaten für die in Artikel 6 Absatz 1 Buchstaben a und b sowie Artikel 6 Absatz 2 Buchstaben a und b der vorgeschlagenen Verordnung genannten Zwecke verarbeiten[7].
- Es sollte klargestellt werden, dass auch bestimmte Verfahren zur Erkennung oder zum Filtern von Spam und zur Entschärfung von Botnetzen als unbedingt erforderlich angesehen werden können, wenn es darum geht, missbräuchliche Nutzungen elektronischer Kommunikationsdienste zu erkennen und zu beenden (Artikel 6 Absatz 2 Buchstabe b). In Bezug auf die Spam-Filterung sollten Endnutzern, die Spam erhalten, granulare Möglichkeiten der Nichtteilnahme angeboten werden, sofern dies technisch möglich ist.
- Es sollte klargestellt werden, dass die Analyse elektronischer Kommunikationsdaten für Dienste für Kunden auch unter die Ausnahme „für die Rechnungstellung erforderlich“ (siehe Artikel 6 Absatz 2 Buchstabe b) fallen können. Die einschlägigen Metadaten können bis zum Ablauf des Zeitraums aufbewahrt werden, in dem eine Rechnung nach den nationalen Rechtsvorschriften rechtlich angefochten oder eine Zahlung angemahnt

[7] In Bezug auf die Notwendigkeit gemäß Artikel 6 Absatz 2 Buchstabe a der vorgeschlagenen Verordnung, verbindliche Dienstqualitätsanforderungen einzuhalten, sollten Anbieter die in der Verordnung (EU) Nr. 15/2120 („Kodex“) dargelegten Voraussetzungen berücksichtigen, insbesondere Artikel 3 sowie die Erwägungsgründe 10 und 13 bis 15. Nach diesen Vorschriften können Anbieter verpflichtet sein, Kommunikationsdaten zu verarbeiten, um Schadsoftware und Spähsoftware zu ermitteln und zu filtern, und es kann ihnen gestattet sein, Daten zu komprimieren.

werden kann. Die einschlägigen Daten (wie URL) dürfen nur auf Antrag des Endnutzers gespeichert werden und dann lediglich für einen Zeitraum, der unbedingt erforderlich ist, um eine Streitigkeit hinsichtlich einer Rechnung zu beenden (was bedeutet, dass Artikel 7 Absatz 3 entsprechend geändert werden sollte).

- Es sollte erlaubt werden, elektronische Kommunikationsdaten zu verarbeiten, um dem Endnutzer von diesem ausdrücklich gewünschte Dienste (beispielsweise eine Such- und Indexierungsfunktion, virtuelle Assistenten, Text-to-Speech-Dienste oder Übersetzungsdienste) zu bieten. Dies macht die Einführung einer Ausnahme für die Analyse solcher Daten für die rein individuelle (häusliche) Nutzung sowie für die individuelle arbeitsbezogene Verwendung[8] erforderlich. Dies wäre also ohne die Einwilligung aller Endnutzer möglich, könnte jedoch nur mit der Einwilligung des den Dienst anfordernden Endnutzers erfolgen. Durch eine solche besondere Einwilligung würde auch ausgeschlossen, dass der Anbieter diese Daten für andere Zwecke verwenden darf.

Das bedeutet, dass die Analyse von Inhalten und/oder Metadaten für alle anderen Zwecke wie Analysen, das Erstellen von Profilen, verhaltensorientierte Werbung oder sonstige dem Anbieter zum (kommerziellen) Vorteil gereichende Zwecke der Einwilligung aller Endnutzer, deren Daten verarbeitet würden, bedarf. In Bezug auf diesen Sachverhalt sollte in der vorgeschlagenen Verordnung präzisiert werden, dass das bloße Senden einer E-Mail oder einer anderen persönlichen Mitteilung von einem anderen Dienst an einen Endnutzer, der persönlich in die Verarbeitung seiner Inhalte und Metadaten eingewilligt hat (beispielsweise, indem er einen Mailservice abonniert hat), keine gültige Einwilligung darstellt.

Schließlich sollte klargestellt werden, dass bei der Verarbeitung von Daten anderer Personen als dem beteiligten Endnutzer (z. B. von Fotos oder von Beschreibungen einer anderen Person in einer Kommunikation zwischen zwei Personen) ebenfalls alle einschlägigen Vorschriften der DS-GVO einzuhalten sind.

19. **Endeinrichtungen und Software müssen *standardmäßig* unrechtmäßigen Eingriffen vorbeugen, sie verhindern und verbieten und Informationen über die Möglichkeiten bereitstellen**. Obwohl die vorgeschlagene Verordnung Anbieter von Software, die eine elektronische Kommunikation erlaubt, dazu verpflichtet, die „Möglichkeit zu bieten", eine eingeschränkte Form von Eingriffen in die Endeinrichtungen zu verhindern und bei der Installation vom Endnutzer die Einwilligung in eine Einstellung zu verlangen (Artikel 10 Absätze 1 und 2), entspricht eine solche Wahl nicht einer *datenschutzfreundlichen Grundeinstellung*. Darüber hinaus besteht bereits die „Möglichkeit", bestimmte Eingriffe zu verhindern

[8] Während Erwägungsgrund 13 der vorgeschlagenen Verordnung Unternehmensnetze ausdrücklich vom Anwendungsbereich der Verordnung ausschließt, sollte diese individuelle Nutzungsausnahme auch auf die Nutzung von Cloud-Diensten durch Beschäftigte für eine arbeitsbezogene Nutzung eingehen, zu denen beispielsweise die Suche in ihren E-Mails zählt.

und das hat bis heute nicht zu einer zufriedenstellenden Lösung des Problems der unrechtmäßigen Verfolgung geführt. Aus genau diesem Grund wurde in der DS-GVO bewusst die Entscheidung getroffen, die Grundsätze des Datenschutzes und der Privatsphäre durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen einzuführen (Artikel 25 DS-GVO). Die vorgeschlagene Verordnung untergräbt diese Grundsätze in Bezug auf Kommunikations- und Gerätedaten. Unterdessen sieht die Funkanlagenrichtlinie 2014/53/EU [9] (die in Erwägungsgrund 10 genannt wird) nur eine sehr geringe Sicherheitsverpflichtung vor, indem sie Folgendes fordert: Funkanlagen „verfügen über Sicherheitsvorrichtungen, die sicherstellen, dass personenbezogene Daten und die Privatsphäre des Nutzers und des Teilnehmers geschützt werden" (Artikel 3 Absatz 3 Buchstabe e). Dies kann keine Standardeinstellungen zugunsten des Schutzes der Privatsphäre in der vorgeschlagenen Verordnung ersetzen. Diesbezüglich sei auch angemerkt, dass in einer Eurobarometer-Befragung zum Thema „e-Privacy", die im Dezember 2016 veröffentlicht wurde, festgestellt wird, dass „[f]ast sieben von zehn Menschen (69 %) vollständig zustimmen, dass durch die Standardeinstellungen ihres Browsers das Teilen ihrer Informationen verhindert werden sollte"[10]. Die Datenschutzgruppe sieht ein anderes Problem in Bezug auf Browser-Einstellungen und die Definition von „Dritten". Siehe Ziffer 24. Dabei sollte nicht vergessen werden, dass diese Vorschrift nicht nur Browser betrifft, die auf Computern verwendet werden, sondern dass sie sich auch auf andere Arten von Software bezieht, die eine Kommunikation ermöglicht (einschließlich Betriebssystemen, Apps und Software-Schnittstellen für Geräte, die mit dem Internet der Dinge verbunden sind). Kurz gesagt, Endeinrichtungen und Software müssen *standardmäßig* Einstellungen zum Schutz der Privatsphäre bieten und die Nutzer durch das Konfigurationsmenü leiten, wenn bei der Installation von diesen Standardeinstellungen abgewichen werden soll. Es sollte während der Nutzung stets einfach sein, auf diese Konfigurationsmenüs zuzugreifen. Die Datenschutzgruppe ermutigt den europäischen Gesetzgeber, den Anwendungsbereich von Artikel 10 in dieser Hinsicht klarzustellen.

20. **Die Verordnung über die Privatsphäre sollte „Tracking Walls" ausdrücklich verbieten**, d. h. die Praxis, dass der Zugang zu einer Website oder einem Dienst verweigert wird, wenn nicht in die Verfolgung auf anderen Websites oder Diensten eingewilligt wird. Wie bereits in der vorherigen Stellungnahme der Datenschutzgruppe zur Datenschutzrichtlinie für elektronische Kommunikation[11] festgestellt wurde, sind solche „Alles-oder-Nichts"-Entscheidungen selten rechtmäßig[12]. Wenn die Nutzung der Verarbeitungs- und Speicherfunktionen von Endeinrichtungen oder die Erhebung von Informationen aus Endeinrichtungen der Endnutzer die Verfolgung der Aktivitäten des Nutzers über einen längeren Zeitraum

[9] Funkanlagenrichtlinie 2014/53/EU.

[10] Siehe Flash Eurobarometer 443, Report e-Privacy (veröffentlicht im Dezember 2016), S. 5.

[11] Siehe z. B. WP240 (Überarbeitung der Datenschutzrichtlinie für elektronische Kommunikation), S. 16 und WP208 (Ausnahme von der Einwilligung), S. 5.

[12] Dieser Standpunkt berührt nicht Artikel 7 Absatz 4 der DS-GVO, nach dem „Alles-oder-nichts-Entscheidungen" auch in anderen Situationen ausgeschlossen werden können, in denen dies angemessen ist.

oder über mehrere Dienste hinweg ermöglicht (z. B. verschiedene Websites oder Apps), können diese Verarbeitungstätigkeiten eine ernsthafte Verletzung der Privatsphäre dieser Endnutzer darstellen. Angesichts der grundlegenden Bedeutung des Internets für die Ausübung des Rechts auf freie Meinungsäußerung, einschließlich des Rechts auf Zugang zu Informationen, sollte die Möglichkeit des Einzelnen, auf Online-Inhalte zuzugreifen, nicht von seiner Einwilligung in der Verfolgung seiner Aktivitäten über Geräte und Websites/Apps hinweg abhängen. Folglich sollte die zukünftige Verordnung über die Privatsphäre deutlich machen, dass der Zugriff auf Inhalte beispielsweise auf Websites oder Apps nicht von der Einwilligung in solche eingreifenden Verarbeitungstätigkeiten abhängig gemacht werden darf, und zwar unabhängig von der zur Verfolgung angewendeten Technologie wie Cookies, der Verfolgung von Gerätekennungen, dem Einfügen eindeutiger Kennungen oder sonstigen Überwachungstechniken. Die Notwendigkeit dieses Verbots wird durch die kürzlich durchgeführte Eurobarometer-Befragung zum Thema „e-Privacy" unterstrichen, in der festgestellt wird, dass „[f]ast zwei Drittel der Befragten (64 %) sagen, es sei inakzeptabel, dass ihre Online-Aktivitäten im Austausch für einen uneingeschränkten Zugang zu einer bestimmten Website verfolgt werden."

21. Zusammengefasst **sollte die vorgeschlagene Verordnung** in Bezug auf die vier vorstehend genannten Punkte **ihr Versprechen einhalten, ein mindestens gleich hohes Schutzniveau zu bieten wie die DS-GVO**. In Erwägungsgrund 5 wird nüchtern festgestellt, dass die vorgeschlagene Verordnung das gemäß der DS-GVO genossene Schutzniveau nicht absenkt. In der jetzigen Form der vorgeschlagenen Verordnung stimmt das jedoch nicht, insbesondere nicht in Bezug auf die Verfolgung von Geräten (Ziffer 17), den fehlenden Grundsatz der datenschutzfreundlichen Voreinstellungen (Ziffer 19) und die Einwilligung (Ziffer 18). Dies ist von besonderer Bedeutung, da in demselben Erwägungsgrund der vorgeschlagenen Richtlinie Folgendes festgestellt wird: „Dieser Vorschlag stellt eine *Lex specialis* zur DS-GVO dar und wird diese im Hinblick auf elektronische Kommunikationsdaten, die als personenbezogene Daten einzustufen sind, präzisieren und ergänzen." Die Datenschutzgruppe schlägt vor, dass der Text der Verordnung über die Privatsphäre zumindest klarstellt, dass

    (i) die Verbote in der Verordnung über die Privatsphäre Vorrang haben vor den Genehmigungen in der DS-GVO (so hat z. B. das Verbot von Eingriffen nach Artikel 5 der Verordnung über die Privatsphäre Vorrang vor den Rechten der Betreiber elektronischer Kommunikationsdienste, personenbezogene Daten nach Artikel 5 Absatz 1 Buchstabe b und Artikel 6 Absatz 4 der DS-GVO weiter zu verarbeiten);

    (ii) die Verarbeitung, wenn sie aufgrund einer Ausnahme (einschließlich Einwilligung) von den Verboten in der Verordnung über die Privatsphäre erlaubt ist, dennoch alle einschlägigen Vorschriften der DS-GVO einhalten muss, wenn sie personenbezogene Daten betrifft;

    (iii) wenn die Verarbeitung aufgrund einer Ausnahme von den Verboten in der Verordnung über die Privatsphäre erlaubt ist, jede andere Verarbeitung auf der Grundlage der DS-GVO dennoch verboten ist, einschließlich der Verarbeitung für einen anderen Zweck auf der Grundlage von Artikel 6 Absatz 4 DS-GVO. Dies würde die für die Verarbeitung Verantwortlichen

nicht davon abhalten, um zusätzliche Einwilligungen in neue Verarbeitungsvorgänge zu ersuchen. Genau so wenig würde es die Gesetzgeber davon abhalten, zusätzliche, begrenzte und spezifische Ausnahmen in der Verordnung über die Privatsphäre bereitzustellen, beispielsweise, um die Verarbeitung zu wissenschaftlichen oder statistischen Zwecken gemäß Artikel 89 DS-GVO zu gestatten oder zum Schutz „lebenswichtiger Interessen" von Einzelperson nach Artikel 6 Buchstabe d DS-GVO.

Darüber hinaus sollte die Auslegung der Verordnung über die Privatsphäre sicherstellen, dass sie mindestens dasselbe Schutzniveau bietet wie die DS-GVO bzw. ein höheres, wenn dies angemessen ist.

4. WEITERE ERFORDERNISSE

Zusätzlich zu den vorstehend genannten Punkten hält die Artikel-29-Datenschutzgruppe folgende Maßnahmen für erforderlich:

DER RÄUMLICHE UND MATERIELLE ANWENDUNGSBEREICH SOLLTE AUSGEWEITET WERDEN

22. **Der Begriff „Metadaten" wird zu eng definiert**. Er wird nun in Artikel 4 Absatz c definiert als „Daten, die in einem elektronischen Kommunikationsnetz zu Zwecken der Übermittlung, der Verbreitung oder des Austauschs elektronischer Kommunikationsinhalte verarbeitet werden" (Hervorhebung hinzugefügt). Die Verwendung des Begriffs „Netz" scheint zu suggerieren, dass nur solche Daten als „Metadaten" gelten, die im Lauf der Bereitstellung von Diensten in der „niedrigeren" Ebene des Netzes generiert wurden. Das könnte bedeuten, dass Daten, die bei der Bereitstellung eines OTT-Dienstes generiert werden, von diesem Anwendungsbereich ausgeschlossen wären. Dies wäre nicht wünschenswert und angesichts der Absicht, den Anwendungsbereich der vorgeschlagenen Verordnung auf die Betreiber von OTT-Diensten auszuweiten, wahrscheinlich auch nicht beabsichtigt. Als Lösung hierfür sollte die Begriffsbestimmung von „elektronische Kommunikationsmetadaten" geändert werden, so dass sie alle Daten umfasst, die zu Zwecken der Übermittlung, der Verbreitung oder des Austauschs elektronischer Kommunikationsinhalte verarbeitet werden.

23. Ein weiteres Anliegen ist, dass **der räumliche Anwendungsbereich der vorgeschlagenen Verordnung in Bezug auf Organisationen ohne Niederlassung in der EU nur Betreiber elektronischer Kommunikationsdienste betrifft**. Ist der Betreiber eines elektronischen Kommunikationsdienstes nicht in der Union niedergelassen, so muss er gemäß der vorgeschlagenen Verordnung schriftlich einen Vertreter in der EU benennen (Artikel 3 Absatz 2). Es wird in Erwägungsgrund 9 auch erwähnt, dass die Verordnung auf die Verarbeitung durch die Betreiber elektronischer Kommunikationsdienste ohne Berücksichtigung des Ortes anzuwenden sei, an dem die Verarbeitung erfolgt. Die Datenschutzgruppe begrüßt diese Klarstellung. Da der Wortlaut jedoch auf die Betreiber elektronischer Kommunikationsdienste beschränkt ist, ist es unsicher, in welchem Umfang dieser territoriale Anwendungsbereich auf andere Arten von Parteien Anwendung findet

(beispielsweise Parteien, die in Informationen, die von den Endgeräten des Endnutzers gesendet werden, eingreifen oder diese erheben, siehe Artikel 3 Absatz 1 Buchstabe c in Verbindung mit Artikel 8 der vorgeschlagenen Verordnung). Deshalb schlägt die Datenschutzgruppe vor, dass Artikel 3 Absätze 2 und 5 dahingehend geändert werden, dass sie für Betreiber öffentlich zugänglicher Verzeichnisse, für Anbieter von Software, die elektronische Kommunikation ermöglicht und für Personen gelten, die mithilfe elektronischer Kommunikationsdienste an Endnutzer gerichtete gewerbliche Direktwerbung betreiben oder Informationen sammeln, die in Endeinrichtungen der Endnutzer gespeichert sind oder sich auf diese beziehen, sobald diese ihre Tätigkeiten auf Nutzer in der EU ausrichten (siehe Erwägungsgrund 8 der vorgeschlagenen Verordnung)[13].

DER SCHUTZ DER ENDEINRICHTUNGEN SOLLTE GESTÄRKT WERDEN

Weitere Bedenken bestehen hinsichtlich des unzureichenden Schutzes, den die vorgeschlagene Verordnung Endeinrichtungen bietet.

24. Erstens **suggeriert die vorgeschlagene Verordnung fälschlicherweise, dass durch unspezifische Browser-Einstellungen eine gültige Einwilligung gegeben werden könne.** Die Datenschutzgruppe erkennt die Überlegung an, dass die Endnutzer derzeit mit Einwilligungsanfragen überhäuft werden (Erwägungsgrund 22). Browser-Einstellungen (und die Einstellungen vergleichbarer Software) spielen bei der Lösung dieses Problems eine Rolle. Da allgemeine Browser-Einstellungen jedoch nicht auf die Anwendung einer Technologie zur Verfolgung in einem Einzelfall anwendbar sein sollen, sind sie nicht geeignet für das Erteilen der Einwilligung gemäß Artikel 7 und Erwägungsgrund 32 der DS-GVO (da die Einwilligung nicht in ausreichendem Maße in Kenntnis der Sachlage und für den konkreten Fall erteilt wird).
    Der Endnutzer muss die Möglichkeit haben, seine Einwilligung gesondert für jede Website oder App und für die Verfolgung für verschiedene Zwecke zu erteilen (wie beispielsweise die Verbreitung von Informationen in sozialen Netzwerken oder Werbung). Ist ein für die Verarbeitung Verantwortlicher für mehrere Websites oder Apps zuständig, kann er auch um die Einwilligung für alle anderen Websites oder Apps ersuchen, für die er zuständig ist, sofern dieses Ersuchen um Einwilligung gesondert gestellt wird.
    Darüber hinaus muss der für die Verarbeitung Verantwortliche alle anderen Anforderungen an die Einwilligung erfüllen, einschließlich der Pflicht, die Nutzer ausreichend zu informieren. Dies bedeutet sowohl für den Browser als auch für den für die Verarbeitung Verantwortlichen, dass es nicht gültig wäre, wenn sie nur die Möglichkeit bieten würden „alle Cookies zu akzeptieren“, da dies den Nutzern nicht

[13] Siehe Artikel 3 Buchstabe f der DS-GVO: „Diese Verordnung findet Anwendung auf die Verarbeitung personenbezogener Daten von betroffenen Personen, die sich in der Union befinden, durch einen nicht in der Union niedergelassenen Verantwortlichen oder Auftragsverarbeiter, wenn die Datenverarbeitung im Zusammenhang damit steht a) betroffenen Personen in der Union Waren oder Dienstleistungen anzubieten, unabhängig davon, ob von diesen betroffenen Personen eine Zahlung zu leisten ist; b) das Verhalten betroffener Personen zu beobachten, soweit ihr Verhalten in der Union erfolgt.“ Diese Pflicht könnte auch Ausnahmen im Sinne von Artikel 27 Absatz 2 DS-GVO umfassen.

die Möglichkeit gäbe, die erforderliche granulare Einwilligung zu erteilen. Es sollte jedoch möglich sein, dass es die Browser den Nutzern ermöglichen, eine bewusste Entscheidung in Kenntnis der Sachlage zu treffen, alle Cookies zu akzeptieren und so zukünftige spezifische Einwilligungsanfragen der von ihnen besuchten Websites zu verhindern.

Die Datenschutzgruppe empfiehlt dringend, dass die Verordnung über die Privatsphäre dazu verpflichtet, bei Browsern technische Mechanismen, wie den Standard „Do Not Track" einzusetzen, um sicherzustellen, dass die Nutzer eine echte Wahlmöglichkeit und die Kontrolle über die Eingriffe in ihre Geräte erhalten.[14]

Es ist allerdings sogar noch wichtiger, dass die Verordnung über die Privatsphäre sicherstellen sollte, dass sowohl die Wahl in Bezug auf die Speicherung der Informationen auf dem Gerät und ein DNT-Signal (Do Not Track) von einem Browser als rechtsverbindlicher Hinweis auf die Einwilligung oder die Ablehnung von allen für die Verarbeitung Verantwortlichen akzeptiert wird. Dies gilt unbeschadet weiterer Leitlinien der Datenschutzgruppe zur Einhaltung des DNT-Standards, unter anderem mit dem Grundsatz der Zweckbindung, wenn der Standard abgeschlossen sein wird (für Ende 2017 geplant).

Implizite Formen der „Einwilligung", wie das Anklicken einer Website oder das Scrollen auf einer Seite können nicht die Entscheidungen hinsichtlich der Speicherung oder des DNT-Signals aufheben. Ein wichtiger Vorteil der Anwendung dieses Standards ist, dass er nicht auf die Technologie von Cookies zur Verfolgung beschränkt ist, sondern sich auch an alle anderen Arten der Verfolgung richtet, wie beispielsweise die Verfolgung von Gerätekennungen.

Die Einhaltung dieses Standards rechtsverbindlich zu machen, löst auch ein anderes Problem mit der derzeitigen Verwendung des Begriffs „Dritte" in Artikel 10. Eine Website oder eine App enthält üblicherweise viele Elemente sowohl von der Website selbst als auch externe Elemente. Im Kontext der besuchten Website kann auch ein externer Code laufen, der an den Server eines Dritten meldet. Ein Verfolgungs-Cookie wird möglicherweise von einer ersten Partei eingesetzt, wenn ein Nutzer beispielsweise eine Seite eines sozialen Netzwerks besucht. Diese Seite eines sozialen Netzwerks könnte auch ein Dritter sein, wenn der Nutzer eine andere Website besucht, die mit dieser Seite eines sozialen Netzwerks interagiert. Dies stellt in allen genannten Fällen einen Eingriff in das Gerät dar, für den eine Einwilligung erforderlich ist (sofern keine der Ausnahmen Anwendung findet), unabhängig davon, ob es sich um „Zugang zu" oder „Speichern von" Informationen auf dem Gerät des Endnutzers handelt. Im DNT-Standard werden deshalb die Begriffe „die Website betreffend" und „das Internet betreffend" verwendet. Zur Verbesserung der Rechtssicherheit aller Interessenträger sollte der Bezug auf „Dritte" in der Verordnung über die Privatsphäre deshalb umformuliert werden, so dass er alle Rechtsträger umfasst, mit denen ein Gerät interagiert (da sie Informationen speichern oder auf Informationen auf dem Gerät zugreifen).

[14] Siehe https://www.w3.org/TR/tracking-compliance. In Punkt 7 werden das Modell für Ausnahmen und der Unterschied zwischen Ausnahmen, die sich auf eine Website beziehen und solchen, die sich auf das gesamte Netz beziehen, erklärt. Punkt 6 nennt die maschinenlesbaren Informationen, welche die für die Verarbeitung Verantwortlichen hinsichtlich der Pflicht zur Bereitstellung von Informationen für das Einholen der Einwilligung bereitstellen können.

Um den Standard „Do Not Track“ mit dem hohen Niveau an Schutz der Vertraulichkeit der Kommunikation und dem hohen Datenschutzniveau vereinbar zu machen, die die Charta gewährt, sollte in der Verordnung über die Privatsphäre festgelegt werden, dass Aufforderungen, die Verfolgung über das Internet und nicht nur auf einer Website zu akzeptieren, gesondert vorgelegt werden müssen und dass die Nutzer die Möglichkeit haben müssen, solche Aufforderungen zu akzeptieren oder abzulehnen. Damit die Nutzer vor häufigen Ersuchen um Einwilligung geschützt werden, sollte die Verordnung über die Privatsphäre darüber hinaus sicherstellen, dass eine Weigerung, in die das ganze Internet betreffende Verfolgung durch eine spezielle Organisation einzuwilligen (über den Standard „Do Not Track“ oder über eine gesonderte Ausschlussliste) diese Organisation für mindestens sechs Monate sperrt, weitere Ersuchen um Einwilligung zu stellen. Diese Vorschrift schließt nicht aus, dass Organisationen, wenn der Nutzer ihre Website direkt besucht (z. B. als erste Partei) die Einwilligung für ihre eigene Website einholen (d. h. ein die eigene Website betreffendes Ersuchen um Einwilligung). In der Praxis bedeutet dies z. B., dass ein Videostreaminganbieter, der Verfolgungs-Cookies einsetzt, den Nutzer um Einwilligung ersuchen kann, wenn dieser die Streaming-Website besucht, dies aber für die Dauer von sechs Monaten nicht erneut tun kann, wenn dieser Nutzer die Einwilligung versagt hat und andere Websites besucht, die Videos bereitstellen, die von dieser Streaming-Website stammen.

25. Darüber hinaus ist **die Ausnahme für „Messung des Webpublikums“ ungenau formuliert**. Artikel 8 Absatz 1 Buchstabe d der vorgeschlagenen Verordnung sieht eine Ausnahme für die Messung des Webpublikums vor. Erstens wird dieser Begriff nicht definiert und kann folglich mit der Erstellung von Nutzerprofilen verwechselt werden. In der Begriffsbestimmung sollte klar gemacht werden, dass diese Ausnahme nicht für die Erstellung von Nutzerprofilen verwendet werden darf. Die Ausnahme sollte lediglich für die Analyse der Nutzung gelten, die erforderlich ist, um die von dem Nutzer gewünschte Analyse der Leistung des Dienstes durchzuführen, aber nicht, um die Nutzer zu analysieren (d. h. um das Verhalten bestimmbarer Nutzer einer Website, einer App oder eines Geräts zu analysieren). Deshalb darf die Ausnahme nicht in Fällen angewendet werden, in denen die Daten mit identifizierbaren Nutzerdaten in Verbindung gebracht werden können, die von dem Betreiber oder von anderen für die Verarbeitung Verantwortlichen verarbeitet werden. Darüber hinaus suggeriert die Beschreibung eine sehr technologiespezifische Anwendung. Der Begriff „Messung des Webpublikums“ sollte folglich auf eine technologisch neutrale Weise umformuliert werden, damit er auch ähnliche analytische Nutzungsdaten betrifft, die von Apps, Wearables oder Geräten des Internets der Dinge abgerufen werden.

Die Datenschutzgruppe schlägt vor, sich an die niederländische Ausnahme anzulehnen. In den Niederlanden findet sie Anwendung, wenn eine Ausnahme unbedingt erforderlich ist, um Informationen über die technische Qualität oder Wirksamkeit eines erbrachten Dienstes der Informationsgesellschaft zu erhalten, und wenn diese keine oder nur geringe Auswirkungen auf die Privatsphäre des betroffenen Teilnehmers oder Endnutzers hat (siehe Artikel 11.7a Absatz 3 Buchstabe b des Telekommunikationsgesetzes der Niederlande). Diese Ausnahme berücksichtigt die Tatsache, dass es sich bei den meisten Daten, die über das Web

oder eine App analysiert werden, nach wie vor um personenbezogene Daten handelt. Das bedeutet, dass die Verarbeitung dieser Daten auch der DS-GVO unterliegt. Dies impliziert beispielsweise, dass die Nutzungsanalyse auch von externen Organisationen durchgeführt werden könnte - allerdings nur, wenn:
(i) diese Organisation als für die Verarbeitung Verantwortlicher handelt;
(ii) ein Auftrag über die Datenverarbeitung geschlossen wird, der die DS-GVO einhält;
(iii) die für die Analyse verwendete Technologie eine erneute Identifizierung verhindert, beispielsweise durch Anonymisierung der IP-Adressen der Nutzer;
(iv) das/die spezifische(n) Cookie(s) oder andere für die Analytik verwendete Daten nur für diese bestimmte Website, App oder das Wearable verwendet werden können und nicht mit anderen identifizierbaren Daten verknüpft werden können;
(v) Nutzer das Recht haben, zu widersprechen (siehe auch die Randnummern 17 und 50 dieser Stellungnahme).

Obwohl keine Einwilligung erforderlich wäre, wenn diese Bedingungen erfüllt sind, müssen die für die Verarbeitung Verantwortlichen den Nutzern dennoch angemessene Informationen zur Verfügung stellen, beispielsweise durch Felder im Standard „Do Not Track", in denen der Status der Verfolgung dargestellt wird[15].

26. Die Verordnung über die Privatsphäre **sollte eng begrenzte und klar formulierte Ausnahmen von der Einwilligungspflicht sicherstellen.** Der Wortlaut der Ausnahme von der Pflicht zur Einwilligung in Eingriffe in Geräte in Artikel 8 Absatz 1 Buchstabe c ist fast identisch mit dem aktuellen Wortlaut in Artikel 5 Absatz 3 der Datenschutzrichtlinie für elektronische Kommunikation *„soweit dies unbedingt erforderlich ist, um einen vom Teilnehmer oder Nutzer ausdrücklich gewünschten Dienst der Informationsgesellschaft zur Verfügung zu stellen"*. Das Wort „unbedingt" wird aber ohne Erklärung ausgelassen. Dies gibt aus zwei Gründen Anlass zur Sorge. Erstens hat die Vorschrift in der Datenschutzrichtlinie für elektronische Kommunikation bereits zwischen Aufsichtsbehörden und Organisationen zu ausführlichen Diskussionen über den Anwendungsbereich geführt, und die Streichung des Wortes „unbedingt" wird zu noch weniger Rechtssicherheit führen. Dies ist der Datenschutzgruppe auch deshalb ein Anliegen, weil sie bereits eine Leitlinie zur Auslegung des Begriffes „unbedingt" in diesem Zusammenhang vorgelegt hat. Die Datenschutzgruppe schlug in der Stellungnahme zur Ausnahme von Cookies von der Einwilligungspflicht (WP194) die folgende Klarstellung vor:
„*Ein Cookie ist unbedingt erforderlich, um dem Nutzer (oder Teilnehmer) eine bestimmte Funktion zur Verfügung zu stellen: Wenn Cookies deaktiviert sind, ist die Funktion nicht verfügbar und die Funktion wurde vom Nutzer (oder Teilnehmer) als Teil eines Dienstes der Informationsgesellschaft ausdrücklich angefordert.*"[16]

Die Datenschutzgruppe hat darüber hinaus Folgendes klargestellt:

[15] Siehe Tracking Preference Expression (DNT), Editor's draft, 7. März 2016.

[16] Artikel-29-Datenschutzgruppe, WP 294, Stellungnahme 04/2012 zur Ausnahme von Cookies von der Einwilligungspflicht, angenommen am 7. Juni 2012, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp194_de.pdf.

„[…] sind Third-Party-Cookies im Sinne der obigen Definitionen für den Nutzer, der eine Website besucht, in der Regel nicht „unbedingt erforderlich", weil sie gewöhnlich mit einem Dienst im Zusammenhang stehen, der sich von dem vom Nutzer ausdrücklich gewünschten Dienst unterscheidet."[17]
Die Datenschutzgruppe fügte hinzu, dass die Verwendung sozialer Plugins, die auf Personen ausgerichtet sind, die bei einer Plattform oder Website nicht angemeldet sind, gleichermaßen nicht als unbedingt erforderlich angesehen würden.

Während Artikel 6 Absatz 1 Buchstabe b der vorgeschlagenen Verordnung die Verarbeitung elektronischer Kommunikationsdaten erlaubt, wenn dies für Sicherheitszwecke „nötig" ist, wird in Erwägungsgrund 49 der DS-GVO darüber hinaus gefordert, dass es „unbedingt notwendig" ist. Die Auslassung des Wortes „unbedingt" mag möglicherweise nicht beabsichtigt gewesen sein, da in Erwägungsgrund 21 der vorgeschlagenen Verordnung erwähnt wird, dass keine Einwilligung für Eingriffe eingeholt werden sollte, die „unbedingt" notwendig sind. Dennoch bietet die vorgeschlagene Verordnung eine Gelegenheit, weiter klarzustellen, dass die Prüfung der Notwendigkeit im Zusammenhang mit dieser Verordnung in Bezug auf alle Ausnahmen eng ausgelegt werden sollte. Deshalb schlägt die Datenschutzgruppe vor, dass in Bezug auf alle Ausnahmen in Artikel 6 und in Artikel 8 Absatz 1 der vorgeschlagenen Verordnung das Wort „unbedingt" vor das Wort „nötig" hinzugefügt wird.

Anderseits sollte die Verordnung über die Privatsphäre Eingriffe in Einrichtungen zur Installation von Sicherheitsupdates ausdrücklich erlauben. Bei den meisten Endeinrichtungen ist die bevorzugte Methode für die Installation von Sicherheitsupdates das Versenden der Sicherheitsupdates über das Internet. Die Installation von Updates wird als Eingriff in die Endeinrichtung angesehen. Es besteht ein berechtigtes Interesse daran, dass die Sicherheit dieser Geräte stets auf dem neuesten Stand bleibt. Ein Anbieter von Sicherheitspatches sollte deshalb die unbedingt nötigen Sicherheitsupdates im Allgemeinen ohne die Einwilligung des Endnutzers installieren können. Es ist jedoch unsicher, ob dieser Eingriff von der Ausnahme der „Informationsgesellschaft" von dem Verbot von Eingriffen (Artikel 8 Absatz 1 Buchstabe c) profitieren kann. Es sollte geklärt werden, dass die Installation von Sicherheitsupdates unter dieser Ausnahme erlaubt sein sollte, aber nur insoweit als (i) die Sicherheitsupdates gesondert gepackt sind und die Funktionalität der Software auf dem Gerät in keiner Weise ändern (einschließlich der Interaktion mit anderer Software oder der vom Nutzer gewählten Einstellungen), (ii) der Endnutzer jedes Mal vor der Installation eines Updates informiert wird und (iii) der Endnutzer die Möglichkeit hat, die automatische Installation dieser Updates abzuschalten.

[17] Ebd.

SCHUTZ VOR DIREKTWERBUNG

Ein weiteres Problem ist der unzureichende Schutz vor Direktwerbung.

27. Erstens findet die Datenschutzgruppe, dass **der Anwendungsbereich von Direktwerbung zu eng gefasst ist.** In Artikel 4 Absatz 3 Buchstabe f der vorgeschlagenen Verordnung ist „Direktwerbung" definiert als „jede Art der Werbung in schriftlicher oder mündlicher Form, die an einen oder mehrere bestimmte oder bestimmbare Endnutzer elektronischer Kommunikationsdienste gerichtet wird". Die Verwendung des Begriffes „gerichtet an" impliziert die Verwendung technologischer Kommunikationsmittel, die notwendigerweise die Übertragung einer Kommunikation umfassen, während die meiste Werbung im Netz (durch Plattformen der sozialen Medien oder einer Website) nicht im strengen Sinn ein „Richten" der Werbung „an" Jemanden umfassen. Dies wird weiter durch die Beispiele unterstrichen, die in dieser Begriffsbestimmung (SMS, E-Mail) und in Erwägungsgrund 33 folgen. Sie verweisen alle auf recht herkömmliche Formen der Werbung, und selbst dann fällt die Verwendung der - recht herkömmlichen - Anrufsysteme wohl nicht in den Anwendungsbereich. Der Artikel und der Erwägungsgrund sollten dahingehend geändert werden, dass sie jede Werbung umfassen, die an einen oder mehrere bestimmte oder bestimmbare Endnutzer *gesendet, gerichtet oder diesem/diesen vorgelegt* wird. Darüber hinaus sollte weiterhin sichergestellt werden, dass verhaltensbezogene Werbung (basierend auf den Profilen der Endnutzer) ebenfalls als Direktwerbung betrachtet wird, die „an einen oder mehrere bestimmte oder bestimmbare Endnutzer elektronischer Kommunikationsdienste" gerichtet wird (da solche Werbung an spezielle, bestimmbare Nutzer gerichtet ist).

    Gemäß dem vorgeschlagenen Anwendungsbereich von „Direktwerbung" wäre darüber hinaus der Schutz nach Artikel 16 Absatz 1 auf Nachrichten beschränkt, die Werbematerial enthalten und würde Einzelpersonen nicht vor anderen Nachrichten schützen, die ihnen für Werbezwecke gesendet, an sie gerichtet oder ihnen vorgelegt werden (wie beispielsweise Nachrichten an Neukunden zur Einholung der Einwilligung, die Einflussnahme auf politische Ansichten oder Wahlpräferenzen, die Reklame für Wohltätigkeitseinrichtungen oder sonstige Organisationen ohne Erwerbszweck oder allgemeines Branding einer Organisation). Außerdem werden nach wie vor Faxgeräte für Direktwerbung genutzt, auch wenn sie in der Definition nicht aufgeführt sind. Folglich sollte Artikel 4 Absatz 3 Buchstabe f jede Form der Werbung, Akquisition und Förderung auch für Organisationen ohne Erwerbszweck umfassen und ausdrücklich Faxgeräte neben E-Mail und SMS einschließen (siehe auch die Vorschläge für eine Klarstellung in Ziffer 43a. Schließlich wird in Erwägungsgrund 32 festgestellt, dass Werbung auch Nachrichten von politischen Parteien umfasst, die für ihre Parteien werben. Das sollte aktualisiert werden, damit auch Politiker und zur Wahl stehende Kandidaten dazu zählen, die Wahlkampf betreiben.

28. Zweitens **ist der Widerruf der Einwilligung in Werbung nicht unentgeltlich und auch nicht so einfach durchzuführen, wie das Erteilen der Einwilligung.** Die Möglichkeit, gemäß der vorgeschlagenen Verordnung eine Einwilligung zu

widerrufen, muss geklärt werden, um Kohärenz sicherzustellen und den Schutz der Empfänger zu verbessern. Artikel 16 Absatz 6 der vorgeschlagenen Verordnung sieht derzeit vor, dass Empfänger von Direktwerbung „die nötigen Informationen [erhalten], damit die Empfänger in einfacher Weise ihr Recht ausüben können, die Einwilligung in den weiteren Empfang von Werbenachrichten zu widerrufen“ (Hervorhebung hinzugefügt). Dies wird in Erwägungsgrund 34 bestätigt. Es ergibt sich jedoch aus Erwägungsgrund 70 der DS-GVO, dass die betroffenen Personen gemäß der DS-GVO nicht nur das Recht haben sollten, der Verarbeitung für Zwecke der Direktwerbung auf einfache Weise zu widersprechen, sondern auch „unentgeltlich“. Dieser Begriff wird auch in Artikel 16 Absatz 2 der vorgeschlagenen Verordnung verwendet, aber nur in Bezug auf die Entscheidung gegen Direktwerbung auf der Grundlage von Daten, die im Zusammenhang mit einem Verkauf erhalten wurden.

Artikel 7 Absatz 3 der DS-GVO legt fest, dass der Widerruf der Einwilligung so einfach wie die Erteilung der Einwilligung sein muss und dass Personen dazu in der Lage sein sollten, ihre Einwilligung jederzeit zu widerrufen. Darüber hinaus hat die Datenschutzgruppe bereits in ihrer Stellungnahme 04/2010 zum FEDMA (WP174) anerkannt, dass es wichtig ist, dem Empfänger die Möglichkeit zu bieten, „sich problemlos, direkt und kostenfrei aus dem entsprechenden Verteiler abzumelden“[18]. Dieser Standard für den Widerruf der Einwilligung sollte in die Vorschriften für Direktwerbung in der vorgeschlagenen Verordnung eingebunden werden. Dasselbe gilt für die Anforderung in Artikel 7 Absatz 3 der DS-GVO, dass der Widerruf der Einwilligung jederzeit so einfach wie die Erteilung der Einwilligung sein muss.

29. Passend dazu **sollte geklärt werden, wie die Einwilligung widerrufen oder Direktwerbeanrufen widersprochen werden kann**. Gemäß Artikel 16 Absatz 4 der vorgeschlagenen Verordnung können Mitgliedstaaten in Bezug auf persönliche Direktwerbeanrufe ein Opt-out-Konzept vorsehen. In der Verordnung über die Privatsphäre sollten die Vorkehrungen für den Widerruf der Einwilligung oder für einen Widerspruch gegen Direktwerbeanrufe dargelegt werden. In Erwägungsgrund 36 wird dargelegt, dass Mitgliedstaaten nationale Opt-out-Systeme einrichten oder beibehalten *können sollten.* Basierend auf dieser Vorschrift könnten Mitgliedstaaten sogar eine Situation zulassen, in der Nutzer ihren Widerspruch jedem einzelnen Kommunikationsdienstleister gegenüber erklären müssen. Eine solche Umsetzung versagt hinsichtlich des Schutzes der Nutzer vor der Belästigung durch unerbetene Kommunikation[19] oder hinsichtlich der Bereitstellung eines die DS-GVO einhaltenden Verfahrens, mit dem die Einwilligung jederzeit und auf einfache Weise widerrufen werden kann. Deshalb könnte in der Verordnung bestimmt werden, dass

18 Artikel-29-Datenschutzgruppe, WP 174, Stellungnahme 4/2010 zum europäischen Verhaltenskodex von FEDMA zur Verwendung personenbezogener Daten im Direktmarketing, angenommen am 13. Juli 2010, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2010/wp174_de.pdf.

19 Im Vereinigten Königreich hat der Telekommunikationsbetreiber BT beispielsweise in einer Woche 31 Millionen belästigende Anrufe verzeichnet. Siehe www.bbc.com/news/business-38635921.

alle Mitgliedstaaten eine nationale Do-Not-Call-Liste erstellen *müssen*. Darüber hinaus sollte in der Verordnung vorgesehen werden, dass Empfängern von persönlichen Anrufen in Bezug auf den Widerruf ihrer Einwilligung zwei Optionen zur Verfügung stehen sollten: zukünftigen Anrufen von diesem Unternehmen oder der Organisation zu widersprechen, und die Möglichkeit, sich während dieser Anrufe in eine nationale Do-Not-Call-Liste aufnehmen zu lassen.

30. Ein weiterer bedenklicher Punkt ist, dass **die Verwendung falscher Identitäten bei der Versendung von Direktwerbung nicht ausdrücklich verboten ist**. In Erwägungsgrund 34 wird festgestellt, dass „die Verschleierung der Identität und die Verwendung falscher Identitäten, falscher Rücksendeadressen oder Rückrufnummern bei der Durchführung unerbetener gewerblicher Direktwerbung" untersagt ist. In Artikel 16 Absatz 6 wird dagegen lediglich festgestellt, dass die Endnutzer über „die Identität der juristischen oder natürlichen Person, in deren Namen die Nachricht übermittelt wird" informiert werden. Diese Pflicht zur Information der Empfänger über die Identität sollte mit dem eindeutigen Verbot ergänzt werden, verschleierte oder falsche Kontaktadressen für Zwecke der Direktwerbung zu verwenden.

31. Dieser Punkt betrifft einen weiteren fraglichen Bereich: **die Vorgabe, für Werbeanrufe eine Vorwahl anzugeben, wird als Alternative zu der Pflicht zur Anzeige der Rufnummer dargestellt**. Gemäß Artikel 16 Absatz 3 sind Direktwerbeanrufe zulässig, wenn der Anrufer entweder (i) eine Rufnummer angibt, unter der die natürliche oder juristische Personen erreichbar ist, die den Anruf tätigt (Artikel 16 Absatz 3 Buchstabe a) oder (ii) einen besonderen Kode/eine Vorwahl angibt, der/die kenntlich macht, dass es sich um einen Werbeanruf handelt (Artikel 16 Absatz 3 Buchstabe b). Obwohl die Datenschutzgruppe die Pflicht in Artikel 16 Absatz 3 Buchstabe b begrüßt, eine Vorwahl zu verwenden, ist sie der Ansicht, dass diese Vorgabe nicht dasselbe Problem behandelt wie die Pflicht in Artikel 16 Absatz 3 Buchstabe a, eine Rufnummer anzugeben. Während die Vorgabe, eine Vorwahl anzugeben, dem Empfänger die Möglichkeit geben soll, einen Werbeanruf direkt als solchen zu erkennen (und Maßnahmen zum Sperren dieser Anrufe zu ergreifen) soll den Empfängern (und den Aufsichtsbehörden) mit der Vorgabe, eine Rufnummer anzugeben, die Möglichkeit gegeben werden, den Anstifter der Werbung zu identifizieren und zu kontaktieren. Dies ist insbesondere bei automatisierten Anrufen relevant, bei denen ein großes Ungleichgewicht zwischen den Möglichkeiten des Vermarkters besteht, belästigende Anrufe zu senden und den Möglichkeiten des Empfängers, diese Anrufe zu vermeiden. Folglich müssen sich die Vorgaben ergänzen, statt Alternativen darzustellen.

ZEITPLAN

32. Die Artikel-29-Datenschutzgruppe empfiehlt der Europäischen Kommission, die Notwendigkeit anzuerkennen, dass die vorgeschlagene Verordnung zusammen mit der DS-GVO im Mai 2018 in Kraft tritt, um Unstimmigkeiten zwischen den beiden Rechtsvorschriften zu vermeiden. Sie hat jedoch nach wie vor Bedenken, dass dies ein ambitionierter Zeitplan ist, der auch einer Finalisierung des Kodexentwurfs bedarf. Deshalb fordert die Datenschutzgruppe alle am Rechtssetzungsprozess Beteiligten dazu auf, die Frist bis Mai 2018 einzuhalten.

SONSTIGE BEDENKEN

In diesem Abschnitt werden eine Reihe weiterer Bedenken dargelegt.

33. Erstens hat die Datenschutzgruppe Bedenken hinsichtlich des **Vorschlags, dass nicht zielgerichtete Maßnahmen zur Vorratsdatenspeicherung zulässig sind.** In der Begründung wird festgestellt, dass es den Mitgliedstaaten gemäß der vorgeschlagenen Verordnung freisteht, nationale Rahmen für die Vorratsdatenspeicherung zu schaffen oder beizubehalten, die u. a. gezielte Vorratsspeicherungen vorsehen (Absatz 1.3). Seit der Entscheidung in der Rechtssache *Tele2/Watson*[20] ist es klar, dass es gemäß der Charta nur zulässig ist, nationale Rahmen für die Vorratsdatenspeicherung zu schaffen, die eine gezielte Vorratsspeicherung vorsehen (und selbst dann wichtigen Bedingungen wie der Überwachung unterliegen) und dass der generelle Zugriff auf Metadaten genau wie der generelle Zugriff auf den Inhalt elektronischer Kommunikation als Verletzung des Wesensgehalts von Artikel 7 angesehen wird (siehe EuGH, Schrems und Randnummer 94). Folglich lässt der Wortlaut dieses Satzes einen gewissen Spielraum für die Mitgliedstaaten in Bezug auf Maßnahmen zur Vorratsdatenspeicherung vermuten, der nicht existiert. Diesbezüglich wird **Metadaten** in der vorgeschlagenen Verordnung **kein ausreichender Schutz zugestanden.** Wie bereits in Ziffer 10 angemerkt, begrüßt die Artikel-29-Datenschutzgruppe die Anerkennung, dass Metadaten sehr sensible Daten offenlegen können. Allerdings erhalten Metadaten in der vorgeschlagenen Verordnung nicht den Schutz, den sie aufgrund dieser Anerkennung erhalten sollten. Angesichts der Sensibilität von Metadaten sollte insbesondere vor einer Analyse gemäß Artikel 6 Absatz 2 Buchstabe c eine Datenschutz-Folgenabschätzung durchgeführt werden.

34. Zweitens **würde die vorgeschlagene Verordnung die Möglichkeiten zur Speicherung von Daten unerwünschterweise ausweiten.** Bei der Beschreibung der Zwecke, für welche die Mitgliedstaaten den Umfang der in den Artikeln 5 bis 8 festgelegten Pflichten und Rechte beschränken können, verweist Artikel 11 der vorgeschlagenen Verordnung auf Artikel 23 Absatz 1 Buchstaben a bis e der DS-GVO. Die DS-GVO sieht solche Beschränkungen in Bezug auf besondere Kategorien von personenbezogenen Daten im Einklang mit den hohen Risiken für die betroffenen Personen nicht vor. Während Artikel 15 der Datenschutzrichtlinie für elektronische Kommunikation derzeit eine ähnliche Beschränkung vorsieht, sieht sie weniger Zwecke vor. Die neue vorgeschlagene Verordnung würde neue Beschränkungen für die Zwecke der „Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit“ (Artikel 23 Absatz 1 Buchstabe d der DS-GVO) und für „den Schutz sonstiger wichtiger Ziele des allgemeinen öffentlichen Interesses der Union oder eines Mitgliedstaats, insbesondere eines wichtigen wirtschaftlichen oder finanziellen Interesses der Union oder eines Mitgliedstaats, etwa im Währungs-, Haushalts- und Steuerbereich sowie im Bereich der öffentlichen

[20] ECLI:EU:C:2016:970, http://curia.europa.eu/juris/celex.jsf?celex=62015CJ0203.

Gesundheit und der sozialen Sicherheit“ (Artikel 23 Absatz 1 Buchstabe e der DS-GVO) ermöglichen. Diese Zwecke sind nicht nur neu, verglichen mit der Datenschutzrichtlinie für elektronische Kommunikation, sondern der letzte Zweck in Artikel 23 Absatz 1 Buchstabe d und der gesamte in Artikel 23 Absatz 1 Buchstabe e genannte Zweck sind extrem breit gefasst formuliert. Deshalb wird vorgeschlagen, den Verweis auf Artikel 23 Absatz 1 Buchstaben a bis e der DS-GVO zu streichen und stattdessen nur die derzeit in Artikel 15 der Datenschutzrichtlinie für elektronische Kommunikation genannten Zwecke zu nennen.

35. **Der Umfang der Pflicht, Nutzer über Sicherheitsrisiken zu informieren, ist minimalistisch**. Die Datenschutzgruppe begrüßt, dass Diensteanbieter Nutzer über Sicherheitsrisiken und über Maßnahmen zur Bekämpfung dieser Risiken, wie beispielsweise die Verschlüsselung, informieren müssen (Artikel 17 und Erwägungsgrund 37). Der Titel dieser Vorschrift lautet jedoch: „Information über erkannte Sicherheitsrisiken“. Die Tatsache, dass im Titel über erkannte Risiken gesprochen wird, lässt vermuten, dass sich diese Vorschrift lediglich auf (mögliche) Sicherheitslücken bezieht, während der Wortlaut der Vorschrift und des Erwägungsgrundes eher auf eine allgemeine Belehrung des Endnutzers hinweisen. Wenn ein Diensteanbieter beispielsweise feststellt, dass das Gerät eines Nutzers mit Schadsoftware infiziert ist und Teil eines Bot-Nets geworden ist, scheint diese Vorschrift den Anbieter direkt dazu zu verpflichten, den Nutzer über die resultierenden Risiken zu informieren. Der Anwendungsbereich dieser Vorschrift könnte jedoch geklärt werden und sollte nicht auf dieses spezielle Szenarium beschränkt sein. Die Vorschrift sollte mindestens die Sicherheitsrisiken abdecken, die in jedem Gerät festgestellt wurden, das der Anbieter dem Endnutzer als Teil des Abonnements zur Verfügung gestellt hat, wie beispielsweise Router und Mobiltelefone, und auch eine Belehrung über die Risiken umfassen, die mit dem Ändern der Einstellungen verbunden sind, die gemäß dem Grundsatz der datenschutzfreundlichen Voreinstellungen auf Schutz der Privatsphäre eingestellt wurden.

    Die Datenschutzgruppe empfiehlt, dass der Anwendungsbereich auf Anbieter von Software ausgeweitet wird, die elektronische Kommunikation ermöglicht (siehe Erwägungsgrund 8) und möglicherweise auch auf eine neue Kategorie: Anbieter von Technologie, die für die Sicherung der Kommunikation grundlegend ist, die aber keine Diensteanbieter sind (z. B. Anbieter von Verschlüsselungstechnologie). Im Fall dieser zuletzt genannten Ausweitung sollte darauf geachtet werden, dass sich diese Pflicht nicht mit der Meldepflicht für Sicherheitsverletzungen in anderen Instrumenten, wie der NIS-Richtlinie[21] und mit anderen Rechtsinstrumenten über Einrichtungen überschneidet, die Zertifikate ausstellen. Da die letztgenannte Kategorie von Technologieanbietern üblicherweise keinen direkten Kontakt mit Endnutzern hat, muss auch erklärt werden, wie sie die gemäß dieser Vorschrift vorgesehene Informationspflicht einhalten können.

[21] Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates vom 6. Juli 2016 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union (ABl. L 194 vom 19.7.2016, S. 1), http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.DEU

36. Die Datenschutzgruppe begrüßt die Bestimmungen der Artikel 2 und 13, die auf nummerngebundene interpersonelle Kommunikationsdienste Anwendung finden. Es ist jedoch nicht unmittelbar ersichtlich, warum für **funktional gleichwertige OTT-Zugangsdienste nicht ein entsprechendes Niveau des Schutzes der Privatsphäre verfügbar ist.**

37. Die Datenschutzgruppe findet auch die **fehlende Klarheit in Bezug auf die granulare Einwilligung für die Umkehrsuche in Verzeichnissen** bedenklich. Artikel 15 Absatz 2 der vorgeschlagenen Verordnung legt fest, dass Betreiber die Einwilligung der Endnutzer einholen müssen, bevor sie Suchfunktionen in Bezug auf die Daten aktivieren (siehe auch Erwägungsgrund 31). Die Datenschutzgruppe begrüßt die Harmonisierung der Einwilligungspflicht in Bezug auf die Aufnahme in Verzeichnisse, bedauert jedoch den Mangel an Granularität in Bezug auf verschiedene Arten der Suche. Basierend auf Artikel 12 Absatz 3 gestattet es die derzeitige Datenschutzrichtlinie für elektronische Kommunikation den Mitgliedstaaten, vorzuschreiben, dass eine gesonderte Einwilligung für die Umkehrsuche eingeholt werden muss. Diese Vorschrift lautet: *„Die Mitgliedstaaten können verlangen, dass eine zusätzliche Einwilligung der Teilnehmer eingeholt wird, wenn ein öffentliches Verzeichnis anderen Zwecken als der Suche nach Einzelheiten betreffend die Kommunikation mit Personen anhand ihres Namens und gegebenenfalls eines Mindestbestands an anderen Kennzeichen dient."* Basierend auf dieser Grundlage wird in vielen Mitgliedstaaten eine gesonderte Einwilligung für Umkehrsuchfunktionen verlangt. Dabei wird dem unterschiedlichen Maß an Bestimmbarkeit und folglich auch des Eindringens in die Privatsphäre der beiden Funktionen Rechnung getragen.

38. Ein eher formaler Punkt ist, dass **die Höhe der Geldbußen nicht für alle Verstöße gegen die Verordnung harmonisiert ist**. Gemäß der vorgeschlagenen Verordnung legen die Mitgliedstaaten Vorschriften über Sanktionen für die in den Artikeln 23 Absätze 4 und 6 und in Artikel 24 der vorgeschlagenen Verordnung genannten Verstöße fest. Im Interesse einer größeren Übereinstimmung sollte dies in der Verordnung über die Privatsphäre selbst geregelt werden.

39. Schließlich **stützt sich die vorgeschlagene Verordnung auf Begriffsbestimmungen, die zu „beweglichen Zielen" werden können**. In Bezug auf eine Reihe von Schlüsselkonzepten verweist die vorgeschlagene Verordnung auf ein anderes Rechtsinstrument, das derzeit in der Entwurfsform vorliegt: nämlich auf den vorgeschlagenen Kodex (siehe beispielsweise Artikel 4 Absatz 1 Buchstabe b). Zwei wichtige Beispiele hierfür sind die Begriffsbestimmung von „Endnutzer", die derzeit natürliche und juristische Personen umfasst und die Begriffsbestimmungen von „elektronischer Kommunikationsdienst" und „interpersoneller Kommunikationsdienst", die in der vorgeschlagenen Verordnung in Artikel 4 Absatz 1 Buchstabe b dargelegt und im letzten Fall in Artikel 4 Absatz 2 weiter spezifiziert werden, so dass auch Dienste darunter fallen, die im Kodex ausdrücklich

ausgeschlossen sind.[22] Die vorliegende Stellungnahme basiert auf den derzeitigen Begriffsbestimmungen. Es ist jedoch recht wahrscheinlich, dass sich der vorgeschlagene Kodex und/oder Schlüsselkonzepte desselben ändern werden. Das hätte auch unmittelbare Auswirkungen auf die Verordnung über die Privatsphäre. Idealerweise sollten alle Begriffe, die aus dem Kodex stammen, unabhängig in der Verordnung über die Privatsphäre definiert werden. Alternativ sollte die vorgeschlagene Verordnung zumindest Klarstellungen enthalten, wenn Begriffe verwendet werden, deren Begriffsbestimmungen von den im Kodex verwendeten abweichen (beispielsweise der vorstehend genannte Fall, dass unter die Begriffsbestimmung von „interpersonelle Kommunikationsdienste" auch Nebendienste fallen. Sollte dies jedoch nicht möglich sein, schlägt die Datenschutzgruppe vor, dass alle am Gesetzgebungsverfahren beteiligten Akteure sicherstellen, dass sowohl die vorgeschlagene Verordnung als auch der Kodex zur selben Zeit debattiert werden und dass zeitgleich über sie abgestimmt wird, damit alle Betroffenen den Anwendungsbereich und die Auswirkungen der neuen Instrumente richtig bewerten können.

5. VORSCHLÄGE FÜR KLARSTELLUNGEN ZUR SCHAFFUNG VON RECHTSSICHERHEIT

Zusätzlich zu den vorstehend ausgeführten Punkten möchte die Datenschutzgruppe noch auf einige Vorschriften in der vorgeschlagenen Verordnung hinweisen, bei denen weitere Klärungen hilfreich wären. Die Datenschutzgruppe hält diese Klarstellungen für erforderlich, um die Rechtssicherheit aller Interessengruppen zu verbessern und damit die Verordnung über die Privatsphäre in der gesamten EU einheitlich verstanden und angewendet wird.

KLARSTELLUNGEN ZUM ANWENDUNGSBEREICH

40. Die Datenschutzgruppe schlägt in Bezug auf den Anwendungsbereich der vorgeschlagenen Verordnung die folgenden Klarstellungen vor:

    a. **Der Begriff „Endnutzer" sollte alle einzelnen Nutzer umfassen**. Artikel 2 Absatz 14 des Kodex definiert „Endnutzer" als einen Nutzer, der keine öffentlichen Kommunikationsnetze oder öffentlich zugänglichen elektronischen Kommunikationsdienste bereitstellt. Es sollte geklärt werden, dass Personen, die zu Netzwerken beitragen - beispielsweise zu Mesh-Netzwerken mit ihrem Wi-Fi-Router - nicht vom Anwendungsbereich des Schutzes der vorgeschlagenen Verordnung ausgeschlossen werden.

[22] Nach Artikel 4 Absatz 2 der vorgeschlagenen Verordnung beispielsweise schließt der Begriff „interpersoneller Kommunikationsdienst" auch Dienste ein, „die eine interpersonelle und interaktive Kommunikation lediglich als untrennbar mit einem anderen Dienst verbundene untergeordnete Nebenfunktion ermöglichen", während Artikel 2 Absatz 5 des Kodex solche Dienste ausdrücklich aus der Begriffsbestimmung ausschließt. (Im Kodex wird der „interpersonelle Kommunikationsdienst" in der weiter gefassten Kategorie „elektronischer Kommunikationsdienst" in Artikel 2 Absatz 4 erfasst.)

b. **Es sollte klargestellt werden, dass sich der räumliche Anwendungsbereich auf alle Endnutzer in der Union erstreckt**. Artikel 3 Absatz 1 Buchstabe a sieht vor, dass die vorgeschlagene Verordnung für die Bereitstellung elektronischer Kommunikationsdienste für Endnutzer „in der Union" gilt, während Artikel 3 Absatz 1 Buchstabe c vorsieht, dass sie für den Schutz von Endeinrichtungen der Endnutzer, die sich in der Union befinden („located in the Union") (Hervorhebung hinzugefügt) gilt. Dies unterscheidet sich in den verschiedenen Übersetzungen. In der deutschen Übersetzung ist diese Unterscheidung nicht enthalten, während es in anderen, wie der französischen, spanischen und dänischen der Fall ist. Aus Erwägungsgrund 9 ergibt sich eindeutig, dass der Anwendungsbereich weit gefasst sein soll, unabhängig davon, ob die Dienste von außerhalb der Union bereitgestellt werden oder ob die Verarbeitung in der Union stattfindet. Deshalb wird vorgeschlagen, „located" in Artikel 3 Absatz 1 Buchstabe c zu streichen, um diesen breiten Anwendungsbereich zu unterstreichen.

c. **Die vorgeschlagene Verordnung scheint vertrauliche Kommunikationen nur *während ihrer Übertragung* zu schützen und nicht, wenn sie *gespeichert* sind**. Nach dem derzeitigen Ansatz der vorgeschlagenen Verordnung wird der Schwerpunkt auf den Schutz bei der Übertragung der Kommunikation gelegt. Siehe beispielsweise Erwägungsgrund 15, der festlegt, dass das Verbot des Abfangens von Kommunikationsdaten während ihrer Übertragung gelten sollte, d. h. bis zum Empfang der Inhalte der elektronischen Kommunikation durch den bestimmungsgemäßen Empfänger. Der Anwendungsbereich des Schutzes basiert auf einem veralteten Rahmenkonzept von Kommunikation. Ein Großteil der Kommunikationsdaten bleibt auch nach ihrem Empfang noch von Dienstleistern gespeichert. Es sollte daher sichergestellt werden, dass die Vertraulichkeit dieser Daten dann weiterhin gewährleistet ist. Darüber hinaus ist die eigentliche Übertragung von Daten im Rahmen der Kommunikation zwischen Teilnehmern desselben Cloud-basierten Dienstes (zum Beispiel Webmail-Anbieter) minimal: Das Senden einer E-Mail wird dabei meistens nur in der Datenbank des Anbieters widergespiegelt, ohne dass eine tatsächliche Übertragung der Kommunikation zwischen Sender und Empfänger stattfindet. Das Argument, dass dies bereits durch die DS-GVO abgedeckt ist, überzeugt nicht: Die vollumfängliche Absicht der vorgeschlagenen Verordnung ist der Schutz jeder vertraulichen Kommunikation, unabhängig von den technischem Mitteln solcher Kommunikation. Möglicherweise ist dies nur ein redaktioneller Fehler, da sich das Verbot in Artikel 5 auf die „Speicherung" und die „Verarbeitung" bezieht.

d. **Alle öffentlichen Internetzugänge über drahtlose Netze sollten in den Anwendungsbereich fallen**. Da die Nutzung drahtloser Hotspots verbreitet ist, ist es nur logisch, dass kein Zweifel an der Vertraulichkeit von Kommunikation bestehen sollte, die über solche Hotspots übertragen wird. Der Versuch, dies in der Verordnung zu klären, schlägt jedoch fehl, da der Anwendungsbereich lediglich auf Netzwerke ausgeweitet wird, die einer „unbestimmten Gruppe von Endnutzern" bereitgestellt wird

(Erwägungsgrund 13). Die Begriffe „unbestimmte Gruppe von Endnutzern“ und „geschlossene Gruppe von Endnutzern“ müssen definiert werden. Es sollte insbesondere geklärt werden, dass auch sichere drahtlose Netze (z. B. solche mit einem Passwort) in den Anwendungsbereich fallen, wenn dieses Passwort einer theoretisch unbegrenzten Gruppe von Nutzern zur Verfügung gestellt wird, deren Identität nicht im Voraus bestimmt werden kann (z. B. Kunden in einem Kaffee, Besucher eines Flughafens). Das diesem Kontext zugrundeliegende Prinzip ist, dass entsprechend der früheren Stellungnahme der Datenschutzgruppe zur Datenschutzrichtlinie für elektronische Kommunikation *„vom Anwendungsbereich des e-Datenschutzinstruments nur Dienste ausgenommen werden können, die in einer offiziellen Situation oder einer Beschäftigungssituation ausschließlich für arbeitsbezogene oder offizielle Zwecke erfolgen, oder technische Kommunikation zwischen nicht-öffentlichen Stellen und öffentlichen Stellen ausschließlich zur Kontrolle von Arbeits- oder Geschäftsprozessen, sowie die Nutzung von Diensten für ausschließlich häusliche Zwecke“.* (S. 8).

e. **Daten, die erhoben werden, während digitale Rundfunk- und Fernsehdienste angeboten werden, sollten unter die vorgeschlagene Verordnung fallen.** Angesichts der sensiblen Natur des Zuschauerverhaltens, das persönliche Interessen und Eigenschaften der Zuschauer offenlegt, sollte in der Verordnung über die Privatsphäre festgelegt werden (möglicherweise in einem Erwägungsgrund), dass der Ausschluss von Diensten, die „Inhalte über elektronische Kommunikationsnetze“ anbieten, von der Begriffsbestimmung von „elektronischen Kommunikationsdiensten“ nicht bedeutet, dass sich die Diensteanbieter, die sowohl elektronische Kommunikationsdienste als auch Inhaltsdienste anbieten, außerhalb des Anwendungsbereiches der Verordnung über die Privatsphäre befinden, die auf die Betreiber elektronischer Kommunikationsdienste abzielt. Dies ist insbesondere relevant, da die Bereitstellung von Diensten, „die Inhalte über elektronische Kommunikationsnetze (...) anbieten“, gemäß dem vorgeschlagenen Kodex (Artikel 2 Absatz 4) von der Definition „elektronischer Kommunikationsdienste“ ausgenommen ist.

f. **Kommunikationsdaten sind generell personenbezogene Daten**. In Erwägungsgrund 4 wird gesagt, dass Kommunikationsdaten personenbezogene Daten enthalten können. Die meisten Kommunikationsdaten sind jedoch personenbezogene Daten,[23] und größtenteils sind sie ziemlich intimer und sensibler Natur. Deshalb sollte dieser Passus dahingehend geändert werden, dass diese Daten generell personenbezogene Daten sind.

g. **Plattform-interne Nachrichten zählen zu vertraulicher Kommunikation**. In Erwägungsgrund 1 wird erklärt, dass der Grundsatz der Vertraulichkeit für

[23] Siehe beispielsweise die Urteile des Gerichtshofs vom 6. November 2003 in der Rechtssache C-101/01, Rdnr. 24 (in Bezug auf eine Telefonnummer), vom 19. Oktober 2016 in der Rechtssache C-582/14 (Breyer), Rdnr. 49 (in Bezug auf dynamische IP-Adressen) und vom 8. April 2014 in den verbundenen Rechtssachen C-239/12 und C-594/12 (Digital Rights Ireland), Rdnr. 26 bis 27 (in Bezug auf die Sensibilität von Metadaten).

„gegenwärtige und künftige Kommunikationsmittel“ gilt. Der Erwägungsgrund führt eine Liste solche Mittel an, einschließlich der „Übermittlung persönlicher Nachrichten über soziale Medien“. Damit sollen wahrscheinlich private Nachrichten zwischen den Nutzern sozialer Netzwerke mit eingeschlossen werden (z. B. Facebook oder Twitter) oder Nachrichten, die auf einer Zeitleiste gepostet werden und einer begrenzten Zahl Personen zur Verfügung stehen. Der Wortlaut ist jedoch nicht klar genug.

h. **Wie die Verordnung über die Privatsphäre auf Kommunikationsvorgänge zwischen Maschinen Anwendung findet.** Wie in Ziffer 9 gesagt, begrüßt die Datenschutzgruppe die Ausweitung auf den Schutz von Kommunikationsvorgängen zwischen Maschinen. Dies wird jedoch nur in Erwägungsgrund 12 erwähnt und in keinem entsprechenden Artikel. Dieser Schutz ist wünschenswert, da solche Kommunikationen häufig Informationen enthalten, die durch das Recht auf Privatsphäre geschützt sind. Andererseits sollte eine eng gefasste Kategorie von reinen Kommunikationsvorgängen zwischen Maschinen ausgenommen werden, wenn diese keine Auswirkungen auf die Privatsphäre oder die Vertraulichkeit der Kommunikation haben. Dies ist beispielsweise der Fall, wenn eine solche Kommunikation auf der Durchführung eines Übertragungsprotokolls zwischen Netzkomponenten (wie Server oder Schalter) über den jeweiligen Aktivitätsstatus beruht.

   Die Anwendung der Verordnung über die Privatsphäre bedarf im Zusammenhang mit dem Bereich intelligenter Verkehrssysteme Erläuterungen. Es ist vorgesehen, dass Fahrzeuge ständig Daten über Funk senden, die eine eindeutige Kennung enthalten. Ohne den zusätzlichen Schutz in der Verordnung über die Privatsphäre in Bezug auf Kommunikationsdaten könnte dies zu einer ständigen Verfolgung der Fahrgewohnheiten des Fahrzeuglenkers, der zurückgelegten Wege und der gefahrenen Geschwindigkeiten führen. Artikel 2 Absatz 1 des Kodex enthält jedoch eine neue und erweiterte Begriffsbestimmung von Kommunikationsnetzen. Sie umfassen Übertragungssysteme, die keine zentrale Verwaltungskapazität haben und die Übertragung von Signalen über Funk ermöglichen. Erwägungsgrund 14 der Verordnung über die Privatsphäre legt fest, dass solche Daten elektronische Kommunikationsdaten sind. Basierend auf Artikel 5 der vorgeschlagenen Verordnung ist jede Art des Abfangens, Überwachens oder Speicherns dieser elektronischen Kommunikationsdaten untersagt, sofern nicht eine der Ausnahmen Anwendung findet. Dennoch besteht Interesse an der Verarbeitung dieser Daten, damit es Objekten wie selbstfahrenden Autos und Geräten ermöglicht wird, sich gegenseitig über ihre Nähe oder andere Gefahren zu informieren. Die Frage ist, welche Ausnahme in diesem Fall Anwendung finden würde. Die Einwilligung der Endnutzer ist keine realisierbare Ausnahme, da es notwendig werden könnte, diese Daten immer verarbeiten zu können. Anbieter sollten sich deshalb auf eine spezifische Ausnahme verlassen können, damit es Objekten wie selbstfahrenden Autos und Geräten ermöglicht wird, sich gegenseitig über ihre Nähe oder andere Gefahren zu informieren.

41. Die Datenschutzgruppe schlägt in Bezug auf den Begriff „Einwilligung“ und seine Anwendung folgende Präzisierungen im aktuellen Vorschlag vor:
    a. **Wie der Begriff der Einwilligung im Zusammenhang mit juristischen Personen anzuwenden ist.** Erwägungsgrund 3 stellt fest, dass die Verordnung sicherstellen sollte, dass Bestimmungen der DS-GVO auch auf Endnutzer anzuwenden sind, die juristische Personen sind. Dies bezieht sich gemäß diesem Erwägungsgrund auch auf die Begriffsbestimmung für „Einwilligung“ in der DS-GVO (siehe auch Erwägungsgrund 18). Wie in Ziffer 13 festgestellt wurde, begrüßt die Datenschutzgruppe die ausdrückliche Einbeziehung juristischer Personen in den Anwendungsbereich der Verordnung. Die praktische Anwendung dieses Grundsatzes ist jedoch nicht klar. Die Begriffsbestimmung von „Einwilligung“ in der DS-GVO verlangt, dass diese „in informierter Weise“ erfolgt und dass die betroffene Person eine Willensbekundung „in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung“ abgibt (Artikel 4 Absatz 11 DS-GVO). Es muss geklärt werden, wann eine juristische Person tatsächlich als „informiert“ angesehen werden kann und wann eine solche Willensbekundung durch eine juristische Person vorliegt.
    b. In diesem Zusammenhang sei auch angemerkt, dass der Arbeitgeber in den meisten Fällen keine Einwilligung für seine Arbeitnehmer erteilen kann. Denn fordert ein Arbeitgeber die Einwilligung von einem Arbeitnehmer und kann angesichts der ungleichen Machtverteilung ein tatsächlicher oder potenzieller Nachteil aus einer Nichteinwilligung erwachsen, ist die Einwilligung nicht gültig ist, da sie nicht ohne Zwang erfolgte.[24] In Bezug auf **Unternehmen, die Personen Geräte oder Einrichtungen zur Verfügung stellen, gibt es in der vorgeschlagenen Verordnung keine (geeignete) Ausnahme** vom Verbot von Eingriffen. Ein Beispiel ist, wenn ein Arbeitgeber ein Telefon aktualisieren möchte, das der Arbeitnehmer von dem Unternehmen erhalten hat. Im zweiten Beispiel bietet ein Arbeitgeber den Angestellten Leasing-Fahrzeuge an und lässt einen Dritten für Verwaltungszwecke über eine Onboard-Unit in den Autos Standortdaten erheben. In beiden Fällen hat der Arbeitgeber Interesse an Eingriffen in die Geräte.

       In Bezug auf diese Eingriffe kann nicht gesagt werden, dass sie für die Bereitstellung eines Dienstes der Informationsgesellschaft (Artikel 8 Absatz 1 Buchstabe c) oder für die Messung des Webpublikums (Artikel 8 Absatz 1 Buchstabe d) nötig sind. Dieses Problem könnte durch die Schaffung einer neuen Ausnahme gelöst werden, damit Situationen erfasst werden, in denen

[24] Siehe die Stellungnahme 15/2011 zur Definition von „Einwilligung“ (WP 187), die Stellungnahme 8/2001 zur Verarbeitung personenbezogener Daten von Beschäftigten und die neue (gleichzeitig mit der vorliegenden Stellungnahme angenommene) Stellungnahme zur Datenverarbeitung am Arbeitsplatz.

(i) der Arbeitgeber bestimmte Einrichtungen im Zusammenhang mit dem Arbeitsverhältnis zur Verfügung stellt, (ii) der Arbeitnehmer der Nutzer dieser Einrichtung ist und (iii) der Eingriff für das Funktionieren der Einrichtung unbedingt nötig ist (das impliziert die Anwendung der Grundsätze der Verhältnismäßigkeit und der Subsidiarität in Bezug auf die Erhebung der Daten). Nur wenn diese Bedingungen erfüllt sind, sollte der Arbeitgeber die Möglichkeit für Eingriffe in das Gerät des Endnutzers haben.

c. **Verbesserung der Kontrolle zur Abstellung der automatischen Anrufweiterschaltung**. Artikel 14 bietet eine wichtige Kontrolle für Endnutzer, eine von einem Dritten veranlasste automatische Anrufweiterschaltung abzustellen. Dieser Schutz kann weiter verbessert werden, indem schon vorher die Einwilligung des Endnutzers in die Einleitung der Weiterschaltung eingeholt werden muss.

KLARSTELLUNG ZUM STANDORT UND ZU ANDEREN METADATEN

42. Die Datenschutzgruppe schlägt vor, dass die folgenden Punkte hinsichtlich Standortdaten und anderer Metadaten geklärt werden.
    a. Die Bedeutung von **„Standortdaten, die in einem anderen Zusammenhang als dem der Bereitstellung elektronischer Kommunikationsdienste erzeugt werden“** in Erwägungsgrund 17 sollte geklärt werden. Es ist nicht klar, ob sich dies auf Standortdaten bezieht, die beispielsweise mit Hilfe von Apps erhoben wurden, die die Daten von GPS-Funktionen in intelligenten Geräten nutzen und/oder anhand von nahe gelegenen Wi-Fi-Routern Standortdaten generieren und/oder auf Standortdaten, die mit internen Navigationsassistenten erhoben werden und/oder auf andere Arten, Standortdaten zu generieren. Durch diesen Mangel an Klarheit entsteht Rechtsunsicherheit hinsichtlich des Anwendungsbereichs der Pflicht. Standortdaten in den Endeinrichtungen natürlicher Personen sind jedenfalls personenbezogene Daten und folglich unterliegt ihre Verarbeitung den Pflichten aus der DS-GVO.
    b. Es sollte klargestellt werden, dass **die rechtmäßige Verarbeitung von Standortdaten und anderen Metadaten in den meisten Fällen <u>keine</u> eindeutigen Kennungen erfordert**. In Erwägungsgrund 17 wird die Erstellung von Heatmaps als ein Beispiel für eine gewerbliche Verwendung elektronischer Kommunikationsmetadaten durch Betreiber elektronischer Kommunikationsdienste genannt. Für das Erstellen einer grundlegenden Heatmap werden jedoch keine eindeutigen Kennungen benötigt, es reicht das rein statistische Zählen. Ein weiteres in dem Erwägungsgrund genanntes Beispiel, die Benutzung und Belastung bestehender Infrastruktur, kann auch durch bestimmte Messpunkte gezählt werden, beispielsweise, indem zusammenfassende Statistiken zur Nutzung von Verkehrstürmen erstellt werden, um einen Hinweis auf die Belastung an einem Standort zu einem bestimmten Zeitpunkt zu liefern, ohne dass auch die Identität der betroffenen Personen benötigt wird.

Darüber hinaus nennt der Erwägungsgrund die Anzeige von Verkehrsbewegungen in bestimmte Richtungen über einen bestimmten Zeitraum, bei der eine Kennung benötigt würde, damit die Positionen von Einzelpersonen in bestimmten Zeitabständen miteinander verknüpft werden können. Mit diesem Beispiel scheint der Erwägungsgrund die weitere Verarbeitung dieser Daten zu legitimieren, um die Analyse von „Big Data" zu unterstützen. Die einzige Bedingung, die in der vorgeschlagenen Verordnung an diese Art der Verarbeitung geknüpft wird, ist die Pflicht zur Durchführung einer Datenschutz-Folgenabschätzung, wenn die Verarbeitung *voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat*. Diese Bedingung reicht nicht aus. Sie verstößt auch gegen die Pflicht nach Artikel 6, nach der diese Art Verarbeitung nur mit der Einwilligung der Nutzer durchgeführt werden darf und nur, wenn die Daten nicht anonymisiert werden können, sie also keine eindeutigen Kennungen aufweisen. Häufig können Nutzer der Erhebung ihrer Daten zur Geolokalisierung durch die Betreiber elektronischer Kommunikationsdienste nicht widersprechen, wenn eine solche Erhebung technisch nötig ist, um die Mitteilung an den Nutzer zu übertragen oder wenn eine solche Verarbeitung zur Bereitstellung des angeforderten Dienstes (beispielsweise Navigation) erforderlich ist. In früheren Stellungnahmen zog die Datenschutzgruppe die Schlussfolgerung, dass solche Standortdaten von intelligenten Geräten personenbezogene Daten sensibler Natur sind und dass die Vorteile der Analyse dieser Daten nicht Vorrang vor dem Recht der Nutzer auf Schutz der Vertraulichkeit ihrer Kommunikationsmetadaten hat und dass sie auch nicht Vorrang vor den allgemeinen Rechten auf Datenschutz nach der DS-GVO hat. Deshalb muss in dem Erwägungsgrund zumindest spezifiziert werden, dass die Betreiber im Fall einer weiteren Verarbeitung der Standortdaten oder anderer Metadaten die Pflichten aus Artikel 25 DS-GVO einhalten müssen. Das bedeutet, dass mindestens die folgenden Maßnahmen ergriffen werden müssen:

(i) die Verwendung temporärer Pseudonyme;

(ii) die Löschung umgekehrter Umsetzungstabellen zwischen diesen Pseudonymen und den Originaldaten zur Identifizierung;

(iii) Bündelung bis zu einer Ebene, auf der der einzelne Nutzer nicht mehr anhand seiner besonderen Pfade identifiziert werden kann und

(iv) Löschung von Ausreißern, in Bezug auf die eine Identifizierung nach wie vor möglich wäre (alle diese Maßnahmen müssen zusammen angewendet werden).

Schließlich muss die Verordnung über die Privatsphäre die Parteien, die mit der Verarbeitung von Standortdaten und anderen Metadaten befasst sind, zur Veröffentlichung ihrer Methoden zur Anonymisierung und zur weiteren Bündelung verpflichten, ohne dass dies die gesetzlich geschützte Geheimhaltung berührt. Dies würde es sowohl den Aufsichtsbehörden als auch der breiten Öffentlichkeit ermöglichen, einfach zu überprüfen, ob die gewählte Methode angemessen ist.

43. Die Datenschutzgruppe schlägt vor, Folgendes in Bezug auf unerbetene Kommunikation zu klären:
    a. **Die Formulierung des Verbots von Direktwerbung ohne Einwilligung**. In Artikel 16 Absatz 1 der vorgeschlagenen Verordnung wird festgestellt, dass elektronische Kommunikationsdienste verwendet werden „können", um Direktwerbung (mit Einwilligung) zu senden. Er enthält jedoch kein ausdrückliches Verbot, Direktwerbung ohne Einwilligung zu senden (an Endnutzer zu richten oder ihnen vorzulegen). Dies steht im Gegensatz zu dem in den anderen Vorschriften gewählten Ansatz, nach dem zuerst ein Verbot formuliert wird, dem dann bestimmte spezifische Ausnahmen folgen. Die derzeitige Formulierung lässt einen weniger strikten Ansatz vermuten (was vermutlich nicht beabsichtigt ist). Die Datenschutzgruppe schlägt einen leicht geänderten Wortlaut für den aktuellen Artikel 13 Absatz 1 der Datenschutzrichtlinie für elektronische Kommunikation vor: „Die Verwendung von elektronischen Kommunikationsdiensten durch natürliche oder juristische Personen, einschließlich persönlicher Anrufe und Anrufe über automatische Anruf- und Kommunikationssysteme, auch halbautomatischer Systeme, die die angerufene Person mit einer einzelnen Person verbinden, von Faxgeräten oder elektronischer Post oder eine andere Verwendung von elektronischen Kommunikationsdiensten für die Zwecke der Direktwerbung darf nur in Bezug auf Endnutzer gestattet werden, die vorher ihre Einwilligung erteilt haben."
    b. **Der Anwendungsbereich der Vorschriften zu Werbung und Anrufen bei bestehenden Kontakten.** Artikel 16 Absatz 2 sieht vor, dass eine Person, wenn sie von einem bestehenden Kunden elektronische Kontaktangaben für E-Mail erhält, diese zur Direktwerbung für eigene ähnliche Produkte oder Dienstleistungen verwenden darf, wenn bei Erlangung der Angaben und bei jedem Versand einer Nachricht klar und deutlich die Möglichkeit aufgezeigt wird, einer solchen Nutzung kostenlos und auf einfache Weise zu widersprechen. Derzeit ist dies auf gewerbliche Kontakte beschränkt, die „im Zusammenhang mit dem Verkauf eines Produkts oder einer Dienstleistung" erhalten wurden und für Werbung für eigene ähnliche Produkte oder Dienstleistungen. Da die Vorschriften zur Direktwerbung gleichermaßen für nicht-kommerzielle Werbetätigkeiten (z. B. von Wohltätigkeitseinrichtungen und politischen Parteien) gelten, sollte die vorliegende Vorschrift geändert werden, damit sie gleichermaßen für nicht-gewerbliche Organisationen gilt, die bestehende Unterstützer kontaktieren, wenn sie ihre eigenen ähnlichen Ziele oder Ideen bewerben. Hier sollte das gleiche Recht auf Widerspruch Anwendung finden, wie bei der Direktwerbung. Zusätzlich sollte im Hinblick auf elektronische Kommunikation für einen gewerblichen, wohltätigen oder politischen Zweck eine Frist für die Gültigkeit „bestehender Kundenkontakte" gesetzt werden, das auch für Direktwerbung gilt. Haben sich die Mitgliedstaaten für ein System des Widerspruchs gegen persönliche Werbeanrufe entschieden, hat das Vorliegen einer „bestehenden Kundenkontakt"- Beziehung Vorrang vor der Aufnahme in einer Do-Not-

Call-Liste. Unter diesen Umständen haben die Endnutzer keine wirksame Möglichkeit, belästigende Anrufe von Unternehmen oder Organisationen zu verhindern, mit denen sie Kontakt hatten, aber nicht mehr wünschen. Deshalb sollte die Verordnung als Daumenregel eine Gültigkeit für die Ausnahme „bestehender Kunde“ in Bezug auf die berechtigten Erwartungen der betroffenen Endnutzer festlegen, beispielsweise von einem oder zwei Jahren.

c. **Die Anwendung der Vorschriften zur Direktwerbung auf juristische Personen**. Artikel 16 Absatz 5 der vorgeschlagenen Verordnung sieht vor, dass die Mitgliedstaaten sicherstellen, dass die berechtigten Interessen von Endnutzern, die juristische Personen sind, in Bezug auf unerbetene Kommunikation ausreichend geschützt werden. In Artikel 13 Absatz 5 der gegenwärtigen Datenschutzrichtlinie für elektronische Kommunikation werden die berechtigten Interessen anderer Teilnehmer als natürlicher Personen beschrieben. Es ist unklar, welche Auswirkungen diese Änderung des Wortlauts hat. Es sollte in den Erwägungsgründen dargelegt werden, dass diese Änderung nicht die Absicht widerspiegelt, ein niedrigeres Schutzniveau zu bieten. In diesem Zusammenhang bezieht sich das Verbot der Direktwerbung ohne Einwilligung auf „Endnutzer, die natürliche Personen sind und ihre Einwilligung erteilt haben“ (Hervorhebung hinzugefügt). Es sollte geklärt werden, dass dazu auch natürliche Personen zählen, die *für* juristische Personen *arbeiten*. Andererseits wäre eine Einwilligung nicht erforderlich, um mit juristischen Personen über allgemeine Kontaktdaten Kontakt aufzunehmen, die diese für diesen Zweck veröffentlicht haben (wie „info@companyname.eu“).

d. **Die Anwendung der Vorschriften zur Direktwerbung auf diejenigen, die als (politische) Repräsentanten tätig sind:** Es ist möglich, dass Artikel 16 in seiner derzeitigen Fassung Mitteilungen, in denen wirtschaftliche Bedenken oder Interessen dargelegt werden und die an gewählte Vertreter gerichtet sind, verhindert. Es sollte geklärt werden, dass die Verordnung solche Kommunikationen nicht verhindert.

KLARSTELLUNGEN ZUR ANWENDUNG VON GRUNDRECHTSINSTRUMENTEN

44. **Die Anwendung der Charta und der EMRK auf nationale Rechtsvorschriften zur Vorratsdatenspeicherung** sollte weiter geklärt werden. Erwägungsgrund 26 sieht vor, dass alle Maßnahmen, die die Mitgliedstaaten zum Schutz des öffentlichen Interesses ergreifen, wie beispielsweise rechtmäßige Maßnahmen zum Abfangen elektronischer Kommunikation, im Einklang mit der Charta stehen müssen (zusätzlich zur EMRK). Dies ist wünschenswert, da es mit der Begründung in der Rechtssache *Tele2/Watson* übereinstimmt, dass alle nationalen Ausnahmen zu EU-Rechtsvorschriften zum Schutz der Datenverarbeitung der Charta unterliegen (und dass folglich Verletzungen durch nationale Rechtsvorschriften dem Europäischen Gerichtshof vorgelegt werden können). Artikel 11 der vorgeschlagenen Verordnung stellt jedoch lediglich fest, dass Beschränkungen des Umfangs der Artikel 5 bis 8 der vorgeschlagenen Verordnung den Wesensgehalt der Grundrechte und Grundfreiheiten achten und eine notwendige und verhältnismäßige Maßnahme darstellen müssen. Hier sollten die Charta und die EMRK ausdrücklich erwähnt werden.

45. **Schutz der Vertraulichkeit der Kommunikation auch nach Artikel 8 der EMRK**. In Absatz 1.1 der Begründung und in Erwägungsgrund 1 wird erklärt, dass die vorgeschlagene Verordnung Artikel 7 der Charta umsetzt. Dies wird in Erwägungsgrund 19 wiederholt. Das Grundrecht auf Vertraulichkeit der Kommunikation wird jedoch nicht nur in dieser Vorschrift geschützt, sondern auch nach Artikel 8 EMRK. Ein entsprechender, ausdrücklicher Hinweis in einem Artikel der vorgeschlagenen Verordnung würde weiter bekräftigen, dass auch die gesamte einschlägige Rechtsprechung des Europäischen Gerichtshofs für Menschenrechte bei der Bewertung der (endgültigen) Verordnung berücksichtigt werden muss. Dieser Bezug befindet sich übrigens bereits in den Erwägungsgründen 20 (bezüglich Endeinrichtungen) und 26 (bezüglich des rechtmäßigen Abfangens) und wird weiter gestützt von den Überlegungen in Absatz 2.1 der Begründung (zur Beziehung zwischen der Charta und der EMRK im Zusammenhang mit juristischen Personen), aber nicht in einem der einschlägigen Artikel, wie Artikel 11 Absatz 1.

WEITERE KLARSTELLUNGEN

46. Es sollte präzisiert werden, dass **die aus der DS-GVO erwachsenden Pflichten (beispielsweise in Bezug auf die Vorschriften zu Datenschutzverletzungen und Datenschutz-Folgenabschätzungen) anwendbar bleiben**, wenn Parteien personenbezogenen Daten im Zusammenhang mit elektronischen Kommunikationsdaten verarbeiten. Da in Erwägungsgrund 5 steht, dass die vorgeschlagene Verordnung *Lex Specialis* zur DS-GVO ist und dass die Verarbeitung elektronischer Kommunikationsdaten durch Betreiber elektronischer Kommunikationsdienste nur im Einklang mit der vorgeschlagenen Verordnung erlaubt sein sollte, könnte die Frage gestellt werden, ob bestimmte Pflichten nach der DS-GVO auch im Zusammenhang mit der vorgeschlagenen Verordnung anzuwenden sind. Dies trifft insbesondere in Fällen zu, in denen die vorgeschlagene Verordnung so ausgelegt werden könnte, dass sie eine bestimmte Pflicht vorsieht, während die DS-GVO diese abdeckt. Folgendes sind diesbezügliche Beispiele:
    (i) die vorgeschlagene Verordnung verpflichtet zu einer bestimmten Meldung „erkannter“ Sicherheitsrisiken (Artikel 17) (siehe auch Ziffer 35), die DS-GVO enthält dagegen eine Vorschrift zur Meldung von Datenschutzverletzungen (Artikel 33 und 34);
    (ii) In der vorgeschlagenen Verordnung wird darauf hingewiesen, dass die Durchführung einer Datenschutz-Folgenabschätzung und eine Konsultation der Aufsichtsbehörde unter bestimmten Umständen in Übereinstimmung mit der DS-GVO vorgeschrieben sind (Erwägungsgründe 17 und 19 und Artikel 6 Absatz 3 Buchstabe b), während in der DS-GVO bereits festgelegt ist, wann eine Datenschutz-Folgenabschätzung durchzuführen ist und wann eine Konsultation erforderlich ist (Artikel 35 und 36);
    (iii) Es wird nicht ausdrücklich gesagt, dass wenn alle für eine Ausnahme von dem Verbot zur Verarbeitung nach Artikel 5 der vorgeschlagenen Verordnung erforderlichen Bedingungen erfüllt sind, dennoch alle einschlägigen Vorschriften aus der DS-GVO erfüllt werden müssen, die die Verarbeitung personenbezogener Daten betreffen, und dass jede sonstige

Verarbeitung nach der DS-GVO verboten ist. Es sollte klargestellt werden, dass der in Artikel 6 Absatz 4 der DS-GVO niedergelegte Test zur Prüfung der Vereinbarkeit deshalb keine Anwendung findet.

(iv) Die vorgeschlagene Verordnung über die Privatsphäre sieht kein Zertifizierungsverfahren ähnlich dem Verfahren aus Artikeln 42 und 43 der DS-GVO vor. Da der Anwendungsbereich von Artikel 42 der DS-GVO streng genommen auf die Entwicklung datenschutzspezifischer Zertifizierungsverfahren, Siegel oder Prüfzeichen beschränkt ist, mit denen die Einhaltung der DS-GVO nachgewiesen werden soll, sollte überlegt werden, ob eine ähnliche Bestimmung eingeführt werden sollte, um die Zertifizierung von Verarbeitungsvorgängen, Standards, Produkten oder Diensten im Hinblick auf ihre Einhaltung der Verordnung über die Privatsphäre zu ermöglichen.

Um sicherzustellen, dass diese fehlende Klarheit nicht als Argument zur Senkung des von der vorgeschlagenen Verordnung gebotenen Schutzniveaus verwendet wird, sollte deutlich gemacht werden, dass die für die Verarbeitung Verantwortlichen in allen diesen Fällen auch die DS-GVO einhalten müssen.

47. Darüber hinaus sollte klargestellt werden, dass **die Vorgabe des Widerrufs der Einwilligung auch im Zusammenhang mit Eingriffen in Endeinrichtungen anwendbar ist**. Artikel 8 Absatz 1 Buchstabe b der vorgeschlagenen Verordnung sieht die Möglichkeit des Eingreifens in die Endeinrichtungen vor, wenn der Endnutzer seine Einwilligung gegeben hat. Artikel 9 Absatz 3 schreibt vor, dass Endnutzern die Möglichkeit eingeräumt wird, ihre Einwilligung jederzeit zu widerrufen. Dies gilt jedoch nur für die Einwilligung in die Analyse von Metadaten und Inhalten. Es sollte klargestellt werden, dass sich diese Pflicht auch auf das Eingreifen in Endeinrichtungen erstreckt.

48. In diesem Zusammenhang sollte präzisiert werden, dass **die Erinnerung an die Möglichkeit zum Widerruf der Einwilligung auch für die Einwilligung durch Browser-Einstellungen gilt.** Artikel 9 Absatz 3 schreibt vor, dass Endnutzer in regelmäßigen Abständen von sechs Monaten an die Möglichkeit erinnert werden, ihre Einwilligung jederzeit zu widerrufen. Während die Datenschutzgruppe die Ansicht vertritt, dass allgemeine Einstellungen von Browsern und anderer Software, einschließlich Betriebssystemen, Apps und Software-Schnittstellen für mit dem Internet der Dinge verbundene Geräte (d. h. nicht auf der Grundlage spezifischer granularer Kontrollen) keine gültige Maßnahme für das Erteilen der Einwilligung sein können, da allgemeine Einstellungen nicht geeignet sind, eine spezifische Einwilligung für ein konkretes Szenarium zu erteilen (siehe Ziffer 24), sollten Standardeinstellungen nutzerfreundlich sein (siehe Ziffer 19). Falls dies so in der vorgeschlagenen Verordnung stehen bleibt, müssen die Einstellungen hinreichend granular sein, so dass alle Datenverarbeitungen kontrolliert werden können, in die der Nutzer einwilligt und alle Funktionen der Ausrüstung abgedeckt sind, die zu einer Datenverarbeitung führen könnten. Darüber hinaus sollte der Endnutzer in regelmäßigen Abständen (d.h. alle sechs Monate) an die Möglichkeit erinnert werden, diese Einstellungen zu ändern.

49. Es wird begrüßt, dass die vorgeschlagene Verordnung vorsieht, dass in Verkehr gebrachte Software den Endnutzer über die Einstellungsmöglichkeiten zur Privatsphäre informieren muss (Artikel 10). **Es ist jedoch nicht klar, wie dies wirksam auf alte Produkte angewendet werden kann** und auf andere, die nicht länger unterstützt werden. Zusätzlich sollten näher präzisiert werden, wie diese Pflicht auf Open-Source-Software Anwendung findet, die auf offene und dezentrale Weise entwickelt wird.

50. Es sollte präzisiert werden, dass **das Anbieten der Möglichkeit nach Artikel 10 der vorgeschlagenen Verordnung, Cookies (Dritter) zu blockieren, Vorrang hat vor der Ausnahme für die Messung des Webpublikums** nach Artikel 8 Absatz 1 Buchstabe d. Anders ausgedrückt: Auch wenn eine Website Analysemethoden für die Messung des Webpublikums nach Artikel 8 Absatz 1 Buchstabe d anwenden darf, sollte der Nutzer das Recht haben, diese Verfolgungstechnologien in seinem Browser zu blockieren.

51. Die **Begriffsbestimmung von (halb)automatischen Anruf- und Kommunikationssystemen sollte geklärt werden**. Die Definition dieses Begriffs in Artikel 4 Absatz 3 Buchstabe h der vorgeschlagenen Verordnung enthält im zweiten Teil des Satzes einen Verweis auf den Begriff selbst („einschließlich Anrufen unter Verwendung automatischer Anruf- und Kommunikationssysteme, die die angerufene Person mit einer einzelnen Person verbinden"). Es wird vorgeschlagen, diesen letzten Satz aus der Begriffsbestimmung zu streichen und die Begriffsbestimmung in Artikel 4 Absatz 3 Buchstabe g dahingehend zu ändern, dass diese Anrufe umfasst, die mit Hilfe halbautomatischer Kommunikationssysteme (beispielsweise mit automatischen Wählvorrichtungen) durchgeführt werden, die die angerufene Person mit einer einzelnen Person verbinden.

52. Es sollte klargestellt werden, was mit **Informationen, die „Teil des Vertrags mit bzw. der Anmeldung bei dem Dienst sind", gemeint ist**. Erwägungsgrund 14 besagt: „Elektronische Kommunikationsmetadaten können Informationen enthalten, die Teil des Vertrags mit bzw. der Anmeldung bei dem Dienst sind, sofern diese Informationen zu Zwecken der Übermittlung, der Verbreitung oder des Austauschs elektronischer Kommunikationsinhalte verarbeitet werden." Es ist nicht klar, was damit gemeint ist.

53. Die **Anwendbarkeit des Kohärenzverfahrens und des Verfahrens zur Zusammenarbeit** sollte näher präzisiert werden. Erwägungsgrund 38 besagt, dass die vorgeschlagene Verordnung dem Kohärenzverfahren der DS-GVO unterliegt. Darüber hinaus sieht Artikel 18 Absatz 1 vor, dass die Kapitel VI und VII der DS-GVO sinngemäß Anwendung finden. Weiter wird in Artikel 19 festgelegt, dass der Europäische Datenschutzausschuss die in Artikel 70 der DS-GVO festgelegten Aufgaben wahrnehmen soll. Auch wenn die Anwendung dieser Bestimmungen relativ eindeutig ist, kann nicht ausgeschlossen werden, dass in Bezug auf die Schlüsselkonzepte des Kohärenzverfahrens und des Verfahrens zur Zusammenarbeit nach der DS-GVO Fragen zur Auslegung aufkommen. Das Verfahren der federführenden Aufsichtsbehörde beispielsweise findet in den Fällen Anwendung, in denen eine „grenzüberschreitende Verarbeitung" vorliegt (Artikel 56 Absatz 1 DS-

GVO): Es ist nicht klar, wie dies im Fall von Eingriffen in Endeinrichtungen oder der Analyse von Inhalt oder Metadaten nach der vorgeschlagenen Verordnung anwendbar ist. Deshalb ist es ratsam, die Anwendung dieser wichtigen Konzepte in einem Erwägungsgrund darzulegen und zu unterstreichen, dass alle verbleibenden Fragen der Anwendbarkeit dieser Kapitel der DS-GVO im Zusammenhang mit der vorgeschlagenen Verordnung durch Auslegung der Bestimmungen dieser Kapitel nach Maßgabe des mit ihnen verfolgten Zwecks zu beantworten sind. Darüber hinaus sollte präzisiert werden, dass Artikel 70 zum Europäischen Datenschutzausschuss im Zusammenhang mit der vorgeschlagenen Verordnung sinngemäß Anwendung findet (dies fehlt bisher in dem Erwägungsgrund).

*** * ***