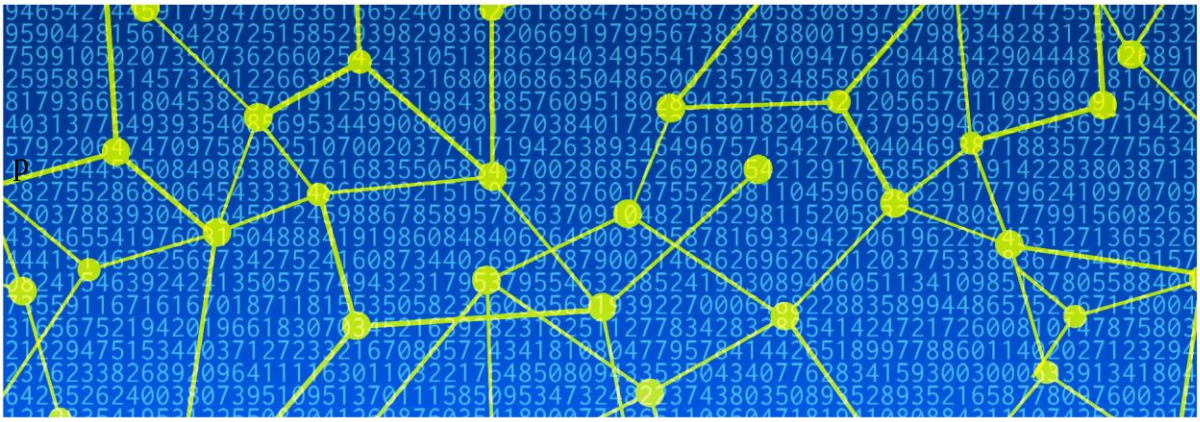

EUROPEAN DATA PROTECTION SUPERVISOR

Stellungnahme 6/2017

Stellungnahme des EDSB zu dem Vorschlag für eine Verordnung über Privatsphäre und elektronische Kommunikation (E-Privacy-VO)

EDPS

Der Europäische Datenschutzbeauftragte (EDSB) ist eine unabhängige Einrichtung der EU und hat nach Artikel 41 Absatz 2 der Verordnung (EG) Nr. 45/2001 „im Hinblick auf die Verarbeitung personenbezogener Daten (...) sicherzustellen, dass die Grundrechte und Grundfreiheiten natürlicher Personen, insbesondere ihr Recht auf Privatsphäre, von den Organen und Einrichtungen der Gemeinschaft geachtet werden"; er ist „für die Beratung der Organe und Einrichtungen der Gemeinschaft und der betroffenen Personen in allen die Verarbeitung personenbezogener Daten betreffenden Angelegenheiten" zuständig. Gemäß Artikel 28 Absatz 2 der Verordnung (EG) Nr. 45/2001 ist die Kommission zur Konsultation des EDSB verpflichtet, „wenn [sie] einen Vorschlag für Rechtsvorschriften bezüglich des Schutzes der Rechte und Freiheiten von Personen bei der Verarbeitung personenbezogener Daten annimmt".

Er wurde zusammen mit dem Stellvertretenden Datenschutzbeauftragten im Dezember 2014 ernannt und spezifisch mit einem konstruktiven und proaktiven Vorgehen beauftragt. In der im März 2015 veröffentlichten Fünf-Jahres-Strategie legt der EDSB dar, wie er diesen Auftrag auf verantwortungsvolle Weise zu erfüllen gedenkt.

Diese Stellungnahme enthält Anmerkungen und Empfehlungen im Hinblick darauf, wie das Recht auf Achtung der Privatsphäre, die Vertraulichkeit der Kommunikation und der Schutz personenbezogener Daten in der vorgeschlagenen Verordnung über Privatsphäre und elektronische Kommunikation, die die Datenschutzrichtlinie für elektronische Kommunikation (2002/58/EG) aufheben und ersetzen soll, besser gewährleistet werden können.

Zusammenfassung

In der vorliegenden Stellungnahme legt der EDSB seine Haltung zu dem Vorschlag für eine Verordnung über Privatsphäre und elektronische Kommunikation dar, die die Datenschutzrichtlinie für elektronische Kommunikation aufheben und ersetzen soll.

Ohne die E-Privacy-VO wäre der Rechtsrahmen der EU für die Achtung der Privatsphäre und den Datenschutz unvollständig. Die DSGVO – Datenschutzgrundverordnung – ist zwar bereits eine große Errungenschaft, doch benötigen wir ein spezifisches Rechtsinstrument zum Schutz des in Artikel 7 der Charta der Grundrechte verankerten Rechts auf Achtung des Privatlebens und zur Wahrung der Vertraulichkeit der Kommunikation als ein wesentlicher Bestandteil dieses Rechts. Daher begrüßt und unterstützt der EDSB den Vorschlag, der genau dies zum Ziel hat. Die Wahl einer Verordnung als ein unmittelbar anwendbares Rechtsinstrument, das ein höheres Maß an Harmonisierung und Kohärenz bewirken kann, wird ebenfalls von dem EDSB begrüßt. Außerdem befürwortet der EDSB die Absicht, ein hohes Schutzniveau sowohl in Bezug auf Inhalt als auch auf Metadaten zu gewährleisten, und unterstützt das Ziel, Vertraulichkeitspflichten auf eine breitere Palette von Diensten auszuweiten, darunter auch die so genannten „over the top“ (OTT)-Dienste, und so dem technologischen Fortschritt Rechnung zu tragen. Ferner ist der EDSB der Ansicht, dass die Entscheidung, Durchsetzungsbefugnisse ausschließlich den Datenschutzbehörden zu erteilen, sowie das Vorhandensein von Kooperations- und Abstimmungsmechanismen innerhalb des neu einzurichtenden Europäischen Datenschutzausschusses („Ausschuss“) zu einer konsequenteren und wirksameren Durchsetzung der Vorgaben überall in der EU beitragen werden.

Gleichzeitig hat der EDSB jedoch Bedenken, ob mit dem Vorschlag in seiner jetzigen Form das Versprechen eines hohen Schutzniveaus der Privatsphäre in der elektronischen Kommunikation auch tatsächlich wahr gemacht werden kann. Wir brauchen einen neuen Rechtsrahmen für den Datenschutz in der elektronischen Kommunikation, doch muss er intelligenter, klarer und stärker sein. In dieser Hinsicht bleibt noch viel zu tun, denn die Komplexität der in dem Vorschlag skizzierten Vorschriften ist eine schwierige Herausforderung. Bei der Kommunikation wird zwischen Metadaten, Inhaltsdaten und von Endgeräten ausgegebenen Daten unterschieden. Für jeden dieser Datentypen gibt es ein anderes Maß an Vertraulichkeit und andere Ausnahmefälle. Diese Komplexität führt zu dem – wohl unbeabsichtigten – Risiko der Regelungslücken.

Die meisten Begriffsbestimmungen, auf die sich der Vorschlag stützt, werden im Rahmen eines anderen Rechtsinstruments verhandelt und beschlossen: dem europäischen Kodex für die elektronische Kommunikation. Es gibt zurzeit keinen rechtlichen Grund für eine so enge Verknüpfung dieser beiden Rechtsinstrumente, und die wettbewerbs- und marktorientierten Begriffsbestimmungen des Kodex sind im Kontext der Grundrechte einfach nicht zweckmäßig. Daher spricht sich der EDSB unter Berücksichtigung des vorgesehenen Anwendungsbereichs und der angestrebten Ziele der E-Privacy-VO dafür aus, eine Reihe notwendiger Begriffsbestimmungen darin aufzunehmen.

Ferner müssen wir insbesondere dem Problem der Verarbeitung von Daten der elektronischen Kommunikation durch Verantwortliche, die nicht Anbieter von elektronischen Kommunikationsdiensten sind, Beachtung schenken. Die zusätzlichen Schutzvorschriften für Kommunikationsdaten wären sinnlos, wenn sie beispielsweise einfach dadurch umgangen werden könnten, dass die Daten an Dritte weitergegeben werden. Es sollte außerdem sichergestellt werden, dass die Vorschriften für den Datenschutz in der elektronischen

Kommunikation nicht ein niedrigeres Schutzniveau als das in der DSGVO verankerte zulassen. So sollte zum Beispiel, wie in der DSGVO verlangt, eine Einwilligung echt sein und Nutzern die Möglichkeit geben, frei eine Entscheidung zu treffen. Es sollte keine „Tracking Walls“ mehr geben. Darüber hinaus müssen die neuen Regeln auch hohe Anforderungen in Bezug auf Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen festlegen. Schließlich spricht der EDSB in dieser Stellungnahme noch weitere dringliche Fragen an, darunter die Beschränkungen des Anwendungsbereichs der Rechte.

INHALTSVERZEICHNIS

DER EUROPÄISCHE DATENSCHUTZBEAUFTRAGTE —

gestützt auf den Vertrag über die Arbeitsweise der Europäischen Union, insbesondere auf Artikel 16,

gestützt auf die Charta der Grundrechte der Europäischen Union, insbesondere auf Artikel 7 und 8,

gestützt auf die Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr und auf die 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),

gestützt auf die Verordnung (EG) Nr. 45/2001 des Europäischen Parlaments und des Rates vom 18. Dezember 2000 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe und Einrichtungen der Gemeinschaft und zum freien Datenverkehr, insbesondere auf Artikel 28 Absatz 2, Artikel 41 Absatz 2 und Artikel 46 Buchstabe d —

HAT FOLGENDE STELLUNGNAHME ANGENOMMEN:

1. EINLEITUNG UND HINTERGRUND

Diese Stellungnahme („Stellungnahme“) ergeht aufgrund eines Ersuchens der Europäischen Kommission („Kommission“) an den Europäischen Datenschutzbeauftragten („EDSB“), als unabhängige Aufsichtsbehörde und als Berater eine Stellungnahme zu dem Vorschlag für eine Verordnung über Privatsphäre und elektronische Kommunikation[1] („Vorschlag“) abzugeben. Der Vorschlag soll die Richtlinie 2002/58/EG über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation) aufheben und ersetzen.[2] Die Kommission ersuchte ferner um die Stellungnahme der Artikel 29-Datenschutzgruppe (WP29), an der der EDSB als Vollmitglied mitarbeitete.[3]

Diese Stellungnahme folgt unserer vorläufigen Stellungnahme 5/2016 zur Überarbeitung der Datenschutzrichtlinie für elektronische Kommunikation (2002/58/EG)[4], abgegeben am 22. Juli 2016. Es ist denkbar, dass der EDSB seinen Rat auch in späteren Phasen des Gesetzgebungsverfahrens erneut einbringen wird.

Der Vorschlag gehört zu den zentralen Initiativen der Strategie für einen digitalen Binnenmarkt[5], mit dem Vertrauen und Sicherheit im Bereich digitaler Dienstleistungen in der EU gestärkt werden sollen, in der Hauptsache jedoch ein hohes Schutzniveau für Bürger und gleiche Wettbewerbsbedingungen für alle Marktteilnehmer überall in der EU hergestellt werden sollen.

Mit dem Vorschlag soll die Datenschutzrichtlinie für elektronische Kommunikation als Teil weiterreichender Bemühungen um einen kohärenten und harmonisierten Rechtsrahmen für den Datenschutz in Europa modernisiert und aktualisiert werden. Die Datenschutzrichtlinie für elektronische Kommunikation stellt eine Detaillierung und Ergänzung der Richtlinie 94/46/EG[6] dar, die durch die vor kurzem angenommene Datenschutz-Grundverordnung (DSGVO)[7] ersetzt werden wird.

Zunächst fasst der EDSB in Abschnitt 2 die wichtigsten Punkte seiner Stellungnahme zu dem Vorschlag zusammen und geht dabei vor allem auf die positiven Aspekte des Vorschlags ein. Danach führt der EDSB in Abschnitt 3 die noch verbleibenden zentralen Fragen auf und unterbreitet Lösungsvorschläge. Weitere Fragen und Empfehlungen zur Verbesserung des Vorschlags werden im Anhang zu dieser Stellungnahme beschrieben, in dem noch detaillierter auf den Vorschlag eingegangen wird. Die Lösung der in dieser Stellungnahme und ihrem Anhang angesprochenen Fragen und eine weitere Verbesserung des Wortlauts der E-Privacy-VO würde nicht nur zu einem höheren Schutzniveau für Endnutzer und andere betroffene Personen führen, sondern auch größere Rechtssicherheit für alle Beteiligten schaffen.

2. BEDARF AN EINEM EIGENSTÄNDIGEN RECHTSINSTRUMENT FÜR DEN DATENSCHUTZ IN DER ELEKTRONISCHEN KOMMUNIKATION

2.1 Die wichtigsten positiven Aspekte des Vorschlags

Der EDSB begrüßt den Vorschlag der Kommission für eine modernisierte, aktualisierte und stärkere E-Privacy-VO. Der EDSB schließt sich auch der von der WP29 sowohl in ihrer vorläufigen als auch in einer neueren Stellungnahme[8] wiederholt geäußerten und von Gruppen der Zivilgesellschaft in deren vorläufigen und neueren gemeinsamen Analyse[9] formulierten Auffassung an, dass weiterhin Bedarf an spezifischen Vorschriften besteht, die die Vertraulichkeit und Sicherheit elektronischer Kommunikation in der EU schützen und die Anforderungen der DSGVO ergänzen und präzisieren. Er ist außerdem der Meinung, dass wir einfache, gezielte und technologisch neutrale gesetzliche Bestimmungen benötigen, die in absehbarer Zukunft starken, intelligenten und wirksamen Schutz bieten.

Der EDSB begrüßt ferner, dass viele der in seiner vorläufigen Stellungnahme und in seinen informellen Kommentaren enthaltenen Anmerkungen aufgegriffen wurden, was erheblich zur Qualität des Vorschlags beigetragen hat. Das erklärte Ziel, sowohl für Inhalt als auch für Metadaten ein hohes Schutzniveau zu bieten, befürwortet der EDSB ebenfalls, und zwar insbesondere:

- die Entscheidung für eine Verordnung anstelle einer Richtlinie als neues Rechtsinstrument, womit ein einheitlicheres Schutzniveau in der gesamten EU gewährleistet werden kann;
- die Ausweitung des Anwendungsbereichs unter Einbeziehung der so genannten OTT („*over-the-top*“)-Anbieter;
- die Zulassung der Datenverarbeitung nur unter klar und eindeutig definierten Bedingungen;
- die Modernisierung der derzeitigen Einwilligungsvorschriften im Rahmen der neuen Artikel 9 und 10;
- die Ausrichtung der Sicherheitsbestimmungen auf spezifische Fragen der Kommunikationsdienste und die Sicherstellung einer vollständigen Angleichung an die DSGVO im Hinblick auf Datenschutzverletzungen;
- die Entscheidung, die Zuständigkeit für die Überwachung der Vorschriften sowohl der DSGVO als auch der E-Privacy-VO den gleichen Behörden zu übertragen;
- und die Opt-in-Regel für alle unerbetenen Werbemitteilungen.

2.2 Die Vertraulichkeit elektronischer Kommunikation muss weiterhin gewahrt sein

Das Recht auf Vertraulichkeit der Kommunikation ist ein durch Artikel 7 der Charta der Grundrechte der Europäischen Union („Charta“) geschütztes Grundrecht – gewissermaßen das moderne Äquivalent traditioneller Vorschriften (der Post) über die Wahrung des Briefgeheimnisses.[10]

Die Vertraulichkeit von Kommunikation spielt eine zentrale Rolle für das Funktionieren moderner Gesellschaften und Volkswirtschaften: Ohne vertrauenswürdige Boten, die den Empfängern Informationen liefern, ohne sie für ihre eigenen Zwecke zu nutzen, an Dritte weiterzugeben, den Inhalt zu ändern, die Lieferung zu unterbinden oder zu verzögern, könnten viele private und öffentliche Aktivitäten nur von Angesicht zu Angesicht erfolgen.

Zwar kann die Bedeutung vertrauensvoller Kommunikation für Wirtschaft und Gesellschaft gar nicht hoch genug eingeschätzt werden, doch besteht ihre zentrale rechtliche Rolle im Schutz des Grundrechts auf Achtung des Privatlebens gegen jeglichen Eingriff, insbesondere von Seiten staatlicher Behörden.

Für die Rechtssicherheit ist von entscheidender Bedeutung, dass klare und spezifische Rechtsvorschriften im Sekundärrecht bestehen, damit der Grundsatz der Vertraulichkeit elektronischer Kommunikation in die Praxis umgesetzt werden kann. Es reicht nicht aus, sich – auf EU-Ebene – nur auf einen einzigen Artikel in der Charta zu beziehen. In dem derzeit bestehenden Rechtsrahmen ist die Datenschutzrichtlinie für elektronische Kommunikation das Instrument des Sekundärrechts der EU, das die notwendigen, speziellen gesetzlichen Anforderungen festlegt.

Die Anerkennung der Vertraulichkeit von Kommunikation als ein Grundrecht in der Charta steht im Einklang mit europäischen Verfassungstraditionen, denn die meisten EU-Mitgliedstaaten erkennen die Vertraulichkeit von Kommunikation ebenfalls in ihrer Verfassung als eigenständiges Recht an[11]. Neue, stärker harmonisierte Vorschriften auf EU-Ebene tragen zu mehr Rechtssicherheit bei. Somit sind sie von Vorteil für natürliche Personen, denen sie überall in Europa den gleichen Schutz gewähren, aber auch für Unternehmen, und hier vor allem den Unternehmen, die in mehreren Rechtsordnungen tätig sind.

2.3 Das bestehende Schutzniveau darf nicht gesenkt werden

Neben der Umsetzung des Grundrechts auf Achtung des Privatlebens in der elektronischen Kommunikation muss die E-Privacy-VO auch dazu dienen, das Grundrecht auf den Schutz personenbezogener Daten gemäß Artikel 8 der Charta zu wahren. Dies ist besonders wichtig im Hinblick auf Situationen, für die in der Datenschutzrichtlinie für elektronische Kommunikation spezifischere Garantien vorgesehen sind als in der DSGVO, um ein höheres Schutzniveau für personenbezogene Daten sicherzustellen und so speziell auf Kommunikationsdaten bezogenen Risiken entgegenzuwirken.

So ist beispielsweise in der DSGVO nicht ausdrücklich festgelegt, welche der möglichen Rechtsgrundlagen für eine Verarbeitung in welchen Situationen zulässig sein könnte, wohingegen die Datenschutzrichtlinie für elektronische Kommunikation und die vorgeschlagene E-Privacy-VO in bestimmten Zusammenhängen präziser formuliert sind, indem die Einwilligung als Rechtsgrundlage verlangt wird[12].

Ebenso wichtig ist es, dass die neuen Regelungen nicht durch die Einführung von Abweichungen von den Vorgaben der DSGVO das in der DSGVO vorgesehene Maß an Schutz unterschreiten.

Darüber hinaus wird neben den Grundrechten von natürlichen Personen auch der Schutz bestimmter Rechte von juristischen Personen aufrechterhalten, und zwar in ihrer Rolle als Teilnehmer an bzw. Nutzer von elektronischen Kommunikationsdiensten im Hinblick auf unerbetene Kommunikation und auch auf andere Aspekte. Obwohl diese Schutzbedürfnisse in der DSGVO nicht berücksichtigt sind[13], sind sie in Anbetracht der wichtigen Rolle, die eine zuverlässige und sichere elektronische Kommunikation für das Funktionieren unserer Gesellschaft und Wirtschaft spielt, ebenso bedeutend[14].

2.4 Zur Sicherstellung von Kohärenz und Rechtssicherheit bedarf es einfacher und unkomplizierter Regeln

Mit der E-Privacy-VO muss auch sichergestellt werden, dass die neuen Regeln einfach und unkompliziert sind und überall in Europa wirksam und einheitlich durchgesetzt werden können. Aus dieser Perspektive betrachtet sind die folgenden Aspekte des Vorschlags besonders zu begrüßen.

Wahl einer Verordnung statt einer Richtlinie

Der EDSB befürwortet, dass sich die Gesetzgeber als Form des neuen Rechtsinstruments, wie in der vorläufigen Stellungnahme des EDSB empfohlen, für eine Verordnung statt einer Richtlinie entschieden haben. Das stimmt mit dem Ansatz der DSGVO überein, gewährleistet ein kohärenteres und gleiches Schutzniveau für natürliche Personen und andere durch die Bestimmungen geschützte Einrichtungen, trägt dazu bei, gleiche Wettbewerbsbedingungen für Organisationen zu schaffen, die die Bestimmungen einhalten müssen, und senkt deren Befolgungskosten.

Aufsicht und Durchsetzung

Der EDSB begrüßt auch, dass Artikel 18 des Vorschlags, wie in seiner vorläufigen Stellungnahme empfohlen, Datenschutzbehörden zur Überwachung der Anwendung der E-Privacy-VO befugt sowie auch zur Überwachung der Anwendung des Verfahrens der Zusammenarbeit und des Kohärenzverfahrens der DSGVO auf Fragen in Zusammenhang mit der E-Privacy-VO. Die Harmonisierung im Hinblick auf die Durchsetzungsbefugnisse, einschließlich der Höhe von Bußgeldern, wird ebenfalls befürwortet.[15]

Bedarf an einfachen und unkomplizierten Vorschriften

Die Datenschutzrichtlinie für elektronische Kommunikation und auch der vorliegende Vorschlag enthalten Vorschriften für eine Reihe von Situationen, in denen es besonders schwierig ist, die Frage, ob eine Verarbeitung personenbezogener Daten vorliegt, wer der für die Verarbeitung Verantwortliche oder Auftragsverarbeiter ist und wer die betroffene Person ist, zu beantworten. Dies betrifft unter anderem technische Gegebenheiten bei bestimmten Vorgängen im Netz (z. B. Anruferidentifizierung), die Integrität der Endpunkte der Nutzer (Information über Endgeräte des Nutzers) und die Verwendung von Kommunikationsdiensten für Direktwerbung.

Es wird daher befürwortet, dass in dem Vorschlag, wie es auch in der Datenschutzrichtlinie für elektronische Kommunikation geschehen ist, derartige Fälle dadurch gelöst werden, dass die mit der Inanspruchnahme von Kommunikationsdienstleistungen verbundenen Rollen und Aktivitäten abgedeckt sind, ohne dass es einer Analyse auf Basis der DSGVO bedarf. In Anbetracht der Tatsache, dass die Bestimmungen der Datenschutzrichtlinie für elektronische Kommunikation unterschiedlich interpretiert wurden, bietet die E-Privacy-VO die Möglichkeit einer Klärung bestimmter Begriffe bzw. Konzepte.

2.5 Eine Ausweitung des Geltungsbereichs der E-Privacy-VO ist unbedingt notwendig

Wir begrüßen das Ziel der Kommission, den Schutzbereich auszuweiten und die Vorschriften so zu aktualisieren, dass sie auch auf neue Methoden zur Erbringung von Kommunikationsdienstleistungen anwendbar sind. Würde lediglich das bestehende Schutzniveau aufrechterhalten, würden diese Rechte für einen ständig wachsenden Anteil an unserer Alltagskommunikation ihres Sinnes entleert.

Instant Messaging und Voice over IP

Wie bereits in unserer vorläufigen Stellungnahme dargelegt, muss natürlichen Personen für alle funktional gleichwertigen Dienste das gleiche Schutzniveau geboten werden, unabhängig davon, ob sie über eine traditionelle Festnetzverbindung oder ein Mobiltelefon und als SMS/MMS einerseits oder als ein OTT-Kommunikationsdienst, wie Voice over IP (VoIP)[16] und Instant-Messaging-Apps, andererseits erbracht werden.

Die Nutzer haben häufig ähnliche Erwartungen im Hinblick auf die Privatheit und Vertraulichkeit dieser Nachrichten und jede Verletzung der Vertraulichkeit wird gleichermaßen als Eingriff gesehen. Ein Nutzer kann zum Beispiel ein Gespräch über die Messaging-Funktion eines Spiels beginnen, dann zu einem OTT-Instant-Messaging-Dienst wechseln, über das Mobiltelefon SMS und MMS austauschen und schließlich einen Anruf zwischen zwei Telefonen beginnen. Alle diese verschiedenen Kommunikationsformen können über die gleichen Geräte laufen, nämlich Smartphones, und für die Nutzer dürfte kaum klar und nachvollziehbar sein, dass es für die von ihnen genutzten Dienste unterschiedliche Rechtsrahmen gibt.

Vor diesem Hintergrund befürwortet der EDSB, dass in Erwägungsgrund 11 des Vorschlags die Notwendigkeit einer Ausweitung des Geltungsbereichs auf funktional gleichwertige Dienste erkannt wird und auch einige Beispiele derartiger Dienste aufgeführt sind, insbesondere „*VoIP-Telefonie, Nachrichtenübermittlung (Messaging) und webgestützte E-Mail-Dienste“*.

Wie ebenfalls in unserer vorläufigen Stellungnahme empfohlen, besteht die Notwendigkeit, hier noch einen Schritt weiter zu gehen: Nicht nur Kommunikationsformen, die den Angeboten traditioneller Telekom-Dienstleister *„funktional gleichwertig“* sind, sondern auch Dienste, die neue Möglichkeiten für Kommunikation eröffnen, vielleicht als Zusatz zu anderen Angeboten, müssen geschützt werden. Im Rahmen dieser Bemühungen muss sichergestellt werden, dass in andere Dienste integrierte Kommunikationsfunktionen (z. B. Messaging-Funktionen in Spiele- und Dating-Apps) in den Genuss des gleichen Schutzes kommen.

Daher begrüßt der EDSB besonders, dass so genannte *„Nebenfunktionen“* in Artikel 4 Absatz 2 des Vorschlags ausdrücklich erwähnt und erfasst sind.

Internet der Dinge (IdD)

Wir sprechen zwar vom Internet der Dinge, doch handelt es sich in Wirklichkeit vielmehr um ein „*Internet der Dinge, die mit Menschen zu tun haben*“: Das Internet der Dinge umfasst Sport-Tracker, Gesundheitssensoren, persönliche Kommunikationsgeräte, Smart-TV, intelligente Autos und viele andere Geräte. Sie sind mit Sensoren für Klang, Video, Bewegungen und physische Parameter ihrer Eigentümer ausgestattet. Die Tatsache, dass sie ihre Datenübermittlungen und Kommunikationsvorgänge manchmal ohne Auslösen durch den Eigentümer (oder sogar ohne dessen Wissen) in Gang setzen, darf kein Grund sein, eine solche häufig sensible Kommunikation weniger zu schützen.

Der Schutz der Privatheit von Kommunikation sollte nicht davon abhängen, ob Menschen selbst den Inhalt einer Kommunikation sprechen oder hören, schreiben oder lesen, oder ob sie sich einfach auf die zunehmend intelligenten Merkmale ihrer Endgeräte bei der Übermittlung von Inhalt in ihren Namen verlassen. Kommunikationsanbieter sollten im Normalfall mit dem Zweck oder Inhalt von Kommunikation gar nichts zu tun haben und sollten von diesen Besonderheiten der über ihre Dienste übermittelten Nachrichten und anderer Formen der Kommunikation noch nicht einmal Kenntnis haben.

Der EDSB befürwortet, dass in Artikel 2 Absatz 1 des Vorschlags[17] klargestellt wird, dass der Zweck und Inhalt einer Kommunikation deren Schutz durch das Recht auf Achtung des Privatlebens nicht berühren darf. Der EDSB befürwortet auch, dass in Erwägungsgrund 12 eigens auf das Internet der Dinge und Kommunikationsvorgänge zwischen Maschinen Bezug genommen wird, um sicherzustellen, dass der Vorschlag unabhängig von der Art des benutzten Netzes oder Kommunikationsdienstes die Maschine-zu-Maschine-Kommunikation in Zusammenhang mit dem Internet der Dinge in allen auch sonst in den Anwendungsbereich des Vorschlags fallenden Netzen und Diensten unzweifelhaft erfasst.

Abdeckung von Netzen verschiedener Art

Der EDSB begrüßt auch das Ziel der Kommission, alle öffentlich zugänglichen Netze und Dienste in den Geltungsbereich der Vertraulichkeitsanforderungen einzubeziehen. Dazu sollten beispielsweise gehören Wi-Fi-Dienste in Hotels, Restaurants, Coffee-Shops, Läden, Zügen, Flughäfen und Netze, die von Krankenhäusern, Universitäten den Nutzern ihrer Hauptdienste (also Patienten bzw. Studierenden) angeboten werden, sowie Wi-Fi-Zugang für Besucher und Gäste in Unternehmen und von Behörden eingerichtete Hotspots.[18]

3. DIE WICHTIGSTEN FRAGEN UND EMPFEHLUNGEN

Der EDSB begrüßt zwar den Vorschlag, doch hat er weiterhin Bedenken in Bezug auf eine Reihe von Bestimmungen, die die Absicht der Kommission, ein hohes Schutzniveau der Privatsphäre in der elektronischen Kommunikation zu gewährleisten, beeinträchtigen könnten. Zu den wichtigsten Fragen des EDSB in dieser Hinsicht gehören insbesondere:

- Die in dem Vorschlag enthaltenen Begriffsbestimmungen dürfen nicht von dem davon unabhängigen Gesetzgebungsverfahren bezüglich der Richtlinie über den europäischen Kodex für die elektronische Kommunikation[19] (Kodex-Vorschlag) abhängig sein;
- Die Bestimmungen über die Einwilligung der Endnutzer müssen stärker formuliert werden. Die Einwilligung muss von den Personen eingeholt werden, die die Dienste benutzen, unabhängig davon, ob sie diese abonnieren oder nicht, sowie von allen an

einem Kommunikationsvorgang Beteiligten. Darüber hinaus müssen andere betroffene Personen, die nicht an den Kommunikationsvorgängen beteiligt sind, ebenfalls geschützt werden;

- Es muss dafür Sorge getragen werden, dass die Beziehung zwischen der DSGVO und der E-Privacy-VO keine Lücken im Schutz personenbezogener Daten offenlässt. Personenbezogene Daten, die aufgrund der Einwilligung der Endnutzer oder aus einem anderen in der E-Privacy-VO vorgesehenen Rechtsgrund erhoben werden, dürfen nicht später außerhalb des Geltungsbereichs dieser Einwilligung oder Ausnahmeregelung aus einem anderen nach der DSGVO möglicherweise bestehenden, jedoch nicht in der E-Privacy-VO verankerten Rechtsgrund weiter verarbeitet werden;
- Dem Vorschlag mangelt es in Bezug auf die so genannten „*Tracking Walls*“ (oder auch „*Cookie Walls*“) an Ehrgeiz. Zugang zu Websites darf nicht davon abhängig gemacht werden, dass die Person gezwungen wird, in die Verfolgung ihrer Aktivitäten auf den Websites „*einzuwilligen*“. Mit anderen Worten fordert der EDSB die Gesetzgeber auf, dafür Sorge zu tragen, dass die Einwilligung wirklich freiwillig erteilt wird;
- Der Vorschlag stellt nicht sicher, dass Browser (und andere auf dem Markt angebotene Softwareprodukte, die elektronische Kommunikation ermöglichen) standardmäßig so eingestellt sind, dass die Verfolgung der von Personen im Internet hinterlassenen digitalen Spuren verhindert wird;
- Die Ausnahmen bezüglich der Standortverfolgung von Endgeräten sind zu allgemein gefasst und bieten keine angemessenen Garantien;
- Der Vorschlag gibt Mitgliedstaaten die Möglichkeit, Beschränkungen einzuführen. Diese machen spezifische Garantien erforderlich.

In Abschnitt 3 werden diese Hauptfragen näher erläutert und Empfehlungen zu ihrer Lösung gegeben.

3.1 Anwendungsbereich und Begriffsbestimmungen

Der EDSB begrüßt die Absicht, den sachlichen Anwendungsbereich der E-Privacy-VO auf Grundlage ihrer Ziele zu definieren, um einen konsequenten und umfassenden Schutz der Grundrechte auf Privatsphäre, Vertraulichkeit der Kommunikation und Datenschutz sicherzustellen. Durch die Schaffung eines eigenständigen Instruments, das nicht mehr in einen am Wettbewerb und an Marktvorschriften orientierten Rahmen fällt, wird es möglich, den Anwendungsbereich der neuen E-Privacy-VO so zu definieren, dass nicht Wirtschaftsfaktoren und Belange des fairen Wettbewerbs und der effizienten Ressourcennutzung, sondern vielmehr der Schutz der Grundrechte im Mittelpunkt dieses Anwendungsbereichs und der Begriffsbestimmungen steht.

Zur vollen Entfaltung der Wirksamkeit der E-Privacy-VO müssen deren Kernkonzepte sorgfältig definiert sein. Der EDSB hegt die Befürchtung, dass diese Wirksamkeit dadurch geschwächt oder beeinträchtigt werden könnte, dass einige Begriffsbestimmungen nicht präzise und deutlich genug formuliert sind und unnötige Abhängigkeiten von dem Kodex-Vorschlag bestehen. Das könnte zu einer ungerechtfertigten Beschneidung der Rechte der betroffenen Personen oder Einschränkung des Anwendungsbereichs der Verordnung führen.

Abhängigkeit von den Kodex-Definitionen vermeiden

Zum Zeitpunkt der Annahme des umfassenden Rechtsrahmens für elektronische Kommunikation im Jahr 2002 war die Datenschutzrichtlinie für elektronische Kommunikation

ein fester Bestandteil dieses Rechtsrahmens. Die Gesetzgeber hatten jedoch erkannt, dass die für einen wettbewerbsstarken und fairen Markt für elektronische Kommunikationsdienste und ähnliche Zwecke erforderlichen Begriffsbestimmungen für den Schutz der Grundrechte nicht gänzlich geeignet waren. Daher wurden zentrale Begriffe des Rechtsrahmens – wie *„Nutzer"* und *„Kommunikation"* – in der Datenschutzrichtlinie für elektronische Kommunikation speziell für dieses Rechtsinstrument und abweichend von den allgemeinen Definitionen in der Rahmenrichtlinie[20] definiert. Mit der Reform des Rechtsrahmens im Jahr 2009 wurde die Verbindung zwischen den Instrumenten beibehalten, aber auch die separaten Definitionen der Datenschutzrichtlinie für elektronische Kommunikation blieben unverändert.

In dem jetzigen Gesetzgebungsverfahren müssen sich die Gesetzgeber mit Vorschlägen für Instrumente befassen, die sehr viel unabhängiger voneinander sind:

- Der Kodex-Vorschlag beinhaltet Vorschriften für den Markt der elektronischen Kommunikation mit dem Ziel, einen echten Binnenmarkt für Kommunikation zu schaffen, eine effiziente Frequenznutzung sicherzustellen, Anreize für Investitionen in Breitbandanbindungen zu geben sowie gleiche Wettbewerbsbedingungen für alle Marktteilnehmer und ein wirksames Regelwerk zu schaffen.
- Der Vorschlag für eine E-Privacy-VO hat dagegen zum Ziel, ein hohes Schutzniveau der Privatsphäre für Nutzer von elektronischen Kommunikationsdiensten zu gewährleisten und das Vertrauen in digitale Dienste und deren Sicherheit zu erhöhen.[21]

Anders als bei den früheren Überprüfungen in den Jahren 2002 und 2009 soll bei der Überprüfung 2017 das Gesetzgebungsverfahren für die beiden verschiedenen Bereiche nicht synchron verlaufen, sondern es wird eindeutig zwischen den Vorschriften in Bezug auf den Markt und denen zum Schutz der Grundrechte unterschieden. Daher arbeiten die Gesetzgeber nicht immer in der gleichen Konfiguration an diesen Vorschlägen, sodass eine Koordination der beiden Verfahren noch unwahrscheinlicher wird.

Der EDSB begrüßt die Abgrenzung zwischen Grundrechteaspekt und wirtschaftlichem Aspekt und die Schaffung eines eigenen und unabhängigen Instruments, dessen Schwerpunkt der Schutz der Grundrechte der Privatsphäre und des Datenschutzes von Personen ist, die elektronische Kommunikationsdienste nutzen. Der EDSB bittet die Gesetzgeber jedoch dringend, die Logik dieses Ansatzes konsequent zu verfolgen. Daher sieht der EDSB keinen Grund dafür, dass die Begriffsbestimmungen des Kodex-Vorschlags in dem vorliegenden Kontext automatisch anwendbar sein sollten. Entscheidend für die Festlegung des Anwendungsbereichs der E-Privacy-VO sollten ja nicht nur wirtschaftliche Faktoren in Bezug auf fairen Wettbewerb und wirksame Ressourcennutzung sein, sondern vielmehr der Schutz der Grundrechte. Und selbst wenn Begriffsbestimmungen im Text der beiden Vorschläge identisch sein sollten, so wäre es dennoch besser, diese als eigenständige Begriffsbestimmungen in die E-Privacy-VO aufzunehmen und sie im Hinblick auf den besonderen Kontext des Schutzes der Grundrechte gegebenenfalls zu präzisieren. Dies würde auch dazu dienen, Änderungen in der Bedeutung der Bestimmungen der E-Privacy-VO zu vermeiden, die sich aufgrund von Änderungen im Gesetzgebungsverfahren für den Kodex ergeben könnten, ohne dass dies nachteilige Auswirkungen auf die erforderliche Kohärenz der beiden Gesetzgebungsbereiche haben würde.

Die Abhängigkeit von zentralen Begriffsbestimmungen in dem Vorschlag von dem parallel verlaufenden Gesetzgebungsverfahren für den Kodex-Vorschlag schafft unnötige und vermeidbare Risiken in Bezug auf die Eindeutigkeit und Wirksamkeit der E-Privacy-VO: Solange der Kodex-Vorschlag noch nicht angenommen ist, können sich dessen Definitionen

noch ändern, und sofern diese Definitionen auch in dem Vorschlag der E-Privacy-VO verwendet werden, würden die Änderungen auch Auswirkungen auf die Bedeutung und Wirkung seiner Bestimmungen haben. Wie sich bereits in der Vergangenheit gezeigt hat, kann man nicht generell davon ausgehen, dass die zum Zweck der wirtschaftlichen Regulierung festgelegten Begriffsbestimmungen als solche auch gleichermaßen zum Schutz der Grundrechte geeignet sind. **Aus diesen Gründen empfiehlt der EDSB, auf die unnötigen Abhängigkeiten von dem Kodex-Vorschlag zu verzichten und zentrale Begriffe in der E-Privacy-VO selbst so zu definieren, dass sie mit dem Kodex-Vorschlag im Einklang stehen, ohne jedoch unbedingt identisch zu sein. Dies würde dem durchschnittlichen Anwender der E-Privacy-VO außerdem das Lesen und Verständnis des Textes erleichtern.**

Klare Bezeichnung der betroffenen Personen

Die Definition *„Endnutzer"* zum Beispiel hat eine zentrale Funktion in dem Vorschlag für eine E-Privacy-VO, denn sie soll denjenigen bezeichnen, deren Grundrechte zu schützen sind. In dem Kodex-Vorschlag bezeichnet der Begriff *„Endnutzer"* natürliche Personen *oder juristische Personen*, die einen Vertrag mit einem Anbieter elektronischer Kommunikationsdienste geschlossen haben und selbst keine elektronischen Kommunikationsdienste anbieten[22]. Die Verwendung des Begriffs *„Endnutzer"* in diesem Sinne garantiert jedoch nicht, dass die Grundrechte aller Personen, die elektronische Kommunikationsdienste nutzen, angemessen geschützt sind. Wenn es um die Grundrechte des Einzelnen geht, sollte in dem Vorschlag ein Begriff verwendet werden, der für diesen Zweck geeignet ist, und sich auf *eine natürliche Person, die elektronische Kommunikationsdienste nutzt, ohne diese notwendigerweise abonniert zu haben*, bezieht. Dies wäre für viele der Bestimmungen angemessen, darunter die Bestimmungen in Artikel 6 und Artikel 8, wohingegen in anderen Bestimmungen der Verweis auf eine Einrichtung, die eine Vertragsbeziehung zu dem Dienstleister hat, zweckdienlich ist (z. B. in Artikel 15 über öffentlich zugängliche Verzeichnisse). Abschnitt 3.2 geht im Einzelnen auf die Risiken ein, die sich daraus ergeben, dass grundrechtsrelevante Entscheidungen nicht den betroffenen Personen, sondern anderen Einrichtungen zugeordnet werden.

Klarheit schaffen in Bezug auf die in den Anwendungsbereich fallenden Dienste

Wie in Abschnitt 2.5 hervorgehoben, betont der EDSB, dass die Ausdehnung des *sachlichen* Anwendungsbereichs eine lange überfällige Anpassung der Gesetzgebung an technologische und wirtschaftliche Entwicklungen darstellt. Unabhängig von der Form der Kommunikation, ob SMS oder ein Internet-Messenger-Dienst, sollten sich Personen auf die Vertraulichkeit ihrer Kommunikation verlassen können. Begriffsbestimmungen, die sich auf verschiedene Untergruppen von Diensten beziehen, sind daher für die Festlegung des Anwendungsbereichs des Rechtsinstruments unverzichtbar. Die Anpassung des Begriffs *„interpersonnelle Kommunikationsdienste"* in Artikel 4 Absatz 2 unter Einbeziehung von Nebendiensten wird daher sehr begrüßt. Diese Anpassung zeigt besonders deutlich, dass die Anwendungsbereiche der E-Privacy-VO und des Kodex-Vorschlags nicht identisch sein sollen und dass daher die E-Privacy-VO gegebenenfalls spezifische oder andere Begriffe benötigt als der Kodex. Für den Schutz der Vertraulichkeit der Kommunikation ist es unerheblich, ob der für die Kommunikation genutzte Dienst aus Sicht des Dienstleisters der Haupt- oder nur ein untergeordneter Nebendienst ist.

Sicherstellen, dass alle Kommunikationsdaten abgedeckt sind

Bei der Definition des Begriffs Kommunikationsmetadaten in Artikel 4 Absatz 3 Buchstabe c, bezieht sich der Vorschlag nur auf „*Daten, die in einem elektronischen Kommunikationsnetz [...] verarbeitet werden"*. Dies könnte zu einer Schutzlücke führen, sofern ein Teil der Daten, die die Verarbeitung von Kommunikationsinhalten bestimmen, von Geräten verarbeitet wird, die zwar zur Infrastruktur des Dienstes gehören, aber nicht als Teil des Netzes verstanden werden. Das wäre beispielsweise der Fall, wenn solche Daten von Geräten verarbeitet werden, die als *„zugehörige Einrichtungen"* im Sinne des Kodex verstanden werden.

Zur Vermeidung derartiger Schutzlücken sollte der Begriff Metadaten in Artikel 4 Absatz 3 Buchstabe c nicht nur alle Daten umfassen, die *„in einem elektronischen Kommunikationsnetz"* verarbeitet werden, sondern auch alle Daten, die von anderen, zur Erbringung der Dienstleistung verwendeten Geräten verarbeitet und nicht als Inhalte betrachtet werden.

Aus der Sicht eines Kommunikationsanbieters, der der E-Privacy-VO unterliegt, kann der Inhalt oder Zweck einer Kommunikation keine Rolle beim Umgang mit deren Vertraulichkeit und Sicherheit spielen. Es sollte dem Anbieter gleichgültig sein, ob es sich bei der übermittelten Nachricht um die Ergebnisse einer Messung der Herzfrequenz oder einen von einer Smart Trading-App kommenden Auftrag für ein Börsengeschäft oder das Foto eines Blumenstraußes auf einer Hochzeitseinladung handelt. Ein wirkungsvoller und effizienter Dienst und die Achtung der Privatsphäre und Wahrung der Sicherheit sind dementsprechend für sämtliche Kommunikationen zu gewährleisten. Sofern spezifische Aktivitäten des Netzwerks für bestimmte Kommunikationsarten erforderlich sind, bieten viele vorhandene Kommunikationsprotokolle die Möglichkeit, diese Anforderungen als Teil der Kommunikationsmetadaten zu spezifizieren. Im Interesse der Vertrauenswürdigkeit der Dienste sollte von dieser Möglichkeit Gebrauch gemacht werden, anstatt zu diesem Zweck die Vertraulichkeitspflicht zu verletzen.

Die Kommunikationsdaten in der „Cloud" schützen

Weiterhin ist zu bedenken, dass die E-Privacy-VO nicht nur eindeutig die Vertraulichkeit und Sicherheit der Kommunikation während ihrer Übermittlung vorsehen muss, sondern auch die Vertraulichkeit und Sicherheit der Geräte der Endnutzer sowie der in der *„Cloud"* gespeicherten Kommunikationsdaten sicherstellen muss. **Der EDSB empfiehlt, Artikel 5 und Erwägungsgrund 15 des Vorschlags dahingehend zu ändern, dass beide Fälle eindeutig abgedeckt sind.**

Erwägungsgrund 15 des Vorschlags in seiner derzeitigen Form scheint sich nur auf Daten zu beziehen, die sich in der Übermittlung befinden: Er sieht vor, 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"*.

Obwohl Artikel 8 Absatz 1 und Absatz 2 auch die auf Endgeräten gespeicherten Kommunikationsdaten schützen würden, sollte die Verordnung darüber hinaus eindeutig das gleiche Schutzniveau für Kommunikationsdaten bieten, die nicht auf den Endgeräten der Nutzer, sondern auf anderen Geräten gespeichert werden, z. B. in von einem Dienstleister betriebenen Mailboxen oder als Teil eines Kommunikationsdienstes in der Cloud.[23] Der EDSB

weist daher nachdrücklich darauf hin, dass mit neuen technischen Paradigmen (z. B. Cloud Computing) die Vertraulichkeit der Kommunikation immer wichtiger wird.[24]

Wie die WP29 in ihrer Stellungnahme 01/2017[25] erläutert, beruht der in dem zitierten Text in Erwägungsgrund 15 beschriebene Anwendungsbereich des Schutzes auf einem veralteten Rahmenkonzept von Kommunikation. Heute wird ein Großteil der Kommunikationsdaten 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 Übermittlung von Daten im Rahmen der Kommunikation zwischen Teilnehmern desselben Cloud-basierten Dienstes (zum Beispiel Webmail-Anbieter) minimal: Die Übermittlung 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.

Eine allgemeinere Empfehlung des EDSB ist die gründliche Prüfung aller Begriffsbestimmungen in der vorgeschlagenen Verordnung im Hinblick auf eine Vermeidung unnötiger Abhängigkeiten von dem Kodex-Vorschlag und um sicherzustellen, dass das Schutzniveau gegenüber der geltenden Datenschutzrichtlinie für elektronische Kommunikation nicht gesenkt wird.

3.2 Einholung der Einwilligung von denjenigen, deren Rechte betroffen sind

Der EDSB befürwortet das erklärte Ziel der Kommission, sowohl für Inhalte als auch für Metadaten ein hohes Schutzniveau zu schaffen, indem sie der Einwilligung im Sinne der DSGVO in Artikel 6 und 8 des Vorschlags eine zentrale Rolle bei der Verarbeitung von elektronischen Kommunikationsdaten zuweist.

Diese Bestimmungen würden allerdings in manchen Fällen Dritten die Möglichkeit geben, ihre Einwilligung für Andere zu geben und so über deren Grundrechte zu entscheiden, was gegen das Prinzip der Selbstbestimmung des Einzelnen verstößt und dem Begriff der *„Einwilligung“* im Sinne der DSGVO im Kern widerspricht.

Ausgehend von den Begriffsbestimmungen des Vorschlags könnte die Einwilligung des Endnutzers zum Beispiel bedeuten, dass anstelle der Arbeitnehmer, die die Dienste benutzen, der Arbeitgeber als der Teilnehmer der Dienste die Einwilligung erteilt. Dies würde in der Regel auch in anderen Fällen zutreffen, wenn eine Organisation Dienste abonniert, die dann auf Basis dieses Abonnements von natürlichen Personen in Anspruch genommen werden, oder wenn Vermieter bestimmte Kommunikationsdienste für ihre Mieter bereitstellen.

Noch komplizierter wird die Situation dadurch, dass in dem Vorschlag nicht einfach die Einwilligung der *„Endnutzer“* zur Datenverarbeitung gefordert wird. Vielmehr werden in Hinblick darauf, wer die Einwilligung erteilen sollte, verschiedene Begriffe verwendet:

- In Artikel 6 Absatz 2 Buchstabe c muss der „*„betreffende Endnutzer“* seine Einwilligung in Bezug auf Metadaten erteilen;
- In Artikel 6 Absatz 3 Buchstabe a und Buchstabe b muss/müssen in Bezug auf Inhalte (für die Bereitstellung eines bestimmten Dienstes für einen Endnutzer) entweder *„der bzw. die betreffenden Endnutzer“* seine/ihre Einwilligung geben oder
- (in allen anderen Fällen) *„alle betroffenen Endnutzer“* ihre Einwilligung geben;
- In Artikel 8 Absatz 1 Buchstabe b, muss in Bezug auf den Schutz von Endeinrichtungen der „*Endnutzer“* einwilligen;

- In Artikel 15 und 16 (öffentlich zugängliche Verzeichnisse und unerbetene Kommunikation) dagegen müssen *„Endnutzer, die natürliche Personen sind“* einwilligen.

Aus diesen Gründen ist in Anbetracht der unklaren Definition des Begriffs *„Endnutzer“* und des uneinheitlichen Wortlauts in den verschiedenen die Einwilligung betreffenden Bestimmungen des Vorschlags nicht klar, wer in welcher Situation seine Einwilligung geben muss. In den folgenden drei Unterpunkten erläutert der EDSB seine drei wichtigsten Fragen in Bezug auf den Begriff der Einwilligung des Endnutzers und macht Vorschläge, wie diese jeweils gelöst werden könnten.

Die Einwilligung muss von denjenigen erteilt werden, die den Dienst in Anspruch nehmen

Zunächst muss der Vorschlag sicherstellen, dass genau die Personen, die den Kommunikationsdienst tatsächlich nutzen, auch diejenigen sind, die das Recht haben zu entscheiden, ob sie die Verarbeitung ihrer Kommunikationsdaten zulassen wollen oder nicht.

Wie bereits an früherer Stelle hervorgehoben sind diejenigen, die einen Dienst abonnieren, nicht immer auch diejenigen (oder die einzigen), die ihn in Anspruch nehmen. Ein Arbeitgeber kann beispielsweise einen Vertrag über Dienste abschließen, die dann von seinen Mitarbeitern und Besuchern genutzt werden, oder eine Hotelkette kann Kommunikationsdienstleistungen vertraglich vereinbaren, um sie ihren Hotelgästen zur Verfügung zu stellen. Ebenso kann ein Vermieter oder ein Familienoberhaupt Dienstleistungen vertraglich beziehen, die dann von mehreren Personen (z. B. anderen Familienmitgliedern, Mietern), die in dem gleichen Gebäude wohnen, (oder auch von Besuchern) genutzt werden.

Wir gehen davon aus, dass die Kommission sicherstellen wollte, dass die Einwilligung von eben den Personen eingeholt werden muss, die den Dienst tatsächlich nutzen, und nicht von denjenigen, die ihn abonnieren. Dies sollte jedoch in dem Vorschlag deutlicher zum Ausdruck kommen.

Der EDSB empfiehlt daher, den Begriff *„Endnutzer“* zum Zweck der Einwilligung zur Verarbeitung von Kommunikationsdaten als eigenständige Begriffsbestimmung in der E-Privacy-VO aufzunehmen. Die Begriffsbestimmung sollte sich auf die folgenden vier Elemente stützen: i) *natürliche Person; ii) die einen öffentlich zugänglichen elektronischen Kommunikationsdienst nutzt; iii) für private oder geschäftliche Zwecke; iv) ohne diesen Dienst notwendigerweise abonniert zu haben*[26].

Außerdem empfehlen wir, einen Erwägungsgrund in den Vorschlag aufzunehmen, der deutlich macht und auch konkrete Beispiele dafür anführt, dass beispielsweise Mitarbeiter, Mieter, Hotelgäste, Familienmitglieder, Besucher und ähnliche Personen, die tatsächlich die Dienste für private oder geschäftliche Zwecke nutzen, auch wenn sie diese nicht unbedingt abonniert haben, ebenfalls zu den Endnutzern zählen.

Die Einwilligung muss von allen an einer Kommunikation beteiligten Parteien eingeholt werden

Die vorgeschlagenen Vorschriften müssten auch deutlich machen, dass grundsätzlich alle Parteien, die an einer Kommunikation beteiligt sind, wie beispielsweise Sender und Empfänger einer elektronischen Nachricht und alle Teilnehmer einer Videokonferenz die Möglichkeit haben müssen, selbst zu entscheiden, ob sie die Verarbeitung ihrer Kommunikationsdaten zulassen wollen oder nicht.

Der EDSB geht davon aus, dass die Kommission – in den meisten typischen Fällen wie dem Einscannen von E-Mail-Inhalten zu Marktforschungszwecken oder für zielgruppenspezifische Werbung – beabsichtigte, die Einwilligung aller an der Kommunikation Beteiligten zu fordern. Gleichzeitig räumt der EDSB ein, dass es besondere Umstände geben kann, unter denen die

Einwilligung nur einer Partei ausreichend sein könnte (z. B. wenn die Standortdaten einer Person so verfolgt werden, dass keine personenbezogenen Daten anderer Personen involviert sind, oder wenn eine Person bestimmte eingeschränkte Dienste wie beispielsweise die Suche oder Organisation eigener empfangener E-Mails aufgrund von Schlüsselbegriffen oder Absendern beauftragt). Für diese Fälle notwendige Ausnahmen können ausdrücklich vorgesehen werden.[27]

Aus diesen Gründen und auch im Hinblick auf eine Vereinfachung des sehr komplexen Vorschlags empfiehlt der EDSB, in allen Fällen, in denen die Einwilligung der Endnutzer erforderlich ist, in dem gesamten Vorschlag durchgehend die gleiche Formulierung, nämlich *„alle Endnutzer“*, zu verwenden.[28] Diese einheitliche Vorgehensweise ist besonders wichtig im Hinblick auf die in Artikel 6 aufgeführten Metadaten und Inhalte sowie alle in Artikel 8 beschriebenen Verarbeitungsvorgänge.[29]

Die Rechte von Personen, die nicht an der Kommunikation beteiligt sind, müssen ebenfalls geschützt werden

Schließlich hat der EDSB auch Bedenken in Bezug auf den Schutz von Personen, die nicht an der Kommunikation beteiligt sind, deren Daten jedoch Teil der Kommunikation sind.[30] Die Verarbeitung derartiger Daten (über den familiären Bereich und ähnliche Ausnahmesituationen hinaus) unterliegt gemäß der DSGVO der Anforderung, dass für die Verarbeitung ein Rechtsgrund nach Artikel 6 vorliegen muss.[31]

Um jede Unklarheit darüber auszuschließen, inwieweit die Bestimmungen der DSGVO in diesen Situationen ebenfalls gelten, **empfiehlt der EDSB, eine materielle Bestimmung hinzuzufügen, die bestätigt, dass *„eine auf der Einwilligung der Endnutzer beruhende Verarbeitung die Rechte und Freiheiten von Personen, deren personenbezogene Daten mit der Kommunikation in Zusammenhang stehen, insbesondere deren Rechte auf Achtung der Privatsphäre und den Schutz ihrer personenbezogener Daten, nicht beeinträchtigen darf“.***

3.3 Beziehung zwischen der DSGVO und der E-Privacy-VO

Der EDSB befürwortet, dass die Beziehung zwischen der DSGVO und der E-Privacy-VO, wie bereits von ihm empfohlen, so komplementär gehalten wird, wie sie es derzeit ist. Die derzeitige Formulierung „*ergänzt und präzisiert“,* die jetzt auch in Artikel 1 Absatz 3 des Vorschlags aufgenommen wurde, ist zur Bestimmung der Beziehung ausreichend.[32]

Der EDSB nimmt auch positiv zur Kenntnis, dass in Erwägungsgrund 5 jetzt eindeutig erklärt wird, dass der Vorschlag zu *„keiner Absenkung des Schutzniveaus führt, das natürliche Personen nach [der DSGVO] genießen“.* Der EDSB empfiehlt, diesen Satz durch Hinzufügen der folgenden Formulierung zu verstärken und seinen Inhalt damit positiver auszudrücken *„- sondern zielt im Gegenteil darauf ab, in Anbetracht des erhöhten Schutzbedarfs bezüglich der Vertraulichkeit der Kommunikation falls erforderlich zusätzliche und ergänzende Garantien zu bieten“.*

Der EDSB weist jedoch darauf hin, dass diese Beziehung die folgende Frage aufwirft: Unterliegt in Fällen, in denen der Endnutzer einem Dienstleister seine Einwilligung zur Übermittlung von Metadaten und/oder Inhaltsdaten an einen Dritten gegeben hat, der damit als für die Verarbeitung Verantwortlicher handelt, die Verarbeitung der Daten durch diesen Dritten der DSGVO oder der E-Privacy-VO?

Die Beantwortung dieser Frage hat erhebliche Auswirkungen. Wenn die weitere Verarbeitung der Daten der DSGVO unterliegt, kann sich der Dritte auf alle in Artikel 6 der DSGVO aufgeführten Rechtsgründe für die Verarbeitung der Daten berufen. Sollte dagegen der Vorschlag für die E-Privacy-VO für die weitere Verarbeitung gelten, so wäre die Verarbeitung nur möglich, wenn eine Einwilligung dafür vorliegt (oder ein bestimmter anderer, in dem Vorschlag festgeschriebener Ausnahmefall zutrifft).

Wird der Vorschlag so verstanden, dass Dritte sich für die Verarbeitung auf einen beliebigen Grund in der DSGVO beziehen können, so würde damit eine Lücke entstehen, die das in der E-Privacy-VO garantierte Schutzniveau erheblich senkt. Kommunikationsdienstleister (die dem Vorschlag unterliegen würden) könnten dann beispielsweise versucht sein, Tochterunternehmen zu gründen, die die strengeren Maßstäbe der E-Privacy-VO umgehen könnten.

Um Rechtssicherheit in diesem Punkt zu schaffen, schlägt der EDSB vor, in dem Vorschlag in Form einer materiellen Bestimmung festzulegen, dass „*weder Anbieter von elektronischen Kommunikationsdiensten noch Dritte personenbezogene Daten, die aufgrund einer Einwilligung oder aus einem anderen Rechtsgrund gemäß der E-Privcay-VO erhoben wurden, aus einem anderen, nicht ausdrücklich in der E-Privacy-VO vorgesehenen Rechtsgrund verarbeiten dürfen“.*

Darüber hinaus empfiehlt der EDSB, dem Vorschlag einen Erwägungsgrund hinzuzufügen, aus dem Folgendes hervorgeht: *„Wenn die Verarbeitung aufgrund einer Ausnahme von den in der E-Privacy-VO aufgeführten Verboten zulässig ist, gilt jede andere Verarbeitung aufgrund von Artikel 6 der DSGVO, einschließlich der Verarbeitung zu einem anderen Zweck nach Artikel 6 Absatz 4 der DSGVO, als unzulässig.“ Dabei würde nichts dagegen sprechen, dass die für die Verarbeitung Verantwortlichen eine zusätzliche Einwilligung für neue Verarbeitungsaktivitäten einholen.*

Dies sollte die Gesetzgeber nicht daran hindern, weitere beschränkte und spezifische Ausnahmen in die E-Privacy-VO aufzunehmen, um beispielsweise „*lebenswichtige Interessen*“ von Personen im Sinne von Artikel 6 Buchstabe d der DSGVO zu schützen oder die Verarbeitung zu wissenschaftlichen Forschungszwecken oder (behördlichen) statistischen Zwecken nach Artikel 89 der DSGVO zuzulassen.[33]

Des Weiteren sieht der vorgeschlagene letzte Satz von Erwägungsgrund 5 vor, dass *„[e]ine Verarbeitung elektronischer Kommunikationsdaten durch Betreiber elektronischer Kommunikationsdienste [...] nur im Einklang mit der vorliegenden Verordnung erlaubt sein [sollte]“*. Dieser Satz ist mehrdeutig, da er durchaus zu der Annahme führen könnte, dass die Verarbeitung elektronischer Kommunikationsdaten durch andere als die Betreiber von elektronischen Kommunikationsdiensten nicht in den Anwendungsbereich der E-Privacy-VO fallen würde. Das stünde jedoch im Widerspruch zu dem Wortlaut in Artikel 2 Absatz 1 und würde das Schutzniveau der E-Privacy-VO senken. Es kommt nicht darauf an, *wer* die Daten verarbeitet, sondern *welche Art von Daten* geschützt ist. Die Verarbeitung von elektronischen Kommunikationsdaten und Informationen, die in Zusammenhang mit den Endgeräten der Nutzer stehen, sollte unabhängig von dem Verarbeiter dieser Daten ganz eindeutig in den Anwendungsbereich der E-Privacy-VO fallen. **Aus diesem Grund empfiehlt der EDSB, den oben zitierten Satz in Erwägungsgrund 5 wie folgt zu ersetzen: *„Eine Verarbeitung elektronischer Kommunikationsdaten sollte nur im Einklang mit der vorliegenden***

Verordnung und aus einem ausdrücklich in dieser Verordnung vorgesehenen Rechtsgrund erlaubt sein".

3.4 Die Einwilligung muss freiwillig erteilt werden: „*Tracking-Walls*" müssen abgeschafft werden

„Tracking-Walls" und der Begriff der freiwillig erteilten Einwilligung

Der auf Artikel 5 Absatz 3 der aktuellen Datenschutzrichtlinie für elektronische Kommunikation beruhende Artikel 8 Absatz 1 verbietet jede *„Nutzung der Verarbeitungs- und Speicherfunktionen von Endeinrichtungen und jede Erhebung von Informationen aus Endeinrichtungen der Endnutzer, auch über deren Software und Hardware"*. Zu den Ausnahmen gehören Fälle nach Artikel 8 Absatz 1 Buchstabe b, in denen „*der Endnutzer [...] seine Einwilligung gegeben [hat]".*

Der EDSB begrüßt diese neuen Bestimmungen und empfiehlt, das derzeitige Erfordernis der Einwilligung beizubehalten, doch räumt er auch ein, dass Artikel 5 Absatz 3 der Datenschutzrichtlinie für elektronische Kommunikation, wie jetzt angewandt, sein Potenzial nicht voll ausgeschöpft hat, eine echte Wahlmöglichkeit zu bieten und natürlichen Personen die Kontrolle zu geben. Stattdessen sind von Unternehmen und anderen Organisationen Einwilligungsregelungen mit dem Ziel entwickelt worden, die zwar angeblich den rein gesetzlichen Anforderungen bezüglich der Einhaltung der Datenschutzrichtlinie für elektronische Kommunikation Genüge tun, aber tatsächlich den Nutzern keine echte Wahlmöglichkeit und keine Kontrolle darüber geben, was mit ihren Daten geschieht.

Dieses Phänomen wird mitunter als Problem der *„Tracking-Walls"* bezeichnet. Tracking-Walls bedeuten, dass Nutzer, die die Verfolgung ihrer Aktivitäten auf anderen Websites nicht akzeptieren, keinen Zugang zu den Websites erhalten, zu denen sie eigentlich Zugang wünschen.[34] Cookies und andere Methoden wie zum Beispiel virtuelle Fingerabdrücke werden dazu verwendet, die digitale Spur der Nutzer im Internet zu verfolgen, und Unternehmen haben darauf Zugriff und können diese Informationen für Profilerstellung, Werbung und andere kommerzielle Zwecke verwenden. Diese angeblich „auf Einwilligung beruhende" und verallgemeinerte Rückverfolgung birgt große Risiken für die Privatsphäre und bedeutet, dass jemand Kontrolle über die personenbezogenen Daten von Menschen bekommt, die nicht das Geringste dagegen unternehmen können.

Tracking-Walls untergraben die Idee, dass eine Einwilligung freiwillig gegeben werden muss; dies ist jedoch ein zentrales Erfordernis sowohl der Richtlinie 94/46/EG als auch der DSGVO. Die DSGVO stellt in dieser Hinsicht eine Verbesserung der Richtlinie 94/46/EG dar, weil sie nicht nur vorsieht, dass die Einwilligung freiwillig erfolgen muss, sondern auch weitere Hinweise dazu gibt, was dies konkret bedeutet. So sieht sie insbesondere vor, dass eine Einwilligung nicht als freiwillig erteilt gilt, wenn die Erbringung einer Dienstleistung von der Einwilligung einer natürlichen Person in die Verarbeitung ihrer personenbezogenen Daten abhängig ist, obwohl diese Verarbeitung für die Erbringung dieser Dienstleistung nicht erforderlich ist.[35] Genau dies trifft auf Tracking-Walls zu, die den Nutzer häufig zur Einwilligung in die Verwendung von Tracking-Cookies Dritter zwingen, die für die Erbringung der betreffenden Dienstleistung nicht erforderlich sind. Es ist äußerst wichtig, dass Nutzer eine Dienstleistung in Anspruch nehmen können, ohne dass ihre Aktivitäten verfolgt werden, besonders wenn es um eine Verfolgung durch Dritte und in Situationen geht, in denen der Nutzer auf die Dienstleistung nicht verzichten kann und keine echte Alternative dazu besteht. Man könnte aufgrund der DSGVO argumentieren, dass derartige Tracking-Walls unter gar

keinen Umständen zulässig sind, da keine *„freiwillig"* und in informierter Weise gegebene Einwilligung vorliegt. Das sollte jedoch im Interesse der Rechtssicherheit in der E-Privacy-VO klar zum Ausdruck gebracht werden.

In Anbetracht der Bedeutung einer freiwillig erteilten Einwilligung und der häufig unzureichenden Umsetzung des derzeitigen Artikels 5 Absatz 3 durch Betreiber von Websites empfiehlt der EDSB ein vollständiges und ausdrückliches Verbot so genannter „Tracking-Walls".

Dementsprechend empfiehlt der EDSB, in die E-Privacy-VO eine materielle Bestimmung aufzunehmen, die besagt, dass *„niemandem der Zugriff auf Dienste der Informationsgesellschaft (egal ob diese vergütet werden oder kostenlos sind) mit der Begründung verweigert werden darf, dass er oder sie die nach Artikel 8 Absatz 1 Buchstabe b erforderliche Einwilligung zur Verarbeitung personenbezogener Daten, die für die Bereitstellung dieser Dienste nicht benötigt werden, nicht gegeben hat".*

Zur Vervollständigung dieser Bestimmung empfiehlt der EDSB außerdem ein zusätzliches, ausdrückliches Verbot der Praxis, Nutzern den Zugriff zu verwehren, die zum Schutz ihrer Informationen und Endgeräte Anti-Werbungssoftware oder andere Anwendungen und Erweiterungen installiert haben.

Zur Klarstellung empfiehlt der EDSB auch in einem Erwägungsgrund ausdrücklich zu bestätigen, dass die *„Verarbeitung von Daten zum Zweck der Bereitstellung zielgerichteter Werbung nicht als für die Erbringung einer Dienstleistung notwendig erachtet werden kann".*

Ein anderes Problem in diesem Zusammenhang ist, dass Endnutzer sich damit konfrontiert sehen können, zur Einwilligung gezwungen zu werden, damit sie ein Smart-Gerät (z. B. Smart-TV) überhaupt erst benutzen können. Im Rahmen des Internets der Dinge sollte sichergestellt werden, dass die Funktion von Smart-Geräten nicht von einer Einwilligung abhängig gemacht wir, die für die gewünschte Funktion gar nicht erforderlich ist. Damit werden die Bedingungen in Artikel 7 Absatz 4 der DSGVO präzisiert und spezifisch auf das Internet der Dinge und auf Fälle bezogen, in denen Endnutzer physische Produkte kaufen und verwenden und bestimmte Funktionen dieser Produkte erwarten können sollten.

Daher empfiehlt der EDSB, ein ähnliches, spezifisches Verbot in den Vorschlag aufzunehmen, und zwar in Form einer materiellen Bestimmung, die besagt, dass *„niemandem eine Funktion eines zum Internet der Dinge gehörenden Gerätes (egal ob diese kostenpflichtig oder kostenlos bereitgestellt wird) mit der Begründung verweigert werden darf, dass er oder sie die nach Artikel 8 Absatz 1 Buchstabe b erforderliche Einwilligung zur Verarbeitung von Daten, die nicht für die gewünschte Funktion benötigt werden, nicht gegeben hat".*

Dieser umfassende Ansatz böte natürlichen Personen das höchste Schutzniveau, aber auch Rechtssicherheit und gleiche Wettbewerbsbedingungen für alle Marktteilnehmer.

Alternative, auf Transparenz und einer intensiveren Einbindung der Nutzer beruhende Geschäftsmodelle

Dieser Ansatz steht der innovativen Verwendung und Wiederverwendung von personenbezogenen Daten in der Welt der *„Big Data"* nicht im Wege. Vielmehr zielt er auf die Stärkung von Grundrechten und gleichzeitig auf die Eröffnung neuer Chancen für Unternehmen ab, auf gegenseitigem Vertrauen beruhende innovative, auf personenbezogenen Daten fußende Dienste zu entwickeln. Die Art und Weise, wie Organisationen personenbezogene Daten verwenden und wiederverwenden muss transparenter werden und die Menschen müssen mehr Kontrolle darüber haben, was mit ihren Daten geschieht. Wie der EDSB bereits in seiner Stellungnahme *„Bewältigung der Herausforderungen in Verbindung mit Big Data"*[36] ausgeführt hat, sollten Unternehmen und andere Organisationen, die viel Zeit und Mühe in innovative Möglichkeiten für die Nutzung personenbezogener Daten investieren, bei der Umsetzung von Datenschutzgrundsätzen das gleiche innovative Denken an den Tag legen.

Telefonunternehmen, Internetdienstleister und andere Organisationen, die Kommunikationsdienste anbieten, die in den Anwendungsbereich der E-Privacy-VO fallen, sind oft in der einmaligen Lage, eine für beide Seiten vorteilhafte und auf gegenseitigem Vertrauen beruhende Beziehung aufzubauen. Auf der Grundlage dieser Vertrauensbeziehung sind Kunden oftmals bereit, sich auf eine Partnerschaft einzulassen und die Verwendung ihrer personenbezogenen Daten für innovative Zwecke zum Vorteil aller Beteiligten zuzulassen[37].

3.5 Die Privatsphäre muss durch datenschutzfreundliche Voreinstellungen geschützt werden

Der EDSB befürwortet mit Nachdruck die Klarstellung in Artikel 9, dass die Einwilligung durch technische Einstellungen zum Ausdruck gebracht werden könnte, sofern dies technisch möglich und wirksam ist. Zur Sicherstellung der Wirksamkeit sind jedoch auch die Anforderungen bezüglich datenschutzfreundlicher Voreinstellungen von größter Wichtigkeit. Tools dieser Art müssen Nutzern sowohl bei der Ersteinrichtung eines Gerätes mit datenschutzfreundlichen Voreinstellungen als auch bei jeder größeren Veränderung der Geräte oder Softwareprogramme durch die Nutzer angeboten werden. Darüber hinaus sollte die Einhaltung akzeptierter technischer und politischer Compliance-Normen durch alle Beteiligten, darunter die Betreiber der Website, verbindlich werden.[38]

Wie in der vorläufigen Stellungnahme des EDSB[39] erläutert, benötigen Nutzer benutzerfreundliche und wirksame Mechanismen für die Erteilung und den Widerruf ihrer Einwilligung. Der EDSB befürwortet daher, dass der Vorschlag die Möglichkeit vorsieht, die Einwilligung der Nutzer zur Verarbeitung durch den Einsatz entsprechender Einstellungen eines Browsers oder einer ähnlichen Anwendung zum Ausdruck zu bringen.

Grundsätzlich ist der Ansatz in Artikel 9 Absatz 2 des Vorschlags, die technischen Konfigurationsmerkmale des Endgerätes eines Nutzers und die darauf installierte Software zur Erteilung der Einwilligung zu verwenden, sinnvoll. Mit der in Artikel 9 Absatz 2 des Vorschlags enthaltenen Formulierung *„[u]nbeschadet des Absatzes 1"* soll sichergestellt werden, dass alle zur Erteilung der Einwilligung verwendeten, benutzerfreundlichen Mechanismen auch den Anforderungen der DSGVO gerecht werden und insbesondere hinreichend spezifisch sein und die Möglichkeit der betroffenen Person zum Widerruf der Einwilligung bieten müssen.

Artikel 10 des Vorschlags dagegen legt fest, dass Endnutzer die *„Möglichkeit"* haben müssen, durch Softwareeinstellungen zu entscheiden, ob sie Dritten erlauben, auf Informationen in ihren Endeinrichtungen zuzugreifen oder Informationen darin zu speichern. Der EDSB hält diese Vorschrift für unvereinbar mit Artikel 25 der DSGVO über *„Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen"*. **Der EDSB**

empfiehlt, dass der Vorschlag vielmehr eine Verpflichtung für Hardware- und Software-Anbieter enthalten sollte, Voreinstellungen umzusetzen, die Endnutzer gegen unerlaubten Zugriff auf Informationen in ihren Geräten und gegen die Speicherung von Informationen in ihren Geräten schützen.

Der EDSB empfiehlt außerdem, dass eine materielle Bestimmung die Einhaltung akzeptierter technischer und politischer Compliance-Normen durch alle Beteiligten, darunter die Betreiber von Websites, vorsehen sollte.

Mit Artikel 10 Absatz 2 werden Softwareanbieter verpflichtet, die Nutzer bei der Inbetriebnahme über die Einstellungsmöglichkeiten zur Privatsphäre zu informieren. Es ist äußerst wichtig hier, dass Nutzern bei dieser Inbetriebnahme eine einfache Auswahlmöglichkeit gegeben wird, mit der sie Tracking vermeiden können. Die Einwilligung der Nutzer zum Tracking sollte jedoch nicht auf der gleichen *„alles oder nichts"*-Entscheidung beruhen. Wie bereits erwähnt, müssen alle technischen Mittel, die zur Erteilung der Einwilligung verwendet werden, die in Artikel 4 Absatz 12 der DSGVO festgelegten Einwilligungsanforderungen erfüllen, darunter nicht nur das Erfordernis der *„freiwillig"* erteilten Einwilligung, sondern auch das Erfordernis der *„für den bestimmten Fall"* und *„in informierter Weise"* gegebenen Einwilligung. Die Bereitstellung allgemeiner Informationen über die Datenschutzeinstellungen bei der Inbetriebnahme der Software, wobei in Bezug auf die zukünftige Nutzung nur die Wahlmöglichkeit *„alles oder nichts"* angeboten wird, würde den Einwilligungsanforderungen in der DSGVO nicht gerecht werden.

Ein weiterer wichtiger Aspekt ist, dass Nutzer nicht nur bei der Installation oder Inbetriebnahme der Software über die Datenschutzeinstellungen informiert werden sollten, sondern auch immer dann, wenn Nutzer erhebliche Änderungen an ihren Geräten oder Softwareprogrammen vornehmen. Solche Hinweise sollten auch dann gegeben werden, wenn Nutzer beispielsweise die Werkeinstellungen auf ihren Geräten wiederherstellen. Auch in solchen Fällen sollten die datenschutzfreundlichen Voreinstellungen erhalten bleiben. Wenn das Gerät in Gebrauch ist, müssen diese jederzeit leicht zugänglich sein.

3.6 Geräte dürfen ohne die Einwilligung der Nutzer nicht verfolgt werden

Ferner hält der EDSB auch die in Artikel 8 Absatz 2 Buchstabe b der E-Privacy-VO vorgeschlagene Ausnahme für bedenklich, die sich auf die Verfolgung der Nutzer von Kommunikationsgeräten in öffentlichen Räumen in der physischen Welt bezieht (zum Teil auch *„Geräte-Ortung"* genannt). Diese Art von Technologie wird beispielsweise bereits zur Messung der Kundenfrequenz in viel besuchten Einkaufszentren oder zur Aufzeichnung von Verkehrsströmen im Straßenverkehr eingesetzt. Obwohl die erhobenen Daten oft lediglich zur Verwendung für statistische Zwecke bestimmt sind, könnten sie auch Auskunft über den Standort und über Verhaltensmuster der Personen geben. Unter bestimmten Umständen, zum Beispiel in der Nähe einer religiösen Einrichtung oder einer Klinik, sind Informationen über den Aufenthaltsort selbst in unaufbereiteter Form ohne umfangreiche Profilierung oder Analyse schon hoch sensibel.

In Anbetracht der möglichen datenschutzrechtlichen Risiken ist es daher besorgniserregend, dass der Vorschlag beinahe eine Pauschalerlaubnis für diese Art der Verfolgung gibt, sofern ein Hinweis angezeigt wird, der dem Nutzer Auskunft darüber gibt, welche Maßnahmen er ergreifen kann, um *„die Erhebung zu beenden oder auf ein Minimum zu beschränken"*.

Es ist schwer nachzuvollziehen, warum diese Art der Nutzung von Standortdaten ein niedrigeres Schutzniveau als andere Nutzungsarten verdient. Nirgendwo sonst in dem Vorschlag ist es Anbietern von Kommunikationsdiensten erlaubt, Informationen über den Standort der Nutzer zu verarbeiten, es sei denn diese Nutzer haben der Verarbeitung

zugestimmt. Die in diesem Zusammenhang der Geräte-Ortung in der physischen Welt verarbeiteten Daten sollten nicht als weniger sensibel betrachtet werden.

Verglichen mit einer Verarbeitung, die auf einer Einwilligung nach dem Opt-in-Prinzip beruht, bietet eine Opt-out-Lösung aufgrund des Default-Effekts ein geringeres Schutzniveau: Die meisten Menschen haben einfach nicht die Zeit oder das Interesse aktiv zu werden; sie nehmen stattdessen die Standardauswahl einfach an und widersprechen nicht. Über dieses eher allgemeine Problem hinaus ist die vorgeschlagene Vorgehensweise eines Hinweises in Kombination mit einer schwachen und unwirksamen „*Opt-out*"-Lösung in verschiedener Hinsicht bedenklich.

Zum einen könnte ein solcher Hinweis an einem viel besuchten und betriebsamen Ort dem nichts ahnenden Nutzer leicht entgehen. Außerdem werden Nutzer dort, wo diese Technologie weiträumig eingesetzt wird, unter Umständen nur in den Randzonen des Einsatzbereichs darüber informiert, sodass das Vorhandensein dieser Technologie dadurch noch unauffälliger wird.

Zum anderen ist es aufgrund der Wortwahl des Vorschlags Nutzern unter Umständen gar nicht möglich, dieser Art der Verfolgung auszuweichen, es sei denn sie schalten Grundfunktionen ihrer Geräte wie beispielsweise den drahtlosen Zugang zum Internet auf ihren Mobiltelefonen einfach ganz aus. Es kann Nutzern nicht zugemutet werden, bei jedem Betreten eines Bereichs, in dem Technologien zur Geräte-Ortung eingesetzt werden, dem Tracking – womöglich mehrfach – aktiv widersprechen zu müssen. Dies gilt besonders dann, wenn mit ihrem Widerspruch der Verlust bestimmter Funktionen ihrer Geräte verbunden ist. In diesem Zusammenhang ist auch die folgende in Erwägungsgrund 18 in Bezug auf die Einwilligung der Nutzer angeführte Überlegung zu unterstreichen: „*Grundlegende breitbandige Internetzugangs- [...]dienste gelten als unverzichtbare Dienste, damit Personen kommunizieren und an den Vorteilen der digitalen Wirtschaft teilhaben können. Eine Einwilligung in die Verarbeitung von Daten [...] ist unwirksam, wenn die betroffene Person keine echte und freie Wahl hat oder ihre Einwilligung nicht verweigern oder widerrufen kann, ohne Nachteile zu erleiden.*"

Außerdem ist darauf hinzuweisen, dass eine Methode, die die Einrichtung einer Opt-out-Lösung technisch ermöglicht wie zum Beispiel durch Registrierung der WLAN MAC-Adresse des Gerätes in einer Datenbank, die der Anbieter des Geräte-Ortungsdienstes überprüfen muss, ebenso gut auch zur Einrichtung eines Opt-in-Verfahrens verwendet werden kann. Eine in informierter Weise und freiwillig gegebene Einwilligung, wie sie in der DSGVO gefordert wird, ist in jedem Fall vorzuziehen.

Vor diesem Hintergrund empfiehlt der EDSB, den derzeitigen Artikel 8 Absatz 2 Buchstabe b sowie Artikel 8 Absatz 3 und Artikel 8 Absatz 4 zu streichen und durch eine - einfachere - Anforderung der Einwilligung (aller betroffenen Endnutzer[40]) zu ersetzen. Darüber hinaus sollte die E-Privacy-VO – wie in Artikel 6 über die Verarbeitung von Inhalt und Metadaten – auch festlegen, dass eine auf Einwilligung beruhende Verarbeitung nur dann zulässig ist, wenn die damit verfolgten Zwecke *„durch eine Verarbeitung anonymisierter Informationen nicht erreicht werden können*[41]*".*

Beschränkte und zielgerichtete Ausnahmen können, falls erforderlich, gemäß Artikel 89 der DSGVO für wissenschaftliche Forschungszwecke und (behördliche) statistische Zwecke und gemäß Artikel 6 Absatz d der DSGVO zum Schutz von „lebenswichtigen Interessen" von Personen vorgesehen werden.[42]

Ein zusätzliche und ebenso beschränkte und eng ihrem Zweck angepasste Ausnahme könnte für Personenzählungszwecke vorgesehen werden (wie zum Beispiel Messungen der Kundenfrequenz und Verkehrsströme), wobei entsprechende Garantien vorzusehen sind, darunter technische und organisatorische Maßnahmen, um sicherzustellen, dass die zu diesen Zwecken verarbeiteten Daten zu keinen anderen Zwecken und insbesondere nicht zur Unterstützung von Maßnahmen oder Entscheidungen verarbeitet werden dürfen, die in Bezug auf die betroffene Person getroffen werden („*funktionelle Trennung*“)[43]. Gleichzeitig muss eine wirksame horizontale Möglichkeit bestehen, der Verarbeitung zu widersprechen (ähnlich wie die Robinsonlisten (Do-Not-Call) bei der unerbetenen Kommunikation oder das Tracking-Verbot (Do-Not-Track) beim Tracking im Internet), und es muss strenge Auflagen in Bezug auf die Aufbewahrungsdauer der Daten geben.

Der EDSB empfiehlt außerdem, dass die E-Privacy-VO konkret auf die Möglichkeit des Europäischen Datenschutzausschusses (EDSA) verweisen sollte, weitere Leitlinien bezüglich der anzuwendenden Garantien bereitzustellen. Diese detaillierteren Leitlinien könnten zum Beispiel eine Empfehlung enthalten, dass in typischen Anwendungsfällen für statistische Zwecke die Kennungen der Endnutzer-Geräte auf keinen Fall direkt gespeichert und verarbeitet werden dürfen, sondern nur als Grundlage zur Berechnung neuer pseudonymisierter Kennungen verwendet werden dürfen, und dass diese Kennungen nicht über verschiedene Verfolgungsdienste hinweg verknüpft werden dürfen und nur für eine kurze, für die statistischen Berechnungen unbedingt erforderliche Zeit bestehen bleiben dürfen.

3.7. Beschränkungen müssen begrenzt sein und Garantien unterliegen

Artikel 11 des Vorschlags entspricht im Großen und Ganzen dem aktuellen Artikel 15 der Datenschutzrichtlinie für elektronische Kommunikation. Artikel 15 Absatz 1 der Datenschutzrichtlinie für elektronische Kommunikation ermöglicht Mitgliedstaaten unter anderem die Einführung nationaler Rechtsvorschriften über die Vorratsspeicherung von Daten, nach denen Dienstleister zur Vorratsspeicherung von elektronischen Kommunikationsdaten zwecks Feststellung, Ermittlung und Verfolgung von schweren Straftaten wie unter anderem Terrorismus verpflichtet sind. Nach dem *Digital Rights* Urteil[44] von 2014, das die Vorratsdatenspeicherungs-Richtlinie (2006/24/EG)[45] für ungültig erklärte, unterliegen Mitgliedstaaten keiner auf ein bestimmtes Rechtsinstrument der Union zurückgehenden gesetzlichen Pflicht mehr, Vorschriften über die Vorratsdatenspeicherung einzuführen oder beizubehalten.

Der EDSB möchte bei dieser Gelegenheit noch einmal darauf hinweisen, dass alle nationalen Vorschriften über die Vorratsdatenspeicherung, wie in der einschlägigen Rechtssprechung des Europäischen Gerichtshofes dargelegt, die Bestimmungen der Charta – und insbesondere der Artikel 7, 8, 11, 47 und 52 – einhalten müssen. Insbesondere müssen Mitgliedstaaten die Rechtsprechung im Fall *Digital Rights Ireland* und damit auch das jüngste Urteil im Fall *Tele 2 Sverige* und *Watson und andere*[46] beachten.

Darüber hinaus unterstützt der EDSB den Ansatz des Vorschlags, nur bestimmte der in Artikel 23 Absatz 1 der DSGVO aufgeführten Gründe als Begründung für eine Beschränkung der in Artikel 5 bis Artikel 8 des Vorschlags niedergelegten Rechte und Pflichten zuzulassen. In Anbetracht der Spezialität des Vorschlags im Vergleich zu der DSGVO wäre es in der Tat unangemessen, *alle* in Artikel 23 der DSGVO aufgeführten Ausnahmegründe zuzulassen[47].

Der EDSB ist jedenfalls der Auffassung, dass die Tatsache als solche, dass der beabsichtigte Anwendungsbereich des Vorschlags im Vergleich zu dem der aktuellen Datenschutzrichtlinie

für elektronische Kommunikation ausgeweitet wurde, nicht so verstanden werden darf, dass er Mitgliedstaaten eine Generalvollmacht erteilt, den Anwendungsbereich aller – bereits vorhandenen oder zukünftigen – Vorschriften über Vorratsdatenspeicherung über die herkömmlichen, in Artikel 15 Absatz 1 der Datenschutzrichtlinie für elektronische Kommunikation erfassten elektronischen Kommunikationsdienste hinaus auszuweiten. Zumindest müsste die Notwendigkeit und Verhältnismäßigkeit aller derartigen Verpflichtungen zur Vorratsdatenspeicherung im Einklang mit der Charta und der oben genannten Rechtssprechung des Gerichtshofes nachgewiesen werden.[48]

Zusätzliche Garantien

Nach Artikel 23 Absatz 2 der DSGVO müssen Gesetzesmaßnahmen, die Beschränkungen einführen, bestimmte, spezifisch aufgeführte Vorschriften enthalten, wie zum Beispiel eine Erläuterung der Verarbeitungszwecke sowie Garantien gegen Missbrauch oder unrechtmäßigen Zugriff bzw. unrechtmäßige Übermittlung. Es sollte außer Zweifel stehen, dass diese in Artikel 23 Absatz 2 vorgesehenen zusätzlichen Spezifikationen und Garantien auch für Beschränkungen gelten müssen, die im Rahmen der E-Privacy-VO eingeführt werden. Dies sollte in dem Vorschlag in Form einer materiellen Bestimmung deutlich gemacht werden.[49]

Darüber hinaus **empfiehlt der EDSB den Gesetzgebern, sorgfältig zu prüfen, welche konkreten Garantien im Rahmen des Vorschlags erforderlich sind**, und zwar unter Berücksichtigung der Tatsache, dass jede Beschränkung nicht nur Auswirkungen auf die Rechte des Einzelnen auf den Schutz seiner personenbezogenen Daten hat, sondern auch einen Eingriff in die Vertraulichkeit der Kommunikation darstellt.

Insbesondere in Fällen, in denen Artikel 23 Absatz 1 Buchstabe e der DSGVO Anwendung findet, empfiehlt der EDSB, in den Vorschlag aufzunehmen, dass Gesetzesmaßnahmen, die Beschränkungen einführen, das Erfordernis einer vorherigen Genehmigung durch eine Justizbehörde für Zugriffe auf Inhalte oder Metadaten vorsehen sollten.[50]

Transparenz im Hinblick auf Auskunftsersuchen staatlicher Stellen

In globalen Netzen überqueren Nachrichten Grenzen, ohne dass die Nutzer dies merken. Nachrichten zwischen EU-Mitgliedstaaten können über Drittländer übermittelt werden und Nachrichten zwischen Drittländern können auch das EU-Hoheitsgebiet durchqueren. So können an Anbieter von Kommunikationsdiensten, die ihren Sitz in der EU haben oder dort ihre Tätigkeit ausüben, Ersuchen um Information über oder Zugriff auf Daten ihrer Nutzer von Strafverfolgungsbehörden oder Sicherheitsdiensten anderer Mitgliedstaaten und Drittländern ergehen, und dies gestützt auf anwendbare nationale Rechtsvorschriften und Praktiken, die Ausnahmen vom Recht auf Vertraulichkeit der Kommunikation festlegen. Nach dem Inkrafttreten der DSGVO dürfen sich solche Ersuchen um die Übermittlung personenbezogener Daten in ein Drittland nur noch auf eine internationale Übereinkunft wie etwa ein Rechtshilfeabkommen stützen.[51]

Der Einsatz von Sicherheits- und Strafverfolgungsbefugnissen zur Verletzung der Vertraulichkeit der Kommunikation muss im Einklang mit den Grundsätzen der Notwendigkeit und Verhältnismäßigkeit stehen. Die Information natürlicher Personen, die Gegenstand solcher Maßnahmen sind, kann natürlich eingeschränkt werden, um beispielsweise die Ziele einer laufenden Ermittlung nicht zu gefährden, doch würde ein allgemeines Bewusstsein für die

Häufigkeit und den Umfang solcher an die Anbieter von Kommunikationsdiensten herangetragenen Ersuchen um Offenlegung den Bürgern ganz allgemein und auch öffentlichen Einrichtungen die Möglichkeit geben, Vergleiche anzustellen und die allgemeine Praxis im Umgang mit diesen Instrumenten zu bewerten. Transparenz im Hinblick auf Auskunftsersuchen staatlicher Stellen kann also eine wichtige Rolle bei der Gewährleistung der Wahrung von Grundrechten spielen.

Demzufolge hatte der EDSB bereits in seiner vorläufigen Stellungnahme empfohlen, in der E-Privacy-VO spezifische Bestimmungen für eine bessere Transparenz vorzusehen[52]. Er empfahl insbesondere, in einer neuen Bestimmung Organisationen dazu zu verpflichten, zumindest regelmäßig und in aggregierter Form Auskunft über Informationsersuchen von Strafverfolgungsbehörden und anderen staatlichen Stellen zu erteilen. Diese Bestimmung sollte für Ersuchen sowohl aus Ländern der EU als auch aus Drittländern gelten. Außerdem hatten wir darauf hingewiesen, dass im Hinblick auf derartige Ersuchen aus Drittländern die Dienstanbieter die in Artikel 48 der DSGVO formulierte Bedingung der Rechtmäßigkeit beachten sollten.

Zwar begrüßt der EDSB, dass in Artikel 11 Absatz 2 bereits Schritte im Sinne einer besseren Transparenz unternommen werden, indem der zuständigen Aufsichtsbehörde auf Anfrage Informationen über diese Verfahren zur Verfügung gestellt werden müssen, doch empfehlen wir den Gesetzgebern die Transparenz durch ein Erfordernis der Veröffentlichung dieser Informationen noch weiter zu erhöhen.

Zudem spricht sich der EDSB dafür aus, dass Aufsichtsbehörden nicht nur „*auf Anfrage*“ Zugang zu diesen Informationen gewährt werden sollte, sondern dass ihnen *von Amts wegen* regelmäßig Bericht erstattet werden sollte.

4. SCHLUSSFOLGERUNGEN

Der EDSB begrüßt den Vorschlag der Kommission für eine modernisierte, aktualisierte und stärkere E-Privacy-VO. Er teilt die Ansicht, dass weiterhin Bedarf an spezifischen Regeln zur Wahrung der Vertraulichkeit und Sicherheit in der elektronischen Kommunikation in der EU und an einer Ergänzung und Präzisierung der DSGVO besteht. Er ist außerdem der Meinung, dass wir einfache, gezielte und technologisch neutrale gesetzliche Bestimmungen benötigen, die in absehbarer Zukunft starken, intelligenten und wirksamen Schutz bieten.

Der EDSB begrüßt die erklärte Absicht, ein hohes Schutzniveau sowohl für Inhalte als auch für Metadaten zu gewährleisten, und insbesondere die in Abschnitt 2.1 genannten wichtigsten positiven Aspekte.

Der EDSB begrüßt zwar den Vorschlag, doch hat er weiterhin Bedenken in Bezug auf eine Reihe von Bestimmungen, die die Absicht der Kommission, ein hohes Schutzniveau der Privatsphäre in der elektronischen Kommunikation zu gewährleisten, beeinträchtigen könnten. Zu den wichtigsten Fragen des EDSB in dieser Hinsicht gehören insbesondere:

- Die in dem Vorschlag enthaltenen Begriffsbestimmungen dürfen nicht von dem davon unabhängigen Gesetzgebungsverfahren bezüglich der Richtlinie über den europäischen Kodex für die elektronische Kommunikation[53] (Kodex-Vorschlag) abhängig sein;
- Die Bestimmungen über die Einwilligung der Endnutzer müssen stärker formuliert werden. Die Einwilligung muss von den Personen eingeholt werden, die die Dienste

benutzen, unabhängig davon, ob sie diese abonnieren oder nicht, sowie von allen an einem Kommunikationsvorgang Beteiligten. Darüber hinaus müssen andere betroffene Personen, die nicht an den Kommunikationsvorgängen beteiligt sind, ebenfalls geschützt werden;

- Es muss dafür Sorge getragen werden, dass die Beziehung zwischen der DSGVO und der E-Privacy-VO keine Lücken im Schutz personenbezogener Daten offen lässt. Personenbezogene Daten, die aufgrund der Einwilligung der Endnutzer oder aus einem anderen in der E-Privacy-VO vorgesehenen Rechtsgrund erhoben werden, dürfen nicht später außerhalb des Geltungsbereichs dieser Einwilligung oder Ausnahmeregelung aus einem anderen nach der DSGVO möglicherweise bestehenden, jedoch nicht in der E-Privacy-VO verankerten Rechtsgrund weiter verarbeitet werden;
- Dem Vorschlag mangelt es in Bezug auf die so genannten „*Tracking Walls*“ (oder auch „*Cookie Walls*“) an Ehrgeiz. Zugang zu Websites darf nicht davon abhängig gemacht werden, dass die Person gezwungen wird, in die Verfolgung ihrer Aktivitäten auf den Websites „*einzuwilligen*“. Mit anderen Worten fordert der EDSB die Gesetzgeber auf, dafür Sorge zu tragen, dass die Einwilligung wirklich freiwillig erteilt wird;
- Der Vorschlag stellt nicht sicher, dass Browser (und andere auf dem Markt angebotene Softwareprodukte, die elektronische Kommunikation ermöglichen) standardmäßig so eingestellt sind, dass die Verfolgung der von Personen im Internet hinterlassenen digitalen Spuren verhindert wird;
- Die Ausnahmen bezüglich der Standortverfolgung von Endgeräten sind zu allgemein gefasst und bieten keine angemessenen Garantien;
- Der Vorschlag gibt Mitgliedstaaten die Möglichkeit, Beschränkungen einzuführen; diese machen spezifische Garantien erforderlich.

Diese Hauptfragen – sowie Empfehlungen zu ihrer Lösung – werden in der vorliegenden Stellungnahme dargelegt. Neben den allgemeinen Anmerkungen und den im Hauptteil der Stellungnahme formulierten zentralen Fragen, hat der EDSB in einem Anhang weitere Anmerkungen und Empfehlungen – zum Teil mehr technischer Art – zu dem Vorschlag zusammengestellt, die die Arbeit der Gesetzgeber und anderer Beteiligter erleichtern sollen, die den Text im Rahmen des Gesetzgebungsprozesses noch weiter verbessern möchten. Abschließend möchten wir noch auf die Wichtigkeit einer zügigen Bearbeitung dieses bedeutenden Dossiers durch die Gesetzgeber hinweisen, um sicherzustellen, dass die E-Privacy-VO wie geplant am 25. Mai 2018, und damit zur gleichen Zeit wie die DSGVO selbst, in Kraft treten kann.

Mit der immer größeren Rolle, die die elektronische Kommunikation in unserer Gesellschaft und Wirtschaft spielt, kommt der Vertraulichkeit von Kommunikation, wie sie in Artikel 7 der Charta verankert ist, ständig wachsende Bedeutung zu. Die in dieser Stellungnahme skizzierten Garantien werden eine zentrale Rolle dabei spielen, den Erfolg der langfristigen Zielsetzungen zu sichern, die die Kommission in ihrer Strategie für einen digitalen Binnenmarkt formuliert hat.

Geschehen zu Brüssel am 24. April 2017

(**gezeichnet)**

Giovanni BUTTARELLI

Europäischer Datenschutzbeauftragter

ANHANG: WEITERE ANALYSE UND EMPFEHLUNGEN

Neben den allgemeinen Anmerkungen und den im Hauptteil der Stellungnahme formulierten zentralen Fragen, hat der EDSB in einem Anhang weitere Anmerkungen und Empfehlungen – zum Teil mehr technischer Art – zu dem Vorschlag zusammengestellt, die die Arbeit der Gesetzgeber und anderer Beteiligter erleichtern sollen, die den Text im Rahmen des Gesetzgebungsprozesses noch weiter verbessern möchten.

Zur Erleichterung der Bezugnahme liegt diesen Anmerkungen der Aufbau des Vorschlags zugrunde, d. h. sie beginnen mit den Erwägungsgründen und behandeln danach die einzelnen Artikel in derselben Reihenfolge wie in dem Vorschlag.

1. Erfassung unterschiedlicher Arten von Netzen (Erwägungsgrund 13)

Wie in Abschnitt 2.5 oben erwähnt, begrüßt der EDSB das Bestreben der Kommission, alle öffentlich zugänglichen Netze und Dienste in den Geltungsbereich der Vertraulichkeitsanforderungen einzubeziehen. Erwägungsgrund 13 führt dazu einige Beispiele an wie *„… „Hotspots", die sich an verschiedenen Orten in einer Stadt wie in Kaufhäusern, Einkaufszentren und Krankenhäusern befinden können".*

Zur Vermeidung von Mehrdeutigkeiten regt der EDSB dazu an, weitere Klärungen und Beispiele anzuführen. Dazu sollten gehören: Wi-Fi-Dienste in Hotels, Restaurants, Coffee-Shops, Läden, Zügen, Flughäfen und Netze, die Universitäten den Studierenden anbieten, sowie Wi-Fi-Zugang für Besucher und Gäste in Unternehmen und von Behörden eingerichtete Hotspots.

Darüber hinaus empfiehlt der EDSB auch, in Erwägungsgrund 13 deutlich zu machen, was unter *„öffentlich zugänglich"* zu verstehen ist. So sollte beispielsweise erläutert werden, dass ein Dienst auch dann noch als öffentlich zugänglich gilt, wenn der Anbieter den Dienst nur registrierten Nutzern bereitstellt, wie im Falle von Organisationen, die ihren Kunden und Besuchern Wi-Fi-Zugang anbieten.[54]

2. Personenbezogene Daten können nicht als Gegenleistung betrachtet werden (Erwägungsgrund 18)

In Erwägungsgrund 18 der vorgeschlagenen E-Privacy-VO heißt es: *„In der digitalen Wirtschaft werden Dienstleistungen oft für andere Gegenleistungen als Geld erbracht, beispielsweise indem Endnutzern Werbung angezeigt wird."* Das könnte bedeuten, dass die Daten von Endnutzern als Gegenleistung verwendet werden, und zwar vor allem dann, wenn man diesen Erwägungsgrund in Verbindung mit Erwägungsgrund 16 des Kodex-Vorschlags betrachtet, in dem es noch direkter heißt: *„Elektronische Kommunikationsdienste werden oftmals für eine andere Gegenleistung als Geld erbracht, z. B. wird Zugang zu personenbezogenen oder sonstigen Daten gewährt."*

Der EDSB weist mit Nachdruck darauf hin, dass personenbezogene Daten nicht als *„Gegenleistung"* für angeforderte Dienstleistungen wie Zugang zu einer Website oder einer App gelten dürfen. Der Grund dafür ist, dass eine Einwilligung nur dann wirksam ist, wenn sie freiwillig gegeben und auch widerrufen werden kann, ohne dass der betroffenen Person dadurch Nachteile entstehen. Wie der EDSB kürzlich in seiner Stellungnahme 4/2017 zu dem Vorschlag für eine Richtlinie über digitale Inhalte[55] erläuterte, schafft der Begriff der „*Gegenleistung"*

zusätzliche Verpflichtungen für Personen und stimmt nicht mit dem Begriff der Einwilligung im Sinne der DSGVO überein bzw. ist nicht mit diesem vereinbar. Die Vorstellung, *„mit personenbezogenen Daten zu bezahlen“* und personenbezogene Daten als *„Gegenleistung“* anzubieten, würde daher in der Tat die geltenden, in Artikel 6 der DSGVO niedergelegten Rechtsgründe für eine rechtmäßige Verarbeitung beeinträchtigen.

Daher empfiehlt der EDSB, die zitierte Formulierung in Erwägungsgrund 18 zu streichen und diesen wie folgt zu ändern: „*In der digitalen Wirtschaft werden Dienstleistungen häufig gegen Zahlung einer Vergütung durch Dritte und nicht durch den Empfänger der Dienstleistung erbracht.“*

3. Nicht nur der Schutz aller Bürger, sondern der Schutz aller Personen muss gewährleistet werden (Erwägungsgrund 33)

Der EDSB empfiehlt, den Begriff „*Bürger*“ in Erwägungsgrund 33 durch den Begriff „*Person*“ zu ersetzen. Das Konzept der Bürgerschaft ist in Bezug auf den Schutz der Grundrechte nicht angemessen, da nicht nur Unionsbürger, sondern alle Personen in der EU im Rahmen der Charta Anspruch auf Schutz haben.

4. Schutz juristischer Personen (Artikel 1)

Obwohl es eindeutig gerechtfertigt ist, dass auch juristische Personen Rechte in Bezug auf ihre elektronische Kommunikation haben und deren Schutz in den Vorschlag aufgenommen werden sollte, muss der Vorschlag in dieser Hinsicht umformuliert werden. Der Bezug in Artikel 1 Absatz 1 auf Grundrechte und Grundfreiheiten *„juristischer Personen“* sollte gestrichen werden. Stattdessen empfiehlt der EDSB, in Bezug auf juristische Personen eine ähnliche Formulierung wie in Artikel 1 Absatz 2 der aktuellen Datenschutzrichtlinie für elektronische Kommunikation zu verwenden.

5. Der räumliche Anwendungsbereich sollte mit der DSGVO übereinstimmen (Artikel 3)

Der EDSB empfiehlt, in der E-Privacy-VO den gleichen *räumlichen* Anwendungsbereich wie in der DSGVO vorzusehen (einschließlich des in Artikel 3 Absatz 2[56] vorgesehenen extra-territorialen Anwendungsbereichs) und bezüglich des auf die Verarbeitung personenbezogener Daten anzuwendenden Rechts den gleichen Ansatz zu verfolgen. Die derzeitige Formulierung in Artikel 3 steht einer solchen Interpretation zwar nicht entgegen, aber sie macht nicht deutlich genug klar, ob der gleiche räumliche Anwendungsbereich beabsichtigt ist, sodass die Bestimmung entsprechend geändert und der gleiche räumliche Bereich abgedeckt werden sollte. Ein Erwägungsgrund könnte hier die Absicht des Gesetzgebers noch deutlicher machen.

Eine wortgetreue Übernahme der Bestimmungen der DSGVO wäre nicht zielführend, da es nicht eine Voraussetzung für die Anwendbarkeit der E-Privacy-VO sein sollte, dass die betroffenen Parteien als *„für die Verarbeitung Verantwortlicher“* oder *„Auftragsverarbeiter“* im Sinne der DSGVO bezeichnet werden können.

6. „Plattform-interne Nachrichten“ (Artikel 4 Absatz 1 Buchstabe b und Erwägungsgrund 1)

Der EDSB begrüßt die Bestätigung in Erwägungsgrund 1, dass der Grundsatz der Vertraulichkeit für *„gegenwärtige und künftige Kommunikationsmittel“* gilt, und dass hierzu Beispiele wie *„Anrufe, Internetzugang, Sofortnachrichtenanwendungen, E-Mail,*

Internettelefonie und Übermittlung persönlicher Nachrichten über soziale Medien" angeführt werden.

Der EDSB schließt sich der in ihrer Stellungnahme 01/2017[57] formulierten Forderung der WP29 nach einer Erläuterung an, dass der Vorschlag ausdrücklich und eindeutig auch für alle plattform-internen Nachrichten zwischen Nutzern eines sozialen Netzwerks (wie zum Beispiel Facebook oder Twitter) gilt.

Darüber hinaus empfiehlt der EDSB, in diesem Erwägungsgrund noch deutlicher zu machen, dass der Begriff Kommunikation nicht nur elektronische Kommunikationsvorgänge zwischen zwei natürlichen Personen (oder Maschinen) umfasst, sondern auch jegliche Kommunikation innerhalb einer bestimmten Gruppe (z. B. eine Telefonkonferenz oder Nachrichten, die an eine festgelegte Gruppe von Empfängern gesandt werden).

Ferner empfiehlt der EDSB, wie bereits in Abschnitt 3.1 oben in Bezug auf Anwendungsbereich und Begriffsbestimmungen erläutert, unabhängige, eigenständige Begriffsbestimmungen, die besser zum Schutz der Privatsphäre und der Vertraulichkeit der Kommunikation geeignet sind, einzuführen, um sicherzustellen, dass plattform-interne Nachrichten eindeutig unter den Begriff *„interpersoneller Kommunikationsdienst"* und damit auch unter die Definition *„elektronischer Kommunikationsdienst"*[58] fallen.

7. Begriffsbestimmung *„elektronische Post"* (Artikel 4 Absatz 3 Buchstabe e)

Der EDSB empfiehlt, den Begriff *„elektronische Post"* in Artikel 4 Absatz 3 Buchstabe e durch einen allgemeineren Begriff wie beispielsweise *„elektronische Nachricht"* zu ersetzen. So wird sichergestellt, dass der Begriff nicht mit den Ausdrücken *„elektronische Post oder E-Mail"*, wie sie allgemein verstanden werden, verwechselt wird. Die Eindeutigkeit der Begriffsbestimmungen ist entscheidend, um Rechtssicherheit im Hinblick auf den Geltungsbereich des Schutzes vor allen in Artikel 16 aufgeführten Arten unerbetener Kommunikation zu schaffen.[59]

Der vorgeschlagene Erwägungsgrund 33 unterstreicht zu Recht, dass die Bestimmungen zu unerbetener Kommunikation technologisch neutral sein müssen. Der EDSB begrüßt, dass in diesem Erwägungsgrund *„Sofortnachrichtenanwendungen, E-Mail, SMS, MMS, [und] Bluetooth*" ausdrücklich als Beispiele angeführt werden. Wir möchten jedoch anregen, in diesem Erwägungsgrund noch weitere Beispiele hinzuzufügen. Im Rahmen des Schutzes vor unerbetener Kommunikation sollte beispielsweise sichergestellt werden, dass natürliche Personen vor unerbetenen Nachrichten geschützt sind, unabhängig davon, ob diese über die Funktion *„Zeitleiste"* oder über die Nachrichtenfunktion eines sozialen Netzes oder die Nachrichtenfunktion einer Spieleanwendung gesandt werden.

Im Sinne der Rechtssicherheit muss die Begriffsbestimmung selbst außerdem hinreichend klar und breit formuliert sein, damit der Begriff neben der herkömmlichen E-Mail-Kommunikation auch alle anderen relevanten Kommunikationskanäle umfasst.[60]

8. Die Verarbeitung in Ausnahmefällen muss „*unbedingt*“ erforderlich sein (Artikel 6 und Artikel 8 Absatz 1)

Der EDSB schließt sich den Empfehlungen der WP29 an, im Hinblick auf alle in Artikel 6 und Artikel 8 Absatz 1 der vorgeschlagenen Verordnung aufgeführten Ausnahmen vor dem Wort „*erforderlich*“ das Wort „*unbedingt*“ einzufügen.[61]

9. Ausnahme zu Sicherheitszwecken (Artikel 6 Absatz 1 Buchstabe b)

Artikel 6 Absatz 1 Buchstabe b erlaubt die Verarbeitung von Inhalten und Metadaten zu Sicherheitszwecken. Der EDSB weist nachdrücklich darauf hin, dass – wie in Abschnitt 8 dieses Anhangs festgestellt – diese Ausnahme enger gefasst werden und auf das unbedingt notwendige Maß beschränkt werden muss. Diesen Grundsätzen zufolge könnten Inhalte nur zur Erkennung und Beseitigung von Bestandteilen verarbeitet werden, die für das Netzwerk oder das Endgerät des Nutzers gefährlich sein könnten, wie z. B. Viren oder anderer Schadcode, aber nicht zu anderen Zwecken. Damit wird nicht ausgeschlossen, dass auf der Grundlage einer Einwilligung der betroffenen Personen und unter Vorbehalt weiterer Garantien wie beispielsweise der in Artikel 6 Absatz 3 Buchstabe b genannten eine zusätzliche Verarbeitung zu diesen Zwecken autorisiert werden könnte. Der EDSB möchte in diesem Zusammenhang auch an die Stellungnahme 02/2006 der WP29 zu Datenschutzfragen bei Filterdiensten für elektronische Post erinnern.[62]

10. Der Schutz von Kommunikationsmetadaten muss verbessert werden (Artikel 6 Absatz 2)

Der EDSB betont, dass die Unterscheidung zwischen Inhalt und „*Metadaten*“ in einem System mit mehreren Diensten wie dem Internet nicht ganz klar ist, denn dort werden bei dem einem Nutzer bereitgestellten Dienst häufig verschiedene technologische Komponenten so miteinander kombiniert, dass das, was bei einer Komponente als Inhalt gilt, bei einer anderen zu den Metadaten gehört.[63]

Die Verarbeitung von Daten über die Kommunikation (wie URL der aufgerufenen Websites, E-Mail-Kopfzeilen, angerufene Telefonnummern und Standorte von Endeinrichtungen) ist häufig genauso aufschlussreich wie der eigentliche Inhalt der Kommunikation. Aus Metadaten über Kommunikation lässt sich ein höchst detailliertes Profil einer natürlichen Person erstellen, und die Verarbeitung dieser Daten kann sich als mindestens so eingreifend erweisen wie die Verarbeitung des Inhalts von Kommunikationsverkehr.

Metadaten lassen beispielsweise die Identifizierung von Zielen von militärischen Drohneneinsätzen zu.[64] Metadaten helfen auch bei der Identifizierung von Strukturen bei politischen Anschlägen und strafrechtlichen Untersuchungen.[65] Untersuchungen haben gezeigt, dass natürliche Personen schon mit sehr wenigen Standortdaten ihres Mobiltelefons identifiziert werden können.[66] Ferner ist nachgewiesen, dass sich intime Einzelheiten über den Lebensstil und die Überzeugungen einer Person, wie politische Ausrichtung und Zugehörigkeit zu politischen Vereinigungen, medizinische Probleme, sexuelle Orientierung oder Gewohnheiten in der Religionsausübung mit Hilfe von Verkehrsdaten eines Mobiltelefons entdecken lassen.[67]

Darüber hinaus war es in Bezug auf bestimmte Arten von Daten nach der Datenschutzrichtlinie für elektronische Kommunikation fraglich, ob diese als Inhalt oder Metadaten anzusehen seien. Erwägungsgrund 2 des Vorschlags macht nun klar, dass eine vollständige URL (die die aufgerufene Website angibt) zur Kategorie Metadaten gehört. In Anbetracht der Sensibilität

dieser Daten muss für diese Art von Daten jedoch ein ebenso hohes Schutzniveau wie für Inhaltsdaten gelten.

Wie auch die WP29 in ihrer Stellungnahme 01/2017[68] erläutert, muss die E-Privacy-VO daher offensichtlich ein hohes Schutzniveau in Bezug auf die Vertraulichkeit der Kommunikation sowohl für *„Inhalt“* als auch für *„Metadaten“* vorsehen. In Erwägungsgrund 2 des Vorschlags wird dem tatsächlich Rechnung getragen, was der EDSB gutheißt.

Doch wird in dem Vorschlag trotz dieser Absicht, ein hohes Schutzniveau für Metadaten zu schaffen, eine Verarbeitung dieser Daten unter Vorbehalt weniger strikter Garantien zugelassen. Zur Gewährleistung eines hohen Schutzniveaus empfiehlt der EDSB, dass in Artikel 6 für die Einwilligung sowohl bei Inhalt als auch bei Metadaten die gleichen Vorschriften gelten sollten.

11. Schutz von Endeinrichtungen: Bedarf an einem technologisch neutralen und inklusiveren Wortlaut (Artikel 8)

Der EDSB begrüßt, dass in Artikel 8 Absatz 1, wie in der vorläufigen Stellungnahme empfohlen, eine Formulierung gewählt wurde, die als technologisch neutral und inklusiv bezeichnet werden kann.[69]

Der EDSB erinnert daran, dass alle derzeitigen und künftigen über Smartphones und IdD-Anwendungen genutzten Tracking-Techniken abgedeckt sein müssen. Die Vorschriften sollten sich insbesondere mit virtuellen Fingerabdrücken sowie allen Formen des „passiven Tracking“ befassen, also dem Einsatz von Identifikatoren und anderen Daten, die von Geräten verbreitet werden. Mit der weiteren Entwicklung des Internets der Dinge werden immer mehr Daten *„standardmäßig“* verbreitet. Als Bedingung sollte weniger formuliert werden, dass Informationen *„bereits im Endgerät gespeichert sind“*; vielmehr sollte die Bedingung alle von dem Gerät *zu gewinnenden* Informationen abdecken. Solche Vorgänge würden mit den Ausnahmen von Übermittlung und Bereitstellung eines Dienstes, wie derzeit geregelt, eine Einwilligung erfordern, mit einer möglichen Erweiterung für einige wenige Fälle einer direkten Verarbeitung im Zusammenhang mit einem Dienst, der vom Nutzer gewünscht und ausschließlich von dem Dienstanbieter erbracht wird.

12. Ausnahme für „*Messung des Webpulikums*“ (Artikel 8 Absatz 1 Buchstabe d)

In der vorläufigen Stellungnahme hatte der EDSB empfohlen, eine Ausnahme für „First-Party-Analysecookies“ vorzusehen, für die angemessene Garantien bestehen müssen.[70] Auf diese Weise könnte sichergestellt werden, dass Daten verarbeitet werden können, wenn dies nur geringe oder gar keine Auswirkungen auf das Recht der Nutzer auf Vertraulichkeit ihrer Kommunikation und Schutz ihrer Privatsphäre hat. Der EDSB empfahl, solche Ausnahmen auf Fälle zu beschränken, in denen die Verwendung derartiger „First-Party-Analysecookies“ ganz klar auf aggregierte statistische Zwecke beschränkt ist. Es müssen darüber hinaus angemessene Garantien gelten, darunter eindeutige Information der betroffenen natürlichen Personen, eine benutzerfreundliche Regelung für eine bewusste Entscheidung gegen jede Datenverarbeitung sowie geeignete Anonymisierungstechniken für erhobene Informationen wie IP-Adressen. Die WP29 hat in ihrer Stellungnahme 04/2012 zur Ausnahme von Cookies von der Einwilligungspflicht[71] die Gesetzgeber bereits zur Schaffung einer solchen Ausnahme aufgefordert.

Was weitere Orientierung zu den anzuwendenden Garantien und die Bedingungen angeht, unter denen ein First-Party-Analysecookie von der Einwilligungspflicht ausgenommen werden kann, hat der EDSB außerdem angeregt, in der E-Privacy-VO auf künftige Leitlinien des EDSA zu verwiesen.

Der EDSB begrüßt, dass eine neue Ausnahme in den Vorschlag aufgenommen wurde. Um jedoch sicherzustellen, dass die Ausnahme beschränkt bleibt, empfiehlt der EDSB, am Ende des Absatzes den Wortlaut *„und sofern keine personenbezogenen Daten Dritten zugänglich gemacht werden“* hinzuzufügen. Damit wird sichergestellt, dass die Ausnahme eng gefasst ist und insbesondere die Inanspruchnahme von Diensten Dritter ausgeschlossen ist, wie von der WP29 beabsichtigt und vorgeschlagen.

Darüber hinaus weist der EDSB darauf hin, dass durch die Ausnahme keine Regelungslücke für die langfristige Speicherung oder weitere Verarbeitung personenbezogener Daten für andere Zwecke entstehen darf. Die Zulässigkeit der Speicherung von Informationen über das Endgerät des Nutzers und des Ablesens von Informationen von den Endeinrichtungen des Nutzers für statistische Zwecke kann nur unter der Voraussetzung akzeptiert werden, dass eine Reihe von Bedingungen erfüllt sind. So dürfen die sich daraus ergebenden Informationen beispielsweise kein detailliertes Bild einzelner Nutzer ergeben und die erlangten Informationen dürfen zu keinen anderen Zwecken verwendet werden als dazu, Erkenntnisse über die Funktionsweise und die Nutzung eines Dienstes in einer aggregierten und allgemeinen Form zu erhalten. Die Informationen dürfen auch nicht mit anderen Informationen zusammengebracht werden, um dadurch das Profil eines Nutzers zu erstellen oder den Nutzer gezielt anzusprechen.

Der Vorschlag sollte durch die Aufnahme wesentlicher Garantien und durch einen Hinweis auf die Möglichkeit der Bereitstellung weiterer Leitlinien durch den EDSA aktualisiert werden[72]. So empfiehlt der EDSB zum Beispiel wie im Fall der Geräte-Ortung (in Abschnitt 3.6 des Hauptteils dieser Stellungnahme), dass für diese Ausnahme zusätzliche Garantien gelten sollten, darunter technische und organisatorische Maßnahmen zur Sicherstellung, dass die zu diesen Zwecken verarbeitenden Daten zu keinen anderen Zwecken und insbesondere nicht zur Unterstützung von Maßnahmen oder Entscheidungen verwendet werden, die in Bezug auf die betroffene Person getroffen werden. Gleichzeitig muss eine wirksame horizontale Möglichkeit bestehen, der Verarbeitung zu widersprechen, und es muss strikte Vorgaben in Bezug auf die Aufbewahrungsdauer der Daten geben.

13. Zusätzliche Empfehlungen bezüglich der Geräte-Ortung (Artikel 8 Absatz 2)

Zum einen empfiehlt der EDSB, die Formulierung *„um sich mit anderen Geräten oder mit Netzanlagen verbinden zu können“* aus dem ersten Satz von Artikel 8 Absatz 2 zu streichen. Damit soll eine technologisch neutrale Abdeckung und der vollständige Schutz aller von Endeinrichtungen ausgesendeten Daten unabhängig vom Zweck sichergestellt werden.

Zum anderen empfiehlt der EDSB hinter *„zum Zwecke der Herstellung einer Verbindung“* die Formulierung *„die die betroffenen Endnutzer autorisiert haben“* (oder eine ähnliche Formulierung) einzufügen. Damit soll erreicht werden, dass die hergestellte Verbindung auch tatsächlich diejenige ist, von der der Nutzer Kenntnis hat und der er oder sie vorab zugestimmt hat. So könnten beispielsweise einige Personen über entsprechende Einstellungen auf ihren Geräten zugelassen haben, dass ihre Geräte in der Nähe eines Wi-Fi-Hotspots immer automatisch nach (vorab spezifizierten) verfügbaren Netzwerken suchen (und vielleicht automatisch zu diesen eine Verbindung aufbauen). Gleichzeitig könnten sie aber nicht autorisiert haben, dass ihr Gesundheits- oder Fitness-Tracker ihre Gesundheits- bzw.

Fitnessinformationen an sämtliche Geräte weitergibt, die für die Erhebung und Verarbeitung dieser Informationen bestimmt sind. In Anbetracht der zunehmenden Verfügbarkeit von Geräten des Internets der Dinge, darunter auch medizintechnische Geräte, kann allein schon die Tatsache, ob man ein bestimmtes Gerät trägt oder nicht, oftmals ein Hinweis auf äußerst sensible Informationen zum Beispiel gesundheitlicher Art sein, sodass hier Vorsicht geboten ist.

14. Widerruf der Einwilligung (Artikel 9 Absatz 3)

Was Artikel 9 Absatz 3 (Möglichkeit des Widerrufs der Einwilligung) betrifft, so empfiehlt der EDSB, zusätzlich zu den bereits vorhandenen Verweisen auf Artikel 6 noch einen Verweis auf Artikel 8 Absatz 1 Buchstabe b hinzuzufügen.

15. *„Machbarkeit“* der Erteilung der Einwilligung über technische Einstellungen (Artikel 9 Absatz 2)

Artikel 9 Absatz 2 sieht vor, dass *„die Einwilligung [...] – soweit dies technisch möglich und machbar ist – in den passenden technischen Einstellungen einer Software, die den Zugang zum Internet ermöglicht, gegeben werden kann“*.

Die Formulierung *„soweit dies technisch möglich und machbar ist“* ist nicht hinreichend deutlich. Sie lässt eine breite Palette von Interpretationsmöglichkeiten zu und könnte daher zu einer völligen Sinnentleerung dieser Verpflichtung führen. Eine mögliche Interpretation ist, dass der Vorschlag mit der Forderung, dass die Erteilung der Einwilligung über die technischen Einstellungen sowohl *„technisch machbar“* als auch *„technisch möglich“* sein muss, einfach nur redundant ist. Eine andere Auslegung wäre, dass der Vorschlag so zu verstehen ist, dass eine zusätzliche Bedingung der eher allgemeinen (als technischen) *„Machbarkeit“* gelten soll, deren Anwendungsbereich eng oder breit ausgelegt werden könnte und womöglich wirtschaftliche Überlegungen umfassen könnte, wie zum Beispiel die Auswirkungen der auf diese Weise erteilten Einwilligung auf vorhandene Geschäftsmodelle oder relevante Märkte im Allgemeinen.

Der EDSB empfiehlt daher, statt *„soweit technisch möglich und machbar“* den Wortlaut *„soweit technisch machbar“* zu verwenden, um Rechtssicherheit in Bezug auf den Geltungsbereich dieser Verpflichtung zu schaffen.[73]

16. Anzeige der Rufnummer des Anrufers und Sperrung eingehender Anrufe (Artikel 12 bis 14)

In dem Vorschlag ist das Recht des Angerufenen geregelt, zu erfahren, wer ihn anruft, und gegen Anrufer vorzugehen, die die Anzeige ihrer Rufnummer unterdrücken. Der EDSB begrüßt, dass dieses Recht aufrechterhalten bleibt, auch in Anbetracht der Tatsache, dass es eine der Schutzvorkehrungen ist, dank derer natürliche Personen gegen Personen vorgehen können, die entgegen geltendem Recht unerbetene Nachrichten senden.

Um die Wirksamkeit der Sperrung eingehender Anrufe zum Schutz vor unerbetenen Nachrichten zu unterstützen, empfiehlt der EDSB ferner, in Artikel 14 Absatz 1 Buchstabe a den Wortlaut *„oder Rufnummern mit einem bestimmten Kode/einer bestimmten Vorwahl, der/die angibt, dass es sich um einen Werbeanruf handelt, wie in Artikel 16 Absatz 3*

Buchstabe b vorgesehen" hinter *„Sperrung eingehender Anrufe von bestimmten Rufnummern"* hinzuzufügen.

17. Öffentlich zugängliche Verzeichnisse (Artikel 15)

Artikel 15 des Vorschlags sieht vor, dass *„Betreiber öffentlich zugänglicher Verzeichnisse [...] die Einwilligung der Endnutzer, die natürliche Personen sind, in die Aufnahme ihrer personenbezogenen Daten in das Verzeichnis [einholen]"*, wohingegen juristische Personen das Recht auf Widerspruch haben.

Die vorläufige Stellungnahme des EDSB enthält die Empfehlung, diese Bestimmung beizubehalten und ihren Anwendungsbereich so auszuweiten, dass sie nicht nur für Telefonverzeichnisse, sondern auch für alle anderen Arten von Verzeichnisdiensten gilt. Des Weiteren empfahl der EDSB, das Erfordernis der Einwilligung für die *„Rückwärtssuche"* auch ausdrücklich auf andere Dienst-Identifikatoren wie E-Mail-Adresse oder Nutzername ausweiten. Wir begrüßen die Klarstellungen, die diesbezüglich in Erwägungsgrund 30 enthalten sind, und dass damit Mobiltelefonnummern, E-Mail-Adressen und Auskunftsdienste jetzt ausdrücklich in den Anwendungsbereich von Artikel 15 fallen.

Wir unterstützen aber dennoch die Empfehlungen der WP29 in ihrer Stellungnahme 01/2017, in dem Vorschlag deutlicher zum Ausdruck zu bringen, dass eine spezifische, separate (d. h. granulare) Einwilligung für die Suche und Rückwärtssuche erforderlich ist. Wir empfehlen außerdem, die Formulierung *„vom Anbieter des Verzeichnisses angegebenen"* aus Artikel 15 Absatz 1 zu streichen.

18. Unerbetene Kommunikation (Artikel 16)

Der EDSB begrüßt, dass Artikel 16 des Vorschlags den derzeit geltenden Schutz vor unerbetener Kommunikation aufrechterhält, aktualisiert und verstärkt. Seit dem ersten Inkrafttreten der Datenschutzrichtlinie für elektronische Kommunikation hat es bei den Mitteln, über die unerbetene Nachrichten übermittelt werden, eine Entwicklung gegeben. So kann beispielsweise bei einem unerbetenen Sprachanruf zunächst ein automatisches Anwahlsystem den Anruf einleiten, dann wird eine aufgezeichnete Nachricht abgespielt und dann ein Chat-Bot für die Interaktion mit der angerufenen Person mit Hilfe einer Reihe automatischer Screening-Fragen eingesetzt. Der Chat-Bot kann dann mit Hilfe der Antworten die angerufene Person an einen Live-Operator weiterverweisen. Diese Art von Direktwerbeanruf wird inzwischen genauso behandelt wie ein voll automatischer Anruf.

Das Bestreben mit dem Vorschlag, einen technologisch neutralen Ansatz zu verfolgen und die Vorschriften zu modernisieren, wie dieses Beispiel zeigt, wird von dem EDSB befürwortet. Das generelle Erfordernis der Einwilligung – unabhängig von der verwendeten Technologie – wird besonders begrüßt.

Es gibt jedoch hier noch weitere Verbesserungsmöglichkeiten. Der Text muss sowohl zur Vermeidung von Regelungslücken als auch im Interesse der Rechtssicherheit in Bezug auf Grenzfälle aussagekräftiger formuliert werden.

Fragen bezüglich des Geltungsbereichs des Schutzes

Artikel 16 des Vorschlags befasst sich ausschließlich mit *„Direktwerbung"*. Allerdings können nicht aller Spam und alle böswilligen unter üblichen wirtschaftlichen Gesichtspunkten oder im

Sinne von Artikel 4 Absatz 3 Buchstabe f, in dem dieser Begriff für die E-Privacy-VO definiert ist, als *„Direktwerbung“* gelten.

Beispielsweise scheinen die folgenden sehr wichtigen Kategorien unerbetener Kommunikation nicht von den Schutzvorschriften erfasst zu sein:

- Bestimmte Nachrichten in Zusammenhang mit versuchten Straftaten, z. B. Phishing-Angriffe und betrügerische Finanzvorschläge, die nicht immer unter die Definition von Direktwerbung fallen.
- Bestimmte Arten von Werbung, die nicht unbedingt unter die Definition von Direktwerbung fallen.
- Nachrichten nicht kommerzieller Art oder Nachrichten, bei denen es aus anderen Gründen nicht offensichtlich ist, ob sie als Direktwerbung gelten können oder nicht (wie beispielsweise bestimmte Arten von Nachrichten von politischen Parteien, religiösen oder gemeinnützigen Organisationen, die um Spenden bitten oder politische, religiöse oder andere Ansichten zu verbreiten suchen[74]).

Aus diesen Gründen empfiehlt der EDSB den Gesetzgebern, umfassenderen Schutz zu gewährleisten, der alle Arten von Spam, unerbetene Telefonanrufe und Werbenachrichten, Phishing und andere böswillige Angriffe abdeckt. Der EDSB empfiehlt daher, sowohl den Geltungsbereich des Begriffes *„Direktwerbung“* zu erweitern und zu klären als auch weitere Begriffe, wie zum Beispiel *„unerbetene Kommunikation“*, einzuführen.

Zum einen kann umfassender Schutz nicht einfach durch die Vorgabe spezifischer Vorschriften für *„Direktwerbung“* erreicht werden. Vielmehr empfiehlt der EDSB, vor der Einführung spezifischer Vorschriften für Direktwerbung zunächst einmal ein klares Verbot aller Arten unerbetener Kommunikation auszusprechen, um Regelungslücken vorzubeugen, die für diverse böswillige oder aus anderen Gründen unerwünschte Arten unerbetener Kommunikation ausgenutzt werden könnten.

Zum anderen ergibt sich in Bezug auf den Geltungsbereich die Frage des Bedarfs an technologisch neutralen Vorschriften. Artikel 16 sollte eindeutig die vorherige Einwilligung von Empfängern aller Arten unerbetener elektronischer Nachrichten verlangen, und zwar unabhängig von den Übertragungsmitteln wie zum Beispiel E-Mail, Sprach- oder Videoanrufe, Fax, Text, aber auch direkte, plattform-interne Nachrichtenübermittlung (also innerhalb eines Dienstes der Informationsgesellschaft). Die Erwägungsgründe geben dazu weitere Beispiele.

Darüber hinaus empfiehlt der EDSB, in den Erwägungsgründen klarzustellen, dass in allen Fällen, in denen eine Direktwerbung an eine natürliche Person gesandt wird, die *für* eine juristische Person *arbeitet*, die für natürliche Personen geltenden Vorschriften anwendbar sind.[75]

Im Hinblick auf die aktuellen Ausnahmen bei bestehenden Kundenbeziehungen und ähnlichen Produkten und Dienstleistungen begrüßt der EDSB, dass diese in Artikel 16 Absatz 2 des Vorschlags beibehalten sind, empfiehlt jedoch, dass möglicherweise in einem Erwägungsgrund in dem Vorschlag erklärt werden sollte, was mit *„ähnlichen Produkten und Dienstleistungen“* gemeint ist und auch, was unter einer *„bestehenden Kundenbeziehung“* zu verstehen ist.

Widerruf der Einwilligung

Der EDSB empfiehlt, in Artikel 16 zu verdeutlichen, dass der Widerruf einer Einwilligung zur Direktwerbung kostenlos und so einfach wie die Erteilung der Einwilligung sein muss. Damit wird die Übereinstimmung mit der DSGVO[76] sichergestellt und der Schutz der Empfänger erhöht. Zwar ist der Begriff *„kostenlos“* in Artikel 16 Absatz 2 der vorgeschlagenen Verordnung enthalten, jedoch nur in Bezug auf eine Widerspruchsmöglichkeit gegen Direktwerbung, die auf im Zusammenhang mit einem Verkauf erhaltenen Kontaktangaben beruht.

Garantien für Direktwerbeanrufe (Artikel 16 Absatz 3)

Nach Artikel 16 Absatz 3 müssen Personen, die Direktwerbeanrufe tätigen, zusätzlich i) eine Rufnummer angeben, unter der die anrufende natürliche oder juristische Person erreichbar ist (Artikel 16 Absatz 3 Buchstabe a) oder ii) einen besonderen Kode/eine Vorwahl angeben, der/die kenntlich macht, dass es sich um einen Werbeanruf handelt (Artikel 16 Absatz 3 Buchstabe b). Die Vorgabe, einen Kode/eine Vorwahl für Werbeanrufe anzugeben, wird also als eine Alternative zu der Vorgabe der Rufnummernangabe, unter der der Anrufer erreichbar ist, genannt.

Der EDSB begrüßt zwar beide Vorgaben, muss jedoch darauf bestehen, dass diese unbedingt als einander ergänzend und nicht als Alternativen zu verstehen sein müssen, um einen wirksamen Widerruf der Einwilligung zu gewährleisten. Beide Vorgaben müssen verbindlich sein. Um dies zu erreichen, sollte das Wort *„oder“* zwischen Punkt a) und Punkt b) durch *„und“* ersetzt werden.

Informationen für Endnutzer (Artikel 16 Absatz 6)

Der EDSB hält es außerdem für bedenklich, dass der Entwurf nicht ausdrücklich die Verwendung einer falschen Identität bei der Übermittlung von Direktwerbung untersagt. Zwar heißt es in Erwägungsgrund 34, dass *„die Verschleierung der Identität und die Verwendung falscher Identitäten, falscher Rücksendeadressen oder Rückrufnummern bei der Durchführung von unerbetener gewerblicher Direktwerbung“* untersagt ist, doch wird in Artikel 16 Absatz 6 lediglich bestimmt, dass Endnutzer über *„die Identität der juristischen oder natürlichen Person, in deren Namen die Nachricht übermittelt wird“* zu informieren sind. Diese Verpflichtung, die Empfänger über die Identität zu informieren, sollte in Form einer materiellen Bestimmung durch ein klares Verbot der Verschleierung der Kontaktangaben oder der Verwendung falscher Kontaktangaben für Direktwerbezwecke ergänzt werden.

Europaweites Opt-out-Register für persönliche Anrufe

Gemäß Artikel 16 Absatz 4 des Vorschlags können Mitgliedstaaten in Bezug auf persönliche Direktwerbeanrufe ein Opt-out-Konzept vorsehen. Ferner wird in Erwägungsgrund 36 dargelegt, dass Mitgliedstaaten nationale Opt-out-Systeme einrichten oder beibehalten *können sollten*.

Sofern sie nicht verbessert werden, enthalten diese Vorschriften eine wesentliche Regelungslücke in Bezug auf den Schutz personenbezogener Daten und tragen außerdem nicht der Absicht Rechnung, eine stärkere Harmonisierung des Rechtsrahmens in ganz Europa zu

erreichen, die sowohl Unternehmen als auch natürlichen Personen zugutekommen würde. Der EDSB zieht grundsätzlich ein Opt-in-Konzept vor. Der EDSB empfiehlt den Gesetzgebern gleichwohl diese Möglichkeit in Bezug auf diejenigen Mitgliedstaaten, die ihre eigenen Systeme aufbauen bzw. beibehalten möchten, zum Aufbau eines europaweiten Opt-out-Systems für den Widerspruch gegen unerbetene Direktwerbeanrufe zu nutzen und in der E-Privacy-VO selbst die Regelungen bezüglich des Widerspruchs gegen persönliche Werbeanrufe festzulegen. Ein einheitliches System, wie beispielsweise eine europäische Do-Not-Call-Liste, könnte somit Mitgliedstaaten bei der Wahl eines Opt-out-Konzeptes für Direktwerbeanrufe als Maßstab dienen.

Andernfalls sollte die Verordnung zumindest eindeutig bestimmen, dass alle Mitgliedstaaten eine nationale Do-Not-Call-Liste schaffen müssen. Es darf in Zukunft auf keinen Fall mehr Situationen geben, in denen Nutzer ihren Widerspruch jedem einzelnen Kommunikationsdienstleister gegenüber erklären müssen, anstatt einfach in eine Do-Not-Call-Liste aufgenommen zu werden.

Darüber hinaus empfiehlt der EDSB, in der Verordnung vorzusehen, dass Empfängern von persönlichen Anrufen in Bezug auf den Widerruf ihrer Einwilligung zwei Optionen zur Verfügung stehen sollten: zum einen die Option, zukünftigen Anrufen von der anrufenden Organisation (sowie von deren verbundenen Organisationen) zu widersprechen, und zum anderen die Möglichkeit, sich während dieser Anrufe in eine nationale (oder europäische) Do-Not-Call-Liste aufnehmen zu lassen.

19. Gewährleistung der Sicherheit der Kommunikation (Artikel 17)

Von entscheidender Bedeutung ist, dass das bestehende Schutzniveau beibehalten wird: Die Gesetzgeber sollten keine regulatorische Lücke schaffen, indem sie bestehende Verpflichtungen zur Sicherheit aus der Datenschutzrichtlinie für elektronische Kommunikation herausnehmen.

Der EDSB begrüßt, dass der Vorschlag in Artikel 17 die in der Datenschutzrichtlinie für elektronische Kommunikation enthaltene Verpflichtung für Dienstanbieter beibehält, die Nutzer ihrer Dienste über bekannte Sicherheitsrisiken zu informieren, die bei der Nutzung der Dienste beachtet werden müssen. Im Hinblick auf die Empfänger dieser Information ist es zwar zweifellos angemessen, die Endnutzer (im Sinne der im Kodex enthaltenen Begriffsbestimmung) über derartige Risiken zu informieren, doch würde eine Klarstellung, dass letztlich diejenigen natürlichen Personen zu informieren sind, die die Dienste in Anspruch nehmen, die Wirksamkeit des Sicherheitshinweises noch verstärken. Die in Abschnitt 3.1 oben vorgeschlagene Anpassung der Begriffsbestimmungen könnte hier die Möglichkeit einer Klarstellung bieten, doch könnte darüber hinaus auch ein Hinweis in dem entsprechenden Erwägungsgrund sinnvoll sein.

Der EDSB erkennt an, dass die Vorschriften zu Datenschutzverletzungen in der Datenschutzrichtlinie für elektronische Kommunikation in der vorgeschlagenen Verordnung nicht erforderlich sind, da das Thema in den entsprechenden Bestimmungen der DSGVO abgedeckt ist.

Dem EDSB ist auch bewusst, dass die Sicherheitsbestimmungen des Kodex sowie der Funkanlagen-Richtlinie[77] zur Sicherheit von Kommunikationsnetzen, -diensten und -endgeräten beitragen sollte. Ferner könnten auch die NIS-Richtlinie[78] und – in geringerem

Maße – die eIDAS-Verordnung[79] einige der in den Anwendungsbereich der vorgeschlagenen E-Privacy-VO fallenden Dienste abdecken. Es muss jedoch darauf hingewiesen werden, dass selbst die Gesamtheit aller von diesen verschiedenen Rechtsinstrumenten erfassten Dienste nicht unbedingt alle in den Anwendungsbereich der E-Privacy-VO fallenden Dienste erfasst. Insbesondere gelten die Verpflichtungen des Kodex-Vorschlags nicht für alle der E-Privacy-VO unterliegenden Dienste, da der sachliche Anwendungsbereich der E-Privacy-VO umfangreicher ist. Die in der DSGVO beschriebenen Sicherheitsanforderungen gelten nur, wenn es um die Verarbeitung personenbezogener Daten geht und die verantwortliche Partei als für die Verarbeitung Verantwortlicher oder als Auftragsverarbeiter bezeichnet wird. Es muss jedoch sichergestellt werden, dass die Vertraulichkeit sämtlicher Kommunikationsdaten gewahrt ist.

Es besteht daher nach wie vor Bedarf an spezifischen Bestimmungen über Sicherheit auch in der E-Privacy-VO.[80] Der EDSB empfiehlt, in der E-Privacy-VO die Erklärung hinzuzufügen, dass die sicherheitsrelevanten Verpflichtungen in Artikel 40 des Kodex-Vorschlags auch entsprechend für alle in den Anwendungsbereich der E-Privacy-VO fallenden Dienstleistungen gelten sollen, unabhängig davon, ob sie zum Anwendungsbereich des Kodex-Vorschlags gehören oder nicht. Diese allgemeine Sicherheitsbestimmung könnte durch einen Erwägungsgrund ergänzt werden, in dem eine Reihe konkreter zusätzlicher Sicherheitsmaßnahmen aufgeführt werden, die in der öffentlichen Konsultation der Kommission erwähnt[81] und von dem EDSB in seiner vorläufigen Stellungnahme zu der Überprüfung unterstützt wurden:

- Entwicklung von Mindeststandards für die Sicherheit und den Datenschutz für Netzwerke und Dienste;

- Ausdehnung der Sicherheitsanforderungen zur Verbesserung der Reichweite von Softwareprogrammen, die in Verbindung mit der Bereitstellung eines Kommunikationsdienstes genutzt werden, wie in Endeinrichtungen eingebettete Betriebssysteme;

- Ausdehnung der Sicherheitsanforderungen zur Verbesserung der Reichweite von „Internet der Dinge“-Geräten, wie die in den Bereichen Wearable Computing, Heimautomatisierung und Fahrzeug-zu-Fahrzeug-Kommunikation genutzten Geräte, und

- Ausdehnung der Sicherheitsanforderungen zur Verbesserung der Reichweite aller Netzwerkkomponenten, einschließlich SIM-Karten, Geräte zur Vermittlung oder Weiterleitung von Signalen usw.

Diese Anforderungen könnten bei der korrekten Umsetzung der Grundsätze Sicherheit durch Technik, Datenschutz durch Technik und Datenschutz durch datenschutzfreundliche Voreinstellungen helfen und würden Herstellern und Softwareanbietern bessere Orientierung bieten. Darüber hinaus könnten sie Hersteller von in elektronischen Kommunikationsdiensten eingesetzten Produkten, Dienstleistungen und Anwendungen dazu anregen, die Rechte auf Achtung der Privatsphäre und Datenschutz in ähnlicher Weise wie in Erwägungsgrund 78 der DSGVO vorgesehen bereits bei der Entwicklung und Gestaltung zu berücksichtigen.

Verschlüsselung

Wie sowohl der EDSB als auch die WP29 in seiner/ihrer vorläufigen Stellungnahme ausgeführt haben, hat sich die Verschlüsselung zu einem entscheidenden Instrument für den Schutz der Vertraulichkeit der Kommunikation innerhalb von elektronischen Kommunikationsnetzen entwickelt. Nach den Enthüllungen über die Bemühungen seitens öffentlicher und privater Organisationen und von Regierungen, sich Zugriff auf den Kommunikationsverkehr zu verschaffen, hat der Einsatz der Verschlüsselung zugenommen.[82]

Der EDSB empfiehlt nach wie vor: Die E-Privacy-VO sollte Nutzern zum Schutz ihrer elektronischen Kommunikation ganz eindeutig die End-zu-End-Verschlüsselung (ohne „Hintertürchen“[83]) erlauben. Ferner empfiehlt der EDSB und schließt sich hier der WP29 an, Entschlüsselung, Reverse Engineering oder Überwachung von durch Verschlüsselung geschützter Kommunikation zu verbieten.

Darüber hinaus sollte die Nutzung der End-zu-End-Verschlüsselung gefördert und bei Bedarf im Einklang mit dem Grundsatz des Datenschutzes durch Technik angeordnet werden. In diesem Zusammenhang empfiehlt der EDSB der Kommission ferner, Maßnahmen zur Förderung der Entwicklung technischer Standards für die Verschlüsselung zu erwägen, auch zur Unterstützung der überarbeiteten Sicherheitsanforderungen in der DSGVO.

Der EDSB empfiehlt weiter, in der E-Privacy-VO Anbietern von Verschlüsselung, Anbietern von Kommunikationsdiensten und allen anderen Organisationen (auf allen Stufen der Lieferkette) zu untersagen, „Hintertürchen“ zuzulassen oder zu fördern.

20 Kollektive Rechtsdurchsetzung (Artikel 21)

Artikel 21 des Vorschlags enthält keinen ausdrücklichen Verweis auf Artikel 80 der DSGVO, der betroffenen Personen das Recht gibt, „*eine Einrichtung, Organisationen oder Vereinigung ohne Gewinnerzielungsabsicht [...] zu beauftragen*“, unter bestimmten Voraussetzungen in ihrem Namen bestimmte Rechte wahrzunehmen, und der Mitgliedstaaten die Möglichkeit einräumt, vorzusehen, dass diese Organisationen ähnliche Funktionen unabhängig von einem Auftrag der betroffenen Person selbstständig ausüben können. Der Grund für das Fehlen dieses Verweises ist nicht klar ersichtlich, sollte doch die E-Privacy-VO die DSGVO *„präzisieren und ergänzen“*, die mehrere mögliche Rechtsbehelfe vorsieht, darunter auch Artikel 80 über kollektive Rechtsdurchsetzung. Hier scheint die E-Privacy-VO ein wichtiges neues Instrument zur Wahrung der Rechte betroffener Personen auszulassen.

Artikel 21 Absatz 2 des Vorschlags weist auf die Möglichkeit von natürlichen und juristischen Personen hin, die *„ein berechtigtes Interesse“* haben, gegen Verstöße gerichtlich vorzugehen, was möglicherweise die Verfügbarkeit der kollektiven Rechtsdurchsetzungsinstrumente gemäß der DSGVO beinhalten soll. Es bedarf jedoch einer Klärung, warum der Gedanke eines berechtigten Interesses eingeführt und auf einen Verweis auf Artikel 80 der DSGVO verzichtet wurde. Der EDSB empfiehlt, dass die Gesetzgeber eine ausdrückliche Bestimmung für die kollektive Rechtsdurchsetzung und wirksame Rechtsbehelfe hinzufügen sollten oder andernfalls den Text näher erläutern sollten (z. B. durch eine ausdrückliche Bestätigung der Anwendbarkeit von Artikel 80 DSGVO), um zu gewährleisten, dass die nach der DSGVO verfügbaren kollektiven Rechtsdurchsetzungsinstrumente voll und ganz zur Verfügung stehen.

21 Weitere Harmonisierung der Verhängung von Geldbußen (Artikel 23 Absatz 4, Artikel 23 Absatz 6 und Artikel 24)

Der EDSB befürwortet die Harmonisierung der Durchsetzungsbefugnisse, darunter auch die Höhe der Geldbußen. Es wäre jedoch wünschenswert, die Bußgelder noch stärker zu harmonisieren. Nach Artikel 23 Absatz 4, Artikel 23 Absatz 6 und Artikel 24 des Vorschlags können Mitgliedstaaten Vorschriften zu Geldbußen für Verletzungen bestimmter Vorschriften der E-Privacy-VO festlegen. Der EDSB unterstützt die Empfehlungen der WP29 in ihrer Stellungnahme 01/2017[84], wonach dies im Interesse einer größeren Übereinstimmung auch in der E-Privacy-VO selbst geregelt werden sollte.

Endnoten

[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), COM(2017) 10 final, 2017/0003 (COD).

[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, geändert durch die Richtlinie 2009/136/EG.

[3] Stellungnahme 1/2017 der Artikel 29-Datenschutzgruppe zu der vorgeschlagenen Verordnung für die Datenschutzrichtlinie für elektronische Kommunikation (2002/58/EG) (WP247), angenommen am 4. April 2017. Siehe auch Stellungnahme 3/2016 der Artikel 29-Datenschutzgruppe zur Evaluierung und Überarbeitung der Datenschutzrichtlinie für elektronische Kommunikation (2002/58/EG) (WP240), angenommen am 19. Juli 2016.

[4] Siehe https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2016/16-07-22_Opinion_ePrivacy_DE.pdf.

[5] „Strategie für einen digitalen Binnenmarkt“ - Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen, 6. Mai 2015, (COM(2015) 192 final.), abrufbar unter: http://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:52015DC0192&from=DE.

[6] Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, ABl. L 281 vom 23.11.1995, S. 31.

[7] 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, abrufbar unter: http://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=OJ:L:2016:119:FULL

[8] Siehe Stellungnahmen 1/2017 und 3/2016 der WP29.

[9] Siehe EDRi, *„EDRi's Position on the proposal of an ePrivacy Regulation“ [Haltung von EDRi zu dem Vorschlag für eine E-Privacy-VO]*, abrufbar unter <https://edri.org/files/epd-revision/ePR_EDRi_position_20170309.pdf> (Positionspapier, 9. März 2017) und „*E-Privacy revision: An analysis from civil society groups“* [Überarbeitung des Datenschutzes in der elektronischen Kommunikation – eine Analyse von Gruppen der Zivilgesellschaft] <https://edri.org/files/epd-revision/EDRi_ePrivacyDir-final.pdf> (Analyse, 6. Juli 2016).

[10] Artikel 7 der Charta schützt auch das Recht auf Achtung des Privatlebens.

[11] Siehe beispielsweise Artikel 10 des deutschen Grundgesetzes, Artikel 37 der slowenischen Verfassung, Artikel 36 der kroatischen Verfassung, Artikel 19 der griechischen Verfassung, Artikel 43 der estnischen Verfassung, Artikel 15 der italienischen Verfassung, Artikel 49 der polnischen Verfassung, Artikel 28 der rumänischen Verfassung, Artikel 72 der dänischen Verfassung, Artikel 13 der niederländischen Verfassung, Artikel 29 der belgischen Verfassung, Artikel 6 von Kapitel 2 der schwedischen Verfassung, Artikel 10 der finnischen Verfassung, Artikel 17 der zyprischen Verfassung, Artikel 18 der spanischen Verfassung, Artikel 10 und 10 a der österreichischen Verfassung, Artikel 13 der tschechischen Verfassung und Artikel 22 der slowakischen Verfassung.

[12] Zum Beispiel wird in Artikel 8 Absatz 1 Buchstabe b des Vorschlags die Einwilligung für *„die Nutzung der Verarbeitungs- und Speicherfunktionen von Endeinrichtungen und jede Erhebung von Informationen aus Endeinrichtungen der Endnutzer“* gefordert. Darüber hinaus wird in Artikel 6 Absatz 2 Buchstabe c und Artikel 6 Absatz 3 die Einwilligung für die Verarbeitung von Inhalten und Metadaten verlangt. Und auch Artikel 16 über unerbetene Kommunikation enthält, abgesehen von einigen Ausnahmefällen, in der Regel die Anforderung der vorherigen Einwilligung als Rechtsgrundlage für Direktwerbung.

[13] Siehe Artikel 1 und Erwägungsgrund 14 der DSGVO mit Blick auf juristische Personen, wo es klar heißt, dass die DSGVO Schutz bei der Verarbeitung personenbezogener Daten nur natürlichen Personen, nicht jedoch juristischen Personen gewährt.

[14] Ohne die Wahrung der Vertraulichkeit wäre der Einsatz elektronischer Kommunikation für viele Geschäftsvorgänge oder den Austausch von Informationen in der öffentlichen Verwaltung unmöglich. Darüber hinaus profitieren auch Organisationen von einem Schutz gegen unerbetene Anrufe, unabhängig davon, ob sie an bestimmte Mitarbeiter oder an eine Telefonzentrale gerichtet sind. Ebenso haben auch juristische Personen ein Recht darauf, eingehende Anrufe nicht nur dann sperren zu lassen, wenn sie an einzelne Mitarbeiter gerichtet sind, sondern auch, wenn sie allgemeine Rufnummern der Organisation betreffen.

[15] Es wäre jedoch wünschenswert, die Bußgelder noch stärker zu harmonisieren. Weitere Einzelheiten siehe Anhang, Abschnitt 21.
[16] Eigentlich ist VoIP eine Familie von Protokollen, die die Erbringung von Telefonie-Diensten über Netze unter Nutzung von Internetprotokollen (hauptsächlich IP) anstelle herkömmlicher Telefonie-Standards unterstützt. Diese Technologien werden von so genannten OTT-Anbietern eingesetzt, aber auch von traditionellen Netzanbietern. Im regulatorischen Kontext wird der Begriff „*VoIP*“ häufig als Synonym für Internettelefonie verwendet, die auf der Grundlage der Basisübertragungsnetze erbracht wird. Diese Bedeutung wird auch in dieser Stellungnahme verwendet.
[17] Artikel 2 Absatz 1 des Vorschlags sieht vor, dass die E-Privacy-VO für „*die Verarbeitung elektronischer Kommunikationsdaten, die in Verbindung mit der Bereitstellung und Nutzung elektronischer Kommunikationsdienste erfolgt, und für Informationen in Bezug auf Endeinrichtungen der Endnutzer“* gilt.
[18] Für weitere empfohlene Klarstellungen siehe Anhang, Abschnitt 1.
[19] Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über den europäischen Kodex für die elektronische Kommunikation COM (2016), 590 final/2, 2016/0288(COD) vom 12.10.2016.
[20] Richtlinie 2002/21/EG des Europäischen Parlaments und des Rates vom 7. März 2002 über einen gemeinsamen Rechtsrahmen für elektronische Kommunikationsnetze und -dienste (Rahmenrichtlinie), in der geänderten Fassung.
[21] Der Kodex-Vorschlag beruht einzig und allein auf Artikel 114 des AEUV, da er auf die Verwirklichung des Binnenmarkts für elektronische Kommunikation und dessen Funktionsfähigkeit ausgerichtet ist. Der Vorschlag für eine E-Privacy-VO dagegen hat eine zweifache Rechtsgrundlage: Artikel 16 AEUV, dieselbe konkrete Rechtsgrundlage wie die der DSGVO, und Artikel 114 AEUV. Artikel 16 AEUV allein hätte nicht ausgereicht, da die neuen Bestimmungen nicht nur einige Bestimmungen der DSGVO *„präzisieren“*, sondern diese auch um Bestimmungen *„ergänzen“*, die sich nicht auf den Schutz personenbezogener Daten beschränken.
[22] Der Begriff „*Teilnehmer“* (bisher in der aktuellen Datenschutzrichtlinie für elektronische Kommunikation enthalten) wird nicht mehr verwendet. Hier bietet sich auch ein Vergleich der vorgeschlagenen neuen Begriffsbestimmung mit dem aktuellen Artikel 2 Buchstabe a der Datenschutzrichtlinie für elektronische Kommunikation an, in dem ein „*Nutzer“* als „*eine natürliche Person, die einen öffentlich zugänglichen elektronischen Kommunikationsdienst für private oder geschäftliche Zwecke nutzt, ohne diesen Dienst notwendigerweise abonniert zu haben“* definiert ist.
[23] Näheres hierzu siehe auch Seite 26 Absatz 40 Buchstabe c der Stellungnahme 01/2017 der WP29.
[24] Siehe z. B. Science and Technology Options Assessment (STOA), Europäisches Parlament, *Potential and impacts of cloud computing services and social network websites*, 2014. PE 513.546. Abrufbar unter http://www.europarl.europa.eu/RegData/etudes/etudes/join/2014/513546/IPOL-JOIN_ET(2014)513546_EN.pdf
[25] Siehe Stellungnahme 01/12017 der WP29, Abschnitt 40 Buchstabe c.
[26] In diesem Zusammenhang ist es sinnvoll, sich Artikel 2 Buchstabe a der Datenschutzrichtlinie für elektronische Kommunikation in Erinnerung zu rufen, in dem ein „*Nutzer“* zurzeit als „*eine natürliche Person, die einen öffentlich zugänglichen elektronischen Kommunikationsdienst für private oder geschäftliche Zwecke nutzt, ohne diesen Dienst notwendigerweise abonniert zu haben“* definiert ist.
[27] Der EDSB empfiehlt den Gesetzgebern, sorgfältig zu prüfen, wie eng gefasste, angemessene Ausnahmen, die diese Situationen abdecken, am besten zu erzielen sind. Siehe hierzu auch Punkt 18, Aufzählungspunkt 4 der Stellungnahme 01/2017 der WP29, in dem eine Ausnahme empfohlen wird, die auf dem Gedanken einer „*Ausnahme für familiäre Tätigkeiten“* gemäß DSGVO beruht, aber auch eine beschränkte berufliche Nutzung für Standardfunktionen wie die Schlagwortsuche umfasst.
[28] Dabei gehen wir von der Annahme aus, dass der Begriff *„Endnutzer“* wie in den Abschnitten 3.1 und 3.2 beschrieben geändert wird oder andernfalls durch einen besser geeigneten Begriff ersetzt wird. Der EDSB weist ferner darauf hin, dass der Begriff *„betroffen“* vermieden werden sollte, da er unnötige zusätzliche Unsicherheit bezüglich der Frage schafft, wer die Einwilligung geben sollte.
[29] Wie bereits in Abschnitt 3.1 zu Begriffsbestimmungen erläutert, ist für die Zwecke mancher Bestimmungen – wie zum Beispiel in Bezug auf öffentlich zugängliche Verzeichnisse in Artikel 15 – ein anderer Begriff geeigneter um sicherzustellen, dass diejenigen, die einen Dienst abonnieren, die Entscheidung treffen können.
[30] Personenbezogene Daten von Dritten sind nämlich häufig Bestandteil sowohl privater als auch geschäftlicher Alltagskommunikation. Einige dieser personenbezogenen Daten – wie beispielsweise der Familie oder engen Freunden anvertraute intime persönliche Angelegenheiten oder unter Ärzten, Rechtsanwälten, Betrugsermittlungsbeamten und in ähnlichen Personenkreisen weitergegebene Kommunikationsinhalte – können besonders sensibel sein.
[31] Siehe auch Punkt 18 der Stellungnahme 01/2017 der WP29, in dem empfohlen wird, deutlich zu machen, dass auch bei der Verarbeitung personenbezogener Daten von anderen Personen als den an der Kommunikation beteiligten Endnutzern (z. B. das Bild oder die Beschreibung eines Dritten in einer Kommunikation zwischen zwei Personen) die Einhaltung der einschlägigen Bestimmungen der DSGVO erforderlich ist.

[32] Wir weisen ferner darauf hin, dass Gegenstand der DSGVO der Schutz personenbezogener Daten ist, also ein eigenständiges Recht, das in einem anderen Artikel der Charta, nämlich Artikel 8, behandelt wird. Auch haben die beiden Instrumente nicht die gleiche Rechtsgrundlage. Schließlich ist der Kreis der geschützten Personen ein anderer, da die Datenschutzrichtlinie für elektronische Kommunikation Schutz auch juristischen Personen gewährt. Außerdem wäre es zwar möglich gewesen, viele Bestimmungen der Datenschutzrichtlinie für elektronische Kommunikation in die DSGVO zu übernehmen, doch ist dies nicht geschehen. In Erwägungsgrund 173 und Artikel 95 der DSGVO wird eine Klarstellung der Beziehung zwischen den beiden Rechtsinstrumenten in dem neuen Rechtsakt für den Datenschutz in der elektronischen Kommunikation gefordert.
[33] Siehe auch Punkt 21, Seite 16 der Stellungnahme 01/2017 der WP29.
[34] Das gleiche Phänomen gibt es auch bei Apps für Mobiltelefone, wenn häufig Apps um die Erlaubnis bitten, Zugang zu verschiedenen Fähigkeiten und Funktionen eines Mobiltelefons zu bekommen, die für das Funktionieren der App und die Erbringung des Dienstes gar nicht erforderlich sind, darunter Zugang zu Wi-Fi, GPS, Kamera, Nachrichten, Kontakte, Browsing-Verlauf oder Bilder. Ein Beispiel hierfür ist die Taschenlampen-App, deren Funktion darin besteht, ein helles Taschenlampenlicht zu verbreiten, die aber übermäßigen Zugang zu vielen der oben genannten Datenkategorien verlangt, der für die eigentliche Funktion der App eindeutig unnötig ist.
[35] Im Erwägungsgrund 42 der DSGVO wird Folgendes unterstrichen: *„Es sollte nur dann davon ausgegangen werden, dass sie [die betroffene Person] ihre Einwilligung freiwillig gegeben hat, wenn sie eine echte oder freie Wahl hat und somit in der Lage ist, die Einwilligung zu verweigern oder zurückzuziehen, ohne Nachteile zu erleiden."* Weiter heißt es dort: *„...eine vom Verantwortlichen vorformulierte Einwilligungserklärung ... sollte keine missbräuchlichen Klauseln beinhalten"*. In Erwägungsgrund 43 heißt es: *„Um sicherzustellen, dass die Einwilligung freiwillig erfolgt, sollte diese in besonderen Fällen, wenn zwischen der betroffenen Person und dem Verantwortlichen ein klares Ungleichgewicht besteht, ... keine gültige Rechtsgrundlage liefern."* Weiter besagt Erwägungsgrund 43: *„Die Einwilligung gilt nicht als freiwillig erteilt, wenn ... die Erfüllung eines Vertrags, einschließlich der Erbringung einer Dienstleistung, von der Einwilligung abhängig ist, obwohl diese Einwilligung für die Erfüllung nicht erforderlich ist."* Letzterer Aspekt wurde in Artikel 7 Absatz 4 der DSGVO noch einmal wiederholt, der lautet: *„Bei der Beurteilung, ob die Einwilligung freiwillig erteilt wurde, muss dem Umstand in größtmöglichem Umfang Rechnung getragen werden, ob unter anderem die Erfüllung eines Vertrags, einschließlich der Erbringung einer Dienstleistung, von der Einwilligung zu einer Verarbeitung von personenbezogenen Daten abhängig ist, die für die Erfüllung des Vertrags nicht erforderlich sind."*
[36] Stellungnahme 7/2015 des EDSB: https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2015/15-11-19_Big_Data_DE.pdf.
[37] Zum Thema der Möglichkeiten zur Entwicklung neuer innovativer Geschäftsmodelle unter Beachtung der europäischen Datenschutzrechte, siehe zum Beispiel die Stellungnahme 9/2016 des EDSB zu Systemen für das Personal Information Management (PIM) mit dem Untertitel „*Hin zu einer intensiveren Einbindung der Nutzer in das Management und die Verarbeitung personenbezogener Daten*".
[38] Eine kürzlich durchgeführte Eurobarometer-Befragung zeigte, dass fast 90 % der EU-Bürger solche datenschutzfreundlichen Voreinstellungen tatsächlich befürworten. *Durchgeführt von TNS Political & Social im Auftrag der Europäischen Kommission, „Flash Eurobarometer 443 - July 2016, „e-Privacy" Report, EN"* (Dezember 2016), auf S. 43.
[39] Siehe Seite 16, unter dem Titel *„Möglichkeiten für Erteilung und Widerruf der Einwilligung".*
[40] Zur Bestimmung des Begriffs Endnutzer siehe unsere Empfehlung in Abschnitt 3.1 und Abschnitt 3.2.
[41] Forschungsergebnisse von Mitgliedern der Organisation EDRi haben gezeigt, dass bei den meisten derzeit angebotenen Diensten, denen Standort-Metadaten zugrunde liegen, anstatt der Einholung einer Einwilligung angeblich eine Anonymisierung erfolgt, was zu der Befürchtung geführt hat, dass eine vollständige Anonymisierung dieser Daten in Wirklichkeit womöglich nicht gegeben ist. https://www.openrightsgroup.org/ourwork/reports/mobile-data.
[42] Zu der Möglichkeit, derartige Ausnahmen vorzusehen, siehe auch Punkt 3.3 weiter oben im Rahmen der Erörterung der Beziehung zwischen der DSGVO und der E-Privacy-VO.
[43] Zu dem Konzept der funktionellen Trennung und zu den organisatorischen und technischen Maßnahmen, die hier zur Sicherstellung verwendet werden können, siehe auch Punkt III.2.3, S. 28-33 der Stellungnahme 03/2013 der WP29 zur Zweckbegrenzung (WP203), die am 2. April 2013 angenommen wurde.
[44] Verbundene Rechtssachen C-293/12 und C-594/12, *Digital Rights Ireland*, ECLI:EU:C:2014:238.
[45] Richtlinie 2006/24/EG des Europäischen Parlaments und des Rates vom 15. März 2006 über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste oder öffentlicher Kommunikationsnetze erzeugt oder verarbeitet werden, und zur Änderung der Richtlinie 2002/58/EG, ABl. L 105 vom 13.5.2006, S. 54.
[46] Verbundene Rechtssachen C-203/15 und C-698/15 *Tele2 Sverige AB and Watson*, ECLI:EU:C:2016:970.

[47] Siehe entsprechend C-275/06 *Promusicae gegen* Telefónica de España SAU, ECLI:EU:C:2007:454, Schlussanträge der Generalanwältin Kokott, Punkte 86-88.
[48] Siehe auch EDSB, Assessing the necessity of measures that limit the fundamental rights to the protection of personal data: A "Toolkit" [Ein Instrumentarium zur Einschätzung der Notwendigkeit von Maßnahmen, die die Grundrechte zum Schutz personenbezogener Daten einschränken], 11. April 2017, abrufbar unter: https://edps.europa.eu/sites/edp/files/publication/17-04-11_necessity_toolkit_en_0.pdf.
[49] Siehe auch Punkt 11 der Stellungnahme der Europäischen Akademie für Informationsfreiheit und Datenschutz (EAID) vom 21. März 2017, abrufbar unter www.eaid-berlin.de/wp-content/uploads/2017/04/EAID_Opinion_E-Privacy-Regulation.pdf (EAID Stellungnahme).
[50] Siehe zum Beispiel die Stellungnahme des EDSB zu den Vorschlägen der Kommission für eine Verordnung des Europäischen Parlaments und des Rates über Insider-Geschäfte und Marktmanipulation und für eine Richtlinie des Europäischen Parlaments und des Rates über strafrechtliche Sanktionen für Insider-Geschäfte und Marktmanipulation, angenommen am 10. Februar 2012 (2012/C 177/01), Abschnitt 2.3.2, insbesondere, Punkte 27 und 28, abrufbar unter https://edps.europa.eu/sites/edp/files/publication/12-02-10_market_manipulation_de.pdf.
[51] Siehe Artikel 48 DSGVO *„Nach dem Unionsrecht nicht zulässige Übermittlung oder Offenlegung"*.
[52] Siehe die vorläufige Stellungnahme des EDSB, Abschnitt X.3, S. 21.
[53] Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über den europäischen Kodex für die elektronische Kommunikation COM (2016), 590 final/2, 2016/0288(COD) vom 12.10.2016.
[54] Diese Anmerkungen knüpfen an frühere Kommentare, die der EDSB bereits in den Jahren 2008 und 2009 zu diesem Thema abgegeben hat, an. Insbesondere anlässlich der letzten Überprüfung der Datenschutzrichtlinie für elektronische Kommunikation im Jahr 2009 verfasste der EDSB in zwei verschiedenen Phasen des Gesetzgebungsverfahrens zwei Stellungnahmen. In seiner ersten Stellungnahme führte der EDSB aus: *„Die wachsende Bedeutung gemischter (privater/öffentlicher) und privater Netze rechtfertigt im täglichen Leben mit entsprechend steigendem Risiko für personenbezogene Daten und die Privatsphäre, dass für solche Dienste das gleiche Regelwerk gelten muss wie für öffentliche elektronische Kommunikationsdienste. Der EDSB ist daher der Auffassung, dass der Anwendungsbereich der Richtlinie so geändert werden sollte, dass solche privaten Dienste eingeschlossen sind."*
In seiner zweiten Stellungnahme, die zu einem späteren Zeitpunkt herausgegeben wurde, als im Zuge des Gesetzgebungsverfahrens konkrete Änderungen erörtert wurden, regte der EDSB an, in den Anwendungsbereich der Datenschutzrichtlinie für elektronische Kommunikation zumindest *„die Verarbeitung personenbezogener Daten in Verbindung mit der Bereitstellung öffentlich zugänglicher Kommunikationsdienste in öffentlichen oder* ***öffentlich zugänglichen privaten Kommunikationsnetzen*** *in der Gemeinschaft"* aufzunehmen (Hervorhebung durch uns).
Weitere Einzelheiten siehe Stellungnahme des Europäischen Datenschutzbeauftragten zum Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates zur Änderung unter anderem der Richtlinie 2002/58/EG über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Richtlinie über den Schutz der Privatsphäre und elektronischen Kommunikation), herausgegeben am 10. April 2008, ABl. C 181 vom 18.7.2008, S.1, abrufbar unter: https://secure.edps.europa.eu/EDPSWEB/webdav/shared/Documents/Consultation/Opinions/2008/08-04-10_e-privacy_DE.pdf Siehe insbesondere die Punkte 22-24. Siehe auch die zweite Stellungnahme des Europäischen Datenschutzbeauftragten zur Überprüfung der Richtlinie 2002/58/EG über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation), herausgegeben am 9. Januar 2009, ABl. C 128 vom 6.6.2009, S. 28, abrufbar unter:
https://secure.edps.europa.eu/EDPSWEB/webdav/shared/Documents/Consultation/Opinions/2009/09-01-09_ePricacy_2_DE.pdf Siehe insbesondere die Punkte 60-72, darunter den zitierten Wortlaut unter Punkt 66.
[55] Stellungnahme 4/2017 zu dem Vorschlag für eine Richtlinie über bestimmte vertragsrechtliche Aspekte der Bereitstellung digitaler Inhalte, 14. März 2017.
[56] Siehe auch *„EDRi's Position on the proposal of an ePrivacy Regulation" (Stellungnahme von EDRi zu dem Vorschlag für eine E-Privacy-Verordnung)* (Stellungnahme, 9. März 2017).
[57] Siehe Stellungnahme 01/12017 der WP29, Punkt 40 Buchstabe g.
[58] In Artikel 2 Absatz 4 des Kodex-Vorschlags sind *„elektronische Kommunikationsdienste"* durch Bezugnahme unter anderem auf *„interpersonelle Kommunikationsdienste"* definiert, die wiederum in Artikel 2 Absatz 5 des Kodex-Vorschlags definiert sind.
[59] Siehe auch Anhang, Abschnitt 18 zu Fragen im Hinblick auf den Anwendungsbereich des Schutzes vor unerbetener Kommunikation.
[60] Siehe auch Punkt 2 Satz 2 der Stellungnahme der EAID.
[61] Zur Begründung und für eine detaillierte Übersicht siehe Stellungnahme 01/2017 der WP29, Punkte 18 und 26.

[62] Stellungnahme 2/2006 der Artikel 29-Datenschutzgruppe zu Datenschutzfragen bei Filterdiensten für elektronische Post (WP118), angenommen am 21. Februar 2006.
[63] Zum technologischen Hintergrund siehe bitte das OSI-Modell https://en.wikipedia.org/wiki/OSI_model und die Internet Protokoll-Suite https://en.wikipedia.org/wiki/Internet_protocol_suite.
[64] *„We kill people based on metadata"* (Wir bringen die Leute mit Hilfe von Metadaten um) erklärte der frühere CIA- und NSA-Direktor Michael Hayden an der John Hopkins University im April 2014. Siehe: Pomerantz, J., Metadata, United States of America: MIT Press 2015, S. 118. Die an der John Hopkins University gehaltene Rede kann abgerufen werden unter:
https://www.youtube.com/watch?v=kV2HDM86XgI, Zitat von Michael Hayden bei Minute 17:59.
[65] Metadaten waren bei einer strafrechtlichen Ermittlung verwendet worden, die zur Festnahme der mutmaßlichen Mörder des früheren Premierministers Rafiq Hariri führten. *„Von den zehn Mobiltelefonen, die in Verbindung mit diesen zehn SIM-Karten verwendet wurden, konnten fünf zu einem Laden in Tripoli zurückverfolgt werden."* United Nations Security Council, Report of the International Independent Investigation Commission established pursuant to Security Council resolution 1595 (2005), S2005/662, Beirut: 19 October 2005, nr. 151, p. 147, abrufbar unter: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N05/563/67/PDF/N0556367.pdf?OpenElement.
[66] De Montjoye, Y. A., Hidalgo, C. A., Verleysen, M., & Blondel, V. D. (2013), *Unique in the Crowd: The privacy bounds of human mobility*, Nature SRep, 3, abrufbar unter: http://www.nature.com/articles/srep01376 zeigte, dass vier Raum-Zeit-Punkte ausreichen, um 95 % der natürlichen Personen eindeutig zu identifizieren.
[67] New York Times Editorial Board, Surveillance: *A Threat to Democracy*, 11. Juni 2013, abrufbar unter: http://www.nytimes.com/2013/06/12/opinion/surveillance-a-threat-to-democracy.html?hp.
[68] Siehe Stellungnahme 01/2017 der WP29, Abschnitt 18 sowie Abschnitte 10, 33 und 46 über Metadaten.
[69] EDSB, vorläufige Stellungnahme, S. 16 und 17.
[70] Aus dem Rechtstext sollte klar hervorgehen, dass in dem Fall einer Organisation, die Analysedienste eines Dritten (wie Google Analytics) in Anspruch nimmt, der seine eigenen Cookies setzt, diese nicht als First-Party-Cookies gelten können.
[71] Stellungnahme 04/2012 der WP29 zur Ausnahme von Cookies von der Einwilligungspflicht (WP194), abrufbar unter: http://ec.europa.eu/justice/data-protection/article-29/documentationopinion-recommendation/files/2012/wp194_de.pdf.
[72] Weitere Empfehlungen siehe auch Stellungnahme 01/2017 der WP29, S. 18-19, Punkt 25.
[73] Siehe auch Punkt 7 der Stellungnahme der EAID.
[74] Wir begrüßen zwar die Bezugnahme in Erwägungsgrund 32 auf Nachrichten von politischen Parteien, die für ihre Parteien werben, und auf Nachrichten von anderen Organisationen ohne Erwerbszweck, die die Zwecke ihrer Organisation zu fördern suchen, doch erachten wir diese nicht als ausreichend, um umfassende Rechtssicherheit für alle relevanten Situationen zu schaffen. Da es sich hier um einen Bereich handelt, in dem die Freiheit der Meinungsäußerung sorgfältig gegen das Recht auf Achtung der Privatsphäre abgewogen werden muss, wäre eine weitere Orientierungshilfe hier besonders hilfreich.
[75] Siehe auch Stellungnahme 01/12017 der WP29, Abschnitt 43 Buchstabe c.
[76] Artikel 7 Absatz 3 der DSGVO bestimmt unter anderem, dass der Widerruf der Einwilligung so einfach sein muss wie die Erteilung der Einwilligung und dass Personen das Recht haben, ihre Einwilligung jederzeit zu widerrufen.
[77] Richtlinie 2014/53/EU des Europäischen Parlaments und des Rates vom 16. April 2014 über die Harmonisierung der Rechtsvorschriften der Mitgliedstaaten über die Bereitstellung von Funkanlagen auf dem Markt und zur Aufhebung der Richtlinie 1999/5/EG, ABl. L 153 vom 22.5.2014, S. 62.
[78] 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.
[79] Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG, ABl. L 257 vom 28.8.2014, S. 73
[80] Das heißt, dass die DSGVO und die E-Privacy-VO im Sinne von Kohärenz aufeinander abgestimmt sein müssen. Der EDSB empfiehlt beispielsweise einen Querverweis auf die Sicherheitsverpflichtungen in der DSGVO (einschließlich Datenschutzfolgenabschätzungen und Rechenschaftspflicht).
[81] Siehe Frage 21 des Fragebogens für die öffentliche Konsultation.
[82] Vorläufige Stellungnahme des EDSB, S. 19; Stellungnahme 03/2016 der WP29, S. 19.
[83] Siehe https://en.wikipedia.org/wiki/Backdoor_(computing).
[84] Siehe Abschnitt 38, Stellungnahme 01/2017 der WP29.