Empfehlungen des EDSB zu bestimmten Aspekten der vorgeschlagenen Verordnung über Privatsphäre und elektronische Kommunikation

5. Oktober 2017

Nach ihrer Annahme wird die vorgeschlagene Verordnung über Privatsphäre und elektronische Kommunikation die „Verkehrsregeln" für Datenschutz und elektronische Kommunikation aktualisieren. Durch sie werden bestehende Grundsätze modernisiert, die technologischen Anforderungen klargestellt und für eine wirksame Durchsetzung gesorgt. Der EDSB äußerte sich zur Überarbeitung der Datenschutzrichtlinie für elektronische Kommunikation in einer vorläufigen Stellungnahme (5/2016) und zu der von der Europäischen Kommission vorgeschlagenen Verordnung in der Stellungnahme 6/2017. In Anbetracht von Entwicklungen im Verlauf der Beratungen über den Vorschlag und zum Nutzen des Mitgesetzgebers haben wir beschlossen, in Anlehnung an unsere bisherigen Stellungnahmen noch einmal Rat und Klarstellung zu einigen spezifischen Fragen anzubieten.[1] Im Mittelpunkt der nachstehenden Empfehlungen steht die Notwendigkeit, für Rechtssicherheit und ein hohes Maß an Schutz der Grundrechte auf Privatsphäre und Datenschutz zu sorgen.

Zentrale Aussagen

- Die Verordnung über Privatsphäre und elektronische Kommunikation sollte die Bedeutung des **Grundsatzes der Vertraulichkeit der Kommunikation** verdeutlichen, der eng mit dem Recht auf Privatleben verknüpft ist und somit durch die EU-Charta der Grundrechte, die Europäische Menschenrechtskonvention sowie die Verfassungs- und Rechtsordnungen der meisten Mitgliedstaaten geschützt ist. Unter die Vertraulichkeit der Kommunikation **fallen sowohl Inhaltsdaten und Metadaten als auch Endeinrichtungen betreffende Daten**. Dies sollte seinen angemessenen Ausdruck in den erlaubten Zwecken der Verarbeitung und in den Rechtsgrundlagen der Verarbeitung finden. **Diese Erwägungen beziehen sich auf alle Bestimmungen der Verordnung über Privatsphäre und elektronische Kommunikation.**

- Die Verordnung über Privatsphäre und elektronische Kommunikation sollte einen echten Schutz im Einklang mit bestehenden und künftig zu erwartenden technologischen Entwicklungen bieten, insbesondere mit Blick auf **Maschine-zu-Maschine-Kommunikation**. Insofern unterstützen wir Änderungsanträge, die ausdrücklich den Schutz der Vertraulichkeit der Kommunikation für *„Daten"* fordern, *„die **im Zusammenhang** mit Endgeräten stehen **oder von diesen verarbeitet** werden"*. Die Vertraulichkeit der Kommunikation sollte ferner gewährleistet sein, wenn Daten **in der Cloud gespeichert werden**, und nicht nur bei der Übermittlung.

- Der Ansatz, dem zufolge **die Verordnung über Privatsphäre und elektronische Kommunikation die Datenschutz-Grundverordnung spezifiziert und ergänzt**,

Postanschrift: Rue Wiertz 60 – 1047 Brüssel, Belgien
Dienststelle: Rue Montoyer 30
E-Mail: edps@edps.europa.eu – Website: www.edps.europa.eu
Tel.: +32 22831900 – Fax: +32 22831950

sollte beibehalten werden, um die Bedeutung der Vertraulichkeit der Kommunikation zu unterstreichen. **Die Verordnung über Privatsphäre und elektronische Kommunikation sollte das in der Datenschutz-Grundverordnung vorgesehene Schutzniveau keinesfalls senken. Vielmehr sollte ein höheres Schutzniveau als das in der Datenschutz-Grundverordnung vorgesehene geboten werden.** Gleichzeitig sollten im Sinne von Klarheit und Rechtssicherheit unnötige Wiederholungen von Bestimmungen der Datenschutz-Grundverordnung vermieden werden; werden selektiv nur einige Bestimmungen der Datenschutz-Grundverordnung wiederholt, besteht die Gefahr, dass wichtige Bestimmungen dabei nicht erfasst werden.[2]

- Eine breit angelegte Rechtsgrundlage für die Verarbeitung von Kommunikationsdaten durch Verweis auf die Datenschutz-Grundverordnung oder durch Zitieren der Datenschutz-Grundverordnung wäre der Begründung eines spezifischen Rechtsinstruments abträglich und würde der Bedeutung des Grundsatzes der Vertraulichkeit der Kommunikation nicht angemessen gerecht, wie er sowohl in der Charta der Grundrechte als auch in der Rechtsprechung von EuGH und EGMR verankert ist. **So sollte nach der Verordnung über Privatsphäre und elektronische Kommunikation auf keinen Fall die Möglichkeit einer Verarbeitung von Metadaten aus Gründen des berechtigten Interesses gegeben sein.** Die Erlaubnis einer Verarbeitung aus Gründen des berechtigten Interesses würde die heute gemäß der Datenschutzrichtlinie für elektronische Kommunikation 2002/58/EG anzuwendenden Standards spürbar senken und den Mehrwert des Verordnungsentwurfs in Frage stellen. In ähnlicher Weise würde die **Weiterverarbeitung von Metadaten ein Schlupfloch schaffen** und ein Umgehen des hohen Schutzniveaus ermöglichen. **Endgeräte betreffende Daten sollten nur nach Einwilligung oder in Fällen verarbeitet werden, in denen dies für einen vom Nutzer verlangten Dienst erforderlich ist, und dann auch nur so lange, wie es für diesen Zweck erforderlich ist.** Wie unterstützen daher Änderungsanträge, die die breit angelegte Rechtsgrundlage für das Tracking natürlicher Personen über Zeit und Raum zu allen Zwecken streichen.

- Damit die Grundrechte in der Praxis geschützt werden können, sind angemessene Begriffsbestimmungen unerlässlich. Daher unterstützen wir Änderungsanträge, die **eigenständige Begriffsbestimmungen** vorsehen, die an die Stelle der Bezugnahme auf den Europäischen Kodex für die elektronische Kommunikation treten und gewährleisten, dass eine Einwilligung, die bei der Abonnieren eines Dienstes durch eine juristische Person gegeben werden muss, von der natürlichen Person erteilt wird, die den Dienst und/oder das Endgerät nutzt. Ferner sind auch wir der Auffassung, dass Dienste, die allein als Nebenfunktion angeboten werden, in die Definition von „interpersonellen Kommunikationsdiensten“ aufgenommen werden sollten. Schließlich empfehlen wir nachdrücklich, dass Daten, die weder für den Zweck der Übermittlung elektronischer Kommunikationsinhalte noch für die Erbringung des Dienstes erforderlich sind, nicht aus der Definition von Metadaten herausgenommen werden. Auf diese Weise entstehen keine Schlupflöcher für die Verarbeitung dieser Daten auf der Grundlage der Datenschutz-Grundverordnung.

- **Eine Einwilligung nach der Verordnung über Privatsphäre und elektronische Kommunikation muss die gleiche Bedeutung haben wie in der Datenschutz-Grundverordnung, sie muss also unter anderem freiwillig und für einen bestimmten Zweck erteilt worden sein.**
    - Daher unterstützen wir Änderungsanträge, mit denen klargestellt wird, dass alle Bestimmungen der Datenschutz-Grundverordnung, darunter Artikel 4 Absatz 11 über die Definition der Einwilligung, Artikel 7 und Artikel 8

Datenschutz-Grundverordnung auch für die Zwecke der Verordnung über Privatsphäre und elektronische Kommunikation gelten.

- Wir unterstützen Änderungsanträge, mit denen klargestellt wird, dass der Zugang zu Diensten und Funktionsmerkmalen **nicht von der Einwilligung in die Verarbeitung** personenbezogener Daten und die Verarbeitung von Informationen in Bezug auf die Endeinrichtungen der Endnutzer oder die durch diese Einrichtungen verarbeiteten Informationen **abhängig gemacht werden darf**.

- Ferner begrüßen wir Änderungsanträge, in denen gefordert wird, dass **bei den technischen Einstellungen, die eine Nutzerkontrolle gemäß Artikel 9 erlauben, ein ausreichender Detailgrad zulässig sein sollte**. Diese Vorgabe entspricht der Vorschrift in der Datenschutz-Grundverordnung, der zufolge eine Einwilligung bestimmten Verantwortlichen (hier Anbietern) für bestimmte Zwecke erteilt werden muss. Wie bereits erwähnt, sollten Bestimmungen aus der Datenschutz-Grundverordnung nicht unnötig wiederholt werden. Wir empfehlen daher, dass die Einstellungen *„dem Nutzer erlauben, aktiv die Zwecke und die Diensteanbieter auszuwählen“*.

- Ohne angemessene **technische und Datenschutzeinstellungen** können Erteilung und Widerruf einer Einwilligung in einem hochentwickelten Online-Umfeld erheblich erschwert werden. Wir unterstützen daher Änderungsanträge zur Stärkung von Artikel 10 und **fordern standardmäßige Datenschutzeinstellungen**. **Darüber hinaus** sollten Datenschutzeinstellungen **die Erteilung und den Widerruf einer Einwilligung auf einfache, verbindliche und durchsetzbare Weise gegenüber allen Parteien** klar unterstützen. Dazu gehört, dass der letzte Satz von Erwägungsgrund 24 des Kommissionsvorschlags eine Bestimmung im verfügenden Teil und rechtliche Auflage wird. Dementsprechend sollte Endnutzern die Gelegenheit eingeräumt werden, *„ihre Einstellungen zur Privatsphäre während der Benutzung jederzeit zu ändern, und sollte dem Nutzer erlaubt werden, Ausnahmen für bestimmte Websites zu machen oder in Listen festzulegen oder anzugeben, von welchen Websites Cookies (auch von Drittanbietern) immer oder niemals angenommen werden sollen“*.

- **Alle Einschränkungen von Rechten im Einklang mit Artikel 11 sollten der Bedeutung der Vertraulichkeit der Kommunikation angemessen Rechnung tragen, wie sie in der ständigen Rechtsprechung des EuGH niedergelegt ist.** Aus diesem Grund sollte der Anwendungsbereich von Einschränkungen kleiner sein als in der Datenschutz-Grundverordnung und sollten spezifische Verpflichtungen im Sinne von mehr Transparenz bei Auskunftsersuchen festgelegt werden. Wird der Anwendungsbereich auf schwere Straftaten beschränkt, ist dieser Begriff näher zu definieren. Die Mindestanforderungen an eine gesetzgeberische Maßnahme in Artikel 23 Absatz 2 sollten in jedem Fall gelten.

- **Die Aufsicht über die Verordnung über Privatsphäre und elektronische Kommunikation sollten den Datenschutzbehörden übertragen werden.** Als Aufsichtsbehörden, die die Einhaltung der Datenschutz-Grundverordnung zu gewährleisten haben, sind sie am ehesten in der Lage, für Rechtssicherheit und eine stimmige Anwendung der beiden so eng miteinander verknüpften Rechtsinstrumente zu sorgen. Außerdem sind die Datenschutzbehörden besser als jeder andere geeignet, eine einheitliche Anwendung der Verordnung über Privatsphäre und elektronische Kommunikation überall in der Union zu gewährleisten, und zwar mit Hilfe des Europäischen Datenschutzausschusses.

- **Es bedarf eines wirksamen Schutzes gegen unerbetene Kommunikation** Wir begrüßen daher Änderungsanträge, denen zufolge halbautomatische Anrufsysteme nur nach Einwilligung erlaubt sind, und fordern den EU-Gesetzgeber auf, dafür zu sorgen, dass solche Systeme eindeutig in die Definition von „automatischen Anruf- und Kommunikationssystemen“ aufgenommen werden. Des Weiteren begrüßen wir Änderungsanträge, die wirksame technische Maßnahmen vorsehen, insbesondere die Kombination von Anzeige der Rufnummer und einer obligatorischen Vorwahl für die Identifizierung unerwünschter Anrufe, und wir unterstützen die Ausdehnung des Schutzes, der für alle Formen unerbetener Kommunikation und nicht nur für „Direktwerbung“ gilt.

Nachstehend unsere spezifischen Empfehlungen zu den genannten zentralen Punkten.

1. Jegliche Verarbeitung von Kommunikationsdaten bedarf einer Rechtsgrundlage im Einklang mit der Verordnung über Privatsphäre und elektronische Kommunikation (Artikel 6, Erwägungsgrund 5)

Einer der größten Pluspunkte des Entwurfs der Verordnung über Privatsphäre und elektronische Kommunikation liegt darin, dass sie – wie heute die Datenschutzrichtlinie für elektronische Kommunikation – durch die Einschränkung und Präzisierung der Rechtsgrundlagen für die Verarbeitung von Kommunikationsdaten zusätzlichen Schutz für elektronische Kommunikation bietet.

Wir begrüßen die vorgeschlagenen Änderungen an Artikel 6, mit denen klargestellt wird, dass **„unbeschadet Artikel 6 [Datenschutz-Grundverordnung]“** elektronische Kommunikationsdaten **„nur dann“** verarbeitet werden dürfen, wenn [die in der Verordnung über Privatsphäre und elektronische Kommunikation aufgeführten rechtlichen Gründe vorliegen]. Dieser Artikel in seiner geänderten Fassung trägt zu Klarheit und Rechtssicherheit bezüglich der Tatsache bei, dass andere rechtliche Gründe, wie das berechtigte Interesse, auf Verarbeitungen nach der vorgeschlagenen Verordnung keine Anwendung finden.

Ferner begrüßen wir LIBE 4, wo mit einer Änderung von Erwägungsgrund 5 klargestellt wird, dass eine Verarbeitung *„nur auf einer durch die Verordnung [über Privatsphäre und elektronische Kommunikation] vorgesehenen Rechtsgrundlage“* erlaubt sein sollte. Als weitere Verbesserung empfehlen wir eine Umformulierung dieses Satzes, damit diese Bestimmung auf alle Parteien anwendbar wird, nicht nur auf Anbieter elektronischer Kommunikationsdienste.

Wie schon in unserer Stellungnahme angeregt, würden wir ferner begrüßen, wenn in einem Artikel geregelt würde, dass *„**weder Anbieter von elektronischen Kommunikationsdiensten noch Dritte personenbezogene Daten, die aufgrund einer Einwilligung oder aus einem anderen Rechtsgrund gemäß der Verordnung über Privatsphäre und elektronische Kommunikation erhoben wurden, aus einem anderen, nicht ausdrücklich in der Verordnung über Privatsphäre und elektronische Kommunikation vorgesehenen Rechtsgrund verarbeiten dürfen“.***

2. Zu den Rechtsgründen gemäß der Verordnung über Privatsphäre und elektronische Kommunikation darf nicht das berechtigte Interesse gehören.

In einigen Änderungsanträgen wird eine weitere Ausnahme von der Vertraulichkeit der Kommunikation aus Gründen des berechtigten Interesses von Diensteanbietern oder anderen Parteien an der Verarbeitung elektronischer Kommunikationsdaten **vorgeschlagen**.

Eine solche Ausnahme ist weder in der derzeitigen Datenschutzrichtlinie für elektronische Kommunikation noch in der vorgeschlagenen Verordnung zu finden, und auch der Berichtsentwurf schlägt solche Ausnahmen nicht vor, weder für Metadaten noch für Inhaltsdaten. Datenschutzbehörden und unabhängige Sachverständige schließen sich dieser Auffassung an und sind sich darin einig, dass **eine weitere Ausnahme aus berechtigtem Interesse, entweder für Metadaten oder für Inhaltsdaten, ein Schlupfloch schaffen und viel von dem Schutz wegnehmen würde, den die Verordnung über Privatsphäre und elektronische Kommunikation für die Vertraulichkeit der Kommunikation vorsieht.** [3]

Der Gesetzgeber sollte bedenken, dass Informationen über die Umstände von Kommunikation und über deren Teilnehmer ausdrücklich als Grundrecht auf Wahrung des Fernmeldegeheimnisses geschützt und somit auch durch die Verfassungen und Rechtsordnungen vieler Mitgliedstaaten geschützt sind. Würde die Verarbeitung von Kommunikationsdaten ohne Einwilligung oder einen begrenzten Zweck erlaubt, der spezifisch und hinreichend genau im Gesetz geregelt ist, würde dies das Wesen dieses Grundrechts berühren und der Tradition vertrauenswürdiger Boten ein Ende bereiten.

Aus diesen Gründen sprechen wir uns klar gegen Änderungsanträge aus, die das berechtigte Interesse als Rechtsgrundlage für eine Verarbeitung nach der Verordnung über Privatsphäre und elektronische Kommunikation einführen würden. **Die Möglichkeit einer Weiterverarbeitung darf auf keinen Fall das hohe Niveau des Schutzes der Vertraulichkeit der Kommunikation senken.**

Begrüßen würden wir Änderungsanträge, die mit einer Bestimmung Folgendes klarstellen würden: ***„Wenn die Verarbeitung aufgrund einer Ausnahme von den in der Verordnung über Privatsphäre und elektronische Kommunikation aufgeführten Verboten zulässig ist, gilt jede andere Verarbeitung aufgrund von Artikel 6 der Datenschutz-Grundverordnung, einschließlich der Verarbeitung zu einem anderen Zweck nach Artikel 6 Absatz 4 der Datenschutz-Grundverordnung, als unzulässig. Dabei würde nichts dagegen sprechen, dass die für die Verarbeitung Verantwortlichen eine zusätzliche Einwilligung für neue Verarbeitungsaktivitäten einholen.“***

Wir nehmen Änderungsanträge zu Artikel 7 zur Kenntnis, in denen vorgeschlagen wird: *„Der Teilnehmer kann die Daten gegebenenfalls im Einklang mit [der Datenschutz-Grundverordnung] weiterverarbeiten“.* Diese Klarstellung könnte, zusätzlich zu den weiter oben angeregten Änderungen, ebenfalls akzeptiert werden.

Gleichzeitig sprechen wir uns klar gegen alle Änderungsanträge aus, die eine Weiterverarbeitung ganz allgemein erlauben würden, da dies, wie in unsrer Stellungnahme ausgeführt, den Schutz der Vertraulichkeit der Kommunikation schwer beeinträchtigen und ein gefährliches Schlupfloch schaffen würde, das ein Umgehen der Verordnung ermöglichen würde.

3. Die Vertraulichkeit der Kommunikationsdaten ist bei „gespeicherten Daten“ und in der Maschine-zu-Maschine-Kommunikation gewährleistet (Artikel 5).

In der Stellungnahme gaben wir zu bedenken, dass die Verordnung über Privatsphäre und elektronische Kommunikation 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. **Wir empfahlen, Artikel 5 und Erwägungsgrund 15 des Vorschlags dahingehend zu ändern, dass beide Fälle eindeutig abgedeckt sind.**

Zu diesem Zweck würden wir ferner anregen, diese Bestimmung auch auf Kommunikationsdaten auszudehnen, die nicht nur in der Übermittlung sind, sondern auch vom

Betreiber oder einer anderen Partei gespeichert werden (ein typisches Beispiel können Inhalte von in der „Cloud“ gespeicherten E-Mails sein). Änderungsanträge zu Artikel 5, die besagen, dass das in Absatz 1 ausgesprochene Verbot auch für ***„elektronische Kommunikationsdaten“*** gilt, ***„die nach dem Abschluss der Übertragung gespeichert werden“*** (siehe LIBE 399 und 400), sind gute Beispiele dafür, wie man dieses Anliegen formulieren könnte. Als hilfreich könnte sich auch die Formulierung in LIBE 401 erweisen, wo von *„übertragenen oder gespeicherten Kommunikationsdaten“* die Rede ist.

Wie in unserer Stellungnahme ausgeführt, **sollte der Schutz der Privatheit von Kommunikation 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**.

In diesem Zusammenhang unterstützen wir Änderungsanträge (gestützt auf LIBE 59, 409, 410), die Folgendes vorsehen: *„Die Vertraulichkeit elektronischer Kommunikation gilt ebenfalls für Daten, **die sich auf Endeinrichtungen beziehen oder in diesen verarbeitet werden** (...)“*. Eine andere Formulierung für dieselbe Bestimmung könnte lauten: *„Das in Absatz 1 vorgesehene Verbot gilt auch für Daten, die sich auf Endeinrichtungen beziehen oder in diesen verarbeitet werden“.*

4. Daten, die sich auf Endeinrichtungen beziehen, verdienen ebenfalls ein hohes Schutzniveau.

Der Schutz von Daten, die sich auf Endeinrichtungen beziehen, sollte je nach den technologischen Entwicklungen und im Einklang mit dem Grundsatz der Vertraulichkeit der Kommunikation und mit der Auflage erfolgen, dass die Verordnung über Privatsphäre und elektronische Kommunikation nicht unter das Schutzniveau rücken sollte, das derzeit von der Datenschutzrichtlinie für elektronische Kommunikation und der Datenschutz-Grundverordnung geboten wird.

Wir begrüßen daher die Änderungsanträge, in denen die Einwilligung des Nutzers gefordert und die übermäßige Ausnahme in Artikel 8 Absatz 2 Buchstabe b des Kommissionsvorschlags entfernt wird. Des Weiteren begrüßen wir, dass im Einklang mit dem Grundsatz der Transparenz die Informationen für Nutzer eine zusätzliche Vorgabe werden, nicht jedoch eine Rechtsgrundlage für das Tracking von Personen über Zeit und Raum für alle möglichen Zwecke. Wir unterstützen Änderungsanträge, die klarstellen, dass eine Verarbeitung, die für den alleinigen Zweck der Herstellung einer Verbindung erlaubt ist, nur für die hierfür erforderliche Zeit erlaubt ist.

Gleichzeitig setzen wir uns nicht für die Aufnahme detaillierter weiterer Rechtsgründe in die Verordnung über Privatsphäre und elektronische Kommunikation ein, die weitere, spezifische Ausnahmen mit sich bringen (mit einer denkbaren, aber ganz genau maßgeschneiderten Ausnahme für die „Zählung von Personen“).

Sollten solche detaillierten Ausnahmen jedoch in irgendeiner Phase des Gesetzgebungsverfahrens im Rahmen eines Kompromisses vorgeschlagen werden, sollte zumindest gewährleistet sein, dass sie so formuliert werden, dass keine unbeabsichtigten Schlupflöcher entstehen. Dies gilt neben der „Zählung von Personen“ auch für die vorgeschlagenen Rechtsgründe im Zusammenhang mit der Herstellung einer Verbindung, Sicherheitsupdates, Beschäftigungsverhältnissen und der Messung des Webpublikums.

- Bezüglich der **„Zählung von Personen“** empfehlen wir als Minimum, Anforderungen hinzuzufügen, damit gewährleistet ist, dass „der Zweck der Verarbeitung allein auf die Zählung von Personen zu statistischen Zwecken beschränkt ist“, dass „Daten so bald wie möglich nach der Erhebung anonymisiert werden“, dass „die Verarbeitung streng auf einen bestimmten und abgegrenzten geografischen Bereich beschränkt ist“ und dass „Nutzer wirksame Möglichkeiten des Opting-out haben“.

- Bezüglich der **„Herstellung einer Verbindung“** unterstützen wir Änderungsanträge, denen zufolge dieser Vorgang „für den alleinigen Zweck der Herstellung einer vom Nutzer gewünschten Verbindung“ erfolgt.

- Bezüglich der **„Messung des Webpublikums“** wiederholen wir unser Anliegen, dass dieser Grund präzise zugeschnitten und ausgelegt werden muss und im Verlauf des Gesetzgebungsverfahrens nicht ungebührlich erweitert werden darf. Änderungsanträge, mit denen die Vorgabe hinzugefügt werden soll, dass „solche Messungen die Grundrechte des Nutzers nicht beeinträchtigen“, begrüßen wir.

- Bezüglich der **„Sicherheitsupdates“** empfehlen wir als Minimum, dass Sicherheitsupdates „unbedingt erforderlich“ sein müssen, „das von den Nutzereinstellungen gebotene Niveau der Vertraulichkeit nicht senken“, und dass der Nutzer „vor jedem Update unterrichtet wird“ und „die Möglichkeit hat, die automatische Installation dieser Updates abzustellen“.

- Zu den vorgeschlagenen **„Ausnahmen im Rahmen von Beschäftigungsverhältnissen“** sei angemerkt, dass jede Ausnahme „streng auf das begrenzt sein muss, was für die Wahrnehmung der Aufgaben eines Beschäftigten erforderlich ist“, „auf Fälle beschränkt sein muss, in denen der Arbeitgeber die Endeinrichtung bereitstellt und/oder der Teilnehmer ist“, und dass der „Arbeitgeber diesen Rechtsgrund nicht zur Überwachung seiner Beschäftigten anführt“.

5. Damit die Grundrechte in der Praxis geschützt werden können, sind angemessene Begriffsbestimmungen unerlässlich (Artikel 4).

5.1 Ersatz des Verweises auf die Begriffsbestimmungen des Europäischen Kodex für elektronische Kommunikation (Kodex) durch eigenständige Definitionen (Artikel 4)

Bei bestimmten zentralen Begriffsbestimmungen[4] verweist der Vorschlag den Leser auf den Europäischen Kodex für elektronische Kommunikation (Kodex).

Wie bereits in unserer Stellungnahme zum Ausdruck gebracht, begrüßen wir die Änderungsanträge, mit denen der Verweis auf den Kodex, der sich noch im Gesetzgebungsverfahren befindet, durch eigenständige Begriffsbestimmungen ersetzt wird (siehe LIBE 46ff.) Es muss unbedingt gewährleistet sein, dass die Begriffsbestimmungen in der Verordnung über Privatsphäre und elektronische Kommunikation von dem Vorschlag für den Kodex unabhängig sind und dass zentrale Begriffe in der Verordnung über Privatsphäre und elektronische Kommunikation definiert werden.

Eigenständige Definitionen sind vor allem in all den Fällen wichtig, in denen sich die Definition in einem oder mehreren bedeutenden Aspekten von der Definition im Kodex unterscheidet, wie

es im Fall der Begriffsbestimmung von „interpersonellem Kommunikationsdienst“ der Fall ist, die auch „Dienste“ einschließt, „die eine interpersonelle und interaktive Kommunikation lediglich als untrennbar mit einem anderen Dienst verbundene untergeordnete Nebenfunktion ermöglichen“. Wir begrüßen Änderungsanträge, die solche Klarstellungen anstreben.

Eigenständige Begriffsbestimmungen sind auch in allen anderen Fällen von Bedeutung, selbst wenn derzeit die Definitionen des Kodex passend erscheinen, denn es ist zu bedenken, dass sich die Begriffsbestimmungen im Kodex im Laufe des noch nicht abgeschlossenen Gesetzgebungsverfahrens noch ändern können. Daher empfehlen wir, auch für „Anruf“ eine eigenständige Definition aufzunehmen und nicht auf Artikel 2 Absatz 21 des Kodex zu verweisen, wie im Berichtsentwurf geschehen.

5.2 Definition von „Nutzer“ und/oder „Endnutzer“

Wir **begrüßen Änderungsanträge, die eine Wiedereinführung der Definition von „Nutzer“ anstreben,** ausgehend von der derzeit bestehenden Definition in der Datenschutzrichtlinie für elektronische Kommunikation, die da lautet: *„natürliche Person, die einen öffentlich zugänglichen elektronischen Kommunikationsdienst nutzt, für private oder geschäftliche Zwecke, ohne diesen Dienst notwendigerweise abonniert zu haben“.*

Wenn diese Änderungen übernommen werden, **ist es jedoch genauso wichtig, dass der Begriff „Nutzer“ dann durchgehend in der Verordnung verwendet wird, und nicht der Begriff „Endnutzer“,** der im Entwurf des Kodex definiert ist und im Kommissionsvorschlag verwendet wurde.

Als Faustregel gilt, dass der Begriff „Nutzer“ in der Verordnung durchgängig in allen Fällen verwendet werden sollte, in denen er auch in gleichartigen Bestimmungen in der derzeitigen Datenschutzrichtlinie für elektronische Kommunikation verwendet wird. Wie wir in unserer Stellungnahme erläutert haben, **muss klar sein, dass eher die betroffenen und beteiligten Personen in der Lage sein sollten, eine gültige Einwilligung in die Verarbeitung ihrer Kommunikation zu erteilen, und weniger ihre Arbeitgeber oder Vermieter**.

Besonders sollte jedoch darauf geachtet werden, dass in manchen Fällen, und hier vor allem, wenn eine Bestimmung spezifisch auf den Schutz von Rechten juristischer Personen abhebt, die einen Dienst beantragen, abonnieren oder nutzen, ein anderer, besserer Begriff und eine andere Definition verwendet werden sollten anstatt des Begriffs „Nutzer“ oder zusätzlich zu ihm, um zu gewährleisten, dass juristische Personen ebenfalls geschützt bleiben. In der derzeitigen Richtlinie wird für diesen Zweck in der Regel der Begriff „Teilnehmer“ verwendet.

5.3 Definition von Metadaten

Die vorgeschlagenen Änderungen zeigen, dass sich die Abgeordneten des EP der Risiken für Privatsphäre und Datenschutz durch die Verarbeitung von Metadaten bewusst sind. Ungeachtet dieses Bewusstseins folgen die Änderungsanträge noch immer dem Ansatz des Vorschlags und **beschränken den Begriff Metadaten** auf Daten, die *„zum Zwecke der Übermittlung, Verbreitung oder Ermöglichung des Austauschs elektronischer Kommunikationsinhalte verarbeitet werden“,* und/oder beschränken ihn auf Daten, die *„für die Erbringung des Dienstes verarbeitet werden“*.

Zwar decken diese Begriffsbestimmungen einen großen Teil der Metadaten ab, doch sind sie nicht vollständig, da alle Metadaten unberücksichtigt bleiben, die weder *zum Zwecke der Übermittlung, Verbreitung oder Ermöglichung des Austauschs elektronischer Kommunikationsinhalte verarbeitet werden* noch *für die Erbringung des Dienstes verarbeitet*

werden. Ein Beispiel hierfür sind Standortdaten in einer Anwendung für Sofortnachrichtenübermittlung (Instant Messaging).

Daher schlägt der EDSB die folgendermaßen geänderte Begriffsbestimmung vor, die alle Metadaten abdeckt:

c) „elektronische Kommunikationsmetadaten": Daten, die in einem elektronischen Kommunikationsnetzwerk verarbeitet werden ***und keine „elektronischen Kommunikationsinhalte" sind, sowie*** *Daten, die von den Endgeräten ausgestrahlt oder gesendet werden und* **weitere Informationen über die Kommunikation bieten oder** *zur Identifizierung der Endgeräte der Endnutzer im Netzwerk verwendet werden* ***oder*** *ihren Anschluss an ein solches Netzwerk oder an andere Endgeräte ermöglichen.*

Zu ihnen zählen, wenn auch nicht ausschließlich, *die zur Verfolgung und Identifizierung des Ausgangs- und Zielpunkts einer Kommunikation verwendeten Daten, Daten über den Standort des Geräts sowie Datum, Uhrzeit, Dauer und Art der Kommunikation.*

6. Die Einwilligung muss die gleiche Bedeutung haben wie in der Datenschutz-Grundverordnung, muss also freiwillig und für einen bestimmten Zweck erteilt werden (Artikel 6, 8 und 9). Technische und Datenschutzeinstellungen sollten die Erteilung und den Widerruf einer Einwilligung wirksam und auf einfache Weise unterstützen (Artikel 9 und 10).

Im Hinblick auf Artikel 9 Absatz 1 würden wir Änderungsanträge begrüßen, **mit denen klargestellt wird, dass alle die Einwilligung betreffenden Bestimmungen der Datenschutz-Grundverordnung** (einschließlich Artikel 8 Datenschutz-Grundverordnung zur Einwilligung von Kindern) **auch für die Zwecke der Verordnung über Privatsphäre und elektronische Kommunikation gelten.** Insbesondere würden wir folgenden Wortlaut begrüßen: *„Die Begriffsbestimmungen von Einwilligung und die Bedingungen für die Einwilligung. wie sie in der Verordnung (EU) 2016/679 festgelegt sind, unter anderem in deren Artikel 4 Absatz 11, in den Artikeln 7 und 8, finden Anwendung".* Sobald dies gewährleistet ist, können überflüssige Wiederholungen von wesentlichen Merkmalen der Einwilligung, wie „für einen bestimmten Zweck" erteilte Einwilligung, wegfallen.

Die Bestandteile der Einwilligung, vor allem ihre Freiwilligkeit, implizieren, dass die Verarbeitung keine nachteiligen Auswirkungen auf die Rechte und Freiheiten natürlicher Personen hat. Wir begrüßen daher Änderungsanträge mit folgender Vorgabe: ***Eine auf Einwilligung beruhende Verarbeitung darf sich nicht nachteilig auf die Rechte und Freiheiten von Einzelpersonen –*** *insbesondere ihr Recht auf Privatsphäre und auf Schutz personenbezogener Daten –* ***auswirken, deren personenbezogene Daten mit einer Kommunikation in Verbindung stehen oder in deren Rahmen übermittelt werden.***

Nachdrücklich unterstützen wir Änderungsanträge, die den Grundsatz stärken, dass die Einwilligung aus freien Stücken gegeben werden muss, und die Konzepte nach dem Alles-oder-Nichts-Grundsatz verbieten. Insbesondere unterstützen wir die vorgeschlagenen Änderungen an Artikel 6, mit denen klargestellt wird, dass die Einwilligung in die Verarbeitung ***„keine Bedingung für den Zugang zu einem Dienst oder dessen Nutzung"*** sein darf. Dies sollte für die Verarbeitung sowohl von Inhalts- als auch von Metadaten gelten.

Ähnlich begrüßen wir die vorgeschlagenen Änderungen an Artikel 8, mit denen klargestellt wird, dass die Einwilligung **„keine Bedingung für den Zugang zu einem Dienst bzw. dessen**

Nutzung oder der Nutzung einer Endeinrichtung“ sein darf. Des Weiteren begrüßen wir die vorgeschlagenen Änderungen, die besagen: ***„Dem Endnutzer darf der Zugang zu einem Dienst der Informationsgesellschaft oder einem elektronischen Kommunikationsdienst – unabhängig davon, ob diese Dienste gegen Entgelt erbracht werden – nicht mit der Begründung verweigert werden, dass der Endnutzer keine Einwilligung gemäß Artikel 8 Absatz 1 Buchstabe b zur Verarbeitung von Daten und/oder zur Nutzung der Speicherfunktionen seiner Endeinrichtungen gegeben hat, die für die Erbringung dieses Dienstes oder der gewünschten Funktion nicht unbedingt nötig sind.“***

Mit Blick auf Artikel 9 Absatz 2 **begrüßen wir Änderungsanträge, die darauf abheben, dass die in diesem Absatz erwähnten technischen Einstellungen im Hinblick auf Zwecke und Anbieter einen ausreichenden Detailgrad zulassen**, gleichzeitig aber Bestimmungen der Datenschutz-Grundverordnung nicht unnötigerweise wiederholen. Im Sinne einer weiteren Verbesserung der vorliegenden Änderungsanträge könnte es in der Bestimmung auch heißen, dass die Einstellungen *„dem Nutzer die Möglichkeit geben, aktiv die Zwecke und die Diensteanbieter auszuwählen“*.

Ferner sollte in diesen Änderungsanträgen näher spezifiziert werden, dass **die technischen Einstellungen, die auf Vorlieben des Nutzers hinweisen, *„verbindlich für etwaige andere Parteien und ihnen gegenüber durchsetzbar sind“*.**

Ferner unterstützen wir auch weitere Klarstellungen dahingehend, dass ein Nutzer, der seine Einwilligung gibt, damit die bereits bestehenden Datenschutzeinstellungen aktualisiert. Diese Aktualisierung sollte jedoch auf die von dem Nutzer für diesen konkreten Dienst gewünschte Verarbeitung beschränkt sein. (So kann beispielsweise ein Nutzer in das Tracking auf einer bestimmten Nachrichten-Website durch ein bestimmtes Werbe-Netzwerk einwilligen. Damit sollte jedoch diesem Werbe-Netzwerk nicht gestattet sein, den Nutzer auf einer anderen Website zu verfolgen, es sei denn, der Nutzer hat ausdrücklich auch in ein Tracking bei Besuchen dieser anderen Website eingewilligt).

Wir würden nachdrücklich Änderungsanträge zur Stärkung von Artikel 10 unterstützen und **fordern standardmäßige Datenschutzeinstellungen**. Entsprechend empfehlen wir, dass **in Verkehr gebrachte Software**, die elektronische Kommunikation ermöglicht, ***„in der Voreinstellung Datenschutzeinstellungen bietet, durch die verhindert wird, dass andere Parteien Informationen in der Endeinrichtung eines Nutzers speichern oder bereits in der Endeinrichtung gespeicherte Informationen verarbeiten.“***

Des Weiteren würden wir Änderungen (siehe LIBE 639, 640) begrüßen, denen zufolge **das Erfordernis der datenschutzfreundlichen Voreinstellungen nicht nur für Software, sondern auch für Hardware gilt**. Dies wäre ein stärkerer und direkterer Anreiz für Anbieter des Internets der Dinge (IoT), Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen in Erwägung zu ziehen.

Schließlich **halten wir es für wesentlich, dass Nutzer auf einfache Weise jederzeit während oder nach der Installation der Software für bestimmte Zwecke und mit Blick auf bestimmte Diensteanbieter detailliert ihre Einwilligung geben bzw. widerrufen können.** Dazu gehört, dass es für sie einfache Möglichkeiten gibt, ihre Datenschutzeinstellungen zu aktualisieren (z. B. eine oder mehrere konkrete Organisationen auf ihre in ihren Datenschutzeinstellungen gespeicherten individuellen weißen und/oder schwarzen Listen zu setzen oder daraus zu streichen), ohne sich bei jeder Navigation zu einer anderen Website durch eine Reihe von Einstellungen und Optionen arbeiten zu müssen.

In der Praxis könnte dies bedeuten, dass Personen, die eine Website aufsuchen und dort zu einer erneuten Einwilligung aufgefordert werden, ihre Datenschutzeinstellungen direkt durch Anklicken einer der auf der Website angebotenen Optionen aktualisieren können, und dass ihre Entscheidung dann in ihren Datenschutzeinstellungen gespeichert wird. Sollte die Person ihre Einwilligung widerrufen wollen, sollte dies auf ähnlich einfache Weise erfolgen können.

Der letzte Satz von Erwägungsgrund 24 weist auf eine solche Möglichkeit bereits hin, denn dort heißt es: *„Es sollte gefördert werden, dass Webbrowser den Endnutzern einfache Möglichkeiten bieten, die Einstellungen zur Privatsphäre während der Benutzung jederzeit zu ändern, und dem Nutzer erlauben, Ausnahmen für bestimmte Websites zu machen oder in Listen festzulegen oder anzugeben, von welchen Websites Cookies (auch von Drittanbietern) immer oder niemals angenommen werden sollen"*. **Wir empfehlen, dass dieser Erwägungsgrund und diese „Förderung" zu einer Bestimmung im verfügenden Teil und einer rechtlichen Auflage gemacht werden.** Diese rechtliche Auflage sollte zudem nicht nur für Webbrowser gelten, sondern auch für alle anderen Anbieter, die in den Anwendungsbereich von Artikel 10 fallen. Dementsprechend **empfehlen wir, dass in Artikel 10 die Vorgabe aufgenommen wird, dass *„in Verkehr gebrachte Hardware und Software, die elektronische Kommunikation ermöglicht, Nutzern während der Nutzung jederzeit einfache Möglichkeiten für die Änderung ihrer Einstellungen zur Privatsphäre bietet".***

7. Der Anwendungsbereich von Einschränkungen der Rechte sollte begrenzt sein (Artikel 11).

In seiner Stellungnahme unterstützte der EDSB den Ansatz des Vorschlags, nur bestimmte der in Artikel 23 Absatz 1 der Datenschutz-Grundverordnung aufgeführten Gründe als Begründung für eine Einschränkung der in der Verordnung über Privatsphäre und elektronische Kommunikation niedergelegten Rechte und Pflichten zuzulassen. Die Wahrung der Vertraulichkeit der Kommunikation, wie sie in Artikel 7 der Charta verankert ist, ist für die Wahrnehmung anderer Grundrechte entscheidend und spielt daher eine herausragende Rolle. Diese Rolle wird in den Verfassungstraditionen vieler Mitgliedstaaten anerkannt, die ein eigenständiges Recht auf Wahrung der Vertraulichkeit der Kommunikation vorsehen. Einige dieser Verfassungstraditionen beschränken die Möglichkeit zur Einschränkung dieses Rechts allein auf die Bekämpfung schwerer Kriminalität. Wir unterstützen daher Änderungsanträge, die auf weniger in die Privatsphäre eindringende Eingriffe abheben und die Kategorien öffentlichen Interesses auf die in Artikel 23 Absatz 1 Buchstaben a bis d Datenschutz-Grundverordnung genannten beschränken.

Aus der Rechtsprechung des EuGH ergibt sich, dass ein Eingriff in die in Artikel 7 und 8 verankerten Rechte unbedingt erforderlich sein muss. Die Bedingung der *unbedingten Erforderlichkeit* ist horizontal zu verstehen, unabhängig von dem betreffenden Sektor, also Wirtschaft oder Strafverfolgung.[5] Wir unterstützen Änderungsanträge mit einem Verweis auf die *„unbedingte Notwendigkeit"* einer Maßnahme, mit der die in Artikel 5 der Verordnung über Privatsphäre und elektronische Kommunikation verankerten Rechte eingeschränkt werden.

Im Einklang mit der Stellungnahme unterstützen wir ferner Änderungsanträge, in denen gefordert wird, dass Rechtsvorschriften der Union oder von Mitgliedstaaten, die die Rechte einschränken, zumindest einige Regelungen enthalten sollten, die dazu beitragen, die Rechtssicherheit und einige Mindestgarantien zu gewährleisten. Diese Auflage setzt eigentlich die ständige Rechtsprechung zu den Bedingungen für eine rechtmäßige Einschränkung von Grundrechten um.[6] So hält beispielsweise ein Gesetz, dass nichts zum Zweck der Verarbeitung oder zu den Datenkategorien aussagt, einer gerichtlichen Überprüfung nicht stand, da es ihm an Vorhersehbarkeit mangelt, es die Rechtssicherheit gefährdet und auch die Notwendigkeit der gesetzgeberischen Maßnahme nicht nachgewiesen werden kann. Folglich ist ein Verweis

auf Artikel 23 Absatz 2 Datenschutz-Grundverordnung umso mehr geboten, wenn das Gesetz eine Einschränkung des in Artikel 5 der Verordnung über Privatsphäre und elektronische Kommunikation vorgesehenen Rechts auf Vertraulichkeit vorsieht.

In Anbetracht der Notwendigkeit klarer und präziser Vorschriften, die die Prüfung der Erforderlichkeit bestehen, sollte in Änderungsanträgen, die von „schweren Straftaten" sprechen, der Grad der Schwere näher definiert werden, da eine solche Definition nicht allein den Mitgliedstaaten überlassen werden kann.[7]

Schließlich setzen wir uns für größtmögliche Transparenz bei Auskunftsersuchen ein. Zu diesem Zweck unterstützen wir im Einklang mit der Stellungnahme Änderungsanträge, die regelmäßige Berichtspflichten der Anbieter gegenüber den Aufsichtsbehörden vorsehen (zusätzlich zu der im Vorschlag bereits enthaltenen Verpflichtung, den Aufsichtsbehörden auf Ersuchen Informationen bereitzustellen). Darüber hinaus unterstützen wir Änderungsanträge, die für die Anbieter die Verpflichtung vorsehen, Informationen zu Auskunftsersuchen zu veröffentlichen.

8. Eine Schwächung der Vertraulichkeit und Integrität von Kommunikation sollte verboten werden (Artikel 19).

Einschränkungen von Rechten gemäß Artikel 11 können technische Maßnahmen beinhalten, mit denen Zugriff auf Kommunikationsdaten erlangt wird. In seiner Stellungnahme setzte sich der EDSB für das Recht der Nutzer auf Verschlüsselung und für das Verbot aller Maßnahmen ein, mit denen Verschlüsselung rückgängig gemacht werden kann. Wir unterstützen daher Änderungsanträge, die die Schwächung von Vertraulichkeit und Integrität elektronischer Kommunikation sowohl auf der Ebene des Dienstes selbst als auch in den Endgeräten des Nutzers (beispielsweise durch den Auftrag, Hintertüren einzubauen) verbieten.

Somit würden wir Änderungen auf der Grundlage von LIBE 776-780 begrüßen.

9. Datenschutzbehörden sollten Aufsichtsbefugnisse erhalten (Artikel 18).

In seiner Stellungnahme unterstützte der EDSB den Vorschlag, der vorsah, Datenschutzbehörden die Aufsicht über die Verordnung über Privatsphäre und elektronische Kommunikation zu übertragen. Wir plädieren auch weiterhin für diesen Ansatz, da er für Rechtssicherheit und eine kohärente Anwendung des Datenschutzrahmens sorgt, beispielsweise im Hinblick auf die Auslegung zentraler Konzepte wie „Einwilligung". Er vermeidet ferner, dass Datenschutzbehörden und andere Behörden die gleiche Rolle erhalten und es dabei zu Kompetenzüberschneidungen kommt, wenn beispielsweise eine andere Behörde als die Datenschutzbehörde für die Vertraulichkeit der Kommunikation zuständig wäre, was die Verarbeitung personenbezogener Daten mit sich brächte. Wir sprechen uns ferner gegen Änderungsanträge aus, denen zufolge alle nationalen zuständigen Behörden (nicht nur Datenschutzbehörden) im Europäischen Datenschutzausschuss vertreten sein sollen. Mit diesen Anträgen würde der in der Datenschutz-Grundverordnung geschaffene institutionelle Rahmen spürbar verändert und entstünde zusätzliche – und möglicherweise nicht zu bewältigende – Komplexität. Derzeit besagen die Vorschriften, dass nur Datenschutzbehörden Mitglieder des Europäischen Datenschutzausschusses sind; sollte es mehr als eine Datenschutzbehörde geben, müssen die Mitgliedstaaten einen gemeinsamen Vertreter benennen.

Auf der anderen Seite unterstützen wir Änderungsanträge, die ein engere Zusammenarbeit zwischen nationalen Regulierungsbehörden und Datenschutzbehörden anstreben. Diese

Änderungsanträge, die eine auf Gegenseitigkeit beruhende Kooperationspflicht fordern, ergänzen den Kommissionsvorschlag, der bereits eine einseitige Verpflichtung für Datenschutzbehörden zur Zusammenarbeit mit nationalen Regulierungsbehörden vorsah.

Schließlich kann eine wirksame Aufsicht nur erfolgen, wenn tatsächlich angemessene Ressourcen bereitgestellt werden. Gemäß der Datenschutz-Grundverordnung übernimmt der EDSB die Funktion des Sekretariats für den Europäischen Datenschutzausschuss und stellt auch das Personal hierfür. Wir würden daher die Aufnahme einer Bestimmung vorschlagen, die von den Mitgliedstaaten und der EU-Haushaltsbehörde die Bereitstellung angemessener Ressourcen für die nationalen Datenschutzbehörden bzw. den EDSB verlangt.

10. Es bedarf eines umfassenden Schutzes gegen unerbetene Kommunikation (Artikel 16).

Wir begrüßen Änderungsanträge, die das Wort *„oder“* zwischen Artikel 16 Absatz 3 Buchstaben a und b durch *„und“* ersetzen wollen. Mit diesen Änderungsanträgen wird nämlich gewährleistet, dass die Angabe einer Rufnummer, unter der die natürliche oder juristische Person, die den Anruf tätigt, erreichbar ist (Artikel 16 Absatz 3 Buchstabe a), und die Verwendung eines besonderen Kodes/einer Vorwahl, der/die kenntlich macht, dass es sich um einen Werbeanruf handelt (Artikel 16 Absatz 3 Buchstabe b), nicht mehr als Alternativen gelten, wie im Vorschlag vorgesehen, sondern beide obligatorisch werden.

Ebenfalls begrüßen wir Änderungsanträge, in denen das Wort „richten“ zu „anzeigen“ hinzugefügt und damit der derzeitige Wortlaut an den technologischen Wandel angepasst wird.

Wir begrüßen Änderungsanträge, die vorsehen, dass halbautomatische Anrufe (bei denen automatische Systeme am Ende den Anrufer mit einer Person verbinden) mit vollautomatischen Systemen gleichbehandelt werden und somit der vorherigen Einwilligung bedürfen. In diesem Fall könnten nationale oder europäische „Robinsonlisten“ für (rein) persönliche Anrufe (ohne halbautomatische Anrufe) erwogen werden.

Wir unterstützen ferner Änderungsanträge, die Folgendes vorsehen: *„Die Verschleierung der Identität und die Verwendung falscher Identitäten, falscher Rücksendeadressen oder Rückrufnummern beim Versand unerbetener Kommunikation ist untersagt“*. Dieses Verbot sollte unabhängig vom Zweck der unerbetenen Kommunikation gelten (so kann z. B. ein Phishing-Versuch genauso ungesetzlich oder sogar ungesetzlicher sein als unerbetene Direktwerbung).

Schließlich würden wir, wie in der Stellungnahme bereits erläutert, auch Änderungsanträge begrüßen, die die Definition und den Anwendungsbereich von *„gewerblicher Direktwerbung“* erweitern und klarstellen sowie Schutz vor allen Formen *„unerbetener Kommunikation“* bieten.

Brüssel, den 5. Oktober 2017

[1] Folgende Dokumente finden in diesen Kommentaren Berücksichtigung: i) der Entwurf des Berichts (*„Berichtsentwurf“*) der von der EP-Abgeordneten Marju Lauristin für den LIBE-Ausschuss erarbeitet wurde; ii) die (Entwürfe der) Stellungnahmen der anderen drei beteiligten Ausschüsse des EP (IMCO, IURI und ITRE) und iii) die zusätzlichen Änderungsanträge 136 bis 827, die Mitglieder des LIBE-Ausschusses zum Berichtsentwurf vorgelegt haben. Alle relevanten Dokumente des EP können bei der

Legislativen Beobachtungsstelle des Europäischen Parlaments unter folgender Adresse abgerufen werden:
http://www.europarl.europa.eu/oeil/popups/ficheprocedure.do?reference=2017/0003(COD)&l=en
Der EDSB nimmt ferner die jüngsten Entwicklungen im Rat zur Kenntnis. Siehe z. B. Ratsdokument 11995/17 vom 8. September 2017.

[2] So wird beispielsweise in einigen Änderungsanträgen zu Artikel 19 vorgeschlagen, eine Liste von Themen aufzustellen, zu denen der Europäische Datenschutzausschuss Leitlinien herausgeben sollte. Eine allgemeine Erwähnung der Möglichkeit, solche Leitlinien herauszugeben, wie sie bereits im Vorschlag der Kommission zu finden ist, sollte hier genügen. Auch die Rechtsbehelfe in Artikel 21 könnten einfach auf die entsprechenden Artikel der Datenschutz-Grundverordnung verweisen und durch die Kategorien von Personen ergänzt werden, die Anspruch auf Rechtsbehelfe haben, wie z. B. Endnutzer.

[3] Siehe EDSB, Stellungnahme 06/2017; Artikel 29-Datenschutzgruppe, Stellungnahme 1/2017 und Berichte unabhängiger Wissenschaftler, wie die für den LIBE-Ausschuss angefertigte Studie, die 2017 von Borgesius und anderen verfasst wurde; abrufbar unter:
http://www.europarl.europa.eu/RegData/etudes/STUD/2017/583152/IPOL_STU(2017)583152_EN.pdf

[4] So z. B. bei den Definitionen für „elektronisches Kommunikationsnetz“, „elektronischer Kommunikationsdienst“, „interpersoneller Kommunikationsdienst“, „nummerngebundener interpersoneller Kommunikationsdienst“, „nummernunabhängiger interpersoneller Kommunikationsdienst“, „Endnutzer“ und „Anruf“.

[5] EDSB, *„Beurteilung der Erforderlichkeit von Maßnahmen, die das Grundrecht auf Schutz personenbezogener Daten einschränken: Ein Toolkit’,* II.4, und das kürzlich ergangene Gutachten des EuGH 1/15, Rn. 140, in dem die Erforderlichkeit des Eingriffs bekräftigt wird.

[6] Siehe ferner das jüngst ergangene Gutachten 1/15 des EuGH, Rn. 141, wo es heißt, dass eine die Rechte einschränkende Maßnahme klare und präzise Regeln für die Tragweite und die Anwendung der Maßnahme festlegen und Mindestanforderungen bezüglich der Umstände und Bedingungen aufstellen muss, unter denen eine Rechte einschränkende Maßnahme ergriffen werden darf.

[7] EuGH, Gutachten 1/15, Rn. 141 in Verbindung mit 177.