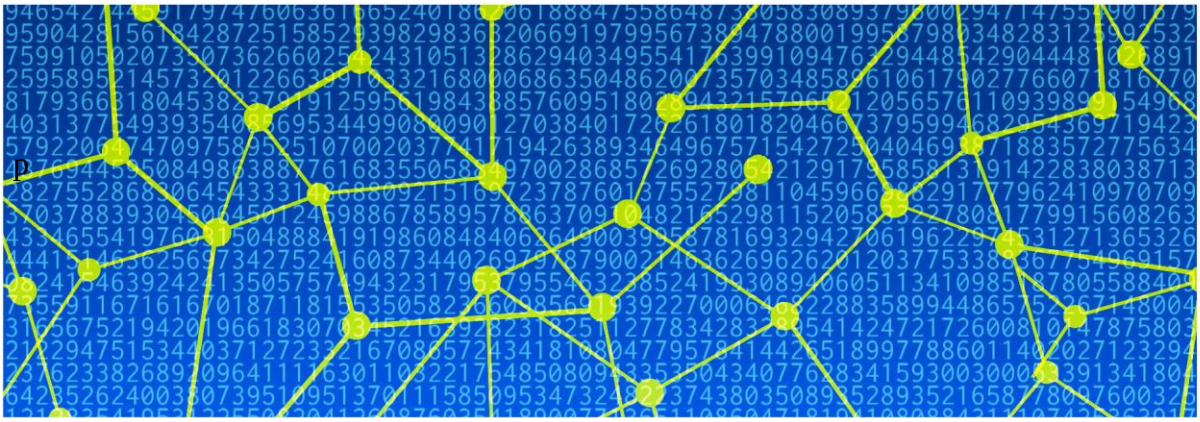

EUROPEAN DATA PROTECTION SUPERVISOR

Stellungnahme 5/2016

Vorläufige Stellungnahme des EDSB zur Überarbeitung der Datenschutzrichtlinie für elektronische Kommunikation (2002/58/EG)

EDPS

22. Juli 2016

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.

In dieser Stellungnahme geht es um den Auftrag des EDSB, die EU-Organe bezüglich der Datenschutzimplikationen ihrer Politiken zu beraten und eine verantwortliche Politikgestaltung zu fördern, im Einklang mit Maßnahme 9 der Strategie des EDSB: „Förderung einer verantwortungsvollen und fundierten politischen Entscheidungsfindung".

Zusammenfassung

In der vorliegenden Stellungnahme hat der EDSB auf Ersuchen der Europäischen Kommission seine Haltung zu den zentralen Fragen in Zusammenhang mit der Überarbeitung der Richtlinie 2002/58/EG über Privatsphäre und elektronische Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation)[1] dargelegt.

Wir brauchen einen neuen Rechtsrahmen für den Datenschutz in der elektronischen Kommunikation, doch muss er intelligenter, klarer und stärker sein: Wie brauchen mehr Klarheit, aber auch bessere Durchsetzung. Wir brauchen ihn, damit die Vertraulichkeit unserer Kommunikation gewahrt wird; dabei handelt es sich um ein in Artikel 7 der Charta der Grundrechte der Europäischen Union verankertes Grundrecht. Darüber hinaus brauchen wir Bestimmungen, die den mit der Datenschutzgrundverordnung (DSGVO) gewährten Schutz ergänzen und bei Bedarf näher spezifizieren. Außerdem müssen wir das bestehende höhere Schutzniveau in Fällen aufrechterhalten, in denen die Datenschutzrichtlinie für elektronische Kommunikation spezifischere Garantien als die DSGVO bietet. Die Begriffsbestimmungen der DSGVO, ihr räumlicher Anwendungsbereich, die Mechanismen für die Zusammenarbeit zwischen Durchsetzungsbehörden und für Kohärenz sowie die Möglichkeit, Flexibilität und Orientierung zu bieten, sollten auch für den Datenschutz in der elektronischen Kommunikation verfügbar sein.

Der Anwendungsbereich des neuen Rechtsrahmens muss ausgeweitet werden. Dabei muss technologischen und gesellschaftlichen Veränderungen Rechnung getragen und dafür gesorgt werden, dass die Menschen für alle funktional gleichwertigen Dienste den gleichen Schutz erhalten, unabhängig davon, ob diese beispielsweise von traditionellen Telefongesellschaften, Voice over IP-Diensten oder über Messaging-Apps auf dem Mobiltelefon angeboten werden. Eigentlich muss man sogar noch weiter gehen und nicht nur „funktional gleichwertige“ Dienste schützen, sondern auch die Dienste, die neue Kommunikationsmöglichkeiten eröffnen. Unabhängig von der Art des benutzten Netzes oder Kommunikationsdienstes sollten die neuen Vorschriften auch ganz unzweideutig weiterhin Maschine-zu-Maschine-Kommunikation im Zusammenhang mit dem Internet der Dinge abdecken. Mit den neuen Vorschriften sollte ferner gewährleistet sein, dass die Vertraulichkeit der Kommunikation der Nutzer in allen öffentlich zugänglichen Netzen geschützt wird, darunter in Wi-Fi-Diensten in Hotels, Coffee Shops, Läden und Flughäfen und in Netzen, die von Krankenhäusern ihren Patienten und von Universitäten ihren Studierenden angeboten werden, sowie an von öffentlichen Verwaltungen eingerichteten Hotspots.

Wie in der DSGVO verlangt, sollte eine Einwilligung echt sein und Nutzern die Möglichkeit geben, frei eine Entscheidung zu treffen. Es sollte nicht länger „Cookie Walls“ geben. Abgesehen von einer Reihe klarer Ausnahmen (wie First-Party-Analyse) sollte bei keiner Form der Kommunikation eine Rückverfolgung und Überwachung ohne eine ohne Zwang gegebene Einwilligung möglich sein, erteilt durch Cookies, virtuelle Fingerabdrücke oder andere technologische Mittel. Die Nutzer brauchen benutzerfreundliche und wirksame Mechanismen, um innerhalb des Browsers (oder einer anderen Software oder eines Betriebssystem) ihre Einwilligung geben und widerrufen zu können.

Damit die Vertraulichkeit elektronischer Kommunikation besser geschützt werden kann, muss auch das bestehende Erfordernis der Einwilligung bei Verkehrs- und Standortdaten erhalten und ausgebaut werden. Der Anwendungsbereich dieser Bestimmung sollte dahingehend

erweitert werden, dass sie für jedermann und nicht nur für traditionelle Telefongesellschaften und Anbieter von Internetdiensten gilt.

Die neuen Vorschriften sollten Nutzern zum Schutz ihrer elektronischen Kommunikation auch ganz eindeutig die End-zu-End-Verschlüsselung (ohne „Hintertürchen“) erlauben. Entschlüsselung, Reverse-Engineering oder Überwachung von durch Verschlüsselung geschützter Kommunikation sollte untersagt werden.

Schließlich sollten die neuen Vorschriften für den Datenschutz in der elektronischen Kommunikation Schutz vor unerbetenen Nachrichten bieten, und sie sollten aktualisiert und insofern verstärkt werden, als sie die vorherige Einwilligung der Empfänger aller Arten unerbetener elektronischer Kommunikation verlangen, unabhängig von deren Übertragungsmitteln.

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,

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:

I. EINLEITUNG UND HINTERGRUND

Diese vorläufige Stellungnahme („Stellungnahme“) ergeht aufgrund eines Ersuchens der Europäischen Kommission („Kommission“) an den Europäischen Datenschutzbeauftragten („EDSB“), als unabhängige Aufsichtsbehörde und als Berater eine Stellungnahme zur Überprüfung der Datenschutzrichtlinie für elektronische Kommunikation abzugeben.[2]

Die Konsultation des EDSB erfolgte zeitgleich mit einer von der Kommission durchgeführten Konsultation der Öffentlichkeit, die bis zum 5. Juli 2016 lief.[3] Die Kommission ersuchte ferner um die Stellungnahme der Artikel 29-Datenschutzgruppe (WP29), an der der EDSB als Vollmitglied mitarbeitete.[4]

In dieser Stellungnahme legt der EDSB seine vorläufige Haltung zur Überarbeitung der Datenschutzrichtlinie für elektronische Kommunikation dar und geht dabei im Wesentlichen auf die Fragen ein, um deren Behandlung ihn die Kommission ausdrücklich ersucht hat. Die Stellungnahme stellt darüber hinaus den Beitrag des EDSB zur öffentlichen Konsultation dar und befasst sich daher möglicherweise auch mit Aspekten, die die Kommission in ihrem Ersuchen um eine Stellungnahme nicht besonders erwähnt hat. Es ist denkbar, dass wir unseren Rat auch in späteren Phasen des Gesetzgebungsverfahrens erneut einbringen.

Die Überarbeitung der Datenschutzrichtlinie für elektronische Kommunikation gehört zu den zentralen Initiativen der Strategie für einen digitalen Binnenmarkt[5], mit der 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 der Überprüfung soll die Datenschutzrichtlinie für elektronische Kommunikation als Teil weiter reichender 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 kurze angenommene Datenschutz-Grundverordnung (DSGVO)[7] ersetzt werden wird. Die Datenschutzrichtlinie für elektronische Kommunikation enthält spezifische Vorschriften, mit denen im Wesentlichen die Vertraulichkeit und Sicherheit des elektronischen Kommunikationsverkehrs gewährleistet werden sollen. Darüber hinaus schützt sie die berechtigten Interessen von Teilnehmern, die juristische Personen sind.

II. BEDARF AN EINEM NEUEN RECHTSINSTRUMENT FÜR DEN DATENSCHUTZ IN DER ELEKTRONISCHEN KOMMUNIKATION

Der EDSB unterstützt die Initiative der Kommission zur Modernisierung, Aktualisierung und Stärkung der Bestimmungen der Datenschutzrichtlinie für elektronische Kommunikation. Wir schließen uns auch der von der WP29 in ihrer jüngsten Stellungnahme[8] geäußerten und von Gruppen der Zivilgesellschaft in einer neueren gemeinsamen Analyse[9] formulierten Auffassung an, dass noch immer Bedarf an spezifischen Vorschriften für den Schutz der Vertraulichkeit und Sicherheit elektronischer Kommunikation in der EU besteht, die die Anforderungen der DSGVO vervollständigen und näher ausführen. Ferner meinen wir, dass wir selektive und gezielte gesetzliche Bestimmungen benötigen, die einen starken, intelligenten und wirksamen Schutz bieten.

Die derzeitige Datenschutzrichtlinie für elektronische Kommunikation bietet Schutz in Bereichen, die nicht unter das Konzept der Verarbeitung personenbezogener Daten fallen, was die Voraussetzung für die Anwendbarkeit zentraler Datenschutzregelwerke wie der Richtlinie 95/46/EG oder der DSGVO ist. Sie enthält vielmehr präzise Vorschriften für spezifische Verarbeitungssituationen, bei denen es auf die potenziellen Auswirkungen der Verarbeitung ankommt. Ferner befasst sie sich mit Phänomenen, bei denen die Verarbeitung personenbezogener Daten nicht unbedingt das Hauptproblem für die betreffende Person ist, wie z. B. die Übermittlung unerbetener Nachrichten.

II.1 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 Datenschutzrichtlinie für elektronische Kommunikation ist das einzige Instrument im Sekundärrecht der EU, das Artikel 7 der Charta in vollem Umfang umsetzt.

Die Richtlinie geht aber über die Umsetzung von Artikel 7 und die Festlegung von Datenschutzbestimmungen für eine bestimmte Branche hinaus. Sie schützt auch die berechtigten Interessen juristischer Personen bezüglich der Vertraulichkeit der Kommunikation. In Anbetracht neuer Entwicklungen, darunter die ständig wachsende Menge elektronischer Kommunikation, die zunehmende Überwachung dieser Kommunikation durch öffentliche und private Stellen und neue technologische Entwicklungen wie Cloud Computing, Internet der Dinge und Big Data, kommt dem Schutz der Vertraulichkeit von Kommunikation eine immer größere Bedeutung zu.

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 eigene Zwecke zu nutzen, an Dritte weiterzugeben, den Inhalt zu ändern, die Lieferung zu unterbinden oder zu verzögern, könnte

das Geschäftsleben nur von Angesicht zu Angesicht ablaufen. Die Datenschutzrichtlinie für elektronische Kommunikation verpflichtet alle Anbieter elektronischer Kommunikation, vertrauenswürdige Boten zu sein, und sie erspart es natürlichen Personen und Organisationen, herauszufinden, auf wen sie sich bei Kommunikationsdiensten verlassen können und auf wen nicht. Dies gilt heute und sollte auch weiterhin für alle Kommunikation gelten, unabhängig von Sender, Empfänger und Inhalt. Der Inhalt einer Nachricht sollte in der Tat dem Anbieter des Kommunikationsdienstes in der Regel unbekannt bleiben.

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. Im derzeitigen Rechtsrahmen ist die Datenschutzrichtlinie für elektronische Kommunikation das Instrument des EU-Sekundärrechts, in dem die erforderlichen spezifischen rechtlichen Anforderungen (bezüglich der Beziehung zwischen der DSGVO und dem künftigen Instrument für den Datenschutz in der elektronischen Kommunikation, siehe weiter unten Anschnitt III.2) niedergelegt sind.

Die Anerkennung der Vertraulichkeit von Kommunikation als einem 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] und verfügen in der Regel auch über ein Gesetzeswerk, das diesen Bereich regelt. In Anbetracht der Existenz einzelstaatlicher Vorschriften tragen neue, stärker harmonisierte Vorschriften auf EU-Ebene 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 in mehreren Rechtsordnungen tätigen.

II.2 Das bestehende Schutzniveau sollte nicht gesenkt werden

Des Weiteren benötigen wir neue Bestimmungen für den Datenschutz in der elektronischen Kommunikation, um das bestehende höhere Schutzniveau für personenbezogene Daten in den Fällen zu erhalten, in denen die Datenschutzrichtlinie für elektronische Kommunikation spezifischere Garantien vorsieht als die DSGVO.

So ist beispielsweise in der DSGVO nicht konkret festgelegt, welche der möglichen Rechtsgrundlagen für die Verarbeitung in welchen Situationen zulässig ist, während sich die Datenschutzrichtlinie für elektronische Kommunikation zu einigen spezifischen Kontexten präziser äußert und die Einwilligung als Rechtsgrundlage verlangt. Als Beispiel sei Artikel 5 Absatz 3 der Datenschutzrichtlinie für elektronische Kommunikation genannt, dem zufolge für die Speicherung von Informationen oder den Zugriff auf Informationen, die im Endgerät gespeichert sind, eine Einwilligung erteilt werden muss (so genannte „Cookie-Vorschrift“). Ferner verlangt Artikel 6 Absatz 3 die Einwilligung für die Verwendung von Verkehrsdaten zu Vermarktungszwecken oder zur Bereitstellung von Diensten mit Zusatznutzen. Auch in Artikel 13 über unerbetene Nachrichten wird die vorherige Einwilligung als Rechtsgrundlage für bestimmte Arten der Kommunikation unter bestimmten Bedingungen verlangt.

Die Datenschutzrichtlinie für elektronische Kommunikation schützt ferner juristische Personen im Hinblick auf unerbetene Nachrichten sowie auf andere Aspekte in ihrer Eigenschaft als Teilnehmer an elektronischen Kommunikationsdiensten. Dieser Bedarf wird durch die DSGVO nicht abgedeckt.[12]

II.3 Präzise Vorschriften für bestimmte Gegebenheiten

Die Datenschutzrichtlinie für elektronische Kommunikation enthält Vorschriften für eine ganze Reihe von Situationen, in denen die Beantwortung der Frage, ob eine Verarbeitung personenbezogener Daten stattfindet, wer der für die Verarbeitung Verantwortliche oder Auftragsverarbeiter und wer die betroffene Person ist, außerordentlich schwierig ist. 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 Werbezwecke.

Grundsätzlich behandelt die Datenschutzrichtlinie für elektronische Kommunikation derartige Situationen, ohne eine Analyse nach den Bedingungen der DSGVO zu verlangen. Allerdings sind die Bestimmungen der Datenschutzrichtlinie für elektronische Kommunikation selber auch unterschiedlich ausgelegt worden. Das neue Instrument sollte daher als Chance begriffen werden, manche Begriffe oder Konzepte zu klären.

III. FRAGEN IM ZUSAMMENHANG MIT DER RECHTSGRUNDLAGE

III.1 Rechtsgrundlage für das neue Rechtsinstrument für den Datenschutz in der elektronischen Kommunikation

Der EDSB empfiehlt der Kommission, für das neue Rechtsinstrument für den Datenschutz in der elektronischen Kommunikation eine doppelte Rechtsgrundlage in Erwägung zu ziehen. Eine davon sollte Artikel 16 des Vertrags über die Arbeitsweise der Europäischen Union (AEUV) sein. Er ist auch die Rechtsgrundlage für die DSGVO. Als zweites sollte die derzeitige Rechtsgrundlage der Datenschutzrichtlinie für elektronische Kommunikation herangezogen werden, nämlich Artikel 114 AEUV über die Angleichung der Rechtsvorschriften (ex-Artikel 95 EGV).

Als einzige Rechtsgrundlage wäre Artikel 16 AEUV unzureichend, da die neuen Bestimmungen nicht nur einige Bestimmungen der DSGVO „näher ausführen“, sondern sie auch mit Bestimmungen „ergänzen“ werden, die sich nicht auf den Schutz personenbezogener Daten beschränken (siehe hierzu auch Abschnitt II zum *Bedarf an einem neuen Rechtsinstrument für den Datenschutz in der elektronischen Kommunikation* und Abschnitt III.2 zur *Beziehung zwischen der DSGVO und dem künftigen Instrument für den Datenschutz in der elektronischen Kommunikation*).

III.2 Beziehung zwischen der DSGVO und den neuen Bestimmungen über den Datenschutz in der elektronischen Kommunikation

Der EDSB empfiehlt, die Beziehungen zwischen der DSGVO und den neuen Bestimmungen über den Datenschutz in der elektronischen Kommunikation so komplementär zu halten, wie sie es derzeit sind. Die derzeitige Formulierung *„stellt eine Detaillierung und Ergänzung dar“* reicht für eine Definition dieser Beziehung völlig aus. Zur weiteren Klarstellung empfehlen wir, in einem Erwägungsgrund klar zum Ausdruck zu bringen, dass die neuen Bestimmungen über den Datenschutz in der elektronischen Kommunikation „unbeschadet“ der derzeitigen

Bestimmungen der DSGVO ergehen. Oder anders gesagt: Die neuen Bestimmungen über den Datenschutz in der elektronischen Kommunikation sollten keine weiteren Ausnahmen von den Vorschriften der DSGVO schaffen.

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 (siehe Abschnitt III.1). Schließlich ist der Kreis der geschützten Personen ein anderer, da die Datenschutzrichtlinie für elektronische Kommunikation Schutz auch juristischen Personen gewährt.

Es wäre zwar möglich gewesen, viele Bestimmungen der Datenschutzrichtlinie für elektronische Kommunikation in die DSGVO zu übernehmen, doch ist dies nicht gemacht worden. In Erwägungsgrund 173 und Artikel 95 wird eine Klarstellung der Beziehung zwischen den beiden Rechtsinstrumenten in dem neuen Rechtsakt für den Datenschutz in der elektronischen Kommunikation gefordert.

III.3 Verordnung oder Richtlinie?

Auch wenn sich die Ziele der Überprüfung möglicherweise auch mit einer Richtlinie erreichen lassen, empfiehlt der EDSB den Gesetzgebern doch, sich beim neuen Rechtsinstrument für eine Verordnung und nicht für eine Richtlinie zu entscheiden. Diese Lösung hätte folgende Vorteile:

- Sie passte besser zu dem in der DSGVO verfolgten Ansatz;
- sie würde für natürliche Personen und andere durch ihre Bestimmungen geschützte Einrichtungen ein kohärenteres und gleiches Schutzniveau gewährleisten;
- des Weiteren würde sie bei der Herstellung gleicher Wettbewerbsbedingungen für Organisationen helfen, die die Bestimmungen der Verordnung einzuhalten haben, und würde ihre Befolgungskosten senken;
- schließlich wäre eine Verordnung besser geeignet, das Verfahren der Zusammenarbeit und Kohärenz sowie andere von der DSGVO angebotene Verfahren für Zusammenarbeit und Kohärenz zu nutzen.

Es kann allerdings nicht ausgeschlossen werden, dass es mitunter erforderlich sein wird, den Mitgliedstaaten einen gewissen Spielraum zu gewähren. Dies lässt sich aber unabhängig von der Form des Rechtsakts bewerkstelligen.

Wir empfehlen, derartige Möglichkeiten für abweichende einzelstaatliche Rechtsvorschriften auf das erforderliche Mindestmaß zu beschränken. Schließlich empfehlen wir, in dem neuen Rechtsinstrument deutlich auf die Tatsache hinzuweisen, dass solche einzelstaatlichen Vorschriften, und hier insbesondere etwaige Ausnahmen (wie die gemäß dem derzeitigen Artikel 15), den Bestimmungen der Charta in vollem Umfang Rechnung tragen müssen.

Fiele die Entscheidung zugunsten einer Verordnung, wäre es auch einfacher, für den Datenschutz in der elektronischen Kommunikation den neuen, durch die DSGVO entstandenen Datenschutzrahmen mit seinem starken und wirksamen Instrumentarium (z. B. bei Begriffsbestimmungen, Festlegung des Anwendungsbereichs und Aufsichtsmechanismen) zu verwenden und auf diese Weise für Rechtssicherheit und Kohärenz zu sorgen. Die Begriffsbestimmungen der DSGVO, ihr räumlicher Anwendungsbereich, die Mechanismen für

die Zusammenarbeit zwischen Durchsetzungsbehörden und für Kohärenz sowie die Möglichkeit, Flexibilität und Orientierung zu bieten, sollten auch für den Datenschutz in der elektronischen Kommunikation verfügbar sein.

In seiner umfassendsten Form könnte dieses Ziel dadurch erreicht werden, dass selektiv so viele neue Bestimmungen wie möglich in die DSGVO integriert werden, sofern dies vorstellbar wäre, ohne den in diesem Fall von den Gesetzgebern gefundenen Interessenausgleich in Frage zu stellen. In diesem Fall könnten die neuen Bestimmungen für den Datenschutz in der elektronischen Kommunikation den für die Verarbeitung Verantwortlichen und natürlichen Personen einen vereinfachten und horizontalen Rahmen für den Schutz der Privatsphäre und den Datenschutz innerhalb ein- und derselben DSGVO bieten. Aber auch wenn diese Option nicht zur Verfügung stehen sollte, sollten die neuen Bestimmungen gewährleisten, dass der DSGVO-Rahmen in vollem Umfang auch für die neuen Bestimmungen für den Datenschutz in der elektronischen Kommunikation genutzt werden kann. Wir empfehlen der Kommission auf jeden Fall, die Option ihrer Abtrennung von den nicht mit Privatsphäre/Datenschutz in Zusammenhang stehenden Bestimmungen für elektronische Kommunikation zu erwägen.

Da die spezifische Rechtsgrundlage möglicherweise ein neues Rechtsinstrument verlangt, sollte das Instrument mit den neuen Bestimmungen für den Datenschutz in der elektronischen Kommunikation auf die DSGVO verweisen und sich insbesondere im Hinblick auf ihre Begriffsbestimmungen, den Anwendungsbereich mit Blick auf juristische Personen, andere als personenbezogene Daten (Metadaten, Sicherheit usw.) und alle die Durchsetzung unterstützenden Elemente anlehnen.

Wir empfehlen dem Gesetzgeber auf jeden Fall, sich selektiv nur auf anscheinend erforderliche Bestimmungen zu konzentrieren und dann von den Bestimmungen der DSGVO, die den Datenschutzbehörden erlauben, Leitlinien für einen flexiblen Umgang mit der Entwicklung neuer Technologien herauszugeben, mit Hilfe der Mechanismen zu profitieren, die die DSGVO dem EDSA eröffnet, beispielsweise zu Verhaltenskodizes und Zertifizierungen.

III.4 Beziehung zu dem Rahmen für elektronische Kommunikation

In ihren öffentlichen Dokumenten für die Konsultation gibt die Kommission keinen klaren Hinweis auf ihre Haltung bezüglich der künftigen Beziehung zwischen einem REFIT-Instrument für den Datenschutz in der elektronischen Kommunikation und dem Rechtsrahmen für elektronische Kommunikation. Derzeit gehört die Datenschutzrichtlinie für elektronische Kommunikation zu den in der Rahmenrichtlinie[13] genannten Einzelrichtlinien. Das bedeutet beispielsweise, dass Begriffsbestimmungen aus der Rahmenrichtlinie in der Datenschutzrichtlinie für elektronische Kommunikation verwendet werden und für den gesamten Rahmen auf einheitliche und kohärente Weise ausgelegt werden müssen, also für Datenschutz genauso wie für die Verwaltung von Funkfrequenzen und für wirtschaftliche Regulierung.

Die Entscheidung der Kommission, Verfahren bezüglich der Datenschutzrichtlinie für elektronische Kommunikation einzuleiten, ohne sie ganz offensichtlich in eine Überprüfung des Gesamtrahmens einzubeziehen, ist ein Hinweis darauf, dass die künftigen Bestimmungen über den Datenschutz in der elektronischen Kommunikation nicht länger Bestandteil des Rechtsrahmens für elektronische Kommunikation wären. Der EDSB würde eine solche Vorgehensweise begrüßen, weil dies dazu beitragen könnte, Probleme mit den derzeitigen Rechtsvorschriften zu überwinden. In einem solchen Szenario könnten insbesondere Anwendungsbereich und Begriffsbestimmungen je nach den spezifischen Zielen der künftigen Bestimmungen für den Datenschutz in der elektronischen Kommunikation festgelegt werden

und müssten sie nicht mehr mit den Erfordernissen der wirtschaftlichen Regulierung in Einklang gebracht werden. Außerdem wäre die potenzielle Überschneidung von Befugnissen der Datenschutzaufsichtsbehörden und anderer für die Beaufsichtigung und Durchsetzung im Bereich elektronischer Kommunikation zuständigen Behörden leichter in den Griff zu bekommen (siehe hierzu auch weiter unten Abschnitt VII zu *Aufsicht und Durchsetzung).*

IV. ANWENDUNGSBEREICH DES NEUEN RECHTSINSTRUMENTS FÜR DEN DATENSCHUTZ IN DER ELEKTRONISCHEN KOMMUNIKATION

Historisch betrachtet hat sich das Recht auf Vertraulichkeit von Kommunikation zunächst aus dem Recht auf Vertraulichkeit von per Post versandten oder erhaltenen Nachrichten entwickelt. Um technologischen Entwicklungen Rechnung zu tragen, wurde dieses Recht dann auf andere Kommunikationsmittel wie Fernschreiber und herkömmliche Telefonie ausgeweitet. In Anbetracht weiterer technologischer Entwicklungen, darunter das Aufkommen von Kommunikation über Anbieter so genannter Over-the-Top-Dienste (OTT)[14], ist es nun an der Zeit, den Schutz erneut zu erweitern.

Die Vorschriften müssen aktualisiert werden, damit sie auch neue Formen der Erbringung von Kommunikationsdienstleistungen abdecken. Würde lediglich das bestehende Schutzniveau aufrechterhalten, würden diese Rechte für einen ständig wachsenden Anteil an unserer Alltagskommunikation ihres Sinnes entleert.

Die Herausforderung liegt darin, dass zum einen gewährleistet sein muss, dass neue Bestimmungen technologisch ausreichend neutral formuliert sind, damit auch neue Dienste erfasst werden können, und dass zum anderen Rechtssicherheit und Vorhersehbarkeit gewährt werden müssen. Eine Ausdehnung des Anwendungsbereich muss ferner so erfolgen, dass für die Nutzer ein hohes Schutzniveau gewährleistet, gleichzeitig aber für die betroffenen Organisationen größere Chancengleichheit gegeben ist.

Schließlich müssen die neuen Bestimmungen für den Datenschutz in der elektronischen Kommunikation dafür sorgen, dass klar und eindeutig feststeht, welche Organisationen welche ihrer Anforderungen erfüllen müssen. Hier wäre ein Überdenken der Begriffsbestimmungen erforderlich. Die Begriffsbestimmungen in der derzeitigen Datenschutzrichtlinie für elektronische Kommunikation wurden für allgemeine Zwecke der wirtschaftlichen Regulierung im Telekom-Sektor erdacht und heben nicht spezifisch auf den Schutz der Privatsphäre ab. Die Bedeutung der Begriffe „öffentliche elektronische Kommunikationsnetze“ und „elektronische Kommunikationsdienste“ sind nicht hinreichend klar und entsprechen nicht mehr der technologischen Realität von heute. Diese Begriffsbestimmungen tragen der Tendenz zur Konvergenz nicht Rechnung, also dem Verschwimmen der Funktionen von Netzanbietern, Betreibern virtueller Netze und Anbietern von OTT-Kommunikationsdiensten wie Internet-Sprachdiensten und Chat-Anbietern. Hierdurch entsteht anhaltende Unsicherheit für Regulierer wie Unternehmen gleichermaßen.[15]

IV.1 Instant Messaging und Voice over IP

Aus Sicht des Nutzers besteht funktionale Äquivalenz zwischen Kommunikationsmitteln wie herkömmlicher Festnetz- oder Mobiltelefonie und Messaging-Diensten (SMS, MMS) auf der einen und OTT-Kommunikationsdiensten wie Voice over IP (VoIP[16]) und Instant Messaging-Apps auf der anderen Seite. Natürlichen Personen muss für alle funktional gleichwertigen Dienste das gleiche Schutzniveau geboten werden, unabhängig davon, ob diese Dienste über

traditionelle Telefongesellschaften, Voice over IP-Dienste oder Messaging-Apps für Mobiltelefone erbracht werden.

In Anbetracht all dessen könnte der Anwendungsbereich der Datenschutzrichtlinie für elektronische Kommunikation zumindest auf die Dienste ausgeweitet werden, die darauf angelegt sind, herkömmlichen elektronischen Kommunikationsdiensten für Audio-, Video- und Textmitteilungen funktional gleichwertige Dienste anzubieten (z. B. Voice over IP- und Instant Messaging-Anbieter wie Skype, Viber, FaceTime, WhatsApp, Signal, Threema, iMessage oder Facebook messenger).

Damit sich die neuen Bestimmungen für den Datenschutz in der elektronischen Kommunikation aber auch wirklich bewähren und einen technologisch neutralen Rahmen mit einem umfassenden Schutzniveau bieten können, muss noch ein Schritt weiter gegangen werden: Es geht nicht nur um den Schutz von Kommunikationsformen, die den Angeboten traditioneller Telekom-Dienstanbieter „funktional gleichwertig" sind, sondern auch von den Diensten, die neue Möglichkeiten für Kommunikation eröffnen, vielleicht als Zusatz zu anderen Angeboten.

Wir empfehlen der Kommission, sorgfältig die Frage zu prüfen, ob es erforderlich und möglich ist, eine noch breitere Palette von Diensten abzudecken. So sollte beispielsweise genau geprüft werden, ob in andere Dienste integrierte Kommunikationsfunktionen (z. B. Messaging-Funktionen in Spiele- oder Dating-Apps) in den Genuss des gleichen oder eines ähnlichen Schutzes kommen sollen. Für eine Ausweitung des Schutzes spricht die Tatsache, dass die Nutzer häufig ähnliche Erwartungen an die Privatheit und Vertraulichkeit dieser Nachrichten haben und dass jede Verletzung der Vertraulichkeit ebenso als Eingriff gesehen wird. Für Nutzer ist es möglich, ein Gespräch über die Messaging-Funktion eines Spiels zu beginnen, dann zu einem OTT-Instant-Messaging-Dienst zu wechseln, über das Mobiltelefon SMS auszutauschen und schließlich einen Anruf zwischen zwei Telefonen zu 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.

IV.2 Internet der Dinge

Die Datenschutzrichtlinie für elektronische Kommunikation gilt für Dienste *„in öffentlichen Kommunikationsnetzen ... einschließlich öffentlicher Kommunikationsnetze, die Datenerfassungs- und Identifzierungsgeräte unterstützen"* (Artikel 3). Mit dieser Bestimmung wird klargestellt, dass Zweck und Inhalt einer Kommunikation deren Schutz durch das Recht auf Achtung des Privatlebens nicht berühren dürfen. Sie gewährleistet, dass der Schutz der Privatheit von Kommunikation nicht davon abhängt, ob Menschen den Inhalt einer Kommunikation sprechen oder hören, schreiben oder lesen, sondern dass sie sich auf die zunehmend intelligenten Merkmale ihrer Endgeräte bei der Übermittlung von Inhalt in ihren Namen verlassen und in den Genuss des erwarteten Schutzniveaus kommen können. 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.

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": Im IdD sind Sport-Tracker, Gesundheitssensoren, persönliche Kommunikationsgeräte, intelligente Fernseher, die ihre

Nutzer beobachten, intelligente Autos, die jede Bewegung ihres Fahrers verfolgen, und viele andere Geräte zu finden. Sie sind mit Sensoren für Klang, Video, Bewegungen und physische Parameter ihrer Eigentümer ausgestattet. Die Tatsache, dass sie ihre Datenübermittlungen und Kommunikationsvorgänge 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.

Aus der Sicht eines Kommunikationsanbieters, der dem Instrument für den Datenschutz in der elektronischen Kommunikation 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, die Wahrung von Privatsphäre und Sicherheit sind dementsprechend für sämtliche Kommunikation zu gewährleisten.

Der EDSB empfiehlt im Hinblick auf die neuen Bestimmungen für den Datenschutz in der elektronischen Kommunikation, dass sie unabhängig von der Art des benutzten Netzes oder Kommunikationsdienstes auch weiterhin ganz eindeutig Maschine-zu-Maschine-Kommunikation im Zusammenhang mit dem Internet der Dinge abdecken. Es sollten Vertraulichkeit und Sicherheit jeglicher elektronischer Kommunikation (in beide Richtungen) mit einem IdD-Gerät (Endgerät) auf allen in den Anwendungsbereich fallenden Netzen und Diensten abgedeckt sein. Dies betrifft alle einschlägigen Bestimmungen, insbesondere aber Artikel 5 über die Pflicht zur Vertraulichkeit sowie die Artikel 6 und 9 über Verkehrs- und Standortdaten.

IV.3 Abdeckung von Netzen verschiedener Art

Die Datenschutzrichtlinie für elektronische Kommunikation bestimmt ihren Anwendungsbereich mit Hilfe von Begriffsbestimmungen aus der Rahmenrichtlinie.[17] Mit diesen Begriffsbestimmungen sollte einer Vielzahl von Zwecken Rechnung getragen werden, darunter Marktregulierung, Frequenzverwaltung, allgemeiner Zugang usw. In einem so komplexen Kontext können allgemeine Begriffsbestimmungen lediglich die Schnittfläche aller Anwendungsbereiche abdecken und können nicht auf die spezifischen Bedürfnisse des Schutzes der Privatsphäre zugeschnitten werden. Darüber hinaus wurden die in diesen Definitionen verwendeten Begrifflichkeiten häufig falsch verstanden. So gibt es beispielsweise noch immer Autoren, die den Begriff „öffentliche Netze“ als „im öffentlichen Besitz befindliche Netze“ deuten, da dieser Begriff mitunter in anderen Zusammenhängen verwendet wird.

Bei unabhängigen Bestimmungen für den Datenschutz in der elektronischen Kommunikation muss nicht länger dafür gesorgt werden, dass ihr Anwendungsbereich einem Instrument gleichwertig ist, das Marktregulierung ermöglicht. Wir empfehlen, in den neuen Bestimmungen für den Datenschutz in der elektronischen Kommunikation ebenfalls sicherzustellen, dass - grundsätzlich - Nutzer in allen Netzen, zu denen sie Zugang haben, den gleichen Schutz genießen. Wir empfehlen eine Erweiterung dahingehend, dass zumindest alle öffentlich zugänglichen Netze und Dienste (einschließlich der ohne jedes kommerzielles Interesse bereitgestellten) in den Geltungsbereich der Anforderungen an die Vertraulichkeit fallen. Dazu würden 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.

Der EDSB empfiehlt weiter, im neuen Rechtsinstrument für den Datenschutz in der elektronischen Kommunikation ebenfalls abzuklären, was unter „öffentlich zugänglich" zu verstehen ist. So sollte beispielsweise deutlich gemacht werden, dass ein Dienst auch dann noch als öffentlich zugänglich gilt, wenn der Anbieter den Dienst nur registrierten Nutzern bereitstellt, wie dies der Fall ist bei einer Organisation, die ihren Kunden und Besuchern Wi-Fi-Zugang anbietet.

Diese Anmerkungen knüpfen an frühere Kommentare des EDSB zu diesem Thema 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[18] 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[19], 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).

V. SCHUTZ DER VERTRAULICHKEIT DER KOMMUNIKATION

Der Schutz der Vertraulichkeit der Kommunikation (Artikel 5) muss zentrales Ziel des neuen Rechtsinstruments für den Datenschutz in der elektronischen Kommunikation bleiben. Der EDSB unterstreicht erneut die große Bedeutung des Rechts auf Vertraulichkeit der Kommunikation, in Umsetzung von Artikel 7 der Charta. Des Weiteren betonen wir, dass dem Schutz von Kommunikation sowohl im Transit als auch im Ruhezustand große Bedeutung zukommt. Ferner weisen wir nachdrücklich darauf hin, dass neue technische Paradigmen (z. B. Cloud Computing) der Vertraulichkeit noch größere Bedeutung beimessen.[20]

Ferner möchten wir betonen, dass die Unterscheidung zwischen Inhalt und „Verkehrsdaten" 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 Verkehrsdaten gehört.[21]

Die Verarbeitung von Daten über die Kommunikation (wie URL der aufgerufenen Websites, E-Mail-Kopfzeilen, Verkehrs- und Standortdaten) ist häufig mindestens so aufschlussreich wie der eigentliche Inhalt der Kommunikation (oder sogar noch aufschlussreicher).

Dies lässt sich mit zahlreichen Beispielen belegen. Metadaten lassen beispielsweise die Identifizierung von Zielen von militärischen Drohneneinsätzen zu.[22] Metadaten helfen auch bei der Identifizierung von Strukturen bei politischen Anschlägen und strafrechtlichen Untersuchungen.[23] Untersuchungen haben gezeigt, dass natürliche Personen schon mit sehr wenigen Standortdaten ihres Mobiltelefons identifiziert werden können.[24] 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, Gewohnheiten in der Religionsausübung und sogar eheliche Untreue mit Hilfe von Verkehrsdaten eines Mobiltelefons entdecken lassen.[25]

Das neue Rechtsinstrument für den Datenschutz in der elektronischen Kommunikation muss daher ganz klar den Schutz der Vertraulichkeit von Kommunikation im Hinblick sowohl auf „Inhalt" als auch auf „Metadaten" (einschließlich Verkehrs- und Standortdaten) gewährleisten.

V.1 Artikel 5 Absatz 1: Schutz von Kommunikation im Transit

Der EDSB empfiehlt, es in dem neuen Rechtsinstrument für den Datenschutz in der elektronischen Kommunikation weiterhin bei dem generellen Verbot des Abfangens/Überwachens von Nachrichten zu belassen und dieses Verbot ganz klar sowohl auf Inhalte als auch auf „Metadaten" (einschließlich Verkehrsdaten) zu beziehen. Des Weiteren empfehlen wir die Ausdehnung dieses Verbots in der oben angeregten Weise.

Im Sinne der Rechtssicherheit empfiehlt der EDSB, in den neuen Bestimmungen für den Datenschutz in der elektronischen Kommunikation die bestehenden Definitionen der Begriffe „Nachricht", „Verkehrsdaten" und „Standortdaten" klarzustellen. Dies sollte im verfügenden Teil des Rechtsinstruments für den Datenschutz in der elektronischen Kommunikation geschehen und durch eine Auflistung von Beispielen für jede Begriffsbestimmung in Erwägungsgründen ergänzt werden. In den Bestimmungen sollte beispielsweise genau festgelegt werden, ob eine vollständige URL (die Auskunft über die aufgerufene Website gibt) zum Inhalt oder zu den Verkehrsdaten gezählt wird. Es sollte dort ferner noch klarer zum Ausdruck gebracht werden, dass der Begriff Kommunikation nicht nur elektronische Kommunikation zwischen zwei natürlichen Personen umfasst, sondern jegliche Kommunikation innerhalb einer bestimmten Gruppe (z. B. eine Telefonkonferenz oder Nachrichten, die an eine festgelegte Gruppe von Empfängern gesandt werden).

Der EDSB empfiehlt mit Blick auf die künftigen Bestimmungen ferner, dort genau festzulegen, dass Abfangen und Überwachen technologisch breitestmöglich auszulegen sind und beispielsweise auch die Hinzufügung von eindeutigen Kennungen zur Nachricht wie beispielsweise Advertising Identifiers, Audio-Beacons oder Super-Cookies umfassen.

V.2 Artikel 5 Absatz 3: Schutz der Endgeräte

Der EDSB empfiehlt, das Erfordernis der Einwilligung im derzeitigen Artikel 5 Absatz 3 beizubehalten und zu verstärken. Er erinnert daran, dass Einwilligung im Sinne von Artikel 5 Absatz 3 auf die gleiche Weise definiert und ausgelegt werden muss wie nach der DSGVO.

Artikel 5 Absatz 3 schützt die Integrität der Geräte des Nutzers gegen alle Arten unzulässiger Eingriffe und Angriffe. Es handelt sich hierbei um eine der spezifischsten Cybersicherheitsvorschriften im EU-Recht. Ist das Endgerät des Nutzers nicht gegen Eingriffe geschützt, wird der Inhalt der Nachricht nur im Netz geschützt, könnte aber durch böswillige Interaktion mit dem Endgerät des Nutzers vor dem Versenden oder nach der Ankunft an ihren

Bestimmungsort abgefangen, verändert oder gelöscht werden: Übermittelte Texte oder Daten könnten auf dem Mobilgerät gelesen oder geändert werden, Passwörter und PIN könnten von den Geräten der Nutzer gestohlen werden, eingebaute Kameras und Mikrophone könnten zum Ausspionieren verwendet werden. Artikel 5 Absatz 3 bietet rechtlichen Schutz gegen derartige Manipulationen und derartigen Missbrauch, und in Zukunft wird ein mindestens gleichwertiges Schutzniveau erforderlich sein, da die Geräte der Nutzer immer mehr wichtige Daten und kritische Zugangsdaten enthalten. In diesem Zusammenhang verweist der EDSB auf seine Stellungnahme 8/2015 vom 15. Dezember 2015 zur Verbreitung und Verwendung von eingreifenden Überwachungstechnologien, in der es heißt, dass *„der effektive Schutz der IKT-Systeme vor jeglichen Angriffen oder illegalen Abhörmaßnahmen für den Schutz der Grundrechte auf Privatsphäre und Datenschutz natürlicher Personen in der EU unbedingt erforderlich"* ist.

Gleichzeitig sollten die Nutzer echte Kontrolle über die Verwendung von Cookies und ähnlichen Tools erhalten. Dazu gehört insbesondere die Wahl des Geräts und seiner Merkmale, seine Verstärkung mit weiteren Komponenten und der Software und die Konfiguration der Merkmale, die den Betrieb des Geräts betreffen. In Erwägungsgrund 66 der Richtlinie 2009/136/EG[26] (Richtlinie über Nutzerrechte) wird bereits das Recht des Nutzers auf Kontrolle des Datenschutzverhaltens seines Geräts durch technische Merkmale anerkannt. In einem Umfeld, in dem sich Angriffe und das Ausnutzen von Sicherheitslücken in der Software zu einer echten Industrie entwickelt haben, ist es nicht hinnehmbar, dass die Rechte von Nutzern auf Wahl technischer Merkmale eingeschränkt werden, mit denen sie ihr Gerät gegen Eingriffe durch Dritte schützen können. Dazu muss auch das Recht gehören, zu entscheiden, welche Elemente von Inhalten von Dritten übernommen und welche blockiert werden, beispielsweise Scripts, die eine Interaktion zwischen dem Gerät des Nutzers und Ad-Exchanges oder ähnlichen Servern in Gang setzen.

Die Einwilligung muss ohne jeden Zweifel gegeben werden

Der EDSB empfiehlt zwar, das derzeitige Erfordernis der Einwilligung beizubehalten, doch räumt er auch ein, dass Artikel 5 Absatz 3, wie jetzt angewandt, sein Potenzial nicht voll ausgeschöpft hat, eine echte Wahlmöglichkeit zu bieten und natürlichen Personen die Kontrolle zurückzugeben. 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 in der Frage lassen, was mit ihren Daten geschieht.
Dieses Phänomen wird mitunter als Problem der „Cookie-Walls" bezeichnet. Cookie-Walls bedeuten, dass Nutzer, die Cookies nicht akzeptieren, keinen Zugang zu den Websites erhalten, zu denen sie eigentlich Zugang wünschen.[27] Viele dieser Cookies verfolgen die Nutzer, wenn sie ihre Spur im Internet hinterlassen, und Unternehmen haben auf sie 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.

Cookie-Walls untergraben die Idee, dass eine Einwilligung ohne jeden Zwang gegeben werden muss; dies ist jedoch ein zentrales Erfordernis sowohl der Richtlinie 94/46/EG als auch der DSGVO. Eine Verbesserung gegenüber der Richtlinie 95/46/EG weist die DSGVO allerdings

auf, denn sie verlangt nicht nur ganz eindeutig, dass die Einwilligung ohne jeden Zwang gegeben werden muss, sondern erläutert auch, was darunter zu verstehen ist. So sieht sie unter anderem vor, dass eine Einwilligung nicht als freiwillig erteilt gilt, wenn die Erbringung einer Dienstleistung von der Einwilligung der natürlichen Person in die Verarbeitung ihrer personenbezogenen Daten abhängig ist, obwohl die Verarbeitung personenbezogener Daten für die Erbringung dieser Dienstleistung nicht erforderlich ist.[28] Genau dies trifft auf Cookie-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.

In Anbetracht der Bedeutung einer freiwillig erteilten Einwilligung und der häufig unzureichenden Umsetzung von Artikel 5 Absatz 3 durch Betreiber von Websites empfiehlt der EDSB den Gesetzgebern, ein vollständiges oder zumindest teilweises Verbot so genannter „Cookie-Walls“ in Erwägung zu ziehen.

Für den Fall eines vollständigen Verbots von Cookie-Walls sollten die neuen Bestimmungen für den Datenschutz in der elektronischen Kommunikation besagen, dass niemandem der Zugang zu irgendwelchen (entgeltlichen oder unentgeltlichen) Diensten der Informationsgesellschaft verweigert werden darf, nur weil er nicht seine Einwilligung gemäß Artikel 5 Absatz 3 erteilt hat. Diese Vorgehensweise böte natürlichen Personen das höchste Schutzniveau, aber auch Rechtssicherheit und gleiche Wettbewerbsbedingungen für alle Marktteilnehmer.

Im anderen Fall, also bei einem teilweisen Verbot, könnten die Gesetzgeber ihr Augenmerk darauf richten, zumindest gegen die eklatantesten Situationen vorzugehen, in denen die Auswirkungen auf die Nutzer am größten sind oder in denen sie die geringste Wahlfreiheit haben. In diesem Fall könnte das neue Rechtsinstrument für den Datenschutz in der elektronischen Kommunikation eine nicht erschöpfende Liste von Situationen enthalten, in denen eine Einwilligung als nicht freiwillig erteilt gilt. Gleichzeitig könnte das neue Rechtsinstrument für den Datenschutz in der elektronischen Kommunikation dem Europäischen Datenschutzausschuss (EDSA) erlauben, weitere Leitlinien herauszugeben und weitere Situationen zu beschreiben, in denen Cookie-Walls verboten sind. Diese Vorgehensweise bietet den Vorteil der Flexibilität, gewährt allerdings möglicherweise natürlichen Personen ein niedrigeres Schutzniveau, weniger Rechtssicherheit und weniger Chancengleichheit.

Bei einem Teilverbot empfiehlt der EDSB, zumindest die folgenden Situationen in die in den neuen Bestimmungen über den Datenschutz in der elektronischen Kommunikation vorgesehene nicht erschöpfende Liste aufzunehmen:

- Situationen, in denen der Anbieter des Dienstes im Hinblick auf den vom Nutzer gesuchten Dienst eine marktbeherrschende Stellung innehat;
- alle anderen Situationen, in denen ein Machtungleichgewicht zwischen Nutzer und Dienstanbieter besteht (die Einzelheiten wären ggf. vom EDSA auszuarbeiten);
- Nachrichten und Dienste, die ganz oder teilweise aus Steuergeldern finanziert werden (z. B. Websites, die elektronische Behördendienste anbieten; neue Medien, die von der Regierung subventioniert werden, oder zwangsweise erhobene Lizenzgebühren);
- alle Situationen, in denen von den erhobenen Daten an sich oder in Kombination mit anderen Daten (z. B. Besuche auf neuen Websites oder Websites mit Gesundheitsinformationen, Online-Buchläden, Verwendung von Fitness-Apps;

Verfolgung von Standortdaten in einem Gotteshaus oder einem Krankenhaus) besondere Datenkategorien abgeleitet werden können;
- Situationen, in denen eine Website oder App ihren Werberaum versteigert und unbekannte Dritte möglicherweise Nutzer über die Website oder App verfolgen und überwachen können;
- gebündelte Einwilligung für mehrere Zwecke (wenn z. B. die Einwilligung für Vermarktungszwecke und für Dienste mit Zusatznutzen nicht getrennt erteilt/verweigert werden kann).

Für den Fall eines Teilverbots empfiehlt der EDSB, in den neuen Bestimmungen für den Datenschutz in der elektronischen Kommunikation vorzusehen, dass unabhängig von der Marktmacht des Dienstanbieters dieser entweder i) den Nutzer wählen lassen muss, ob er in eine Verarbeitung von Daten einwilligt oder nicht, die für die Erbringung des Dienstes nicht erforderlich sind, und dies, ohne dadurch Nachteile zu erleiden, oder ii) zumindest zu einem vernünftigen Preis (ohne verhaltensorientierte Werbung und Datenerhebung) einen Zahldienst als Alternative zu den mit den persönlichen Daten der Nutzer bezahlten Diensten bereitstellen muss. Diese Möglichkeit war auch von der Kommission in ihrer öffentlichen Konsultation erwähnt worden.[29]

Möglichkeiten für Erteilung und Widerruf der Einwilligung

Schließlich weist der EDSB nachdrücklich darauf hin, dass Nutzer benutzerfreundliche und wirksame Mechanismen für die Erteilung bzw. den Widerruf ihrer Einwilligung benötigen. In Anlehnung an Erwägungsgrund 66 der bereits erwähnten Richtlinie über Nutzerrechte empfiehlt der EDSB, in den neuen Bestimmungen über den Datenschutz in der elektronischen Kommunikation eine praxisnahe rechtliche Anforderung dahingehend vorzusehen, dass die Einwilligung des Nutzers in die Verarbeitung durch Verwendung entsprechender Einstellungen eines Browsers oder einer anderen Anwendung zum Ausdruck gebracht werden könnte.

Das bedeutet, dass das neue Instrument für den Datenschutz in der elektronischen Kommunikation sich nicht mehr allein auf den Betreiber einer Website verlässt, um die Einwilligung im Namen Dritter (wie Werbungs- und soziale Netze) einzuholen, sondern verlangen kann, dass Browser und andere Software oder Betriebssysteme innerhalb des Browsers (oder einer anderen Software oder eines Betriebssystems) Kontroll-Tools wie Do Not Track (DNT) oder andere technische Vorkehrungen vorsehen, die es Nutzern einfach machen, ihre Einwilligung zu erteilen oder zu verweigern.

Solche Tools müssen dem Nutzer bei der Inbetriebnahme mit datenschutzfreundlichen Voreinstellungen angeboten werden.

Die Einhaltung akzeptierter technischer und politischer Compliance-Normen durch alle Beteiligten, darunter die Betreiber der Website, sollte verbindlich werden.

Bedarf an einem technologisch neutralen und inklusiveren Wortlaut

Der derzeitige Wortlaut von Artikel 5 Absatz 3: die *„Speicherung von Informationen“* oder der *„Zugriff auf Informationen, die bereits“* im Endgerät von Nutzern *„gespeichert sind“*, hat einen gewissen Spielraum für abweichende Interpretationen in der Frage gelassen, welche Arten der Interaktion eines Dritten mit dem Endgerät des Nutzers gemeint sind, und dies vor allem im

Hinblick auf die Bedeutung von *„Zugriff auf Informationen, die bereits gespeichert sind"*. Es ist zwar klar, dass jeder unerlaubte Eingriff in das Gerät abgedeckt sein sollte, doch gibt es auch weniger eindeutige Fälle. Sollte man bei der Erhebung und Verwendung von Daten, die das Gerät des Nutzers standardmäßig als Teil des Standardkommunikationsverhaltens bereitstellt, von einem Zugriff auf bereits gespeicherte Informationen sprechen? Sollte für den Fall, dass die Daten nicht standardmäßig bereitgestellt werden, ein Informationsersuchen, das von dem zwischen Endgerät und Drittem verwendeten Kommunikationsprotokoll unterstützt wird, als Zugriff gewertet werden? Sollten Informationen, die erst als Reaktion auf Ersuchen eines Dritten erstellt werden (z. B. Akku-Stand, gemessen als Reaktion auf das Ersuchen) als bereits gespeicherte Information betrachtet werden? Wie steht es um Informationen, die mit dem Endgerät des Nutzers verbunden und über dieses Gerät zugänglich sind, jedoch dort nicht physisch gespeichert sind und auf ein Ersuchen des Dritten hin von einem Cloud-Dienst heruntergeladen werden?

In Anbetracht der vorstehend aufgeführten Beispiele ist der EDSB der Auffassung, dass die technische Umsetzung nicht das Kriterium sein sollte, das über das Schutzniveau für den Nutzer entscheidet, zumal in einigen Fällen möglicherweise weder der Nutzer noch der um Informationen ersuchende Dritte die genauen technischen Umstände eines Informationsersuchens kennt. Daher sollte das Instrument so technisch neutral und so inklusiv wie möglich formuliert sein. So sollte beispielsweise gewährleistet sein, dass alle derzeitigen und künftigen über Smartphones und IdD-Anwendungen genutzten Tracking-Techniken abgedeckt sind. 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 Internet 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.

Ausnahme für First-Party-Analysecookies

Das neue Rechtsinstrument für den Datenschutz in der elektronischen Kommunikation sollte einerseits den Geltungsbereich des Erfordernisse der Einwilligung klarstellen, andererseits aber auch eine weitere Ausnahme für „First-Party-Analysecookies" vorsehen, für die angemessene Garantien bestehen müssen.[30] 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 empfiehlt, 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-Adresssen. Die Artikel 29-Datenschutzgruppe hat in ihrer Stellungnahme 04/2012 zur Ausnahme von Cookies von der Einwilligungspflicht[31] 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, darf das neue Rechtsinstrument für den Datenschutz in der elektronischen Kommunikation gerne auf künftige Leitlinien des EDSB verweisen.

V.3 Verkehrsdaten und Standortdaten

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.

Diese Daten werden nicht länger nur von herkömmlichen Telefon- und Internetdienstanbietern erhoben. Eine ganze Reihe neuer Dienstanbieter kann sich ebenfalls einen sehr detaillierten Überblick über die Reise- und Kommunikationsmuster eines Nutzers, seine Aktivitäten in sozialen Netzwerken und anderes verschaffen. Gleichzeitig unterliegen diese Dienstanbieter derzeit nicht den sich aus der Datenschutzrichtlinie für elektronische Kommunikation ergebenden Pflichten.

Die derzeitige Datenschutzrichtlinie für elektronische Kommunikation verlangt für die Verarbeitung von Verkehrs- und Standortdaten eine Einwilligung und bietet damit ein höheres Schutzniveau als die DSGVO. Zumindest potenziell lässt die DSGVO andere Rechtsgrundlagen zu, wie berechtigte Interessen oder die Erfüllung eines Vertrags. Ein für die Verarbeitung Verantwortlicher könnte nun beispielsweise argumentieren, das Tracking von Nutzern im Internet und die Erstellung detaillierter Profile für sie wäre Teil seines berechtigten Interesses, seine Dienstleistungen und Produkte zu vermarkten.

Im Sinne eines besseren Schutzes der Vertraulichkeit elektronischer Kommunikation empfiehlt der EDSB, in der Datenschutzrichtlinie für elektronische Kommunikation das bestehende Erfordernis der Einwilligung für Verkehrs- und Standortdaten beizubehalten und auszubauen. Insbesondere empfiehlt er, bei der Überarbeitung der Datenschutzrichtlinie für elektronische Kommunikation die Verpflichtung zur Einholung einer einzigen Einwilligung für die Verarbeitung von Metadaten aufzunehmen. Sie soll für alle Verkehrs- und Standortdaten unabhängig davon gelten, wer solche Daten erhebt und verarbeitet. Mit anderen Worten: Der Anwendungsbereich dieser Bestimmung sollte ähnlich wie bei Artikel 5 Absatz 3 dahingehend erweitert werden, dass sie für jedermann und nicht nur für traditionelle Telefongesellschaften und Anbieter von Internetdiensten gilt.

VI. SCHUTZ DER SICHERHEIT DER KOMMUNIKATION

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.

Die Sicherheitsanforderungen in der DSGVO gelten nur für Fälle, in denen es um personenbezogene Daten geht. Es muss jedoch gewährleistet sein, dass auch andere Daten, z. B. vertrauliche Geschäftsinformationen, die nicht immer zwangsläufig auch personenbezogene Daten enthalten, nach wie vor geschützt sind. Andere Rechtsinstrumente, wie die so genannte NIS-Richtlinie[32], decken ebenfalls nur bestimmte Situationen ab.

Es besteht daher nach wie vor Bedarf an spezifischen Bestimmungen über Sicherheit auch im neuen Rechtsrahmen für den Datenschutz in der elektronischen Kommunikation.[33]

Ferner sollte keinerlei Zweifel bezüglich des Geltungsbereichs aller Verpflichtungen zum Schutz der Sicherheit von Kommunikation bestehen: Die neuen Bestimmungen über den Datenschutz in der elektronischen Kommunikation sollten ganz klar (und zwar im verfügenden Teil, nicht nur in einem Erwägungsgrund) nicht nur die Vertraulichkeit und Sicherheit von Kommunikation im Transit vorsehen, sondern auch die Vertraulichkeit und Sicherheit der Geräte der Endnutzer schützen. Der EDSB empfiehlt, Artikel 4 der Datenschutzrichtlinie für elektronische Kommunikation dergestalt zu ändern, dass er klar beide Situationen abdeckt. Die neuen Bestimmungen über den Datenschutz in der elektronischen Kommunikation sollten ferner sicherstellen, dass Artikel 5 Absatz 3 oder eine ähnliche Bestimmung auch in Zukunft die Geräte der Endnutzer vor Spyware schützt.

VI.1 Bedarf an zusätzlichen Sicherheitsmaßnahmen in den neuen Bestimmungen über den Datenschutz in der elektronischen Kommunikation

Nach Auffassung des EDSB wären ferner die folgenden, in der öffentlichen Konsultation der Kommission[34] erwähnten zusätzlichen Sicherheitsmaßnahmen erforderlich:

- 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.

Standards können Sicherheitsanforderungen so ausdehnen, dass Netzanbieter, Anbieter von Netzkomponenten, in Verbindung mit der Bereitstellung elektronischer Kommunikationsdienste verwendete Endgeräte (einschließlich IdD) oder ergänzende Ausrüstung (einschließlich Software) abgedeckt sind.

VI.2 Verschlüsselung

Wie auch die WP29 ausgeführt hat, *„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".[35]

Der EDSB empfiehlt: Die neuen Vorschriften für den Datenschutz in der elektronischen Kommunikation sollten Nutzern zum Schutz ihrer elektronischen Kommunikation auch ganz eindeutig die End-zu-End-Verschlüsselung (ohne „Hintertürchen"[36]) 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 dem neuen Rechtsinstrument für den Datenschutz in der elektronischen Kommunikation Anbietern von Verschlüsselung, Anbietern von Kommunikationsdiensten und allen anderen Organisationen (auf allen Stufen der Lieferkette) zu untersagen, „Hintertürchen" zuzulassen oder zu fördern.

VI.3 Verletzungen des Datenschutzes

Der EDSB empfiehlt die Streichung von Artikel 4 Absätze 3 und 4 der Datenschutzrichtlinie für elektronische Kommunikation über Verletzungen des Datenschutzes, da die DSGVO bereits von allen Verantwortlichen verlangt, Teilnehmern und zuständigen nationalen Behörden Verletzungen des Schutzes personenbezogener Daten (vorbehaltlich einiger Ausnahmen) zu melden. Zur Vermeidung von Doppelmeldungen empfehlen wir, dass alle Verletzungen des Schutzes personenbezogener Daten den in der DSGVO vorgesehenen Aufsichtsbehörden gemäß den Bestimmungen dieser Verordnung gemeldet werden sollten.

VII. AUFSICHT UND DURCHSETZUNG

Gemäß der derzeitigen Datenschutzrichtlinie für elektronische Kommunikation gibt es eine ganze Reihe unterschiedlicher Behörden, die für die Aufsicht und die Durchsetzung der Bestimmungen der Richtlinie zuständig sind. Die Erfahrungen haben gezeigt, dass es innerhalb Europas hier große Unterschiede gibt und dass sich die Rollen der verschiedenen Aufsichtsbehörden auch überschneiden oder mehrfach wahrgenommen werden.[37] Der bestehende Rahmen sollte daher vereinfacht werden.

Es ist ferner zu bedenken, dass die DSGVO neue Verpflichtungen für die Aufsichtsbehörden schafft, wie Zusammenarbeit zwischen zuständigen nationalen Behörden, Kohärenzverfahren und Rolle des EDSA. Sollte die Aufsicht über das neue Rechtsinstrument für den Datenschutz in der elektronischen Kommunikation (oder einen Teil davon) durch eine Behörde erfolgen, die keine Datenschutzbehörde ist, muss für diese Behörde eine wirksame Regelung geschaffen werden, damit sie in den Kooperationsmechanismen der Datenschutzbehörden vertreten ist. Dies könnte die ohnehin bereits komplizierten Kooperationsregelungen weiter verkomplizieren.

In Anbetracht dieser Überlegungen empfehlen wir in allen Fällen, in denen eine Aufgabe wirksam von einer nationalen Datenschutzbehörde wahrgenommen werden kann, im Sinne der

Rechtssicherheit und der einfachen praktischen Umsetzung, die nationalen Datenschutzbehörden als die zuständigen Behörden zu betrachten.

VIII. UNERBETENE NACHRICHTEN

Der EDSB empfiehlt, bei der Überarbeitung die derzeitigen Vorschriften in der Datenschutzrichtlinie für elektronische Kommunikation für den Schutz vor unerbetenen Nachrichten zu erhalten, zu aktualisieren und auszubauen. 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 eine Reihe automatischer Screening-Fragen eingesetzt. Der Chat-Bot kann dann mit Hilfe der Antworten die angerufene Person an einen Live-Operator weiterverweisen.

Daher empfiehlt der EDSB, in den neuen Bestimmungen über den Datenschutz in der elektronischen Kommunikation einen technologisch neutralen Ansatz zu verfolgen. Artikel 13 sollte die vorherige Einwilligung von Empfängern aller Arten unerbetener elektronischer Nachrichten verlangen, und zwar unabhängig von den Übertragungsmitteln (z. B. E-Mail, Sprach- oder Videoanrufe, Fax, Text, aber auch Direct Messaging (also innerhalb eines Dienstes der Informationsgesellschaft) und verhaltensorientierte Werbung). Das Schutzniveau sollte ferner gleichwertig sein, unabhängig davon, ob der Nutzer/Teilnehmer eine natürliche oder eine juristische Person ist.

Aktuelle Ausnahmen bezüglich bestehender Beziehungen und ähnlicher Produkte und Dienstleistungen sollten erhalten bleiben, doch empfehlen wir, in den neuen Bestimmungen über den Datenschutz in der elektronischen Kommunikation klarzustellen, was unter bestehenden Beziehungen und ähnlichen Produkten und Dienstleistungen zu verstehen ist.

In der derzeitigen Datenschutzrichtlinie für elektronische Kommunikation steht die „kommerzielle“ Kommunikation im Mittelpunkt. Allerdings können nicht aller Spam und alle böswilligen Nachrichten als kommerziell im üblichen Sinn gelten. Genau genommen können Nachrichten im Zusammenhang mit versuchten Straftaten, z. B. Phishing-Angriffe und betrügerische Finanzvorschläge, nicht immer unter diese Qualifikation fallen. Dem Gesetzgeber sei empfohlen, Möglichkeiten einer umfassenderen Definition zu prüfen, die alle Arten von Spam, unerbetene Telefonanrufe und Marketingnachrichten, Phishing und andere böswillige Angriffe abdeckt.

IX. TEILNEHMERVERZEICHNISSE

Artikel 12 der Datenschutzrichtlinie für elektronische Kommunikation sieht für Teilnehmer das Recht vor,*„festzulegen, ob ihre personenbezogenen Daten in ein öffentliches (gedrucktes oder elektronisches) Verzeichnis aufgenommen werden“*.

Der EDSB empfiehlt die Beibehaltung dieser Bestimmung und die Ausdehnung ihres Geltungsbereichs auf alle Arten von Verzeichnisdiensten. Des Weiteren sollte das Erfordernis der Einwilligung für die Rückwärtssuche auch ausdrücklich auf andere Dienst-Identifikatoren wie E-Mail-Adresse oder Nutzername ausgedehnt werden.

X. WEITERE EMPFEHLUNGEN

X.1 Anzeige der Rufnummer des Anrufers

In der Datenschutzrichtlinie für elektronische Kommunikation ist das Recht des Angerufenen geregelt, zu erfahren, wer ihn anruft, und gegen Anrufer vorzugehen, die die Anzeige ihrer Rufnummer unterdrücken. Der EDSB empfiehlt, dieses Recht aufrechtzuerhalten, da es eine der Schutzvorkehrungen ist, dank derer natürliche Personen gegen Personen vorgehen können, die entgegen geltendem Recht unerbetene Nachrichten senden.

X.2 Räumlicher Anwendungsbereich und geltendes Recht

Der EDSB empfiehlt, in den neuen Bestimmungen über den Datenschutz in der elektronischen Kommunikation grundsätzlich den gleichen räumlichen Anwendungsbereich wie in der DSGVO vorzusehen (einschließlich des in Artikel 3 Absatz 2 vorgesehenen extra-territorialen Anwendungsbereichs)[38], und grundsätzlich bezüglich des auf die Verarbeitung personenbezogener Daten anzuwendenden Rechts den gleichen Ansatz zu verfolgen.

Es ist allerdings zu bedenken, dass möglicherweise ein paar technische Anpassungen im Wortlaut dieser Bestimmungen vorzunehmen sind. So findet beispielsweise Artikel 5 Absatz 3 der Datenschutzrichtlinie für elektronische Kommunikation Anwendung, unabhängig davon, ob die Person, die ein Cookie gesetzt oder eine Spyware installiert hat, gemäß der DSGVO als „Verantwortlicher“ gilt oder nicht, und ob überhaupt personenbezogene Daten verarbeitet werden. Es könnte also erforderlich sein, beim räumlichen Anwendungsbereich auf diese Unterschiede einzugehen.

X.3 Transparenz im Hinblick auf Auskunftsersuchen staatlicher Stellen

In globalen Netzen überqueren Nachrichten Grenzen, ohne dass die Nutzer dies merken. So können auf der einen Seite Nachrichten zwischen EU-Mitgliedstaaten durch Drittländer gehen und auf der anderen Seite Nachrichten zwischen Drittländern über EU-Hoheitsgebiet übermittelt werden. 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 schaffen. Nach dem Inkrafttreten der DSGVO werden sich solche Ersuchen um die Übermittlung personenbezogener Daten in ein Drittland nur noch auf eine internationale Übereinkunft wie etwa ein Rechtshilfeabkommen stützen können.[39]

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.

Daher empfiehlt der EDSB, in den neuen Bestimmungen über den Datenschutz in der elektronischen Kommunikation spezifische Bestimmungen für eine bessere Transparenz vorzusehen. Er empfiehlt 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. Im Hinblick auf derartige Ersuchen aus Drittländern sollten die Dienstanbieter die in Artikel 48 der DSGVO formulierte Bedingung der Rechtmäßigkeit beachten.

XI. SCHLUSSFOLGERUNGEN

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

(**gezeichnet)**

Giovanni BUTTARELLI

Europäischer Datenschutzbeauftragter

Hinweise

[1] 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.

[2] Ref. Ares(2016)2310042 - 18/05/2016.

[3] Siehe https://ec.europa.eu/digital-single-market/en/news/public-consultation-evaluation-and-review-eprivacy-directive. Der Fragebogen ist abrufbar unter: https://ec.europa.eu/eusurvey/runner/EPRIVACYReview2016.

[4] Stellungnahme 03/2016 der Artikel 29-Datenschutzgruppe zur Evaluierung und Überarbeitung der Datenschutzrichtlinie für elektronische Kommunikation (2002/58/EG) (WP240), angenommen am 19. Juli 2016.

[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 Endnote 4.

[9] Siehe https://edri.org/files/epd-revision/EDRi_ePrivacyDir-final.pdf.

[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] 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.

[13] 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.

[14] Der Begriff Over-the-Top (OTT) bezeichnet Dienste und Anwendungen, die über das Internet zugänglich sind und über ein Netz laufen, das für Internetzugangsdienste bereitgestellt wird. Als Beispiele seien Kommunikationsdienste (Sprache und Messaging) wie Skype, WhatsApp und Facebook Messenger genannt, aber auch eine ganze Palette anderer Dienste und Anwendungen wie soziale Netzwerke wie Facebook, Twitter oder LinkedIn oder Video- und Audio-Streamingdienste wie Netflix oder YouTube. Nähere Informationen zu OTT z. B. unter:
http://www.europarl.europa.eu/RegData/etudes/STUD/2015/569979/IPOL_STU(2015)569979_EN.pdf.

[15] Es sei auch darauf hingewiesen, dass häufig ein Nutzer eine Sprach- oder Textmitteilung über einen OTT-Kommunikationsdienst auf den Weg bringt, der Empfänger aber über konventionelle Mittel die Nachricht empfängt oder an der Kommunikation teilnimmt (z. B. indem er eine SMS auf seinem Mobiltelefon oder einen VoIP-Anruf auf seinem traditionellen Festnetzanschluss erhält).

[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] Siehe Endnote 13.

[18] 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.

[19] 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.

[20] Siehe z. B. Science and Technology Options Assessment (STOA), EuropäischesParlament, *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

[21] 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.

[22] „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.

[23] 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.

[24] 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.

[25] New York Times Editorial Board, Surveillance: *A Threat to Democracy*, 11 June 2013, abrufbar unter: http://www.nytimes.com/2013/06/12/opinion/surveillance-a-threat-to-democracy.html?hp.

[26] Richtlinie 2009/136/EG des Europäischen Parlaments und des Rates vom 25. November 2009 zur Änderung der Richtlinie 2002/22/EG über den Universaldienst und Nutzerrechte bei elektronischen Kommunikationsnetzen und –diensten, der Richtlinie 2002/58/EG über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation und der Verordnung (EG) Nr. 2006/2004 über die Zusammenarbeit im Verbraucherschutz, ABl. L 337 vom 18.12.2009, S. 11, abrufbar unter. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:337:0011:0036:de:PDF.

[27] 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.

[28] 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."

[29] Siehe Frage 22 der öffentlichen Konsultation der Kommission: „Dienste der Informationsgesellschaft sollten als Alternative zur Zahlung der Dienste durch die persönlichen Daten der Nutzer auch kostenpflichtig verfügbar gemacht werden (ohne verhaltensorientierte Werbung)."

[30] 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.

[31] Stellungnahme 04/2012 der Artikel 29-Datenschutzgruppe 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.

[32] 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.

[33] Das heißt, dass die DSGVO und das neue Rechtsinstrument für den Datenschutz in der elektronischen Kommunikation im Sinne von Kohärenz aufeinander abgestimmt sein müssen. Der EDSB empfiehlt beispielsweise einen Querverweis auf die Sicherheitsverpflichtungen in der DSGVO (einschließlich Datenschutzfolgenabschätzungen und Rechenschaftspflicht).

[34] Siehe Frage 21 des Fragebogens für die öffentliche Konsultation.

[35] Siehe die in Endnote 4 zitierte Stellungnahme der WP29, S. 19.

[36] Siehe https://en.wikipedia.org/wiki/Backdoor_(computing).

[37] Studie mit dem Titel „ePrivacy Directive: assessment of transposition, effectiveness and compatibility with proposed Data Protection Regulation" (Datenschutzrichtlinie für elektronische Kommunikation: Bewertung der Umsetzung, Wirksamkeit und Vereinbarkeit mit der vorgeschlagenen Datenschutzverordnung) (SMART 2013/0071), Abschnitt 3.2.3 zu *Supervision* (Aufsicht) (S. 33 und 34). verfügbar unter: https://ec.europa.eu/digital-single-market/en/news/eprivacy-directive-assessment-transposition-effectiveness-and-compatibility-proposed-data.

[38] Siehe auch die weiter oben in Endnote 9 erwähnte gemeinsame Analyse von Gruppen der Zivilgesellschaft.

[39] Siehe Artikel 48 DSGVO *„Nach dem Unionsrecht nicht zulässige Übermittlung oder Offenlegung"*.