



MASTER THESIS

Titel der Master Thesis / Title of the Master's Thesis

„Analyse des Entwurfs der e-privacy Verordnung“

verfasst von / submitted by

Mag. Keren Shatkin

angestrebter akademischer Grad / in partial fulfilment of the requirements for the degree of

Master of Laws (LL.M.)

Wien, 2018 / Vienna 2018

Studienkennzahl lt. Studienblatt /
Postgraduate programme code as it
appears on
the student record sheet:

A 992 548

Universitätslehrgang lt. Studienblatt /
Postgraduate programme as it appears on
the student record sheet:

Europäisches und Internationales Wirtschaftsrecht /
European and International Business Law

Betreut von / Supervisor:

Dr. Maria Sturm, LL.M.

Inhaltsverzeichnis

Inhaltsverzeichnis.....	0
Vorwort.....	1
1.Einleitung	3
2.Das Grundrecht auf Datenschutz und Anwendungsbereich der e-Privacy Verordnung.....	6
2.1 Rechtsgrundlage für die e-Privacy Verordnung.....	6
2.2 Sachlicher Anwendungsbereich	7
2.3 räumlicher Anwendungsbereich.....	15
3.Schutz der elektronischen Kommunikation	20
3.1 Vertraulichkeit elektronischer Kommunikationsdaten.....	20
3.2 Erlaubte Verarbeitung elektronischer Kommunikationsdaten	23
4.Webtracking und Cookies	33
4.1 Schutz der in Endeinrichtungen gespeicherten Informationen	33
4.2 Einstellungsmöglichkeiten zur Privatsphäre.....	37
5.Sonderbestimmungen zu nummerngebundener interpersoneller Kommunikation.....	42
5.1. Anzeige und Unterdrückung einer Rufnummer	43
5.2 Ausnahmen für die Anzeige der Rufnummer des Anrufers und des Angerufenen und deren Unterdrückung	44
5.3. Sperrung eingehender Anrufe	46
6.Öffentliche zugängliche Verzeichnisse.....	47
7.Unerbetene Kommunikation	52
7.1. Einwilligung oder Widerspruch	52
7.2. Werbeanrufe	54
7.3 Juristische Personen	57
8.Rechtsbehelfe, Haftung und Sanktionen	57
8.1 Zuständige Aufsichtsbehörde.....	57
8.2 Rechtsbehelfe	59
8.3 Haftung und Recht auf Schadenersatz	61
8.4 Geldbußen und Sanktionen	61
9.Abstract	66
9.1 Abstract in Deutsch	66
9.2 Abstract in English.....	69
Literaturverzeichnis.....	71
Abbildungsverzeichnis	76

Abkürzungsverzeichnis

aaO	am angegebenen Ort
ABl	Amtblatt
Abs	Absatz
AEUV	Vertrag über die Arbeitsweise der Europäischen Union
Art	Artikel
DSG	Datenschutzgesetz
DSGVO	Datenschutzgrundverordnung
EECC	European Electronic Communication Codex (Europäischer Kodex zur elektronischen Kommunikation)
ErwG	Erwägungsgrund
EU	Europäische Union
EUR	Euro
EuGH	Gerichtshof der Europäischen Union
GRCh	Charta der Grundrechte der Europäischen Union
iab	Internet Advertising Bureau - Verein zur Förderung der Online Werbung
i.d.F.	in der Fassung
iVm	In Verbindung mit

IoT	Internet of Things (Internet der Dinge)
iSv / iSd	im Sinne von / im Sinne des
M2M	Maschine-Maschine-Kommunikation
OTT	Over The Top
PStSG	Polizeiliches Staatsschutzgesetz
RTR	Rundfunk und Telekom Regulierungs – GmbH
TKG	Telekommunikationsgesetz
TKK	Telekom-Control-Kommission

Vorwort

Die Europäische Union hat im Jahr 2015 eine Strategie zum europäischen digitalen Binnenmarkt veröffentlicht. Sie plant kostenlose und frei zugängliche WLAN-Standorte in Stadtzentren in allen europäischen Hauptstädten sowie den Zugang zu schnellem mobilen Internet im gesamten europäischen Raum. Auch 5G und die damit verbundenen Möglichkeiten und Technologien stehen im Zentrum von nationalen und internationalen Zukunftsplänen. Selbstfahrende Autos, Operationen durch Roboterarme, die von Ärzten auf der anderen Seite der Erdkugel in Echtzeit gesteuert werden oder die Etablierung von Programmen als Hologramm im Schulbereich, in Universitäten oder auch im Haushalt sind nur die bekanntesten Beispiele, die in naher Zukunft Realität sein sollen. Viele technische Innovationen sind heute schon möglich und werden auch von immer mehr Herstellern angeboten. Beispielsweise ermöglicht „Smart Home“ die Steuerung von Haushaltsgeräten wie Fernseher, Kühlschränke, Heizungen, Glühbirnen, etc. durch ein App. Alexa, ein Gerät, das von Amazon verkauft und aktuell sehr stark beworben wird, kann durch Sprachsteuerung Zeitungsartikel zusammenfassen, Einkaufslisten erstellen sowie alle mit dem Internet verbundenen Haushaltsgeräte bedienen.

All diese technischen Erfindungen sind erst durch ein schnelles und billigeres mobiles Internet möglich geworden. Damit die Kommunikation durch Alexa und Co gewährleistet werden kann, müssen diese Geräte mit dem Internet verbunden werden. Damit diese erbracht werden können, werden immer mehr Daten, vor allem personenbezogene Daten, zwischen den Endgeräten und Router oder dem Kommunikationsbetreiber verschickt, aber auch gesammelt. Und diese Daten geben nicht nur an, was die Leute interessiert, wie Fernsehprogramme, besuchte Internetseiten oder Einkaufslisten, sondern zeigen durch sogenannte Verkehrsdaten auf, wo sich die Nutzer befinden und beispielsweise auch wann und wie oft die genutzten Dienste verwendet werden. Diese Daten sind einerseits notwendig, um den genutzten Dienst erbringen zu können, sie dienen jedoch auch für weitere Anwendungen, wie beispielsweise Big Data oder Profiling. Mit den Möglichkeiten steigt aber auch die Gefahr von Hackerangriffen und auch das Gefühl der Nutzer, dass sie die Herrschaft ihrer personenbezogenen Daten verlieren und von den Anbietern abhängig sind.

Eine weitere Gefahr sehen Datenschützer in dem Sammeln von gewissen Informationen um einem Konsumenten passende Angebote bei Besuchen auf Webseiten vorschlagen zu können. Durch sogenannte Cookies werden die Interessen des Einzelnen Nutzers gesammelt. So können Online-Werbendienste immer an den Besucher angepasste Werbung schalten. Viele Endnutzer

verstehen oft gar nicht, was diese Cookies genau machen und wünschen sich mehr Transparenz und Mitspracherechte zur Setzung der Cookies.

Angepasst an die neuen Technologien und Herausforderungen, soll die e-Privacy Richtlinie als Verordnung aktualisiert und angepasst werden. Diese Verordnung schützt die personenbezogenen Daten, die bei der elektronischen Kommunikation entstehen und bietet einen höheren Schutz als die DSGVO. Die e-Privacy Verordnung sollte ursprünglich gleichzeitig mit der DSGVO, dem 25. Mai 2018 in Kraft treten. Aufgrund vieler Differenzen im Europäischen Rat befindet sich die e-privacy Verordnung immer noch im Entwurfsstadium und viele stellen sich die Frage, ob sie überhaupt noch notwendig ist, wenn sie nicht bald in Kraft treten wird.

Den Betreibern von Kommunikationsdiensten, aber auch den Online-Werbetreibenden gehen die Entwürfe der e-privacy Verordnung viel zu weit. Sie sehen hier eine Einschränkung für alle europäischen Unternehmen und eine weitere Stärkung von großen US-amerikanischen Unternehmen. Aus der Perspektive des Europäische Parlaments sowie die Artikel 29 Gruppe, dem Europäischen Ausschuss, der sich aus den Datenschutzbehörden der Mitgliedstaaten zusammensetzt, sieht der Entwurf aber auch die folgenden Änderungsvorschläge keine strengeren Regelungen als die DSGVO vor, was für sie nicht verständlich ist. Sie sehen hier eine Gefährdung von Endnutzerrechten, da sie den Schutz der DSGVO als absolute Mindestanforderung verlangen und diesen nicht in allen Artikeln erkennen können.

In dieser Master Thesis werden die Schwerpunkte des ursprünglichen Entwurfs der e-privacy Verordnung vom 10. Jänner 2017 sowie die Änderungsvorschläge der estnischen und bulgarischen Ratspräsidentschaft analysiert und die Positionen von Wirtschaft einerseits und von Datenschutzrechtlern und -organisationen andererseits dargestellt.

1. Einleitung

Der Rat der Europäischen Union veröffentlichte 2015 seine Strategie für einen digitalen Binnenmarkt in Europa¹. Hier werden unterschiedliche Aspekte vorgestellt, die Europa auf die digitale Zukunft vorbereiten und weiterhin einen hohen Lebensstandard für seine Bürger gewährleisten sollen.² Hierbei ist dem Europäischen Rat auch bewusst, dass Big Data, Cloud-Dienste und das Internet der Dinge wichtige Voraussetzungen für die Wettbewerbsfähigkeit von europäischen Unternehmen auf dem Weltmarkt sind.³ Gleichzeitig soll jedoch der Umgang mit den daraus entstehenden und gespeicherten Daten neu geregelt werden. Aus diesem Grund löst die DSGVO⁴ die veraltete Richtlinie zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und freiem Datenverkehr ab.⁵ Diese tritt mit 25. Mai 2018 in Kraft.

Am selben Tag sollte auch die Verordnung des Europäischen Parlaments und des Rates über die Achtung des Privatlebens und den Schutz personenbezogener Daten in der elektronischen Kommunikation und zur Aufhebung der Richtlinie 2002/58/EG, kurz e-privacy Verordnung, in Kraft treten. Aufgrund der neuen Technologien und der neuen datenschutzrechtlichen Bestimmungen der DSGVO sollte die veraltete Richtlinie 2002/58/EG abgelöst werden.⁶ Die e-privacy Verordnung befindet sich jedoch seit Jänner 2017 noch im Entwurf-Stadium und ist noch immer nicht fertig. Derzeit ist es nicht absehbar, wann die e-Privacy Verordnung in Kraft treten wird. Viele Unternehmen, die durch die e-Privacy Verordnung zusätzlich zur DSGVO Einschränkungen bei der Verarbeitung von Daten erhalten, versuchen diese zu verhindern.

¹ Rat der Europäischen Union, Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen – Strategie für einen digitalen Binnenmarkt für Europa, Brüssel, 06. Mai 2015, 8672/15.

² aaO, 20.

³ aaO, 16.

⁴ 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, kurz DSGVO), ABl. L 2016/119, 1ff.

⁵ 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 1995/281, 31ff.

⁶ 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 2002/201, 37ff.

Der erste Entwurf der e-privacy Verordnung vom 10. Jänner 2017 hat laut der Europäischen Kommission⁷ drei Schwerpunkte, nämlich die Schaffung eines level playing fields zwischen klassischen Telekommunikationsanbietern und sogenannten over the top-playern (OTTs), eine neue Regelung wie in Zukunft mit Cookies auf Webseiten umzugehen ist sowie die Harmonisierung der unerbetenen Kommunikation. Klar ist, dass die e-Privacy Verordnung nicht nur die Telekommunikationsanbieter regulieren soll, sondern die gesamte elektronische Kommunikation, die jedes Unternehmen, das eine Webseite, Newsletter oder Werbung auf einer Webseite anbietet, betrifft.

Diese Master Thesis behandelt in ihrem ersten Kapitel die Rechtsgrundlage, auf die sich die Europäische Kommission stützt, die e-privacy Verordnung zu erlassen sowie die Ausdehnung der bestehenden Regulierung und den Versuch der europäischen Kommission ein level playing field zu schaffen. Im zweiten Kapitel werden das Kommunikationsgeheimnis sowie die Verarbeitung der elektronischen Kommunikation und die damit verbundenen Einschränkungen im Verhältnis zur DSGVO dargestellt. Das dritte Kapitel beschäftigt sich mit der neuen Bestimmung für Webtracking und Cookies und die damit verbundenen Befürchtungen, vor allem der Werbevermarkter. Das vierte Kapitel beschäftigt sich mit Regelungen zu Rufnummern, die vor allem die klassischen Telekommunikationsanbieter anspricht. Diese Bestimmungen wurden von der derzeit noch gültigen e-privacy Richtlinie übernommen, jedoch von den Mobilfunkunternehmen in der Regel bis jetzt nicht umgesetzt, da bereits alle Endgeräte diese Anforderungen erfüllen. Hier fordern die Telekommunikationsanbieter, dass die ihrer Meinung nach unnötigen Bestimmungen wieder gestrichen werden. Im fünften Kapitel wird die neue Regelung für öffentliche Verzeichnisse sowie die damit verbundenen Argumente von betroffenen Unternehmen beleuchtet. Das sechste Kapitel widmet sich den Bestimmungen über die unerbetene Kommunikation. Hier werden zum Großteil die Bestimmungen der e-Privacy Richtlinie übernommen. Dies führt jedoch dazu, dass die Erleichterungen der DSGVO bei Direktwerbung durch elektronische Kommunikationsdienste ausgehebelt werden. So würde die Werbung, die mit der Post zugestellt wird, wieder deutlichen Aufschwung bekommen, wenn Unternehmen nicht entsprechend gültige Einwilligungen ihrer Kunden einholen können. Das siebte Kapitel geht unter anderem auf die Sanktionen ein, die bei einem Verstoß gegen diese Verordnung drohen. Die e-privacy Verordnung lehnt sich an der Struktur der DSGVO an und regelt Geldbußen in einer Höhe von bis zu 20 Millionen Euro bzw. 4% des gesamten weltweit

⁷ Europäische Kommission, Commission Staff Working Document, SWD, 2017, 3 final, 5.

erzielten Jahresumsatzes des vorangegangenen Geschäftsjahres, je nachdem welcher Betrag höher ist.

In diesen Kapiteln werden zusätzlich zu der Analyse des Entwurfstextes sowie der Änderungsvorschläge der estnischen und bulgarischen Ratspräsidentschaft auch die Stellungnahmen der Art 29 Gruppe und anderen Organisationen gegenüber gestellt, die in vielen Punkten einen schärferen Schutz für die personenbezogenen Daten der Nutzer von Handys, Tablets oder PCs verlangen.

Zum Entwurf der e-Privacy Verordnung bringen Unternehmen aus ganz Europa ihre Stellungnahmen ein und lobbyieren gegen diese Bestimmungen. Die europäischen Unternehmen vertreten die Position, dass durch die zusätzlichen Einschränkungen gegenüber der DSGVO viele Unternehmen ihre Wettbewerbsfähigkeit im Vergleich zu anderen Unternehmen, die nicht dieser europäischen Regulierung unterliegen, verlieren. Die Artikel 29 Gruppe, ein Ausschuss der sich aus den Datenschutzbehörden der Mitgliedstaaten zusammensetzt, legt in ihrer Stellungnahme dar, dass der Schutz für die Kommunikationsdaten nicht ausreichend genug ist.

In dieser Master Thesis wird auf diese strittigen Punkte eingegangen und die verschiedenen Standpunkte beschrieben. Die Zukunft wird zeigen, welche dieser Positionen sich im Europäischen Parlament und Rat durchsetzen wird.

2. Das Grundrecht auf Datenschutz und Anwendungsbereich der e-Privacy Verordnung

2.1 Rechtsgrundlage für die e-Privacy Verordnung

Die im Jahr 2000 erlassene Charta der Grundrechte der Europäischen Union regelt in den Art 7 (Achtung des Privat- und Familienlebens) das Grundrecht auf das Kommunikationsgeheimnis und in Art 8 den Schutz personenbezogener Daten, worauf sich jede Person berufen kann. Somit handelt es sich bei dem Schutz von personenbezogenen Daten um ein Menschenrecht und nicht bloß um ein Bürgerrecht.⁸ Bei diesem Grundrecht handelt es sich um ein Grundrecht mit Drittwirkung, da sich der Schutz sowohl gegen den Staat als auch gegen private Datenverarbeiter richtet.⁹

Art 7 der GRCh schützt das Grundrecht auf Achtung des Privat- und Familienlebens, der Wohnung sowie der Kommunikation. Das Kommunikationsgeheimnis umfasst jene Informationen, die zwischen den Endnutzern ausgetauscht werden. Hier fallen auch die bei der Kommunikation entstandenen Verkehrsdaten bzw. nach der Terminologie der e-Privacy Verordnung – Kommunikationsmetadaten – hinein. Diese sagen aus welcher Teilnehmer, zu welchem Zeitpunkt, in welcher Zelle mit wem kommuniziert hat. Durch das Kommunikationsgeheimnis sind auch Metadaten als personenbezogene Daten zu schützen und nicht an Dritte weiterzugeben.¹⁰

Art 8 Abs 2 GRCh gibt bereits vor, dass personenbezogene Daten ausschließlich nach Treu und Glauben für festgelegte Zwecke und mit Einwilligung der betroffenen Person oder auf einer sonstigen gesetzlich geregelten legitimen Grundlage verarbeitet werden dürfen. Somit besteht für das Verbot der Datenverarbeitung ein Erlaubnisvorbehalt¹¹, der vor allem in der e-privacy Verordnung sehr großen Stellenwert bekommt, da die rechtlichen Grundlagen für die

⁸ Ernst (2017): Kapitel I. Allgemeine Bestimmungen. B. Grundrechte (Abs. 2) In Paal – Pauly (Hrsg.): Datenschutz-Grundverordnung, 11.

⁹ aaO, 11.

¹⁰ Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über die Achtung des Privatlebens und den Schutz personenbezogener Daten in der elektronischen Kommunikation und zur Aufhebung der Richtlinie 2002/58/EG (Verordnung über Privatsphäre und elektronische Kommunikation), Brüssel, 10.01.2017, ErwG 1.

¹¹ Ernst (2017): Kapitel I. Allgemeine Bestimmungen. B. Grundrechte (Abs. 2) In Paal – Pauly (Hrsg.): Datenschutz-Grundverordnung, 11.

Datenverarbeitung im Verhältnis zu Art 6 DSGVO stark reduziert werden und somit die Einwilligung für die Datenverarbeitung einen noch höheren Stellenwert erhält.

Auch die Rechte auf Auskunft über die gespeicherten personenbezogenen Daten sowie auf Berichtigung, die in der DSGVO als Betroffenenrechte statuiert werden, sind bereits in der Charta der Grundrechte festgehalten.

Der EuGH wendet in allen den Datenschutz betreffenden Entscheidungen die Art 7 GRCh und Art 8 GRCh nebeneinander an.¹² ErwG 4 der DSGVO hält fest, dass es sich bei dem Recht auf Schutz der personenbezogenen Daten um kein uneingeschränktes Recht handelt, vielmehr muss es unter Wahrung des Verhältnismäßigkeitsprinzips gegen alle Grundrechte abgewogen werden.

Um eine EU-weite Harmonisierung zu schaffen, wurde, wie auch bei der DSGVO, die Form einer Verordnung gewählt. So soll in allen Mitgliedstaaten ein einheitlicher hoher Standard geschaffen werden. Diese Entscheidung wird sowohl von der Art 29 Gruppe¹³, als auch von den Unternehmen unterstützt, da international tätige Betreiber durch die Harmonisierung auch eine einheitliche Umsetzung der Regulierung planen können.

Für die Erlassung der e-privacy Verordnung stützt sich die Europäische Kommission in der Präambel des Entwurfes für die e-privacy Verordnung auf Art 16 und Art 114 AEUV als rechtliche Grundlage.

2.2 Sachlicher Anwendungsbereich

Eine Studie der Europäischen Kommission führte zu dem Schluss, dass sich EU BürgerInnen in ihrer Privatsphäre nicht ausreichend und wirkungsvoll geschützt fühlen.¹⁴ Gemäß dieser Umfrage haben 90% der befragten TeilnehmerInnen und Behörden die Meinung vertreten, dass eine Regelung der elektronischen Kommunikation zusätzlich zur DSGVO notwendig sei. Dies hat den europäischen Gesetzgeber darin bestärkt, dass weiterhin Bedarf für eine Regulierung der elektronischen Kommunikation besteht und somit die Bestimmungen der e-Privacy Richtlinie anhand der neuen Prinzipien der DSGVO und neuen Technologien aktualisiert und adaptiert werden müssen. Im Gegensatz hierzu nehmen vor allem Betreiber von Kommunikationsdiensten

¹² aaO, 11.

¹³ Article 29 Data Protection Working Party, Opinion 01/2017 on the Proposed Regulation for the e-Privacy Regulation (2002/58/EC), 2017; 6, Rn. 4.

¹⁴ Arbeitsunterlage der Kommissionsdienststellen, Zusammenfassung der Folgenabschätzung, 2017, 2.

die Position ein, dass die DSGVO sowie andere Bestimmungen zur elektronischen Kommunikation, wie beispielsweise die Richtlinie zur Netz- und Informationssicherheit, ausreichen und keine weitere Regulierung notwendig ist.¹⁵

In Art 1 der e-Privacy Verordnung wird zuerst der Gegenstand der geplanten Verordnung beschrieben. Im Unterschied zur DSGVO gilt der Schutz dieser Verordnung nicht nur für natürliche, sondern auch für juristische Personen. Dieser Grundsatz besteht bereits in der derzeit gültigen e-privacy Richtlinie und wird weiterhin für die gesamte Verordnung beibehalten. Es kann davon ausgegangen werden, dass dies auf die Judikatur des EuGH zurückgeführt werden kann, in der er bereits bestätigt hat, dass die in Art 7 und Art 8 GRCh gewährten Grundrechte für juristische Personen nicht ausgeschlossen werden dürfen.¹⁶ Dies gilt vor allem für das in Art 8 GRCh geregelte Recht auf das Kommunikationsgeheimnis, das in Art 5 der e-Privacy Verordnung geregelt ist und in Kapitel 3 genauer beschrieben wird.

Telekommunikationsbetreiber sehen durch die Ausdehnung des Schutzes auf juristische Personen eine Schlechterstellung gegenüber anderen Unternehmen, die sich ausschließlich an die Bestimmungen der DSGVO zu halten haben.¹⁷ Ihrer Meinung nach sollte ausschließlich das in Art 5 e-privacy Verordnung geregelte Kommunikationsgeheimnis für natürliche und juristische Personen zur Anwendung kommen. Die anderen Bestimmungen der e-Privacy Verordnung sollten jedoch, wie auch die DSGVO, ausschließlich die elektronische Kommunikation von natürlichen Personen schützen. Diese Unterscheidung ist vor allem in Hinblick auf neue Technologien wie IoT oder M2M – Kommunikation wichtig, da hier in der Regel zwischen Maschinen beispielsweise Messwerte oder einfache Befehle kommuniziert werden. Hierbei werden keine personenbezogenen Daten verarbeitet. Gemäß der DSGVO würden solche Anwendungsfälle keinen Schutz genießen. Hingegen begrüßt die Art 29 Gruppe, dass die Bestimmungen für alle Endnutzer gleich sind, unabhängig, ob es sich um eine natürliche oder

¹⁵ Schrefler, Lorna, Review of the ePrivacy Directive, Directive 2002/58 concerning the processing of personal data and the protection of privacy in the electronic communications sector, 2017, 10, gesamter Absatz.

¹⁶ Rechtssache C-450/06 Varec SA, ECLI:EU:C:2008:91, Rn.48.

¹⁷ Schubert, Maximilian (2017): ISPA Stellungnahme betreffend den Entwurf der Verordnung über Privatsphäre und elektronische Kommunikation (e-Privacy-VO). Onlinedokument: https://www.ispa.at/filed/0/0/1498408297/530f4cf428655c3a6477cca77f252c970e16925f/filadmin/content/5_Wissenspool/Stellungnahmen/2017/20170317_BMvit_E-Privacy/201703013_ISPA_Stellungnahme_E-Privacy_final.pdf; Download am 15.07.2017.

juristische Person handelt¹⁸. So haben auch Unternehmen das Recht sich bei der zuständigen Behörde zu beschweren. Die Art 29 Gruppe sieht dies gerade in Hinblick auf die neuen Möglichkeiten in der Zukunft als einen wichtigen Schritt¹⁹.

In ErwG 1 der e-Privacy Verordnung wird erklärt, dass die Kommunikation ausschließlich zwischen den beteiligten Personen einer Kommunikation ausgetauscht werden soll. Damit soll die Vertraulichkeit der elektronischen Kommunikation gewährt bleiben. Außer den Teilnehmern der Kommunikation hat niemand das Recht in diese einzugreifen. Dies gilt auch für die sogenannten Metadaten, die unter anderem angeben wann, woher und an wen die Kommunikation stattgefunden hat. Der Vorschlag der bulgarischen Ratspräsidentschaft betont hier zusätzlich noch einmal die Gleichbehandlung zwischen natürlichen und juristischen Personen²⁰. So wird sichergestellt, dass auch juristische Personen ein Recht auf das Kommunikationsgeheimnis haben.

Art 1 Abs 3 erklärt, dass die e-privacy Verordnung als Präzisierung und Ergänzung der DSGVO zu verstehen ist. ErwG 5 des ursprünglichen Entwurfs, der in einem späteren Entwurf der bulgarischen Ratspräsidentschaft²¹ durch ErwG 2a ersetzt wird, weist darauf hin, dass es sich bei den folgenden Tatbeständen um eine *lex specialis* gegenüber der DSGVO handelt. Die e-privacy Verordnung soll demnach nicht zu einer Absenkung des hohen Schutzniveaus der DSGVO führen. Diesen Standpunkt vertritt selbstverständlich auch die Artikel 29 Gruppe, die in ihrer Stellungnahme zum Entwurf der e-Privacy Verordnung an mehreren Stellen betont, dass immer wieder Erleichterungen gegenüber der DSGVO zu finden sind, die aus ihrer Sicht jedenfalls zu verhindern sind²².

¹⁸ Article 29 Data Protection Working Party, Opinion 01/2017 on the Proposed Regulation for the ePrivacy Regulation (2002/58/EC), 2017, 8, Rn. 8.

¹⁹ aaO, 9, Rn. 13.

²⁰ Proposal for a regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) – Examination of the Presidency text; Brussels, 12. June 2018, 9958/18, Erw 1, 5.

²¹ aaO, ErwG 2a, 6.

²² Article 29 Data Protection Working Party, Opinion 01/2017 on the Proposed Regulation for the ePrivacy Regulation (2002/58/EC), 2017, 10 ff.

Zu Beginn der bulgarischen Ratspräsidentschaft wurde im Diskussionspapier²³ die Frage aufgeworfen, bei welchen Bestimmungen die e-Privacy Verordnung als *lex specialis* gegenüber der DSGVO anzusehen ist und in welchen Fällen als *lex generalis*, da jene Datenverarbeitungen nicht in den Anwendungsbereich der DSGVO fallen. Diese Frage wird vor allem von den Betreibern der Telekommunikationsdienste aufgegriffen. Die österreichische Wirtschaftskammer betont in ihrer Stellungnahme, dass große Unsicherheiten für die Unternehmen bestehen bleiben, solange keine deutliche und verständliche Trennung zwischen der DSGVO und der e-Privacy Verordnung getroffen wurde²⁴.

Art 2 der e-Privacy Verordnung beschreibt den sachlichen Anwendungsbereich und erörtert in Abs 1, dass diese Verordnung für die Verarbeitung elektronischer Kommunikationsdaten gilt, die in Verbindung mit der Bereitstellung und Nutzung elektronischer Kommunikationsdienste erfolgt sowie für Informationen in Bezug auf die Endeinrichtungen der Endnutzer. In den weiteren Änderungsvorschlägen der estnischen und bulgarischen Ratspräsidentschaften wurde der Anwendungsbereich in Abs 1 genauer präzisiert²⁵. Somit soll die e-Privacy Verordnung in folgenden Fällen anwendbar sein:

- a) Verarbeitung von elektronischen Kommunikationsinhalten und -metadaten, die bei der Erbringung eines elektronischen Kommunikationsdienstes entstehen;
- b) Informationen, die auf dem Endgerät des Endnutzers gespeichert sind;
- c) Inverkehrbringen von Software, die elektronische Kommunikation ermöglicht, einschließlich dem Abrufen oder Darstellen von Informationen im Internet;
- d) Bereitstellen von öffentlichen Verzeichnissen, in denen Daten von Endnutzern elektronischer Kommunikationsdienste veröffentlicht werden sowie
- e) Kommunikation zu Zwecken des Direktmarketings an Endnutzer.

²³ Proposal for a regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) – Examination of the Presidency discussion paper; Brussels, 11. January 2018, 5165/18.

²⁴ Illibauer, Ursula, Positionspapier zum Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über die Achtung des Privatlebens und den Schutz personenbezogener Daten in der elektronischen Kommunikation und zur Aufhebung der Richtlinie 2002/58/EG (Verordnung über Privatsphäre und elektronische Kommunikation), 5.3.2018, 4.

²⁵ Proposal for a regulation of the European Parliament and the Council concerning the respect for private life and protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) - Examination of the Presidency text, Brussels, 12 June 2018, 9958/18, Art 2 Abs 1, 41.

Mit dieser Bestimmung soll der Datenschutz in der elektronischen Kommunikation an die aktuelle Marktsituation angepasst werden und ein sogenanntes „level playing field“ zwischen Telekommunikationsbetreibern und Online-Diensten geschaffen werden. Darunter ist die technologieneutrale Gleichbehandlung und Chancengleichheit in der Regulierung zu verstehen. Vor allem Telekombetreiber setzen sich dafür ein, dass ein level playing field geschaffen wird, da sie sehr stark reguliert werden²⁶. Andere Unternehmen, die überwiegend aus den USA stammen und ähnliche Daten verarbeiten, haben oft nicht die gleichen strengen Auflagen zu erfüllen. So entstehen ein Ungleichgewicht sowie ein Wettbewerbsnachteil für die strenger regulierten Betreiber.

In ErwG 11 wird angeführt, dass nicht nur herkömmliche Übermittlungsdienste für Sprachtelefonie, Textnachrichten (SMS) und E-Mail in dieser Verordnung reguliert werden sollen. Endnutzer verwenden immer häufiger gleichwertige Online-Dienste wie Voice over IP-Telefonie, Nachrichtenübermittlung (Messaging) und webgestützte E-Mail-Dienste. Diese Online-Dienste werden over-the-top-Kommunikationsdienste genannt, da sie ihre Dienstleistung im Telekommunikationsnetz anbieten und daher keine eigene Netzinfrastruktur benötigen. Dies ist nur durch die Nutzung der Infrastruktur der klassischen Telekommunikationsanbieter möglich.

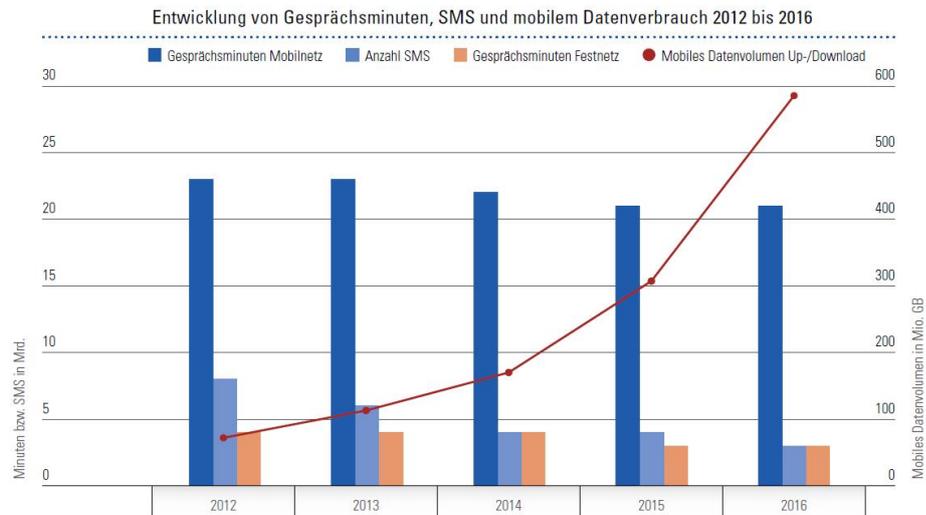
Eine Umfrage, die in 11 Mitgliedstaaten durchgeführt wurde, hat ergeben, dass Endnutzer OTT-Dienste in sehr hohem Ausmaß täglich oder fast täglich verwendet, angeführt von Spanien (70%), Niederlande (61%), Italien (57%) und Deutschland (51%).²⁷

In Österreich hat die Rundfunk und Telekom Regulierungs-GmbH, kurz RTR, eine Studie zur Nutzung von OTT-Diensten erstellt²⁸. In dieser Studie wird sehr genau beschrieben, wie der Verbrauch von Gesprächsminuten und SMS pro durchschnittlichen Endnutzer in den Jahren 2012 bis 2016 zurückgegangen und gleichzeitig der Bedarf an Datenvolumen drastisch steigt.

²⁶ VATM (2015), The OTT-challenge – OTTs verändern die Märkte. Onlinedokument: http://www.vatm.de/724.0.html?&tx_ttnews%5Btt_news%5D=2071&cHash=1721966e9bff7327487d1aa755cc1d34; Download am 17.07.2018.

²⁷ aaO, 7.

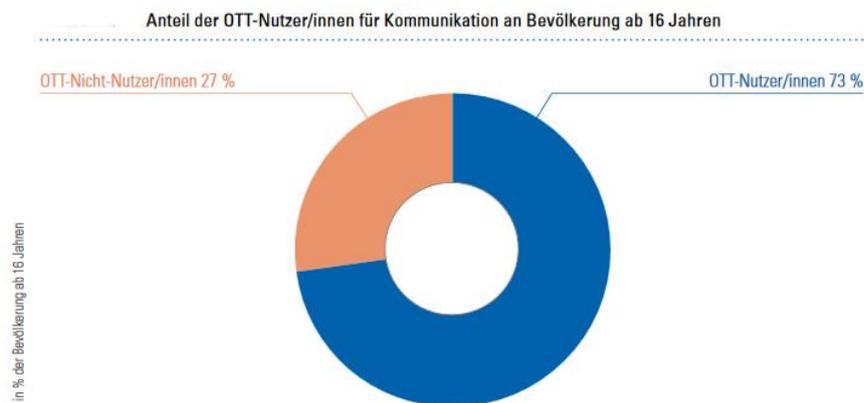
²⁸ RTR, Die Konkurrenz aus dem Netz, OTT-Dienste in Medien und Telekommunikation, Wien, Juni 2017.



→ Die Anzahl telefonierter Minuten und SMS sinkt, während der Verbrauch von mobilem Datenvolumen stark wächst.

Abbildung 1: Entwicklung von Gesprächsminuten, SMS und mobilem Datenverbrauch 2012 bis 2016, Die Konkurrenz aus dem Netz, 30.

Wie auch in der Umfrage der Europäischen Kommission nutzen auch Endnutzer in Österreich gerne Online-Dienste. 73% der befragten ÖsterreicherInnen ab 16 Jahren nutzen wie in der folgenden Grafik dargestellt OTT-Dienste.



→ Fast drei Viertel der österreichischen Bevölkerung ab 16 Jahren nutzen OTT-Dienste für Telekommunikation.

Abbildung 2: Anteil der OTT-Nutzer/Innen für Kommunikation an Bevölkerung ab 16 Jahren, Die Konkurrenz aus dem Netz, OTT-Dienste in Medien und Telekommunikation, 32.

Die beliebtesten OTT-Dienste sind in allen Altersgruppen WhatsApp, Facebook Messenger, Skype und Snapchat, wobei Snapchat bei den 16 bis 29-Jährigen beliebter als Skype ist.

Insgesamt werden mehr Nachrichten über OTT-Dienste versendet als über die herkömmlichen Netzbetreiber telefoniert wird. Ungefähr 80% der österreichischen OTT-NutzerInnen versenden OTT-Nachrichten mehrmals täglich oder nahezu täglich.

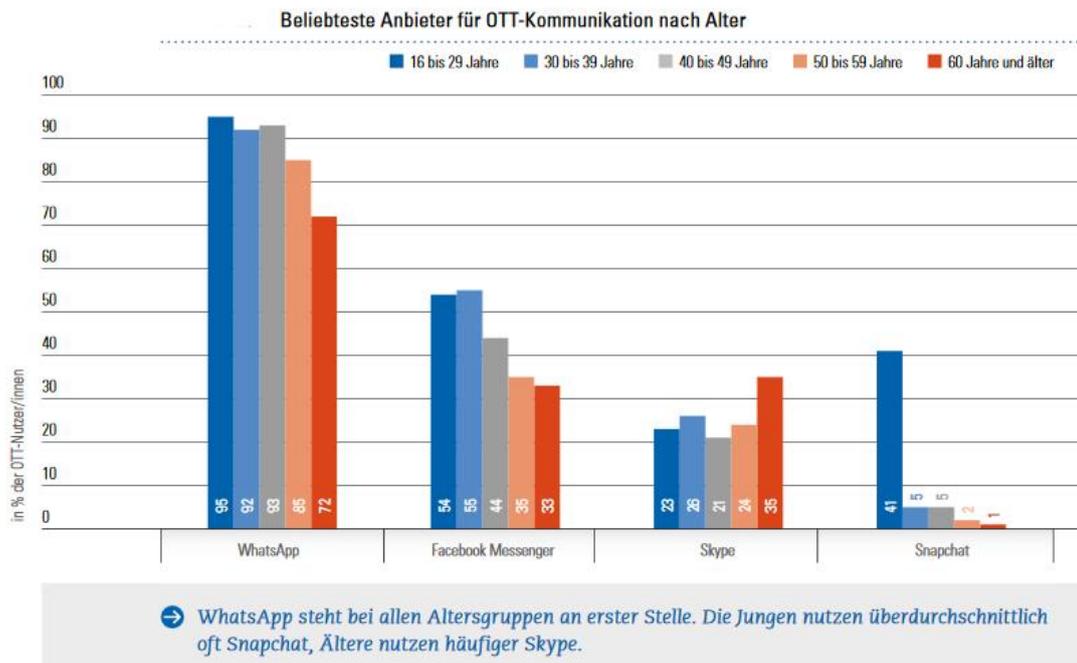


Abbildung 4: Beliebteste Anbieter für OTT-Kommunikation nach Alter, Die Konkurrenz aus dem Netz, OTT-Dienste in Medien und Telekommunikation, 39.

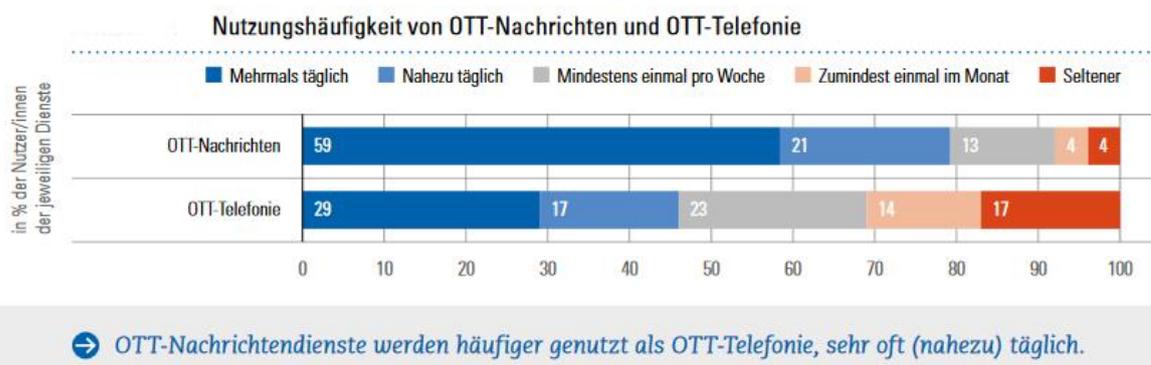


Abbildung 3: Nutzungshäufigkeit von OTT-Nachrichten und OTT-Telefonie, Die Konkurrenz aus dem Netz, OTT-Dienste in Medien und Telekommunikation, 35.

Die Wahrnehmung dieser Entwicklung ist sehr wichtig, da die aktuelle e-privacy Richtlinie ausschließlich Kommunikationsdaten reguliert hat, die klassische nummernbasierte Kommunikationsbetreiber verarbeitet haben. OTT-Dienste mussten sich ausschließlich an die weniger strenge Datenschutzrichtlinie halten. Zudem war die Datenschutzrichtlinie nicht für Unternehmen anwendbar, deren Sitz außerhalb der EU lag. Dies hat ein Ungleichgewicht zwischen den Anbietern geschaffen, da die Telekommunikationsbetreiber nicht nur die gesamte Infrastruktur für die Kommunikation geschaffen haben, sondern auch Beschränkungen bei der Verarbeitung der Daten unterliegen. Durch das Ungleichgewicht sind OTT-Dienste in der Lage den Endnutzern ein günstigeres Produkt als europäische Telekommunikationsanbieter, die der e-Privacy Richtlinie unterliegen, zu unterbreiten. Aus datenschutzrechtlicher Sicht ist dieser Rechtszustand fragwürdig, da das Kommunikationsgeheimnis unabhängig vom Kommunikationsdienst denselben Schutz erhalten sollte. Durch die derzeitige Regulierung ist es beispielsweise WhatsApp möglich Nutzerdaten zu Werbezwecken weiterzugeben²⁹. Ziel der DSGVO und e-privacy Verordnung ist es diesen Missstand zu beenden. Jede elektronische Kommunikation, unabhängig von Technologie und Anbieter, soll den gleichen Schutz von personenbezogenen Daten gewährleisten und somit soll ein level playing field zwischen den elektronischen Kommunikationsanbietern geschaffen werden.³⁰

Die e-privacy Verordnung ist jedoch in folgenden Fällen nicht anwendbar:

- a) Tätigkeiten, die nicht in den Anwendungsbereich des Unionsrechts fallen;
- aa) Tätigkeiten, die in den Anwendungsbereich der Sicherheit oder Verteidigung fallen³¹;
- b) Tätigkeiten der Mitgliedstaaten, die in den Anwendungsbereich von Titel V Kapitel 2 des Vertrages über die Europäische Union fallen;
- c) elektronische Kommunikationsdienste, die nicht öffentlich zugänglich sind;

²⁹ RTR, Die Konkurrenz aus dem Netz, OTT-Dienste in Medien und Telekommunikation, Wien, Juni 2017, 40.

³⁰ European Commission, Commission Staff Working Document, Impact Assessment, Accompanying the document Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications), Brussels, 10.01.2017, 7.

³¹ Ergänzung laut Änderungsvorschlag der bulgarischen Ratspräsidentschaft: Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) – Examination of the Presidency text; Brussels, 12. June 2018, 9958/18, Art 2 Abs 2, 41.

- d) Tätigkeiten zuständiger Behörden zu Zwecken der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit.
- e) Verarbeitung elektronische Kommunikationsinhalte, die vom Endnutzer selbst oder durch einen Dienstleister, der vom Endnutzer beauftragt wurde, die Daten nach ihrem Empfang aufzuzeichnen, zu speichern oder in anderer Weise zu verarbeiten³².

Art 2 Abs 2 Buchstabe c der e-privacy Verordnung bestimmt, dass elektronische Kommunikationsdienste, die nicht öffentlich zugänglich sind, nicht in den sachlichen Anwendungsbereich der Verordnung fallen. Hier stellen europäische Unternehmen in Frage ob die getroffene Formulierung eindeutig ist. Aufgrund ErwG 13 ist zu schließen, dass beispielsweise Unternehmensnetze, bei denen der Zugang auf die Angehörigen des Unternehmens beschränkt ist, unter Buchstabe c zu subsumieren sein könnten. Die getroffene Formulierung „nicht öffentlich zugänglich“ ist jedoch sehr weit gefasst und könnte auch bedeuten, dass solche Kommunikationsdienste nicht umfasst sind, für die eine eigene Anmeldung erforderlich ist. Somit würden gerade OTT-Dienste, die ein Anlass für die Regulierung sind, nicht in den Anwendungsbereich der e-Privacy Verordnung fallen, da gerade sie in der Regel immer eine Anmeldung oder Registrierung verlangen.³³

In ErwG 12 wird klargestellt, dass auch die M2M – Kommunikation in den Anwendungsbereich dieser Verordnung fällt. Geräte und Maschinen kommunizieren in der heutigen Zeit immer mehr miteinander, diese Kommunikation ist vor allem für das Internet der Dinge notwendig. Um das Recht auf Privatsphäre und die Vertraulichkeit der Kommunikation vollständig gewährleisten zu können, ist auch der Datenschutz im Internet der Dinge sicherzustellen, damit der Kommunikationsanbieter den Inhalt der Kommunikation nicht kennt.

2.3 räumlicher Anwendungsbereich

Art 3 regelt den räumlichen Anwendungsbereich der e-privacy Verordnung. Übereinstimmend mit der DSGVO ist die e-Privacy Verordnung für jede Bereitstellung elektronischer

³² aaO, 41.

³³ Schubert, Maximilian (2017): ISPA Stellungnahme betreffend den Entwurf der Verordnung über Privatsphäre und elektronische Kommunikation (e-Privacy-VO). Onlinedokument: https://www.ispa.at/filedl/0/0/1498408297/530f4cf428655c3a6477cca77f252c970e16925f/filadmin/content/5_Wissenspool/Stellungnahmen/2017/20170317_BMvit_E-Privacy/201703013_ISPA_Stellungnahme_E-Privacy_final.pdf; Download am 15.07.2017.

Kommunikationsdienste für Endnutzer innerhalb der EU anwendbar, unabhängig davon wo sich der Betreiber befindet. Ausschlaggebend ist, dass die jeweilige Dienstleistung wie beispielsweise der Kommunikationsdienst dem Endnutzer innerhalb der EU angeboten wird. Hierbei gibt es keine Unterscheidung, ob für die Erbringung der Kommunikationsdienstleistung eine Bezahlung verlangt wird oder nicht.³⁴ Die Europäische Kommission stellt im Entwurf der Richtlinie über den europäischen Kodex für die elektronische Kommunikation, kurz EECC³⁵, klar, dass elektronische Kommunikationsdienste oft nicht mehr gegen Entgelt erbracht werden, sondern vielmehr personenbezogene Daten oder Werbung als Gegenleistung verlangen³⁶. Aus diesem Grund werden auch diese Gegenleistungen als Entgelt gewertet. Des Weiteren werden auch Informationen in Bezug auf die Endeinrichtungen der Endnutzer, öffentliche Verzeichnisse oder auch das Übermitteln von Direktmarketing an Endnutzer innerhalb der EU geschützt³⁷.

Ist der Betreiber nicht innerhalb der EU niedergelassen, so hat er schriftlich einen Vertreter in der EU zu benennen³⁸. Hierbei muss sich der Vertreter in einem Mitgliedsstaat befinden, indem sich auch Endnutzer des jeweiligen Kommunikationsdienstes befinden³⁹. Der Vertreter muss gemäß Art 3 Abs 4 der e-Privacy Verordnung befugt sein für alle Belange im Zusammenhang mit der Verarbeitung elektronischer Kommunikationsdaten Fragen zu beantworten sowie Auskünfte zu erteilen.

Im Änderungsentwurf der bulgarischen Präsidentschaft wurde eine Ausnahme für das Erfordernis der Bestellung eines Vertreters hinzugefügt, die vor allem beim Direktmarketing durch Unternehmen, mit Sitz außerhalb der EU zur Anwendung kommen könnte. Findet die Datenverarbeitung nur gelegentlich statt und besteht für den Endnutzer mit hoher Wahrscheinlichkeit keinerlei Risiko in der Datenverarbeitung durch die Art, die Umstände, dem

³⁴ Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über die Achtung des Privatlebens und den Schutz personenbezogener Daten in der elektronischen Kommunikation und zur Aufhebung der Richtlinie 2002/58/EG (Verordnung über Privatsphäre und elektronische Kommunikation), Brüssel, 10.01.2017, Art 3 Abs 1 Buchstabe a.

³⁵ Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über den europäischen Kodex für die elektronische Kommunikation, kurz EECC, Brüssel, 12.10.2016.

³⁶ aaO, ErwG 16.

³⁷ Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über die Achtung des Privatlebens und den Schutz personenbezogener Daten in der elektronischen Kommunikation und zur Aufhebung der Richtlinie 2002/58/EG (Verordnung über Privatsphäre und elektronische Kommunikation), Brüssel, 10.01.2017, Art 3 Abs 1 Buchstabe c.

³⁸ aaO, Art 3 Abs 2.

³⁹ aaO, Art 3 Abs 3.

Umfang oder den Zweck der Datenverarbeitung, so muss durch den Verantwortlichen der Datenverarbeitung kein Vertreter bestellt werden. Diese Regelung entspricht auch Art 27 Abs 2 lit a DSGVO, die bestimmt, dass ein Verantwortlicher einer Datenverarbeitung, der nicht in der Union niedergelassen ist, keinen Vertreter ernennen muss, wenn die Datenverarbeitung nur gelegentlich erfolgt, keine Daten im Sinne des Art 9 Abs 1 oder Art 10 DSGVO verarbeitet werden sowie unter Berücksichtigung der Art, der Umstände, dem Umfang und der Zwecke der Verarbeitung voraussichtlich kein Risiko für die Rechte und Freiheiten des Betroffenen besteht.

Art 4 der e-privacy Verordnung erklärt die Begriffsbestimmungen. Hier ist darauf hinzuweisen, dass die Begriffe des Art 4 Abs 1 Buchstabe b „elektronisches Kommunikationsnetz“, „elektronischer Kommunikationsdienst“, „interpersoneller Kommunikationsdienst“, „nummerngebundener interpersoneller Kommunikationsdienst“, „nummernunabhängiger interpersoneller Kommunikationsdienst“, „Endnutzer“ und „Anruf“ nicht in der Verordnung selbst erklärt werden, sondern auf den EECC verwiesen wird. Hierbei ist anzumerken, dass sich dieser Kodex bei Erstellung des Entwurfs ebenfalls im Entwurfsstadium befand. Da die e-Privacy Verordnung nicht zum geplanten Termin, dem 25. Mai 2018 fertig verhandelt wurde und in Kraft getreten ist, hat sich diese Situation bereits entschärft. Mittlerweile besteht eine endgültige Version des EECC, auf die sich die Europäische Kommission, das Europäische Parlament und der Europäische Rat einigen konnten⁴⁰. Dieser Entwurf soll noch 2018 beschlossen werden. Zum Zeitpunkt, in dem der Entwurf der e-Privacy Verordnung veröffentlicht wurde, hat der Verweis auf eine Richtlinie, die sicherlich nicht vor Mai 2018 fertig verhandelt ist, viele Unsicherheiten geschaffen. Dies wurde in sämtlichen Stellungnahmen, sowohl von der Artikel 29 – Datenschutzgruppe⁴¹ sowie auch Kommunikationsbetreiber und deren Interessensvertretungen⁴² stark kritisiert.

⁴⁰ Lechien, Oliver, GSMA (2018); GSMA comments on the Agreement on EECC: Europe passes up opportunity to demonstrate 5G Leadership. Onlinedokument: <https://www.gsma.com/gsmaeurope/whats-new/gsma-comments-on-the-agreement-on-eecc/>; Download am 23.07.2018.

⁴¹ Article 29 Data Protection Working Party, Opinion 01/2017 on the Proposed Regulation for the e-Privacy Regulation (2002/58/EC), 2017, 23.

⁴² Pöchersdorfer, Winfried, Vorschlag der Europäischen Kommission für die Überarbeitung der Richtlinie über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation – Richtlinie 2002/58/EG, COM (2017) 10 final v 10.01.2017 [Vorschlag EK-DSVO] – Stellungnahme, 10.04.2017, 2.

Die e-privacy Verordnung unterscheidet zwischen elektronischen Kommunikationsdaten, Kommunikationsinhalten und Kommunikationsmetadaten. Der neue Begriff „Kommunikationsmetadaten“ löst den Begriff „Verkehrsdaten“ der e-Privacy Richtlinie ab und bezeichnet laut der Definition in Art 4 Abs 3 lit c e-Privacy Verordnung sämtliche Daten, die in einem Kommunikationsnetz „zur Verfolgung und Identifizierung des Ausgangs- und Zielpunkts einer Kommunikation verwendete Daten, die im Zusammenhang mit der Bereitstellung elektronischer Kommunikationsdienste erzeugten Daten über den Standort des Geräts sowie Datum, Uhrzeit, Dauer und Art der Kommunikation“.

Die Art 29 Gruppe befürchtet in ihrer Stellungnahme zum Entwurf der Verordnung, dass der neue Begriff der Kommunikationsmetadaten doch enger als der Begriff der Verkehrsdaten definiert wurde. Es könnte davon ausgegangen werden, dass nur die unterste Ebene eines Netzwerks als Metadaten qualifiziert werden würden. Das könnte dazu führen, dass die von OTT verarbeiteten Daten gar nicht mehr unter den Begriff der Kommunikationsmetadaten fallen würden. Die Definition in Art 4 Abs 3 lit c sollte somit alle verarbeiteten personenbezogenen Daten umfassen, die für den Zweck der Übermittlung, Verbreitung oder des Austauschs von Kommunikationsinhalten erfüllen⁴³.

Mit den Änderungen der e-Privacy Verordnung ist der Europäische Rat auf diese Bedenken eingegangen. Der Begriff der Kommunikationsmetadaten wurde auf alle Kommunikationsdienste ausgeweitet und beschränkt sich nicht mehr ausschließlich um die Daten, die innerhalb eines Kommunikationsnetzes verarbeitet werden⁴⁴.

Unter elektronische Kommunikationsinhalte sind alle Inhalte zu verstehen, die mittels elektronischer Kommunikationsdienste übermittelt werden, wie der Text einer SMS, Telefongespräche, Videos, Bilder oder Tonaufnahmen.⁴⁵

⁴³ Article 29 Data Protection Working Party, Opinion 01/2017 on the Proposed Regulation for the ePrivacy Regulation (2002/58/EC), 2017, 16.

⁴⁴ Proposal for a regulation of the European Parliament and the Council concerning the respect for private life and protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) - Examination of the Presidency text, Brussels, 12. June 2018, 9958/18, 45.

⁴⁵ Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über die Achtung des Privatlebens und den Schutz personenbezogener Daten in der elektronischen Kommunikation und zur Aufhebung der Richtlinie 2002/58/EG (Verordnung über Privatsphäre und elektronische Kommunikation), Brüssel, 10.01.2017, Art 4 Abs 3 lit c.

Der Begriff elektronische Kommunikationsdaten umfasst die Begriffe Kommunikationsinhalte und Kommunikationsmetadaten. Wie bereits in Kapitel 2.2 beschrieben, werden die Begriffe absichtlich sehr allgemein formuliert, um sowohl die klassischen Telekommunikationsdienste, als auch OTT-Dienste von der Regulierung zu umfassen.

3. Schutz der elektronischen Kommunikation

3.1 Vertraulichkeit elektronischer Kommunikationsdaten

Art 5 der e-privacy Verordnung ersetzt Art 5 der e-privacy Richtlinie und regelt weiterhin die Vertraulichkeit der Kommunikation. Mit dieser Bestimmung wird das Grundrecht auf das Kommunikationsgeheimnis des Art 7 GRCh gewährleistet und schützt Endnutzer vor Eingriffen in elektronische Kommunikationsdaten durch Mithören, Abhören, Speichern, Beobachten, Scannen oder andere Arten des Abfangens oder Überwachens bzw. jegliche andere Verarbeitung von elektronischer Kommunikationsdaten durch andere Personen als die Endnutzer selbst, sofern der Endnutzer einer Verarbeitung nicht zustimmt oder dies nicht durch diese Verordnung erlaubt wird.

Das Kommunikationsgeheimnis ist in Österreich in § 93 TKG bereits umgesetzt worden. In Abs 1 wird hier klargestellt, dass sämtliche Datenarten und somit Inhaltsdaten und Verkehrsdaten inklusive Standortdaten dem Kommunikationsgeheimnis unterliegen. Dies gilt jedoch nicht bei der Rückverfolgung von Notrufen, bei Aufzeichnungen im Rahmen einer Fangschaltung, der Überwachung nach § 11 Abs 1 Z 7 PStSG sowie wenn eine Speicherung für die Erbringung des Kommunikationsdienstes aus technischen Gründen notwendig ist⁴⁶.

Kommunikationsbetreiber vertreten die Position, dass ausschließlich die Bestimmung des Art 5 der e-Privacy Verordnung auch für juristische Personen anwendbar sein sollte⁴⁷ und nicht wie geplant, die gesamte Verordnung. Hier wird eine Gleichstellung zur DSGVO angestrebt. Kommunikationsbetreiber sehen hier einen Wettbewerbsnachteil gegenüber anderen Unternehmen, die nicht von der e-Privacy reguliert werden. Hinzu kommt, dass die Kommunikation nicht mehr unbedingt zwischen zwei Menschen stattfinden muss. Bei einer M2M – Kommunikation werden oft nur Befehle oder gewisse Messwerte ausgetauscht. Hier besteht kein Eingriff in die Privatsphäre einer einzelnen Person. Jedoch könnten auch Geschäftsgeheimnisse von Unternehmen betroffen sein, die ebenfalls geschützt werden sollten. Diese Fragen hat sich vor allem der Europäische Rat während der estnischen Ratspräsidentschaft

⁴⁶ § 93 Abs 3 TKG

⁴⁷ Pöchersdorfer, Winfried, Vorschlag der Europäischen Kommission für die Überarbeitung der Richtlinie über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation – Richtlinie 2002/58/EG, COM (2017) 10 final v 10.01.2017 [Vorschlag EK-DSVO] – Stellungnahme, 10.04.2017, 3.

gestellt. Es wurde auch ein zweiter Absatz hinzugefügt, der regelt, dass bei der M2M - Kommunikation der Art 5 der e-Privacy Verordnung nur dann anwendbar sein soll, wenn sich die Kommunikation auf einen Endnutzer bezieht und durch einen elektronischen Kommunikationsdienst erbracht wird⁴⁸. Dieser Vorschlag wurde bereits nach einem Monat abgeändert und der Bezug auf den Endnutzer entfernt⁴⁹. Durch diesen Entwurf wurde nun auch klargestellt, dass das Kommunikationsgeheimnis auch für die M2M – Kommunikation anzuwenden ist. Dies wurde vorher ausschließlich im ErwG 12 beschrieben, jedoch nicht im eigentlichen Verordnungstext. Jedoch wurde der gesamte Abs 2 in der bulgarischen Ratspräsidentschaft wieder gestrichen⁵⁰.

Wenn die Kommunikation der Endnutzer vertraulich ist, stellt sich die Frage, wie eine Überwachung der Telekommunikation oder die Einführung von Bundestrojanern, die in Deutschland⁵¹ und Österreich⁵² rechtlich möglich sein kann. Bereits jetzt ist es den Sicherheitsbeamten rechtlich möglich auf Stammdaten, Verkehrsdaten sowie Inhaltsdaten innerhalb des Telekommunikationsdienstes zuzugreifen. In Österreich wird die Überwachung in § 94 TKG geregelt und bestimmt, dass Telekommunikationsanbieter Einrichtungen bereitzustellen haben, die zur Überwachung von Nachrichten und zur Auskunft über Daten einer Nachrichtenübermittlung dienen. Diese Bestimmung wurde nun ausgedehnt, da auch Kriminelle und Terroristen immer mehr auf OTT-Dienste gewechselt haben und somit laut den Behörden eine ausreichende Überwachung nicht mehr möglich war. Der Wechsel auf OTT-Dienste erleichtert nicht nur die internationale Kommunikation, sondern verhindert auch das Mithören,

⁴⁸ Proposal for a regulation of the European Parliament and the Council concerning the respect for private life and protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) - Examination of the Presidency text, Brussels, 08. September 2017, 11995/17, 17.

⁴⁹ Proposal for a regulation of the European Parliament and the Council concerning the respect for private life and protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) - Examination of the Presidency text, Brussels, 06. October 2017, 12955/17, Art 5, 20.

⁵⁰ Proposal for a regulation of the European Parliament and the Council concerning the respect for private life and protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) - Examination of the Presidency text, Brussels, 12. June 2018, 9958/18, Art 5, 48.

⁵¹ Flade, Florian, Welt (19.06.2017); Bei WhatsApp und Co. muss der Staat selbst zum Hacker werden. Onlinedokument: <https://www.welt.de/politik/deutschland/article165688690/Bei-WhatsApp-und-Co-muss-der-Staat-selbst-zum-Hacker-werden.html>; Download am 18.07.2017.

⁵² Standard (06.07.2017), Doppelmord in Linz: Sobotka fordert erneut Whatsapp-Überwachung. Onlinedokument: <http://derstandard.at/2000060900352/Doppelmord-in-Linz-Sobotka-fordert-erneut-WhatsApp-Ueberwachung?ref=rec>; Download am 18.07.2017.

Beobachten und Überwachen durch die Sicherheitsbehörden. Der Einsatz von sogenannten Bundestrojanern ist unter den Datenschutzrechtlern sehr umstritten⁵³, aber rechtlich möglich, da Art 1 Abs 3 der e-Privacy Richtlinie bestimmt, dass sie nicht anwendbar ist, solange es sich um Tätigkeiten zuständiger Behörden handelt um Straftaten zu verhindern, ermitteln, aufzudecken oder zu verfolgen, einschließlich zur Abwehr von Gefahren für die öffentliche Sicherheit. Dies wird auch in Art 2 Abs 2 lit d im Entwurf der e-Privacy Verordnung erlaubt.

Die Art 29 hat in ihrer Erklärung vom April 2018⁵⁴ klar und deutlich gemacht, dass die gesamte Kommunikation „end-to-end“ verschlüsselt sein muss, damit keine Kommunikation abgefangen oder abgehört werden kann. Die Art 29 Gruppe stellt fest, dass eine verschlüsselte und sichere Kommunikation im öffentlichen Interesse durch die die Hersteller der Endeinrichtungen sowie die Betreiber der Kommunikationsdienste gewährleistet werden muss und Stand der Technik werden sollte⁵⁵. Es wird auch darauf hingewiesen, dass das Einführen von sogenannten „Hintertüren“ bei der Verschlüsselung in der Vergangenheit zu großen Schäden geführt haben, wie beispielsweise der „WannaCry“-Virus, der über 230.000 Computer in 150 Länder infiziert hat⁵⁶. Die Sicherheitslücke wurde von einer großen nationalen Sicherheitsbehörde geschaffen, die dann von Kriminellen als Hackingwerkzeug benutzt wurde um die „WannaCry“ - Ransomware zu erstellen⁵⁷. Die Art 29 Gruppe erklärt sich streng gegen die Idee, dass Mitgliedstaaten genau diese Hintertüren als Bundestrojaner zur Überwachung von Kriminellen verwenden, da so auch immer Sicherheitslücken bestehen bleiben, die allen Endnutzern schaden.

⁵³ Epicenter.Works, (10.07.2017), Österreich steht vor beispielloser Ausweitung des Überwachungsstaats. Onlinedokument: <https://epicenter.works/content/oesterreich-steht-vor-beispielloser-ausweitung-des-ueberwachungsstaats>; Download am 18.07.2017.

⁵⁴ Article 29 Data Protection Working Party, Andrea Jelinek, (11. April 2018), Statement of the WP29 on encryption and their impact on the protection of individuals with regard to the processing of their personal data in the EU. Onlinedokument: [https://iapp.org/media/pdf/resource_center/20180413_Article29WPStatementonencryptionP rivacypdf%20\(1\).pdf](https://iapp.org/media/pdf/resource_center/20180413_Article29WPStatementonencryptionP rivacypdf%20(1).pdf); Download am 31.07.2018.

⁵⁵ aaO, 1.

⁵⁶ Der Standard (28. Oktober 2017), „Wanna Cry“: Mindestmaß an IT-Security hätte Chaos verhindert. Onlinedokument: <https://derstandard.at/2000066778145/WannaCry-Mindestmass-an-IT-Security-haette-Chaos-verhindert>; Download am 31.07.2018.

⁵⁷ Article 29 Data Protection Working Party, Andrea Jelinek, (11. April 2018), Statement of the WP29 on encryption and their impact on the protection of individuals with regard to the processing of their personal data in the EU. Onlinedokument: [https://iapp.org/media/pdf/resource_center/20180413_Article29WPStatementonencryptionP rivacypdf%20\(1\).pdf](https://iapp.org/media/pdf/resource_center/20180413_Article29WPStatementonencryptionP rivacypdf%20(1).pdf); Download am 31.07.2018, 2.

Die Mitgliedstaaten sollten stattdessen ihre bestehenden rechtlichen Möglichkeiten ausnutzen und nicht zusätzliche Sicherheitslücken schaffen⁵⁸.

3.2 Erlaubte Verarbeitung elektronischer Kommunikationsdaten

Um als Verantwortlicher⁵⁹ einer Datenverarbeitung personenbezogene Daten entsprechend der DSGVO verarbeiten zu dürfen, muss im ersten Schritt ein eindeutig festgelegter Zweck für die Verarbeitung der Daten definiert werden, der im zweiten Schritt einer rechtlichen Grundlage gemäß Art 6 Abs 1 DSGVO zugeordnet wird. Die DSGVO zählt sechs rechtliche Grundlagen für die Verarbeitung von personenbezogenen Daten taxativ auf, wobei immer mindestens eine davon zutreffen muss. Rechtliche Grundlagen sind unter folgenden Voraussetzungen gegeben:

- a) die Einwilligung, die freiwillig und aktiv durch die betroffene Person für einen oder mehrere bestimmte Zwecke gegeben wird;
- b) die Verarbeitung dient zur Erfüllung eines Vertrages, dessen Vertragspartei die betroffene Person ist bzw. die Verarbeitung ist zur Durchführung vorvertraglicher Maßnahmen erforderlich;
- c) die Verarbeitung ist zur Erfüllung einer rechtlichen Verpflichtung erforderlich, der der Verantwortliche unterliegt;
- d) die Verarbeitung ist erforderlich, um lebenswichtige Interessen der betroffenen Person oder einer anderen natürlichen Person zu schützen;
- e) die Verarbeitung ist für die Wahrnehmung einer Aufgabe erforderlich, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde;
- f) die Verarbeitung ist zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen, insbesondere dann, wenn es sich bei der betroffenen Person um ein Kind handelt.

⁵⁸ aaO, 3.

⁵⁹ Gemäß Art 4 Ziffer 7 DSGVO ist der „Verantwortliche“ eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet; sind die Zwecke und Mittel dieser Verarbeitung durch das Unionsrecht oder das Recht der Mitgliedstaaten vorgegeben, so kann der Verantwortliche beziehungsweise können die bestimmten Kriterien seiner Benennung nach dem Unionsrecht oder dem Recht der Mitgliedstaaten vorgesehen werden.

Die bestehende e-privacy Richtlinie und auch der Entwurf der e-privacy Verordnung schränken jeweils in Art 6 die Verarbeitung elektronischer Kommunikationsdaten im Vergleich zur DSGVO sehr stark ein und geben ganz genau vor, welche personenbezogenen Daten für welche Zwecke verarbeitet werden dürfen.

Gemäß Art 6 Abs 1 des Entwurfs der e-privacy Verordnung dürfen elektronische Kommunikationsdaten ausschließlich zur Übermittlung der Kommunikation und für die hierfür notwendige Dauer (lit a) sowie für die „Aufrechterhaltung oder Wiederherstellung der Sicherheit der elektronischen Kommunikationsnetze und -dienste oder zur Erkennung von technischen Defekten und Fehlern bei der Übermittlung“ und für die hierfür notwendige Dauer (lit b) verarbeitet werden.

Elektronische Kommunikationsmetadaten dürfen gemäß Art 6 Abs 2 des ersten Entwurfes der Europäischen Kommission ausschließlich zur Einhaltung verbindlicher Dienstqualitätsanforderungen nach dem EECC (lit a), zur Rechnungslegung, Berechnung von Zusammenschaltungszahlungen und Vermeidung von betrügerischer oder missbräuchlicher Nutzung (lit b) bzw. für jene Fälle, in denen der Endnutzer seine Einwilligung zur Verarbeitung seiner Kommunikationsmetadaten für einen oder mehrere bestimmte Zwecke gegeben hat, sofern die betreffenden Zwecke nicht durch die Verarbeitung von anonymen Daten erreicht werden können (lit c), verarbeitet werden.

Gerade die Bestimmung des lit c zeigt, dass die Privatsphäre der Endnutzer am besten geschützt wird, wenn die Daten entweder gelöscht oder anonymisiert werden. Dies führt eben auch dazu, dass Betreiber von Kommunikationsdiensten die Einholung einer Einwilligung zur Verarbeitung von Kommunikationsmetadaten gar nicht erlaubt ist, wenn der Zweck auch mit anonymen Daten erreicht werden könnte.

Vor allem diese Bestimmung ist für alle Kommunikationsanbieter sehr wichtig, da gerade die Kommunikationsmetadaten für Big Data – Anwendungen essentiell sind. Denn genau diese Daten beinhalten sämtliche Informationen zur Verfolgung und Identifizierung des Ausgangs- und Zielpunkts einer Kommunikation bzw. den Standort eines Endgeräts⁶⁰. Viele Unternehmen

⁶⁰ Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über die Achtung des Privatlebens und den Schutz personenbezogener Daten in der elektronischen Kommunikation und zur Aufhebung der Richtlinie 2002/58/EG (Verordnung über Privatsphäre und elektronische Kommunikation), Brüssel, 10.01.2017, Art4 Abs 3 lit c S 2.

erhoffen sich mit Hilfe dieser Daten neue Geschäftsmodelle schaffen zu können. Ob und in welchem Umfang Kommunikationsmetadaten genutzt werden können, bestimmt die Regulierung der e-privacy, da sie gegenüber der DSGVO als *lex specialis* anzusehen ist und viel strengere Maßstäbe ansetzt. Aus diesem Grund wird diese Bestimmung von den Kommunikationsbetreibern als ein Wettbewerbsnachteil gegenüber anderen Unternehmen kritisiert, die ausschließlich den allgemeinen Datenschutzbestimmungen der DSGVO unterliegen. Diese haben nämlich gemäß den Grundsätzen der DSGVO die Möglichkeit auch zusätzliche Sicherheitsmaßnahmen zur Reduktion des Risikos der Rechte und Freiheiten der betroffenen Person einzusetzen, wie beispielsweise die Pseudonymisierung oder Verschlüsselung von personenbezogenen Daten⁶¹. Durch die Pseudonymisierung kann ein Risiko für die Rechte und Freiheiten der betroffenen Person abgemildert werden, indem die betroffene Person „nur unter Hinzuziehung der gesondert aufbewahrten ... Informationen wieder identifiziert werden“ können⁶². Wird das Risiko durch geeignete Garantien, Verschlüsselung oder Pseudonymisierung reduziert, so ist gemäß Art 6 Abs 4 lit e DSGVO die Verarbeitung von personenbezogenen Daten, die zu einem anderen Zweck erhoben wurden, erlaubt, wenn der ursprüngliche Zweck mit dem neuen Zweck vereinbar bzw. kompatibel ist.

Mit Hilfe solcher Maßnahmen entstehen für Unternehmen neue Geschäftsmodelle, die beispielsweise die Verfolgung von Menschenströmen durch Kommunikationsmetadaten. Würde man den Personenbezug sofort löschen, könnte die Bewegung der einzelnen Person nicht nachverfolgt werden, sondern nur wissen, dass sich eine Person an einem Punkt aufgehalten hat. Die einzelnen Punkte könnten aber nicht miteinander verbunden werden. In diesem Beispiel ist es nicht interessant, welche Person sich genau von einem Ort zu einem anderen Ort bewegt. Es ist nur die Bewegung an sich interessant.

Der Entwurf der e-privacy Verordnung kennt jedoch keine solchen Sicherheitsmaßnahmen, die eine Datenverarbeitung für andere Zwecke erlaubt, als die in Art 6 beschrieben. Möchte der

⁶¹ Pöcherstorfer, Winfried, Vorschlag der Europäischen Kommission für die Überarbeitung der Richtlinie über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation – Richtlinie 2002/58/EG, COM (2017) 10 final v 10.01.2017 [Vorschlag EK-DSVO] – Stellungnahme, 10.04.2017, 3.

⁶² Schwartmann / Weiß (Hrsg.), 2017: Whitepaper zur Pseudonymisierung der Fokusgruppe Datenschutz der Plattform Sicherheit, Schutz und Vertrauen für Gesellschaft und Wirtschaft im Rahmen des Digital-Gipfels 2017 – Leitlinien für die rechtssichere Nutzung von Pseudonymisierungslösungen unter Berücksichtigung der Datenschutz-Grundverordnung, Kölner Forschungsstelle für Medienrecht, Köln.

Kommunikationsbetreiber Kommunikationsmetadaten für andere Zwecke verarbeiten, so ist eben eine Einwilligung vom Endnutzer einzuholen. Aufgrund dieser Situation fordern die betroffenen Unternehmen die Anwendbarkeit sämtlicher Rechtfertigungsgründe, die in Art 6 DSGVO vorgesehen sind, vor allem des berechtigten Interesses gemäß Art 6 Abs 1 lit f DSGVO für die Datenverarbeitung⁶³.

Die Artikel 29 Gruppe sieht den Entwurf der e-privacy Verordnung problematisch und verlangt nicht nur die Zustimmung des Endnutzers, sondern auch die Zustimmung sämtlicher betroffenen Personen⁶⁴. Kommunikationsmetadaten beinhalten nicht nur personenbezogene Daten des Kunden des Kommunikationsbetreibers, sondern auch seiner Gesprächspartner. Nach Ansicht der Artikel 29 Gruppe sind Sender und Empfänger einer Kommunikationsverbindung gleichwertig zu schützen. Eine solche Forderung stellen Unternehmen in Frage, da beispielsweise für die Anwendung einer Anti-Spam-Software nicht nur der Nutzer, sondern auch der Absender um Einwilligung für die Zuordnung einer Nachricht als Spam gefragt werden müsste. Eine solche Regelung würde einige Produkte, die es bereits am Markt gibt und dem Nutzer dienen sollen, verhindern⁶⁵.

Die Artikel 29 Gruppe sieht ausschließlich unter folgenden Voraussetzungen eine Ausnahme für die Notwendigkeit der Einholung von Einwilligungen durch die betroffenen Personen⁶⁶:

- Der Zweck der Datenverarbeitung ist ausschließlich die statistische Zählung oder für Sicherheitsüberprüfungen.
- Die Daten werden unmittelbar nach Auswertung gelöscht oder anonymisiert.
- Das Prinzip der Datenminimierung der DSGVO muss eingehalten werden⁶⁷.

⁶³ Pöcherstorfer, Winfried, Vorschlag der Europäischen Kommission für die Überarbeitung der Richtlinie über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation – Richtlinie 2002/58/EG, COM (2017) 10 final v 10.01.2017 [Vorschlag EK-DSVO] – Stellungnahme, 10.04.2017, 3.

⁶⁴ Article 29 Data Protection Working Party, Opinion 01/2017 on the Proposed Regulation for the ePrivacy Regulation (2002/58/EC), 2017, 13.

⁶⁵ EuroISPA, Mai 2017: Position about ePrivacy Regulation concerning the respect of private life and the protection of personal data in electronic, 4.

⁶⁶ Article 29 Data Protection Working Party, Opinion 01/2017 on the Proposed Regulation for the ePrivacy Regulation (2002/58/EC), 2017, 12.

⁶⁷ Art 5 Abs 1 lit c DSGVO beschreibt das Prinzip der Datenminimierung: Personenbezogene Daten müssen dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein.

- Es gibt für die betroffenen Personen eine Möglichkeit der Datenverarbeitung zu widersprechen.
- Es muss dem Recht auf Information gemäß Art 13 und 14 DSGVO entsprochen werden.

Im Laufe der Verhandlungen des Entwurfstextes zur e-privacy Verordnung wurde dieser Absatz einige Male abgeändert. Im Verordnungsentwurf der österreichischen Ratspräsidentschaft wurden die Zwecke, in denen Kommunikationsmetadaten verarbeitet werden dürfen ein weiteres Mal erweitert⁶⁸.

Laut des österreichischen Vorschlags zur e-Privacy Verordnung wird vorgeschlagen, dass die Kommunikationsmetadaten für folgende Zwecke entsprechend der Grundsätze der Datenminimierung und Speicherbegrenzung nur in einem Umfang und Dauer wie für die Zweckerfüllung notwendig verarbeiten dürfen:

- lit a) Zur Erfüllung des Netzwerkmanagements oder der Optimierung des Netzwerks, insofern der Zweck nicht mit anonymen Daten erfüllt werden kann sowie zur Erfüllung der Anforderungen, die im EECC und in der Verordnung (EU)2015/2120⁶⁹ vorgegeben sind;
- lit b) Zur Berechnung und Abrechnung von Rechnungen von Interconnection – Zahlungen. Hierbei handelt es sich um Abrechnungen zwischen Kommunikationsbetreibern, wenn ein Endkunde das Netz eines anderen Betreibers nutzt. Dies ist beispielsweise beim Roaming der Fall. Dieser Änderungsvorschlag ist für die Kommunikationsbetreiber sehr wichtig, da sonst die Verrechnung dieser Zahlungen keine rechtliche Grundlage hätten. Des Weiteren ist eine Verarbeitung von Kommunikationsmetadaten zur Vertragserfüllung mit dem Endnutzer erlaubt, wenn dies zur Rechnungslegung bzw. zur Erkennung und Verhinderung von betrügerischer oder missbräuchlicher Nutzung dient;

⁶⁸ Proposal for a regulation of the European Parliament and the Council concerning the respect for private life and protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) - Examination of the Presidency text, Brussels, 10 July 2018, 10975/18, Art 6 Abs 2, 18.

⁶⁹ Verordnung (EU) 2015/2120 des Europäischen Parlaments und des Rates vom 25. November 2015 über Maßnahmen zum Zugang zum offenen Internet und zur Änderung der Richtlinie 2002/22/EG über den Universaldienst und Nutzerrechte bei elektronischen Kommunikationsnetzen und -diensten sowie der Verordnung (EU) Nr. 531/2012 über das Roaming in öffentlichen Mobilfunknetzen in der Union, ABl. L 2015/310, 1ff.

- lit c) Der Endnutzer seine explizite Einwilligung für die Verarbeitung der Daten zu einem oder mehrere eindeutig festgelegte Zwecke erteilt, vorausgesetzt die Zwecke können nicht mit Hilfe von anonymen Daten erfüllt werden;
- lit d) Zum Schutz lebenswichtiger Interessen einer natürlichen Person im Notfall auf Anfrage einer zuständigen Behörde im Einklang mit dem Recht der Europäischen Union oder des jeweiligen Mitgliedstaates;
- lit f) Zur statistischen Zählung oder für wissenschaftliche Forschungszwecke, vorausgesetzt, diese beruhen auf dem Recht der Europäischen Union oder dem jeweiligen Mitgliedstaat. Die Verarbeitung muss verhältnismäßig sein und es sind geeignete Maßnahmen wie Verschlüsselung oder Pseudonymisierung zum Schutz der Grundrechte und der Interessen des einzelnen Endnutzers einzusetzen. Die Bestimmungen des Art 21 Abs 6 sowie Art 89 Abs 1, 2 und 4 DSGVO sind bei diesen Datenverarbeitungen anzuwenden. Demzufolge ist gemäß Art 21 Abs 6 DSGVO den betroffenen Endnutzern ist ein Widerspruchsrecht einzuräumen, es sei denn, die Verarbeitung ist zur Erfüllung einer im öffentlichen Interesse liegenden Aufgabe erforderlich. Art 89 DSGVO bestimmt, dass bei der Verarbeitung im öffentlichen Interesse, zu wissenschaftlichen oder historischen Forschungszwecken geeignete Garantien zu treffen sind. Insbesondere ist der Grundsatz der Datenminimierung einzuhalten.

Mit der österreichischen Ratspräsidentschaft wurden im Entwurf die Absätze 2a und 2aa eingefügt, die die Voraussetzungen für den neuen Abs 2 lit f festlegen sollen. Abs 2a regelt zusätzliche Bestimmungen für jene Fälle, in denen die Kommunikationsmetadaten nicht auf der rechtlichen Grundlage der Einwilligung des Endkunden oder dem Unionsrecht bzw. Recht eines Mitgliedstaates – wobei in diesen Fällen die Voraussetzungen des Art 11 der e-privacy Verordnung zur Anwendung kommen sollen - verarbeitet werden sollen. Des Weiteren hat der Kommunikationsbetreiber, der die Daten für einen anderen Zweck verarbeiten möchte als jener Zweck für den die Daten ursprünglich erhoben wurden, die Verbindung zwischen den Zwecken (lit a), die jeweilige Beziehung zwischen dem Endnutzer und dem Betreiber (lit b), die Prüfung, ob auch besondere Kategorien von Daten gemäß Art 9 DSGVO verarbeitet werden (lit c), die möglichen Risiken für den Endnutzer (lit d) sowie die eingesetzten Maßnahmen (lit e) zu berücksichtigen.

Des Weiteren wird ein weiteres Mal in Abs 2a festgehalten, dass die Verarbeitung von personenbezogenen Kommunikationsmetadaten nur erlaubt sein soll, wenn der Zweck mit der Verarbeitung von anonymen Daten nicht erfüllt werden kann, die Daten pseudonymisiert werden und die Metadaten nicht dazu verwendet werden ein Profil des einzelnen Endnutzers zu erstellen.

Abs 2aa regelt für jene Zwecke, die gemäß Abs 2a verarbeitet werden könnten, dass die Kommunikationsmetadaten an Dritte ausschließlich in anonymer Form übermittelt werden dürfen. Hier ist festzuhalten, dass Auftragsverarbeiter des Kommunikationsbetreibers gemäß den Grundsätzen der DSGVO keine Dritte sind, sondern dem Betreiber zuzurechnen sind. Auftragsverarbeiter verarbeiten gemäß den Begriffsbestimmungen in Art 4 Z 8 DSGVO immer personenbezogene Daten im Auftrag des Verantwortlichen, in diesem Fall, des Kommunikationsbetreibers. Des Weiteren wird bestimmt, dass der Verarbeiter der Daten eine Datenschutzfolgenabschätzung durchzuführen hat und entsprechend den Bestimmungen des Art 36 DSGVO die zuständige Behörde, in Österreich die Datenschutzbehörde, konsultieren muss. Diese Bestimmung wäre gegenüber der DSGVO eine Verschärfung, da dort eine vorherige Konsultation der Behörde nur in jenen Fällen vorausgesetzt wird, in denen die Datenschutzfolgenabschätzung ein hohes Risiko für die betroffene Person ergibt, dieses Risiko nicht reduziert werden kann und der Verantwortliche die Datenverarbeitung dennoch durchführen möchte⁷⁰. Der Entwurf der e-privacy Verordnung würde aber bestimmen, dass unabhängig vom Risiko für den Endnutzer die Behörde in jedem Fall herangezogen werden muss. Überdies ist dem Endnutzer jederzeit, einfache und kostenlose Widerspruchsmöglichkeit einzuräumen.

Es wird sich noch zeigen, ob sich dieser Vorschlag durchsetzt oder in weiteren Entwürfen verworfen wird. Diese Ergänzungen zeigen jedoch sehr deutlich, wie sehr die Betreiber ihren Standpunkt im Europäischen Rat durchsetzen konnten.

Art 6 Abs 3 regelt die Datenverarbeitung von elektronischen Kommunikationsinhaltsdaten. Der erste Entwurf der europäischen Kommission zur e-privacy Verordnung bestimmt in lit a, dass Inhaltsdaten ausschließlich für den Zweck der Bereitstellung eines Dienstes für einen Endnutzer verarbeitet werden dürfen, wenn dieser in die Verarbeitung der Daten eingewilligt hat und die Dienstleistung ohne Verarbeitung dieser Inhalte nicht erbracht werden kann. Diese Bestimmung widerspricht den Grundsätzen der DSGVO, die bereits für die Erfüllung eines Vertrages eine

⁷⁰ Art 36 Abs 1 DSGVO.

rechtliche Grundlage für die Verarbeitung von personenbezogenen Daten vorsieht. Sind die personenbezogenen Daten für die Erbringung einer angebotenen Dienstleistung notwendig, wird in der DSGVO keine zusätzliche Einwilligung vorausgesetzt. Eine Einwilligung nach den Voraussetzungen des Art 7 DSGVO, die auch in der e-privacy Verordnung verlangt werden, ist nur dann notwendig, wenn der Dienst auch ohne personenbezogene Daten erbracht werden kann. Gemäß Art 6 Abs 3 lit a e-privacy VO ist somit zusätzlich zur Vertragserfüllung noch eine gültige Einwilligung einzuholen. Dies ist jedoch nur unter der Bedingung erlaubt, dass die versprochene Dienstleistung nicht ohne der Inhaltsdaten erbracht werden kann.

Art 6 Abs 3 lit b des ursprünglichen Entwurfs der e-privacy Verordnung erlaubt zum anderen auch dann die Verarbeitung von Kommunikationsinhaltsdaten von mehreren betroffenen Endnutzern, wenn sie alle ihre Einwilligung für einen oder mehrere bestimmte Zwecke gegeben haben und das Ziel der Verarbeitung nicht mit anonymisierten Informationen erreicht werden kann. Zusätzlich hat der Kommunikationsbetreiber für die Verarbeitung der Daten immer die Aufsichtsbehörde gemäß Art 36 Abs 2 und 3 DSGVO im Vorhinein zu konsultieren.

Die DSGVO sieht in Art 35 für bestimmte Verarbeitungsvorgänge, die aufgrund ihrer Art, des Umfangs, der Umstände oder der Zwecke der Datenverarbeitung eine Datenschutz-Folgenabschätzung vor, die noch vor Beginn der Datenverarbeitung die Risiken und Folgen der vorgesehenen Verarbeitungsvorgänge analysieren und bewerten soll. Eine Datenverarbeitung darf nur dann durchgeführt werden, wenn das Risiko für die betroffenen Personen niedrig ist. Geht aus der Datenschutz-Folgenabschätzung ein hohes Risiko hervor und möchte der Verantwortliche die Daten weiterhin verarbeiten, bedarf es gemäß Art 36 Abs 1 einer vorherigen Konsultation der Aufsichtsbehörde. Der Entwurf der e-privacy VO verlangt in Art 6 Abs 3 lit b eine Konsultation der Aufsichtsbehörde bei jeder Verarbeitung von Kommunikationsinhaltsdaten mehrerer Endnutzer, unabhängig davon, wie hoch das Risiko in der Datenschutz-Folgenabschätzung ist.

Auch dieser Absatz wurde während sämtlichen Konsultationen mehrmals überarbeitet. Der Vorschlag der österreichischen Ratspräsidentschaft hat Abs 3 lit a ganz neu in lit aa formuliert und erlaubt die Verarbeitung von elektronischen Kommunikationsinhalten für jene Zwecke, in denen Dienste explizit vom Endnutzer für seinen individuellen Nutzen angefordert sowie seine

Einwilligung für die Verarbeitung gegeben hat⁷¹. Des Weiteren darf die Datenverarbeitung zu keinen Nachteilen für die Rechten und Freiheiten einer anderen Person führen und die Dauer ist so kurz wie für die Erfüllung des Zwecks notwendig zu halten. In dem Änderungsvorschlag fällt die Anforderung weg, dass eine Verarbeitung von elektronischen Kommunikationsinhaltsdaten nur dann erfolgen darf, wenn diese nicht mit anonymen Daten erbracht werden kann. Sonst bleibt die Bestimmung im Wesentlichen gleich. Sind mehrere Endnutzer betroffen, so bleibt die Voraussetzung gemäß Abs 3 lit b weiterhin bestehen und setzt zusätzlich die Konsultation der Aufsichtsbehörde voraus. Der hinzugefügte Abs 4 bestimmt, dass sich Kommunikationsbetreiber für die Verarbeitung von Kommunikationsdaten Auftragsverarbeiter im Sinne von Art 28 DSGVO bedienen dürfen. Dies wäre wahrscheinlich auch ohne dieser Bestimmung möglich, da dies kein Widerspruch zu den allgemeinen Datenschutzbestimmungen darstellt und es keine Bestimmungen in der e-privacy Verordnung gibt, die dies nicht erlauben würden.

Es stellt sich an dieser Stelle die Frage, ob für die eigentliche Erbringung der Kommunikation, die per se auch schon eine Verarbeitung von Kommunikationsinhaltsdaten bedeutet, auch bereits in die Bestimmungen des Art 6 Abs 3 fällt und zusätzlich zum Vertrag eine Einwilligung verlangt oder ob nur zusätzliche Verarbeitungen von Inhaltsdaten gemeint sind. Wäre dies der Fall, dann ist die einfache Erbringung der Kommunikation nicht in der Verordnung geregelt.

Die bestehende e-privacy Richtlinie sieht keine Regelungen zu Inhaltsdaten vor. Wie mit Inhaltsdaten umzugehen ist, wurde bis jetzt von den Mitgliedstaaten selbst geregelt. Das österreichische TKG bestimmt in § 101, dass Inhaltsdaten – sofern die Speicherung nicht ein wesentlicher Bestandteil des Kommunikationsdienstes darstellt – gar nicht gespeichert werden dürfen. Ist eine kurzfristige Speicherung aufgrund von technischen Gründen erforderlich, so ist das erlaubt. Der Betreiber hat die Daten jedoch zu löschen, sobald diese Gründe wegfallen. Darüber hinaus dürfen keine Inhaltsdaten verarbeitet werden. Es besteht nach dem TKG auch keine Möglichkeit eine Einwilligung des Endnutzers für zusätzliche Dienste einzuholen.

Sämtliche Entwürfe der e-privacy Verordnung würden jedenfalls die Prinzipien des österreichischen TKG ändern. Es müsste allein schon für die Erbringung der Kommunikation eine Einwilligung der Endnutzer eingeholt werden, da nichts Weiteres geregelt ist. Eine solche

⁷¹ Proposal for a regulation of the European Parliament and the Council concerning the respect for private life and protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) - Examination of the Presidency text, Brussels, 10 July 2018, 10975/18, Art 6 Abs 3, 21 f.

Bestimmung würde unter anderem allen Kommunikationsbetreibern und ihren Entwicklern erlauben die Inhalte von E-Mails oder anderen Nachrichten zu lesen bzw. zu analysieren um mit diesen Informationen Algorithmen zu erstellen oder zu verbessern⁷². Mit der entsprechenden Einwilligung durch den Nutzer ist das Mitlesen und Auswerten von Inhalten erlaubt.

Art 7 der e-Privacy Verordnung regelt die Speicherung und Löschung der elektronischen Kommunikationsdaten. Kommunikationsinhalte sind gemäß Art 7 Abs 1 unmittelbar nach Empfang der Daten zu löschen oder zu anonymisieren. Eine Speicherung der Daten darf nach den Prinzipien der DSGVO vom Endnutzer oder einem Dritten, der vom Endnutzer mit der Aufzeichnung betraut wurde, erfolgen. Dies würde bedeuten, dass die Kommunikationsinhalte von einem Dienstleister, jedoch nicht dem Betreiber der elektronischen Kommunikation, gespeichert werden dürfen, wenn dieser eine rechtliche Grundlage gemäß Art 6 DSGVO für die Speicherung oder weitere Verarbeitung der Daten hat. Der Betreiber der elektronischen Kommunikation, in der Regel der Telekommunikationsanbieter, hat die Daten jedoch zu löschen, auch dann, wenn er gemäß Art 6 DSGVO eine rechtliche Grundlage hätte.

Kommunikationsmetadaten sind gemäß Art 7 Abs 2 e-privacy Verordnung unmittelbar nach Übermittlung der Kommunikation zu löschen, es sei denn, diese Daten werden für Abrechnungszwecke benötigt (Abs 3). In der Regel werden Entgeltnachweise für die Nachvollziehbarkeit und Anfechtung der Rechnung erstellt und dem Endnutzer zur Verfügung gestellt. § 100 TKG stellt klar, dass Entgeltnachweise Verkehrsdaten sind und somit auch dieselben Löschfristen für diese heranzuziehen sind. Diese sind so lange aufzubewahren, wie die Rechnung nach nationalem Recht rechtmäßig angefochten werden kann. In Österreich beträgt die Einspruchsfrist gemäß § 71 Abs 1a TKG drei Monate. Jedoch handelt es sich hier um Verfahren gemäß dem Außerstreitgesetz und für diese gilt eine einjährige Einspruchsfrist. Somit ist davon auszugehen, dass die Einspruchsfrist gemäß § 6 AStG ein Jahr beträgt.

⁷² golem.de (3. Juli 2018) Drittfirmen lesen massenweise Gmail-Postfächer. Onlinedokument: <https://www.golem.de/news/datenschutz-drittfirmen-lesen-massenweise-gmail-postfaecher-1807-135289.html>; Download am 07.08.2018.

4. Webtracking und Cookies

4.1 Schutz der in Endeinrichtungen gespeicherten Informationen

ErwG 20 der e-privacy Verordnung betont, dass nicht nur die elektronische Kommunikation unter den Schutz der GRCh fällt, sondern auch sämtlich Informationen, die auf Endeinrichtungen gespeichert oder ausgesendet, von ihnen angefordert oder verarbeitet werden, um sich mit anderen Geräten oder mit Netzanlagen verbinden zu können. Die Informationen sollen einen erhöhten Schutz unterliegen, da diese „einen tiefen Einblick in komplexe emotionale, politische und soziale Aspekte der Persönlichkeit einer Person geben können“. Hier sind Nachrichteninhalte, Bilder aber auch Standorte zu subsumieren, die ohne das Wissen des Endnutzers durch Verfolgungswerkzeuge wie beispielsweise Spyware, Webbugs oder Verfolgungs-Cookies ermittelt werden können. Aus diesem Grund sollten derartige Eingriffe nur mit Einwilligung des Endnutzers für ganz bestimmte transparente Zwecke erlaubt werden. Gemäß Art 8 Abs 1 des Entwurfs der e-privacy Verordnung ist die Verarbeitung dieser Daten auch erlaubt, wenn sie für die Erbringung eines elektronischen Kommunikationsdienstes bzw. einer anderen Dienstleistung notwendig ist.

Eine Ausnahme von diesem Prinzip sollte nur dann möglich sein, wenn der Eingriff in die Privatsphäre sehr gering ist. ErwG 21 hält fest, dass Cookies nicht nur zur Verfolgung von Internetnutzern dienen, sondern auch ein „legitimes und nützliches Hilfsmittel“ sind. Sie dienen beispielsweise zur Messung des Webdatenverkehrs einer Webseite oder erleichtern dem Nutzer gewisse Anwendungen, wie beispielsweise das Speichern von ausgefüllten Feldern für die Dauer eines Besuches einer Webseite als Ausfüllhilfe von Online-Formularen, die sich auf mehreren Seiten erstrecken. Dies sind sogenannte Session Cookies⁷³. Art 8 Abs 1 lit d der e-privacy Verordnung nennt als weitere Ausnahme für eine notwendige Einwilligungserklärung durch den Nutzer die Messung von Besuchern einer Webseite mittels Cookies. Der Änderungsvorschlag der weiteren Ratspräsidentenschaften präzisiert in Art 8 Abs 1 lit d e-privacy Verordnung, dass Cookies von Drittanbietern ausschließlich im Auftrag des Anbieters ohne Einwilligung des Nutzers

⁷³ CHIP Digital GmbH (12.07.2015), Cookies akzeptieren oder nicht? Das sollten sie tun. Onlinedokument: https://praxistipps.chip.de/cookies-akzeptieren-oder-nicht-das-sollten-sie-tun_42136; Download am 18.02.2018.

eingesetzt werden dürfen. Handelt es sich nicht um eine Auftragsverarbeitung gemäß Art 28 DSGVO, ist eine Einwilligung einzuholen⁷⁴.

Diese Ausnahmebestimmungen spiegeln im Grunde die rechtliche Grundlage des berechtigten Interesses gemäß Art 6 Abs 1 lit f DSGVO wieder, die eine Datenverarbeitung im Interesse des Verantwortlichen oder eines Dritten erlaubt. Dies gilt auch für den neuen Zusatz zu lit d. Aus diesem Grund fordern die Wirtschaftskammer sowie Unternehmen die Streichung dieser Bestimmung⁷⁵. Andererseits gibt die DSGVO nicht vor, welches berechtigte Interesse eines Verantwortlichen oder eines Dritten gegenüber den Interessen und Grundfreiheiten der betroffenen Person überwiegen. Art 8 e-privacy Verordnung könnte somit auch als Klarstellung und als ein Anwendungsbeispiel verstanden werden, die den Verantwortlichen einer Datenverarbeitung auch hilfreich sein kann.

Mit den Änderungsvorschlägen des Entwurfs wurden auch zusätzliche Ausnahmebestimmungen hinzugefügt. Art 8 Abs 1 lit da bestimmt, dass eine Einwilligung für Verarbeitung und Speicherung bzw. Erhebung von Informationen aus den Endeinrichtungen auch dann nicht notwendig, wenn diese notwendig sind um die Sicherheit der Dienste aufrechtzuerhalten bzw. wiederherzustellen, Betrug zu vermeiden oder Fehler zu entdecken. Die Daten dürfen so lange gespeichert werden, wie für die Erfüllung des Zwecks notwendig ist⁷⁶. Ein weiterer Ausnahmetatbestand ist gemäß der neuen lit e gegeben, wenn die Informationen unter den Bedingungen für Sicherheitsupdates erforderlich sind, dass die Sicherheitsupdates notwendig sind und die vom Endnutzer eingestellten Datenschutzeinstellungen nicht ändern, der Endnutzer immer vor der Installation des Updates rechtzeitig informiert wird und die Möglichkeit hat eine automatische Installation der Updates zu deaktivieren.

⁷⁴ Proposal for a regulation of the European Parliament and the Council concerning the respect for private life and protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) - Examination of the Presidency text, Brussels, 10 July 2018, 10975/18, Art 8 Abs 1, 23.

⁷⁵ Pöcherstorfer, Winfried, Vorschlag der Europäischen Kommission für die Überarbeitung der Richtlinie über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation – Richtlinie 2002/58/EG, COM (2017) 10 final v 10.01.2017 [Vorschlag EK-DSVO] – Stellungnahme, 10.04.2017, 4.

⁷⁶ Proposal for a regulation of the European Parliament and the Council concerning the respect for private life and protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) - Examination of the Presidency text, Brussels, 10 July 2018, 10975/18, Art 8 Abs 1, 23.

Art 8 Abs 2 des ersten Entwurfs zur e-privacy Verordnung untersagt bis auf die vorgeschriebenen Ausnahmen jede Erhebung von Informationen durch den elektronischen Kommunikationsdienstleister oder einem Dritten, die vom Endgerät einer Person ausgesendet werden um sich mit anderen Geräten oder Netzanlagen zu verbinden. Von dem Verbot ausgenommen sind erstens gemäß lit a jene Zwecke die der Herstellung einer Verbindung für die dazu notwendige Dauer dienen und zweitens laut lit b, wenn über die Erhebung gemäß Art 13 DSGVO in hervorgehobener Weise informiert wird. Die Art 29 Gruppe spricht sich gegen diese Bestimmung aus, da man davon ausgehen könnte, dass man für das Sammeln von Daten durch Tracking auf öffentlichen Plätzen keine Einwilligung benötigen würde, solange nur die Informationspflichten erfüllt sind⁷⁷. Eine solche Auslegung würde jedoch der DSGVO widersprechen, die bei WIFI – Tracking bzw. Bluetooth – Tracking eine Einwilligung für das Verarbeiten von personenbezogenen Daten verlangt bzw. nur eine anonymisierte Datenverarbeitung erlauben würde. Die Artikel 29 Gruppe ist besorgt, dass Endnutzer immer häufiger von privaten und öffentlichen Organisationen getrackt werden. Aus diesem Grund fordert sie den europäischen Gesetzgeber auf einen technischen Standard für Endeinrichtungen zu verlangen, mit dem ein Endnutzer sicherstellen kann, dass er nicht getrackt wird⁷⁸.

Dieser Einwand wurde in den Änderungsvorschlägen aufgenommen und diese Ausnahmebestimmung wurde zur Gänze verworfen. Die Version der österreichischen Ratspräsidentschaft bestimmt nur mehr in Art 8 Abs 2 lit b, dass die Daten mit Zustimmung des Endnutzers gespeichert werden dürfen. Es wurde aber eine weitere Ausnahmebestimmung in lit c eingeführt, die die Verarbeitung zu Zwecken der statistischen Zählung erlaubt, insofern nur so wenig Daten wie für die Zweckerfüllung notwendig mit einer zeitlichen und räumlichen Beschränkung verarbeitet werden⁷⁹. Sobald der Zweck wegfällt, sind die Daten zu anonymisieren oder zu löschen. Art 8 Abs 2a bestimmt, dass der Endnutzer entsprechend dem Recht auf Information des Art 13 DSGVO in den Fällen der Einwilligung und der statistischen Zählung transparent über die Zwecke, den Verantwortlichen und die Art der Verarbeitung zu informieren ist. Des Weiteren wird in Abs 2b auf die Einführung von technischen und organisatorischen Maßnahmen gemäß Art 32 DSGVO verwiesen. Diese beiden Absätze

⁷⁷ Article 29 Data Protection Working Party, Opinion 01/2017 on the Proposed Regulation for the e-Privacy Regulation (2002/58/EC), 2017, 11, Rn. 17.

⁷⁸ aaO, 12, Rn. 17.

⁷⁹ Proposal for a regulation of the European Parliament and the Council concerning the respect for private life and protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) - Examination of the Presidency text, Brussels, 10 July 2018, 10975/18, Art 8 Abs 2, 24.

wiederholen wie im ersten Entwurf der e-privacy Verordnung ausschließlich die Prinzipien der DSGVO und schaffen im Grunde keinen zusätzlichen Schutz für die Endnutzer, da die DSGVO grundsätzlich die Mindestanforderungen im Datenschutz bestimmt.

Art 9 des ersten Entwurfs der e-privacy Verordnung bestimmt, dass eine Einwilligung nur dann gültig zustande kommt, wenn die Voraussetzungen von Art 7 DSGVO erfüllt werden. Eine schriftliche Einwilligung benötigt demnach eine transparente Erklärung in leicht verständlicher und zugänglicher Form über den Zweck der Datenverarbeitung, die Dauer der Speicherung der personenbezogenen Daten und Information ob Daten an einen Empfänger übermittelt werden⁸⁰. Die Einwilligungserklärung muss sich klar von anderen Sachverhalten unterscheiden und darf somit beispielsweise nicht in AGB eingearbeitet werden.

Der Verantwortliche hat nachzuweisen, dass die betroffene Person der Datenverarbeitung eingewilligt hat⁸¹. Die Einwilligung kann durch die betroffene Person jederzeit widerrufen werden⁸². Hierbei muss die Abgabe des Widerrufs der Einwilligung genauso einfach wie die Erteilung der Einwilligung sein⁸³. Eine weitere Voraussetzung für eine gültige Einwilligung ist die Freiwilligkeit. Die Erbringung einer Dienstleistung darf nicht an eine Einwilligung gekoppelt werden⁸⁴.

Der ursprüngliche Entwurf der Europäischen Kommission zur e-privacy VO sieht in Art 9 Abs 3 vor, dass Endnutzer ihre Einwilligung zur Verarbeitung von elektronischen Kommunikationsdaten nach Art 6 Abs 2 lit c und Art 6 Abs 3 lit a und b e-privacy VO gemäß Art 7 Abs 3 DSGVO jederzeit widerrufen können sowie alle sechs Monate an diese Möglichkeit erinnert werden sollen. Um eine Einwilligung widerrufen zu können, muss der Endnutzer auch wissen, welche Einwilligungserklärungen er abgegeben hat. Somit besteht für den Betreiber von elektronischen Kommunikationsdiensten eine Verpflichtung alle Einwilligungserklärungen zu verwalten und den Endnutzer in dem vorgegebenen Zeitraum über die vorhandenen Einwilligungserklärungen zu informieren. Der Entwurf der estnischen Ratspräsidentschaft⁸⁵ hat

⁸⁰ Diese Informationen ergeben sich aus Art 13 DSGVO.

⁸¹ Art 7 Abs 1 DSGVO.

⁸² Art 7 Abs 2 DSGVO.

⁸³ Art 7 Abs 3 letzter Satz DSGVO.

⁸⁴ Koppelungsverbot der Einwilligung: Die Einwilligung für eine Datenverarbeitung darf nicht an die Erbringung einer Dienstleistung abhängig gemacht werden, wenn die Einwilligung nicht für die Erfüllung des Vertrages erforderlich ist (Art 7 Abs 4 DSGVO).

⁸⁵ Proposal for a regulation of the European Parliament and the Council concerning the respect for private life and protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) -

Art 9 auf Art 4a in den Abschnitt der Begriffsbestimmungen geschoben und den Zeitraum für die Erinnerung an eine Widerrufsmöglichkeit auf alle 12 Monate verlängert. Mit den Änderungsvorschlägen wurde auch dieser Vorschlag endgültig verworfen und die Belehrung über die Widerrufsmöglichkeit ist entfallen.

In Art 4a Abs 1a wurde klargestellt, dass bei juristischen Personen jene Personen befugt sind gültig einzuwilligen, die zu Vertragsabschlüssen oder zu Vertretungen bei Gerichtsverfahren befugt sind.

4.2 Einstellungsmöglichkeiten zur Privatsphäre

Ein neuer Grundsatz der DSGVO ist Datenschutz durch datenschutzfreundliche Voreinstellungen. Art 25 Abs 2 DSGVO bestimmt, dass der Verantwortliche durch Voreinstellungen sicherstellt, dass nur jene personenbezogenen Daten verarbeitet werden, die für den jeweiligen bestimmten Verarbeitungszweck erforderlich sind. Somit soll sichergestellt werden, dass der Umfang der Verarbeitung, die Speicherdauer und die Zugänglichkeit zu den Daten den Grundsätzen der DSGVO entsprechen.

Art 9 Abs 1 e-privacy Verordnung erlaubt in seinen ersten Fassungen die Abgabe einer Einwilligung für die Zwecke des Art 8 e-privacy Verordnung „in den passenden technischen Einstellungen einer Software, die den Zugang zum Internet ermöglicht“. ErwG 22 stellt klar, dass der Endnutzer immer häufiger aufgefordert wird seine Einwilligung in die Speicherung von Verfolgungs-Cookies zu geben. Dies führt dazu, dass der Endnutzer mit Aufforderungen zur Erteilung von Einwilligungserklärungen überhäuft wird. Um dieses Problem zu beheben, sieht diese Verordnung vor, dass die Einwilligung durch Einstellungen in einem Webbrowser oder einer anderen Anwendung erteilt werden kann. Die gewählte Einstellung des Endnutzers sollte dann auch für Dritte verbindlich und ihnen gegenüber rechtlich durchsetzbar sein.

Diese Bestimmung wurde von den europäischen Unternehmen sehr stark kritisiert. Denn mit einer solchen Regelung würde durch die allgemeinen Browsereinstellungen bestimmt werden, ob bei einem Besuch jedweder Webseite Cookies gespeichert werden dürfen. Derzeit gibt es bei den Browsereinstellungen die Möglichkeit alle Cookies zuzulassen, Cookies nur für besuchte Webseiten zu erlauben bzw. gar keine Speicherung von Cookies zu gewähren. Die Browser unterstützen jedoch nicht die Möglichkeit unterschiedliche Einstellungen je nach Webseiten vorzunehmen. Der Entwurf der e-privacy Verordnung unterscheidet hingegen zwischen Cookies

Examination of the Presidency text (Art 1-5 and related recitals, Brussels, 06. October 2017, 11955/17, 19.

der Webseitenbetreiber und Cookies von Drittanbietern. So soll der Endnutzer einstellen können, ob er nur die Cookies der von ihm besuchten Webseite erlaubt oder auch Drittanbieter – Cookies, die zusätzlich beim Besuch der Webseite gespeichert werden. In vielen Fällen handelt es sich bei Cookies von Drittanbietern um Tracking- bzw. Targeting-Cookies, die zur Schaltung von personalisierter Werbung notwendig sind.

Die europäische Wirtschaft befürchtet in der vorgeschlagenen Lösung der Europäischen Kommission eine Ungleichbehandlung gegenüber den großen internationalen „Big Playern“ Google, Apple, Microsoft und Mozilla⁸⁶. Mit dieser Bestimmung würde man gerade diesen vier großen Unternehmen die Verantwortung übertragen die europäischen Datenschutzbestimmungen umzusetzen. Gleichzeitig verwenden diese großen Unternehmen überwiegend ihre eigenen Cookies, die auch von vielen anderen Unternehmen in Anspruch genommen werden. Europäische Unternehmen, vor allem die Online-Werber sind auf diese Drittanbieter-Cookies für ihre Webanalysen und Schaltung von Online-Werbung angewiesen. Diese Bestimmung würde dazu führen, dass dieselben Cookies je nach ihrem Anwender durch die Browsereinstellungen des Endnutzers unterschiedlich behandelt würden.⁸⁷

Art 10 e-Privacy Verordnung regelt in Abs 1, dass eine Software, die eine elektronische Kommunikation erlaubt, auch die Möglichkeit bieten muss, dass Dritte keine Informationen in der Endeinrichtung eines Endnutzers speichern oder bereits in der Endeinrichtung gespeicherte Informationen verarbeiten. Dies gilt unter anderem auch für jene Software, die das Abrufen und Darstellen von Informationen aus dem Internet ermöglicht⁸⁸. Auch hier sind die Webbrowser gemeint.

⁸⁶ European Publishers Council (29.05.2017), Open letter to the European Parliament/Council, Trust, privacy and news – the need to rethink ePrivacy proposals. Onlinedokument: <http://epceurope.eu/wp-content/uploads/2017/05/FNL-ePrivacy-letter-1.pdf>; Download am 18.02.2018, 1.

⁸⁷ Pöcherstorfer, Winfried, Vorschlag der Europäischen Kommission für die Überarbeitung der Richtlinie über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation – Richtlinie 2002/58/EG, COM (2017) 10 final v 10.01.2017 [Vorschlag EK-DSVO] – Stellungnahme, 10.04.2017, 4.

⁸⁸ Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über die Achtung des Privatlebens und den Schutz personenbezogener Daten in der elektronischen Kommunikation und zur Aufhebung der Richtlinie 2002/58/EG (Verordnung über Privatsphäre und elektronische Kommunikation), Brüssel, 10.01.2017 10, Art Abs 1.

Diese Bestimmung erfüllt laut der Artikel 29 Gruppe nicht die Voraussetzungen des Art 25 DSGVO⁸⁹. Alle Endeinrichtungen bzw. jede in Verkehr gebrachte Software hat dem Grundsatz „Datenschutz durch datenschutzfreundliche Voreinstellungen“ zu entsprechen. Demnach ist immer die datenschutzfreundlichste Voreinstellung, je nach Zweck der Datenverarbeitung, zu wählen. Art 10 e-Privacy Verordnung bestimmt jedoch nur, dass eine Datenverarbeitung durch Dritte verboten werden muss. Es wird jedoch nicht festgehalten, dass der Betreiber der Software nur jene Daten verarbeiten darf, die für die Erfüllung des Zwecks notwendig sind. Möchte er mehr Daten verarbeiten, ist gemäß der DSGVO hierfür eine Einwilligung vom Endnutzer einzuholen.

Art 10 Abs 2 e-Privacy Verordnung bestimmt, dass der Endnutzer bei der Installation einer Software über die möglichen Einstellungsmöglichkeiten zu informieren ist und dieser sich für eine der möglichen Einstellungen entscheiden muss. Gemäß Abs 3 hat eine Software, die vor Inkrafttreten der e-Privacy Verordnung bereits installiert ist, spätestens mit der ersten Aktualisierung die Anforderungen des Abs 2 zu erfüllen.

Hier ist anzumerken, dass die DSGVO eine Unterscheidung zwischen Auftragsverarbeiter und Drittem trifft. Art 25 DSGVO verlangt, dass nur jene personenbezogenen Daten verarbeitet werden, die für die Erfüllung eines Zwecks notwendig sind. Bedient sich ein Verantwortlicher bzw. in diesem Fall ein Webseitenbetreiber eines Auftragsverarbeiters⁹⁰, so hat er die Einhaltung der datenschutzrechtlichen Grundsätze mittels einer Auftragsverarbeitervereinbarung gemäß Art 28 DSGVO sicherzustellen. Ist für die Erfüllung des Zwecks eine Übermittlung an einen Dritten⁹¹ notwendig, so ist weiterhin der Grundsatz „Datenschutz durch datenschutzfreundliche Voreinstellungen“ erfüllt. Genau diese Unterscheidung wird, wie bereits im Kapitel 4.1 beschrieben, sehr stark von den Interessensverbänden der Online- Werbung kritisiert. Eine Software kann technisch nicht zwischen Auftragsverarbeiter oder Dritten unterscheiden. Somit würden auch alle Cookies eines Auftragsverarbeiters als Drittanbieter – Cookies behandelt. Auf diese Weise würden sehr viele Datenanwendungen nicht mehr möglich werden.

⁸⁹ Article 29 Data Protection Working Party, Opinion 01/2017 on the Proposed Regulation for the ePrivacy Regulation (2002/58/EC), 2017, 14, Rn. 19.

⁹⁰ Gemäß Art 4 Z 8 DSGVO ist ein Auftragsverarbeiter eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet.

⁹¹ Gemäß Art 4 Z 10 ist ein Dritter eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, außer der betroffenen Person, dem Verantwortlichen, dem Auftragsverarbeiter und den Personen, die unter der unmittelbaren Verantwortung des Verantwortlichen oder des Auftragsverarbeiters befugt sind, die personenbezogenen Daten zu verarbeiten.

Die Artikel 29 Gruppe hält auch fest, dass Art 10 e-Privacy Verordnung nicht nur für Browsereinstellungen gilt, sondern für jede Software, die elektronische Kommunikation ermöglicht. Hierunter fallen beispielsweise auch Apps oder Software Schnittstellen von mit IoT verbundenen Geräten⁹². Des Weiteren fordert die Artikel 29 Gruppe ein generelles Verbot von Tracking. Das grundlegende Recht auf Meinungsäußerung sowie das Recht auf Information sollte ihrer Ansicht nach nicht von der Zustimmung von Tracking auf Endgeräten oder Webseiten abhängig gemacht werden⁹³. Im Gegensatz dazu befürchtet der Europäische Verlegerrat, dass mit einer solchen Regelung viele Zeitungen, deren Einnahmequelle auf Cookies basierte personalisierte Werbung ist, an ihrer hohen Qualität ihrer Services verlieren werden, wenn diese Einnahmequelle verboten bzw. erschwert wird⁹⁴. Der Standard hat bereits reagiert und erlaubt ohne der Einwilligung zur Verwendung von Cookies ausschließlich Abo-Mitgliedern die Verwendung der Webseite www.derstandard.at.

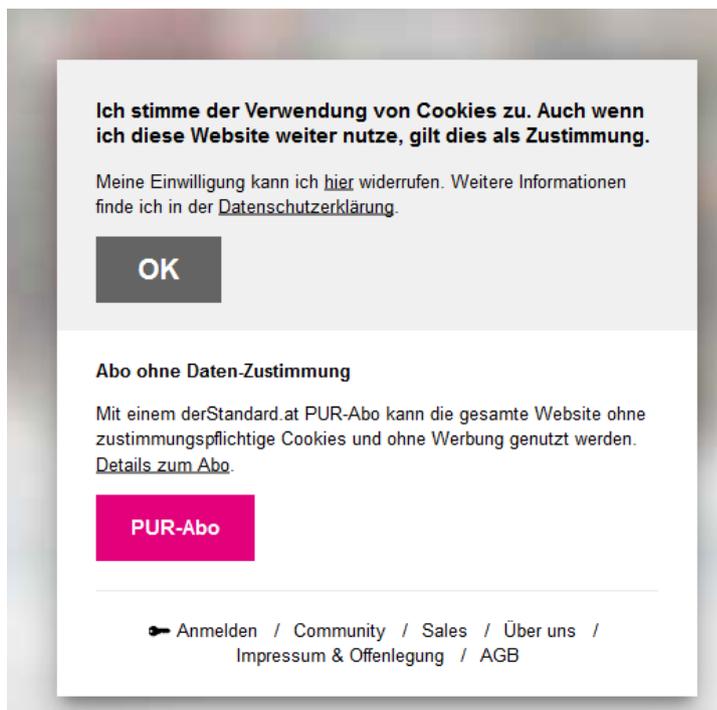


Abbildung 5: Cookie - Einwilligung auf www.derstandard.at seit 25.08.2018

⁹² Article 29 Data Protection Working Party, Opinion 01/2017 on the Proposed Regulation for the ePrivacy Regulation (2002/58/EC), 2017, 14, Rn. 19.

⁹³ Article 29 Data Protection Working Party, Opinion 01/2017 on the Proposed Regulation for the ePrivacy Regulation (2002/58/EC), 2017, 15, Rr. 20.

⁹⁴ European Publishers Council (29.05.2017), Open letter to the European Parliament/Council, Trust, privacy and news – the need to rethink ePrivacy proposals. Onlinedokument: <http://epceurope.eu/wp-content/uploads/2017/05/FNL-ePrivacy-letter-1.pdf>; Download am 18.02.2018, 1.

Die Konferenz der unabhängigen Datenschutzbehörden des Deutschen Bundes und der Länder, kurz Datenschutzkonferenz, hat in seiner Positionsbestimmung zur Anwendbarkeit des Telemediengesetzes für nicht-öffentliche Stellen ab dem 25. Mai 2018 einen Monat vor Inkrafttreten der DSGVO veröffentlicht, dass eine „Einwilligung beim Einsatz von Tracking-Mechanismen, die das Verhalten von betroffenen Personen im Internet nachvollziehbar machen und bei der Erstellung von Nutzerprofilen“ bereits gemäß der DSGVO notwendig ist und nicht erst mit Inkrafttreten der e-privacy Verordnung⁹⁵. Diese Position hat die Stellungnahme der Art 29 Gruppe bekräftigt und noch einmal verdeutlicht, dass der Endnutzer nur eine gültige Einwilligungserklärung abgeben kann, wenn pro Zweck und nicht pro Cookie – Anbieter unterschieden wird. Dies hat dazu geführt, dass die österreichische Ratspräsidentschaft in ihrem Entwurf zur e-privacy Verordnung den gesamten Art 10 gestrichen hat⁹⁶. Art 9 Abs 2, der nur auf die Möglichkeiten in Art 10 verweist, wurde bereits in früheren Änderungsvorschlägen gestrichen.

Art 11 ermöglicht den Mitgliedstaaten die Art 5 – 8 zu gemäß den Prinzipien des Art 23 Abs 1 lit a - e DSGVO zu beschränken, die eine Einschränkung der Betroffenenrechte in der DSGVO regeln. Demnach ist eine Beschränkung erlaubt, solange der Wesensgehalt der Grundrechte und Grundfreiheiten geachtet wird und in einer demokratischen Gesellschaft eine notwendige und verhältnismäßige Maßnahme darstellt und Folgendes sicherstellt:

- a) die nationale Sicherheit;
- b) die Landesverteidigung;
- c) die öffentliche Sicherheit;
- d) die Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder die Strafvollstreckung, einschließlich des Schutzes vor und die Abwehr von Gefahren für die öffentliche Sicherheit;

⁹⁵ Datenschutzkonferenz (26. April 2018), Positionsbestimmung der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder, Zur Anwendbarkeit des TMG für nicht-öffentliche Stellen ab dem 25. Mai 2018. Onlinedokument: https://www.ldi.nrw.de/mainmenu_Datenschutz/submenu_Technik/Inhalt/TechnikundOrganisation/Inhalt/Zur-Anwendbarkeit-des-TMG-fuer-nicht-oeffentliche-Stellen-ab-dem-25_-Mai-2018/Positionsbestimmung-TMG.pdf; Download am 08.08.2018.

⁹⁶ Proposal for a regulation of the European Parliament and the Council concerning the respect for private life and protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) - Examination of the Presidency text, Brussels, 10 July 2018, 10975/18, Art 10, 25.

- e) den Schutz sonstiger wichtiger Ziele des allgemeinen öffentlichen Interesses der Union oder eines Mitgliedstaats, insbesondere eines wichtigen wirtschaftlichen oder finanziellen Interesses der Union oder eines Mitgliedstaats, etwa im Währungs-, Haushalts- und Steuerbereich sowie im Bereich der öffentlichen Gesundheit und der sozialen Sicherheit.

Gemäß Art 11 Abs 2 der e-privacy Verordnung haben die Kommunikationsbetreiber interne Verfahren zur Beantwortung von Anfragen auf Zugang zu elektronischen Kommunikationsdaten durch Endnutzer einzurichten. Die Aufsichtsbehörde wird auf Anfrage über die Zahl der eingegangenen Anfragen und die vorgebrachten rechtlichen Begründungen und Antworten informiert. Mit dieser Bestimmung wird dem Endnutzer das Recht auf Auskunft gemäß Art 15 DSGVO eingeräumt, was vor allem für Endnutzer, die juristische Personen sind, wichtig ist, die nach der DSGVO keine Betroffenenrechte haben.

5. Sonderbestimmungen zu nummerngebundener interpersoneller Kommunikation

Die in den Art 12 bis 14 des Entwurfes zur e-privacy Verordnung enthaltenen Bestimmungen sind bereits in der derzeit noch gültigen e-Privacy Richtlinie geregelt und wurden somit bereits in den einzelnen Mitgliedstaaten durch nationale Gesetze rechtlich umgesetzt. In Österreich wurde die e-Privacy Richtlinie im datenschutzrechtlichen Teil des TKG umgesetzt. Die Bestimmungen der Art 12 – 14 der e-privacy Verordnung richten sich im ursprünglichen Entwurf ausschließlich an Betreiber öffentlich zugänglicher nummerngebundener interpersoneller Kommunikation. In dem Änderungsvorschlag der bulgarischen Ratspräsidentschaft wurde „öffentlich zugänglich“ gestrichen⁹⁷. Wie bereits in Kapitel 2.3 dargelegt, wird bei der Begriffsbestimmung auf den Begriff der „nummerngebundenen interpersonellen Kommunikation“ auf den EECC verwiesen.

Art 2 lit 5 EECC definiert „interpersoneller Kommunikationsdienst“ als „gewöhnlich gegen Entgelt erbrachter Dienst, der einen direkten interpersonellen und interaktiven Informationsaustausch über elektronische Kommunikationsnetze zwischen einer endlichen Zahl von Personen ermöglicht, wobei die Empfänger von den Personen bestimmt werden, die die

⁹⁷ Proposal for a regulation of the European Parliament and the Council concerning the respect for private life and protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) - Examination of the Presidency text, Brussels, 12 June 2018, 9958/18, Art 12-14, 59ff.

Kommunikation veranlassen oder daran beteiligt sind; dazu zählen keine Dienste, die eine interpersonelle und interaktive Kommunikation lediglich als untrennbar mit einem anderen Dienst verbundene untergeordnete Nebenfunktion ermöglichen“;

Art 2 lit 6 EECC definiert „nummerngebundener interpersoneller Kommunikationsdienst“ als „ein interpersoneller Kommunikationsdienst, der an das öffentliche Fernsprechnetz angebunden ist, entweder mittels zugewiesener Nummerierungsressourcen, d.h. Nummern nationaler oder internationaler Telefonnummernpläne, oder durch Ermöglichung der Kommunikation über Nummern nationaler oder internationaler Telefonnummernpläne“.

5.1. Anzeige und Unterdrückung einer Rufnummer

Art 12 e-Privacy Verordnung regelt bereits wie Art 8 e-Privacy Richtlinie unter welchen Bedingungen eine Rufnummer des Anrufers bzw. des Angerufenen unterdrückt werden muss. Diese Bestimmung wurde bereits in § 104 TKG umgesetzt und hat sich im neuen Entwurf der e-Privacy Verordnung nicht geändert.

Art 12 Abs 1 bestimmt, dass jeder Anrufer die Möglichkeit haben muss, die Anzeige seiner Rufnummer für einen einzelnen Anruf, für eine bestimmte Verbindung oder dauerhaft zu verhindern⁹⁸. Auch der angerufene Endnutzer soll die Möglichkeit haben, die Anzeige der eingehenden Rufnummer zu unterdrücken⁹⁹. Insbesondere telefonische Beratungsdienste haben ein Interesse daran die Anonymität ihrer Anrufer zu gewährleisten¹⁰⁰. Der Angerufene soll auch einstellen können, dass eingehende Anrufe mit unterdrückter Rufnummer abgewiesen werden¹⁰¹. So kann der Angerufene verhindern, dass er durch unbekannte Anrufer belästigt wird.

Des Weiteren wird bestimmt, dass auch der Angerufene die Möglichkeit haben muss, dass seine Rufnummer beim Anrufer nicht angezeigt wird¹⁰². Diese Einstellung ist vor allem für Unternehmen oder Behörden wichtig, die mit vielen Durchwahlklappen arbeiten. Der anrufende Kunde, der weiterverbunden wird, soll die Durchwahl des bearbeitenden Mitarbeiters nicht

⁹⁸ Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über die Achtung des Privatlebens und den Schutz personenbezogener Daten in der elektronischen Kommunikation und zur Aufhebung der Richtlinie 2002/58/EG (Verordnung über Privatsphäre und elektronische Kommunikation), Brüssel, 10.01.2017, Art 12 Abs 1 lit a.

⁹⁹ aaO, Art 12 Abs 1 lit b.

¹⁰⁰ aaO, ErwG 27.

¹⁰¹ aaO, Art 12 Abs 1 lit c.

¹⁰² aaO, Art 12 Abs 1 lit d.

sehen. So wird sichergestellt, dass der Anrufer bei einer weiteren Frage, nicht direkt beim Mitarbeiter, sondern an der Servicehotline anruft.

Der Betreiber des nummerngebundenen interpersonellen Kommunikationsdienstes hat diese Möglichkeiten auf einfache Weise und kostenlos bereitzustellen¹⁰³. Die Betreiber der Kommunikationsdienste sowie die Österreichische Wirtschaftskammer kritisieren die Beibehaltung dieser Bestimmung, da eine solche Rufnummernunterdrückung nicht im Kommunikationsnetz durchgeführt werden kann. „Die ausgewiesenen Unterdrückungstatbestände und Sperrverpflichtungen bewirken nur technischen Aufwand und erhebliche Kosten für Unternehmen, für den Kunden allerdings keinerlei Vorteil“, weil im Endgerät des jeweiligen Endnutzers die Unterdrückung einer Rufnummer des Anrufers, aber auch des Angerufenen eingestellt werden kann¹⁰⁴. Sollte die Rufnummer im Netz von den Kommunikationsbetreibern unterdrückt werden, so wäre die Rufnummer unwiederbringlich unterdrückt und somit in jenen Fällen, in denen die Rufnummer doch klar erkennbar sein müsste, wie in Kapitel 5.2 beschrieben oder bei einer behördlichen Überwachung ebenfalls nicht verfügbar. Aus diesem Grund ist diese Bestimmung im Kommunikationsnetz durch die Betreiber gar nicht umsetzbar.

5.2 Ausnahmen für die Anzeige der Rufnummer des Anrufers und des Angerufenen und deren Unterdrückung

Art 13 Abs 1 e-Privacy Verordnung ersetzt Art 10 lit b der bestehenden e-Privacy Richtlinie und regelt, dass Betreiber von nummerngebundenen interpersonellen Kommunikationsdiensten die Rufnummern von Endnutzern, die einen Notrufdienst anrufen, anzuzeigen haben. Diese Anzeige der Rufnummer hat auch dann zu erfolgen, wenn der Endnutzer seine Rufnummer normalerweise unterdrückt bzw. keine Einwilligung für die Verarbeitung von Metadaten gegeben hat. Die Anzeige der Rufnummer erfolgt zum Zwecke der Beantwortung der Anrufe und ist anschlussbezogen bei den Einrichtungen einzurichten, die die Notrufe bearbeiten, einschließlich der Notrufabfragestellen. In ErwG 28 wird erläutert, dass die Anzeige der Rufnummer des anrufenden Endnutzers sowie seine Standortdaten, wenn erforderlich, an Notrufdienste wie

¹⁰³ aaO, Art 12 Abs 2.

¹⁰⁴ Pöchersdorfer, Winfried, Vorschlag der Europäischen Kommission für die Überarbeitung der Richtlinie über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation – Richtlinie 2002/58/EG, COM (2017) 10 final v 10.01.2017 [Vorschlag EK-DSVO] – Stellungnahme, 10.04.2017, 2.

beispielsweise eCall übermittelt werden sollen, damit diese ihre Aufgaben so effektiv wie möglich erfüllen können.

Art 10 lit b e-Privacy Richtlinie wurde in § 98 TKG - Auskünfte an Betreiber von Notrufdiensten - umgesetzt. In § 98 Abs 1 TKG wird präzisiert, dass die „Voraussetzung für die Zulässigkeit der Übermittlung ein Notfall ist, der nur durch Bekanntgabe dieser Information abgewehrt werden kann“. Somit erlaubt § 98 TKG nur dann eine Ausnahme zu § 104 TKG, wenn mit der Übermittlung der Daten einem Menschen in einem Notfall geholfen werden kann. „Den Betreiber des Notrufdienstes trifft die Verantwortung für die rechtliche Zulässigkeit des Auskunftsbegehens“¹⁰⁵.

Betreiber von Kommunikationsdiensten haben gemäß § 98 Abs 1 TKG Betreibern von Notrufdiensten auf deren Verlangen Auskünfte über Stammdaten iSv § 92 Abs 3 Z 3 lit a¹⁰⁶ sowie über Standortdaten iSd § 92 Abs 3 Z 6¹⁰⁷ zu erteilen. Die im TKG vorgesehene Übermittlung der Stammdaten ist jedoch weder in Art 10 lit b e-Privacy Richtlinie, noch in dem Entwurf der e-Privacy Verordnung erwähnt. Hier stellt sich die Frage, in wie weit die Stammdaten bei einem Notfall behilflich sind. Die Betreiber der Kommunikationsdienste haben immer nur den Namen des Vertragsinhabers gespeichert und bei einem Anruf ist es nicht klar, wer das Endgerät tatsächlich nutzt. Dies muss nicht der eigentliche Vertragspartner, sondern kann auch ein Mitarbeiter, Kind oder Partner des Vertragspartners sein.

Art 13 Abs 2 e-Privacy Verordnung regelt die Fangschaltung, die bisher in Art 10 lit a e-Privacy Richtlinie geregelt ist. Diese bestimmt, dass die Unterdrückung einer Rufnummer des Anrufers

¹⁰⁵ § 98 Abs 1 letzter Satz TKG.

¹⁰⁶ Definition von Stammdaten iSv § 92 Abs 3 Z 3 TKG: alle personenbezogenen Daten, die für die Begründung, die Abwicklung, Änderung oder Beendigung der Rechtsbeziehungen zwischen dem Benutzer und dem Anbieter oder zur Erstellung und Herausgabe von Teilnehmerverzeichnissen erforderlich sind; dies sind:

- a) Name (Familiename und Vorname bei natürlichen Personen, Name bzw. Bezeichnung bei juristischen Personen),
- b) akademischer Grad bei natürlichen Personen
- c) Anschrift (Wohnadresse bei natürlichen Personen, Sitz bzw. Rechnungsadresse bei juristischen Personen),
- d) Teilnehmernummer und sonstige Kontaktinformation für die Nachricht,
- e) Information über Art und Inhalt des Vertragsverhältnisses,
- f) Bonität

¹⁰⁷ Definition von Standortdaten iSd § 92 Abs 3 Z 6 TKG: Daten, die in einem Kommunikationsnetz oder von einem Kommunikationsdienst verarbeitet werden und die den geografischen Standort der Telekommunikationseinrichtung des Nutzers eines öffentlichen Kommunikationsdienstes angeben, im Fall von festen Telekommunikationsendeinrichtungen sind Standortdaten die Adresse der Einrichtung.

vorübergehend aufgehoben werden soll, wenn auf Antrag eines Endnutzers böswillige oder belästigende Anrufe zurückverfolgt werden.

Die Fangschaltung ist in Österreich in § 106 TKG umgesetzt worden und wird in Abs 1 als „die vom Willen des Anrufenden unabhängige Feststellung der Identität eines anrufenden Anschlusses“ definiert. Gemäß § 106 Abs 3 TKG gibt der Betreiber des Kommunikationsdienstes dem belästigten Endnutzer die Rufnummer bekannt, damit dieser gegen die andere Person rechtlich vorgehen kann.

5.3. Sperrung eingehender Anrufe

Betreiber öffentlich zugänglicher nummerngebundener interpersoneller Kommunikationsdienste haben gemäß Art 14 des Entwurfs zur e-Privacy Verordnung Maßnahmen zu treffen, die dem Stand der Technik entsprechen, um den Erhalt von unerwünschten Anrufen durch Endnutzer zu beschränken. Die getroffenen Maßnahmen sind kostenlos zur Verfügung zu stellen und sind jedenfalls, die Sperrung eingehender Anrufe von bestimmten Rufnummern oder von anonymen Quellen¹⁰⁸ sowie die Abstellung einer von einem Dritten veranlassten automatisierten Anrufweitschaltung zur Endeinrichtung des Endnutzers¹⁰⁹. Darunter fällt auch die Sperrung stiller Anrufe, wie beispielsweise durch Wählcomputer¹¹⁰ und anderer betrügerischer und belästigender Anrufe¹¹¹. Die Diskussionspapiere der Ratspräsidentenschaften sehen zusätzlich eine Sperrung von speziellen Rufnummern oder Vorwahlen vor, die in Art 16 Abs 3a e-Privacy Verordnung geregelt werden. Dazu wird in Kapitel 7 eingegangen.

Das Abstellen der automatisierten Anrufweitschaltung ist bereits in Art 11 e-Privacy Richtlinie geregelt und in Art 105 TKG umgesetzt worden. Diese Bestimmung sollte den Endnutzer vor eventuellen Belästigungen schützen.¹¹² Auch hier kritisiert die österreichische

¹⁰⁸ Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über die Achtung des Privatlebens und den Schutz personenbezogener Daten in der elektronischen Kommunikation und zur Aufhebung der Richtlinie 2002/58/EG (Verordnung über Privatsphäre und elektronische Kommunikation), Brüssel, 10.01.2017, Art 14 lit a.

¹⁰⁹ aaO, Art 14 lit b.

¹¹⁰ Beispiel siehe Stern.de (21.09.2019), Der Terror der Geisteranrufe. Onlinedokument: <https://www.stern.de/digital/smartphones/automatische-waehlcomputer-der-terror-der-geisteranrufe-3532052.html>; Download am 01.05.2018.

¹¹¹ Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über die Achtung des Privatlebens und den Schutz personenbezogener Daten in der elektronischen Kommunikation und zur Aufhebung der Richtlinie 2002/58/EG (Verordnung über Privatsphäre und elektronische Kommunikation), Brüssel, 10.01.2017, ErwG 29.

¹¹² 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

Wirtschaftskammer die Beibehaltung dieser Bestimmung, da die Sperre wie auch die Unterdrückung der Rufnummer durch Einstellungen in den Endgeräten vom Endnutzer selbst vorgenommen werden kann¹¹³. Eine Sperre im Kommunikationsnetz könnte auch zu Problemen führen und ist nicht mehr zeitgemäß.

Die Betreiber der Kommunikationsdienste haben gemäß ErwG 29 die Endnutzer auch über das Vorhandensein solcher Funktionen zu informieren, wie beispielsweise über Hinweise auf ihrer Webseite.

6. Öffentliche zugängliche Verzeichnisse

Art 15 Abs 1 des Entwurfs der Europäischen Kommission zur e-Privacy Verordnung regelt, dass Betreiber von öffentlich zugänglichen Verzeichnissen die Einwilligung von Endnutzern, die eine natürliche Person sind, einzuholen haben, wenn ihre personenbezogenen Daten in ein Verzeichnis aufgenommen werden. Des Weiteren sollen die Endnutzer die Möglichkeit haben die veröffentlichten Daten zu überprüfen und gegebenenfalls zu berichtigen bzw. zu löschen. Diese Möglichkeit muss gemäß Abs 4 kostenlos zur Verfügung gestellt werden. Gemäß Abs 2 soll der Endnutzer über die verfügbaren Suchfunktionen des Verzeichnisses informiert werden. Ist der Endnutzer eine natürliche Person, so hat dieser der Aktivierung einer Suchfunktion explizit einzuwilligen. Die Voraussetzungen für eine gültige Einwilligung sind Art 7 DSGVO zu entnehmen.

Die Art 29 Gruppe kritisiert in ihrer Stellungnahme zum Entwurf der Europäischen Kommission, dass die Voraussetzungen für das Erfordernis der Einwilligung zu undeutlich sind¹¹⁴. Der ErwG 31 konkretisiert, dass die natürliche Person, die die Einwilligung gibt, auch entscheiden können muss, welche Datenkategorien in das Verzeichnis aufgenommen werden und nach welchen Suchkriterien gesucht werden darf. Dies ist dem eigentlichen Verordnungstext nicht so klar zu

elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation), ErwG 37, ABl. L 2002/201, 37ff.

¹¹³ Illibauer, Ursula, Positionspapier zum Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über die Achtung des Privatlebens und den Schutz personenbezogener Daten in der elektronischen Kommunikation und zur Aufhebung der Richtlinie 2002/58/EG (Verordnung über Privatsphäre und elektronische Kommunikation), 5.3.2018, 4.

¹¹⁴ Article 29 Data Protection Working Party, Opinion 01/2017 on the Proposed Regulation for the e-Privacy Regulation (2002/58/EC), 2017, 25, Rn. 37.

entnehmen. Anschließend kritisiert die Art 29 Gruppe, dass juristische Personen gemäß Art 15 Abs 3 des Entwurfs zur e-Privacy Verordnung nur der Aufnahme in ein öffentliches Verzeichnis widersprechen können und nicht, wie auch natürliche Personen, die explizite Einwilligung geben sollen¹¹⁵.

Der Entwurf der e-Privacy Verordnung ist gegenüber der bestehenden Regelung in Art 12 e-Privacy Richtlinie sehr viel strenger, da bis jetzt der Endnutzer nur vor der Aufnahme in das Teilnehmerverzeichnis über den Zweck der Aufnahme der Daten in ein Teilnehmerverzeichnis bzw. über weitere Nutzungsmöglichkeiten wie die Suchfunktion informiert werden musste. Die Einholung der expliziten Einwilligung war bis jetzt nicht notwendig und ist in der Realität auch gar nicht so leicht möglich. In Österreich sind aufgrund Art 6 RL 98/10/EG und §18 iVm §69 Abs 3 TKG Betreiber von öffentlichen Telefondiensten, die mit dem der Endnutzer in einem Vertragsverhältnis stehen, verpflichtet die Teilnehmerdaten an die Betreiber von öffentlichen Teilnehmerverzeichnissen zu übermitteln¹¹⁶. Die Einwilligung oder Ablehnung zur Übermittlung der Daten wird somit durch die Telekombetreiber im Zuge der Vertragsbeziehung mit dem jeweiligen Endnutzer eingeholt. Der Betreiber der Teilnehmerverzeichnisse selbst hat zu keinem Zeitpunkt Kontakt zu den Endnutzern. Daher stellt sich für diese die Frage, wie sie eine Einwilligung iSd Entwurfs der e-Privacy Verordnung einholen können. Die Betreiber der öffentlichen Verzeichnisse haben keinen direkten Vertrag mit den Teilnehmern und dürfen somit den Teilnehmer nicht telefonisch oder mittels E-Mail kontaktieren¹¹⁷.

Die Befürchtungen der Betreiber öffentlicher Verzeichnisse wurden bereits von der estnischen Ratspräsidentschaft aufgegriffen und in einem entsprechenden Änderungsvorschlag¹¹⁸ zerstreut. Dieser bestimmt in Abs 1 der Adaptierung zur e-Privacy Verordnung nun, dass Betreiber von nummernbasierten interpersonellen Kommunikationsdiensten Endnutzern, die natürliche Personen sind, die Möglichkeit zu geben haben, bestimmen zu können, welche Datenkategorien

¹¹⁵ aaO, 25.

¹¹⁶ Pöchersdorfer, Winfried, Vorschlag der Europäischen Kommission für die Überarbeitung der Richtlinie über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation – Richtlinie 2002/58/EG, COM (2017) 10 final v 10.01.2017 [Vorschlag EK-DSVO] – Stellungnahme, 10.04.2017, 7.

¹¹⁷ aaO, 7.

¹¹⁸ Proposal for a regulation of the European Parliament and the Council concerning the respect for private life and protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) - Examination of the Presidency text (Articles 12 to 20 and related recitals, Brussels, 16. October 2017, 13217/17, 13.

in öffentlich zugänglichen Verzeichnissen enthalten sein sollen. Vorausgesetzt wird, dass nur jene Daten an die Betreiber der öffentlichen Verzeichnisse übermittelt werden, die für diesen Zweck erforderlich sind. Somit bleibt auch die bestehende Regelung bestehen, dass keine explizite Einwilligung für die Aufnahme in ein öffentlich zugängliches Verzeichnis, wie ein Telefonbuch, eingeholt werden muss.

Auch während der bulgarischen Ratspräsidentschaft wurden Adaptierungen vorgeschlagen. Es wurde im März 2018 der Abs 1a eingeführt, der dem Endnutzer das Recht gibt, die personenbezogenen Daten im öffentlichen Verzeichnis zu überprüfen, zu berichtigen oder zu löschen. Hierfür sind sowohl die Betreiber der öffentlichen Verzeichnisse als auch die Betreiber der Kommunikationsdienste zuständig¹¹⁹. Mit den Adaptierungen vom Juni 2018 wurde der Abs 1a wieder gestrichen und durch den Abs 1aa ersetzt. Dieser räumt den Mitgliedstaaten das Recht ein in der nationalen Gesetzgebung zu bestimmen, dass Endnutzer, die natürliche Personen sind, der Eintragung in öffentliche Verzeichnisse widersprechen können. Diese Bestimmung hätte zur Folge, dass es innerhalb der Europäischen Union zu unterschiedlichen nationalen Bestimmungen führen würde. Aus der Sicht der Unternehmen wird eine generelle opt-out Variante bevorzugt, da dies aus ihrer Sicht auch dem Zwecke der Verzeichnisse entsprechen würde¹²⁰. Jedoch liegt es im Interesse vor allem von internationalen Unternehmen, dass alle Mitgliedstaaten dieselben gesetzlichen Bestimmungen haben und so weniger Anpassungen für Endkunden in unterschiedlichen Mitgliedstaaten getroffen werden müssen. Daher setzt sich die österreichische Wirtschaftskammer für eine Variante ein, in der die Betreiber der Kommunikationsdienste die Endnutzer über die Aufnahme nur informieren und ihnen eine Widerspruchsmöglichkeit für den Eintrag in die öffentlichen Verzeichnisse einräumen¹²¹.

Gemäß Abs 2 des Vorschlages der estnische Ratspräsidentschaft soll der Betreiber der Kommunikationsdienste den Endnutzer, der eine natürliche Person ist, auch über die möglichen Suchfunktionen informieren und hierfür eine Einwilligung einholen, bevor diese aktiviert

¹¹⁹ Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) – Examination of the Presidency discussion paper; Brussels, 22. March 2018, 7207/18, 17 f.

¹²⁰ Illibauer, Ursula, Positionspapier zum Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über die Achtung des Privatlebens und den Schutz personenbezogener Daten in der elektronischen Kommunikation und zur Aufhebung der Richtlinie 2002/58/EG (Verordnung über Privatsphäre und elektronische Kommunikation), 5.3.2018, 4.

¹²¹ aaO, 5.

werden. Auch hier relativiert der Entwurf der bulgarischen Ratspräsidentschaft, indem eine Zustimmung für eine Suchfunktion nur dann eingeholt werden soll, wenn diese nicht auf dem Namen beruht¹²².

Gemäß Art 15 Abs 3 können Endnutzer, die juristische Personen sind, ihren Widerspruch für die Aufnahme in ein öffentlich zugängliches Verzeichnis bei ihrem Betreiber des Kommunikationsdienstes einlegen¹²³. Dieser ist des Weiteren auch Ansprechperson für die Endnutzer, unabhängig ob es sich um eine natürliche oder juristische Person handelt, wenn sie ihre personenbezogenen Daten gemäß Abs 3a überprüfen, korrigieren oder löschen möchten. Zusätzlich können die Mitgliedstaaten nach Abs 3aa mittels nationalem Recht bestimmen, dass die in Art 15 beschriebenen Pflichten auch oder nur für den Betreiber der öffentlichen Verzeichnisse anzuwenden sind.

Die Wirtschaftskammer Österreich setzt sich auch mit der Frage auseinander, ob Art 15 e-Privacy Verordnung auch für Suchmaschinen anwendbar ist. Diese bieten ebenfalls eine Suchfunktion von natürlichen Personen sowie ihrer Kommunikationsdaten mittels Algorithmen an, wenn diese im Internet veröffentlicht wurden. Sind diese Bestimmungen nicht anwendbar, so müssen Suchmaschinen zwar gemäß Art 17 DSGVO – Recht auf Vergessenwerden – eine Löschung der Daten ermöglichen, jedoch keine Einwilligung der jeweiligen betroffenen Person einholen. Dies würde für Betreiber öffentlicher Verzeichnisse eine klare Benachteiligung sowie einen Wettbewerbsnachteil von nationalen Betreibern gegenüber Suchmaschinenbetreibern bedeuten, da beide Unternehmensbranchen dieselben personenbezogenen Daten verarbeiten¹²⁴.

Endnutzer, die juristische Personen sind, sollen gemäß Abs 3 die Möglichkeit haben, dem Eintrag in das öffentliche Verzeichnis zu widersprechen. Die Voraussetzungen für das Recht auf

¹²² Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) – Examination of the Presidency discussion paper; Brussels, 22. March 2018, 7207/18, 17.

¹²³ Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) – Examination of the Presidency discussion paper, Brussels, 12. June 2018, 9958/18, 63.

¹²⁴ Pöchersdorfer, Winfried, Vorschlag der Europäischen Kommission für die Überarbeitung der Richtlinie über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation – Richtlinie 2002/58/EG, COM (2017) 10 final v 10.01.2017 [Vorschlag EK-DSVO] – Stellungnahme, 10.04.2017, 7.

Widerspruch sind in Art 21 DSGVO geregelt. Demnach hat die betroffene Person das Recht jederzeit gegen die Verarbeitung der sie betreffenden personenbezogenen Daten Widerspruch einzulegen, die aufgrund der rechtlichen Grundlage iSd Art 6 Abs 1 lit e oder f DSGVO erfolgt. So könnte man annehmen, dass die Verarbeitung der Daten einer juristischen Person in einem öffentlich zugänglichen Verzeichnis auf der rechtlichen Grundlage des berechtigten Interesses des Verantwortlichen oder eines Dritten beruht. In diesem Fall ist die DSGVO jedoch nicht anwendbar, da es sich hier um Daten von juristischen Personen handelt und diese nicht in den Anwendungsbereich der DSGVO fallen. ErwG 14 stellt eindeutig fest, dass personenbezogene Daten einer juristischen Person, einschließlich Name, Rechtsform sowie die Kontaktdaten eines Unternehmens nicht vom Schutz der DSGVO umfasst sind. Die e-Privacy Verordnung möchte hier entgegenwirken und den juristischen Personen ein Widerspruchsrecht für die Verarbeitung und somit auch Veröffentlichung ihrer Daten zur Verfügung stellen. Unternehmensvertreter sehen hier eine Systemwidrigkeit zur DSGVO und lehnen diese Regelung ab¹²⁵. Dies würde aber zur Folge haben, dass juristische Personen überhaupt kein Recht eingeräumt wird über die Veröffentlichung oder eben Nicht-Veröffentlichung zu bestimmen.

Als Übergangsbestimmung wird in Abs 4a geregelt, dass Endnutzer der Verarbeitung ihrer personenbezogenen Daten widersprechen können, die bereits vor Inkrafttreten der e-Privacy Verordnung in einem öffentlichen Verzeichnis aufgenommen wurden¹²⁶. In diesem Fall wäre der Eintrag im öffentlichen Verzeichnis mit dem Widerspruch zu löschen.

¹²⁵ aaO, 7.

¹²⁶ Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) – Examination of the Presidency discussion paper, Brussels, 12. June 2018, 9958/18, 64.

7. Unerbetene Kommunikation

7.1. Einwilligung oder Widerspruch

In Art 21 DSGVO wird geregelt, dass betroffene Personen der Verarbeitung von personenbezogenen Daten zur Direktwerbung sowie Profiling, das mit Direktwerbung in Verbindung steht, jederzeit widersprechen können müssen¹²⁷. Dies führt zu dem Schluss, dass für Direktwerbung keine explizite Einwilligung eingeholt werden muss. Was unter Direktwerbung zu verstehen ist, ist jedoch nicht in der DSGVO, sondern in den Begriffsbestimmungen in der e-Privacy Verordnung definiert:

Art 4 Abs 3 lit f e-Privacy Verordnung versteht unter Direktwerbung: „jede Art der Werbung in schriftlicher oder mündlicher Form, die an einen oder mehrere bestimmte oder bestimmbare Endnutzer elektronischer Kommunikationsdienste gerichtet wird, auch mittels automatischer Anruf- und Kommunikationssysteme mit oder ohne menschliche(r) Beteiligung, mittels E-Mail, SMS-Nachrichten, usw.“

Gemäß diesen Begriffsbestimmungen wird nicht unterschieden, ob zwischen der werbenden Person und dem Endnutzer ein Kundenverhältnis besteht oder nicht. Auch zwischen den Kommunikationsarten wird kein Unterschied gemacht. Mit der e-Privacy Verordnung wird offensichtlich versucht der unternehmensfreundlichen Bestimmung entgegenzusteuern indem davon ausgegangen wird, dass es sich bei Werbung grundsätzlich immer um unerbetene Kommunikation handelt. Aus diesem Grund wurde dieses Kapitel auch bereits in der e-Privacy Richtlinie und im TKG immer als „unerbetene Kommunikation“ tituliert.

Art 16 Abs 1 e-Privacy Verordnung regelt somit, dass Direktwerbung an eine natürliche Person nur dann erlaubt ist, wenn sie dieser ausdrücklich zugestimmt hat. Als *lex specialis* geht die e-Privacy Verordnung der DSGVO vor und verdrängt damit den Art 21 DSGVO in vielen Anwendungsbereichen.

In dem ersten Entwurf der Europäischen Kommission zur e-Privacy Verordnung wird in Abs 2 eine Ausnahme zu dem allgemeinen Verbot von Direktwerbung ohne Einwilligung gesetzt. Hat die werbende Person die Kontaktdaten im Zusammenhang mit dem Verkauf eines Produkts oder einer Dienstleistung erhalten, so darf die E-Mail-Adresse zum Zwecke der Direktwerbung von

¹²⁷ Art 21 Abs 2 DSGVO.

eigenen ähnlichen Produkten oder Dienstleistungen verwendet werden. Dies ist jedoch auch nur unter der Voraussetzung erlaubt, wenn der Kunde bei der Angabe seiner Kontaktdaten die Möglichkeit hatte, der Direktwerbung auf einfache Weise und kostenlos zu widersprechen. Zudem muss der Kunde auch bei jedem Versand jeder Nachricht die Möglichkeit haben der Zusendung von Direktwerbung einfach zu widersprechen.

Diese Bestimmung entspricht der bisherigen Regelung in der e-Privacy Richtlinie sowie auch der österreichischen Umsetzung in § 107 TKG. Da nur elektronische Kommunikationsdienste in diese Regulierung hineinfallen, ist die Werbung mittels „altmodischer“ Post nicht von dieser Bestimmung betroffen. Die Wirtschaftskammer Österreich¹²⁸ kritisiert nicht nur diesen Umstand, sondern auch, dass die Direktwerbung ausschließlich auf die Kommunikation per E-Mail mit einer Widerspruchsmöglichkeit erlaubt wird. Andere Kommunikationskanäle wie beispielsweise Telefonie, SMS oder Instant Messaging bedürfen weiterhin einer Einwilligung. Diese Bestimmung sei im Zuge der Schnellebigkeit der von den Kunden verwendeten Technologien nicht mehr zeitgemäß und auch nicht technologieneutral.

Auch in diesem Punkt hat die bulgarische Ratspräsidentschaft versucht in seinem Änderungsvorschlag den Einsprüchen der Unternehmensvertreter entgegenzukommen und erlaubt die Direktwerbung über sämtliche elektronischen Nachrichtenformen¹²⁹. Mit dieser Erweiterung kann die werbende Person zusätzlich zu E-Mail auch die Kommunikationskanäle SMS, MMS und ähnliche Applikationen oder Technologien nutzen¹³⁰. Der Änderungsvorschlag hebt zudem auch noch einmal hervor, dass der Kunde bei der Angabe der Kontaktdaten die Möglichkeit haben muss, der Nutzung seiner Kontaktdaten für Direktmarketing zu widersprechen. Im Änderungsvorschlag wurde in Abs 2a die Möglichkeit für Mitgliedstaaten ergänzt, dass sie in nationalen Gesetzen den Zeitraum bestimmen können, in dem die Daten ohne

¹²⁸ Pöchersdorfer, Winfried, Vorschlag der Europäischen Kommission für die Überarbeitung der Richtlinie über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation – Richtlinie 2002/58/EG, COM (2017) 10 final v 10.01.2017 [Vorschlag EK-DSVO] – Stellungnahme, 10.04.2017, 8.

¹²⁹ Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) – Examination of the Presidency discussion paper; Brussels, 22. March 2018, 7207/18, 18.

¹³⁰ Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) – Examination of the Presidency discussion paper, Brussels, 12. June 2018, 9958/18, 45.

Einwilligung verwendet werden dürfen¹³¹. Im ersten Entwurf des Abs 2a wurde die Verarbeitung der Kontaktdaten zum Zwecke des Direktmarketings ohne Einwilligung des Endnutzers nur für den Zeitraum von 12 Monaten bestimmt¹³². Möchte das Unternehmen seine Kunden über den Zeitraum hinaus Werbung übermitteln, so müsste es hierfür eine explizite Einwilligung einholen.

Natürliche und juristische Personen, die Direktwerbung übermitteln, haben sich gemäß Art 16 Abs 6 e-Privacy Verordnung an gewisse Informationspflichten zu halten. Sie haben die Endnutzer über den Werbecharakter der Nachricht zu informieren. Auch die Identität der natürlichen oder juristischen Person ist bekannt zu geben, in deren Namen die Nachricht übermittelt wird. Im Änderungsentwurf wurde noch hinzugefügt, dass ausschließlich echte Kontaktdaten angegeben werden dürfen, damit diese vom Endnutzer auch tatsächlich erreicht werden können¹³³. Des Weiteren hat die Nachricht die notwendigen Informationen zu beinhalten, die es dem Empfänger ermöglichen auf einfache Weise sein Recht auszuüben, die Einwilligung in den weiteren Empfang von Werbenachrichten zu widerrufen.

7.2. Werbeanrufe

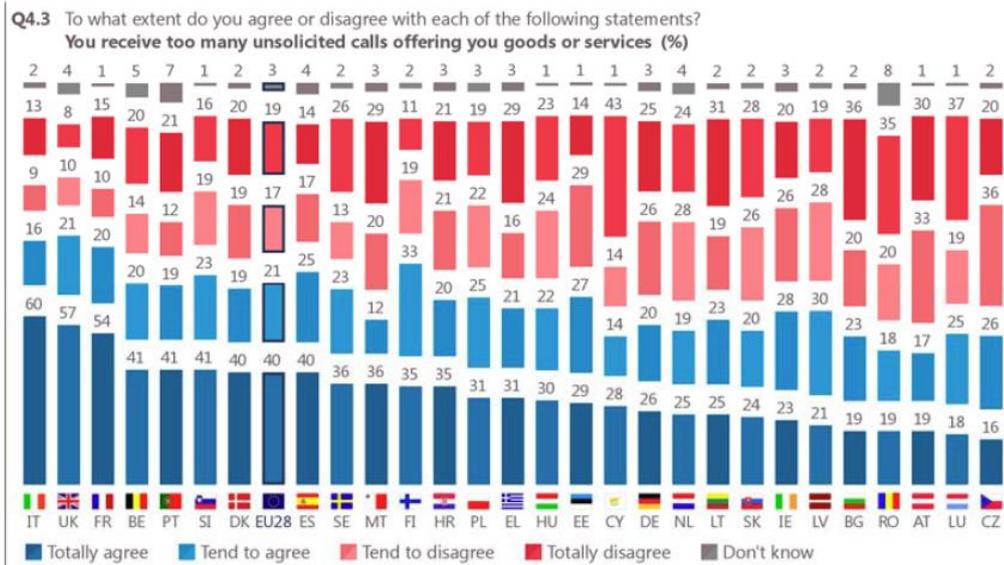
Die Eurobarometer Studie aus dem Jahr 2016¹³⁴ hat ergeben, dass sich 61% der befragten EU-Bürger durch Werbeanrufe belästigt fühlen und sich wünschen, dass diese leichter erkennbar werden. Befragte Personen aus Italien, Großbritannien und Frankreich fühlen sich mit zwischen 54% und 60% der Umfrageteilnehmer am meisten durch Werbeanrufe belästigt. In diesen Ländern besteht im Gegensatz zu Österreich eine Widerspruchs - Regelung für Werbeanrufe.

¹³¹ aaO, 65.

¹³² Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) – Examination of the Presidency discussion paper; Brussels, 22. March 2018, 7207/18, 19.

¹³³ aaO, 20.

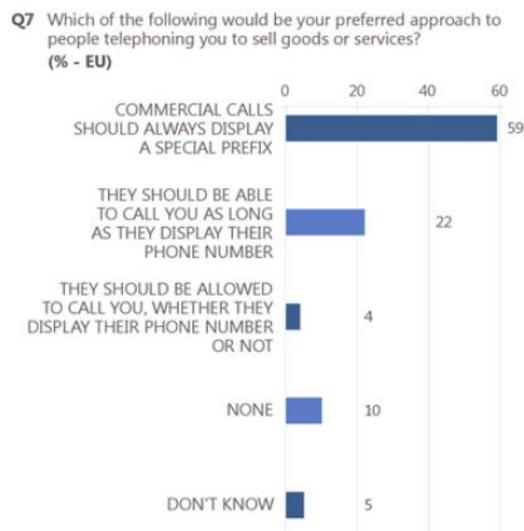
¹³⁴ European Commission, Flash Eurobarometer 443, Briefing note on e-Privacy (July 2016). Onlinedokument: <http://ec.europa.eu/commfrontoffice/publicopinion/index.cfm/ResultDoc/download/DocumentKy/76378>; Download am 19.06.2018.



Base: Respondents who use a fixed phone line or a mobile phone (N=26,241)

Abbildung 6: Ergebnis der Eurobarometer – Studie 2016: Belästigung durch zu viele Direktwerbeanrufe nach EU-Mitgliedstaaten

Diese Umfrage hat des Weiteren ergeben, dass 59% der Studienteilnehmer sich wünschen, dass man Werbeanrufe durch die Vorwahl erkennen kann. Nur 22% der Befragten sind der Meinung, dass es ausreicht, wenn die Rufnummer angezeigt wird. 4% sind der Meinung, dass es unwichtig ist, ob überhaupt eine Rufnummer bei Werbeanrufen angezeigt wird.



Base: Respondents who use a fixed phone line or a mobile phone (N=26,241)

Abbildung 7: Ergebnis der Eurobarometer Studie 2016: Erkennung von Direktwerbeanrufen

Aufgrund der Umfrageergebnisse der Eurobarometer Studie aus dem Jahr 2016 ist die Europäische Kommission zu dem Schluss gekommen, dass der Umgang mit Direktwerbeanrufen

nicht ausreichend reguliert ist¹³⁵. Die e-Privacy Richtlinie sieht keine Bestimmung zum Umgang mit Direktwerbeanrufen vor. Dies hat dazu geführt, dass es Mitgliedstaaten gibt, die sogenannte „Cold Calls“, also Werbeanrufe ohne vorherige explizite Einwilligung des Endnutzers oder Kundenbeziehung ganz verbieten, andere Mitgliedstaaten sehen nur einen Widerspruch vor. Aufgrund der unterschiedlichen rechtlichen Voraussetzungen, sind auch die Umfrageergebnisse der Eurobarometer Studie je nach Mitgliedstaat unterschiedlich ausgefallen. Die Europäische Kommission hat sich daher eine einheitliche Regelung für alle Mitgliedstaaten im Entwurf der e-Privacy Verordnung als Ziel vorgenommen.

Art 16 Abs 3 e-Privacy Verordnung regelt, dass natürliche oder juristische Personen, die Direktwerbeanrufe tätigen, eine Rufnummer anzugeben haben unter der sie erreichbar sind¹³⁶. Laut Abs 3a des Änderungsvorschlags der bulgarischen Ratspräsidentschaft können die Mitgliedstaaten durch nationales Recht bestimmen, dass die werbetreibenden Personen eine bestimmte Vorwahl oder Code anzuwenden haben, der den Endnutzer eindeutig erkennen lässt, dass es sich um Direktwerbeanrufe handelt¹³⁷.

Unabhängig davon haben die Mitgliedstaaten die Möglichkeit durch nationale Rechtsvorschriften zu bestimmen, dass Endnutzer, die natürliche Personen sind, nur dann angerufen werden dürfen, wenn sie dem Erhalt von Direktwerbeanrufen nicht vorher widersprochen haben¹³⁸. Diese Bestimmung erlaubt den Mitgliedstaaten von dem allgemeinen Gebot abzugehen, dass immer eine Einwilligung des Endnutzers für Direktwerbeanrufe einzuholen ist.

¹³⁵ European Commission, Commission Staff Working Document, Impact Assessment, Accompanying the document Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications), Brussels, 10.01.2017.

¹³⁶ Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über die Achtung des Privatlebens und den Schutz personenbezogener Daten in der elektronischen Kommunikation und zur Aufhebung der Richtlinie 2002/58/EG (Verordnung über Privatsphäre und elektronische Kommunikation), Brüssel, 10.01.2017, Art 16 Abs 3 lit a.

¹³⁷ Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) – Examination of the Presidency discussion paper, Brussels, 12. June 2018, 9958/18, 65.

¹³⁸ Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über die Achtung des Privatlebens und den Schutz personenbezogener Daten in der elektronischen Kommunikation und zur Aufhebung der Richtlinie 2002/58/EG (Verordnung über Privatsphäre und elektronische Kommunikation), Brüssel, 10.01.2017, Art 16 Abs 4.

7.3 Juristische Personen

Die oben beschriebenen Bestimmungen des Art 16 der e-Privacy Verordnung schützen ausschließlich Endnutzer, die natürliche Personen sind. Dies ist eine Ausnahme zu den anderen Bestimmungen der e-Privacy Verordnung, da diese grundsätzlich immer natürliche und juristische Personen gleich schützt. Um diesem Umstand entgegen zu treten, regelt Abs 5, dass die Mitgliedstaaten im Rahmen des Unionsrechts sicherzustellen haben, dass die Interessen von Endnutzern, die juristischen Personen sind, ausreichend geschützt werden. Wie dieser Schutz aussieht, kann jeder Mitgliedstaat selbst entscheiden.

Aus diesem Grund hat die Wirtschaftskammer Österreich angeregt, dass es eine „opt-out Lösung für Unternehmen“ geben soll¹³⁹. Die Wirtschaftskammer unterscheidet in ihrer Stellungnahme absichtlich nicht zwischen natürlicher und juristischer Person, sondern zwischen Unternehmen und Konsumenten. So soll Direktwerbung an Unternehmen, auch wenn es sich um natürliche Personen handelt, ohne explizite Zustimmung möglich sein. Ein Widerspruch, nach dem Vorbild des Art 21 DSGVO, soll den Unternehmen gewährt werden.

8. Rechtsbehelfe, Haftung und Sanktionen

8.1 Zuständige Aufsichtsbehörde

In Verbindung mit der e-Privacy Richtlinie wurde die VO (EU) 611/2013¹⁴⁰ erlassen, die die Meldung von Datensicherheitsverletzungen regelt. Diese bestimmt, dass Betreiber von öffentlichen Kommunikationsdiensten die zuständige Aufsichtsbehörde bei einer Verletzung des Schutzes von personenbezogenen Daten innerhalb von 24 Stunden benachrichtigen müssen. Eine Zweitmeldung mit genaueren Informationen kann innerhalb von drei weiteren Tage erfolgen. Gemäß § 95a TKG ist für diese Meldungen die österreichische Datenschutzbehörde die zuständige Behörde. Mit Inkrafttreten der DSGVO besteht gemäß Art 33 eine Meldepflicht von Datensicherheitsverletzungen für alle Verantwortlichen einer Datenverarbeitung innerhalb von

¹³⁹ Pöchersdorfer, Winfried, Vorschlag der Europäischen Kommission für die Überarbeitung der Richtlinie über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation – Richtlinie 2002/58/EG, COM (2017) 10 final v 10.01.2017 [Vorschlag EK-DSVO] – Stellungnahme, 10.04.2017, 8.

¹⁴⁰ Verordnung (EU) Nr. 611/2013 der Kommission vom 24. Juni 2013 über die Maßnahmen für die Benachrichtigung von Verletzungen des Schutzes personenbezogener Daten gemäß der Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates (Datenschutzrichtlinie für elektronische Kommunikation), ABl. L 2013/173, 2ff.

72 Stunden. Auch in diesen Fällen ist in Österreich die Datenschutzbehörde die zuständige Behörde¹⁴¹. Da VO (EU) 611/2013 als *lex specialis* zur DSGVO anzusehen ist, haben Betreiber von öffentlichen Kommunikationsdiensten weiterhin Datensicherheitsverletzungen innerhalb von 24 Stunden an die Datenschutzbehörde zu melden.

Der Entwurf der Europäischen Kommission zur e-Privacy Verordnung bestimmt in Art 18 Abs 1, dass die zuständigen Behörden nach der DSGVO auch für die Überwachung der Einhaltung der e-Privacy Verordnung zuständig werden¹⁴². Dies wurde in den weiteren Änderungsvorschlägen adaptiert. So bestimmt Art 18 im Entwurf der bulgarischen Ratspräsidentschaft, dass die Mitgliedstaaten zuständige Aufsichtsbehörden zur Überwachung der e-Privacy Verordnung selbst benennen sollen¹⁴³. Jedoch sollen jene Aufsichtsbehörden, die auch gemäß der DSGVO zuständig sind, für die Einhaltung der Bestimmungen in Kapitel II der e-Privacy Verordnung zuständig bleiben. Hier handelt es sich um die Art 5 – 11 e-Privacy Verordnung. Die Kapitel VI (Unabhängige Aufsichtsbehörden) und Kapitel VII (Zusammenarbeit und Kohärenz) der DSGVO werden auch für die e-Privacy Verordnung anwendbar. Dies bedeutet, dass die zuständigen Aufsichtsbehörden im Sinne der DSGVO auch für die Beschwerden der Endnutzer im Sinne der e-Privacy Verordnung verantwortlich sind.

Die neu eingeführten Absätze 1a und Abs 1aa bestimmen, dass die Mitgliedstaaten selbst bestimmen sollen, welche kompetente Aufsichtsbehörde die Einhaltung des Kapitels III überwachen soll. Hier wurde von der österreichischen Wirtschaftskammer kritisiert, dass sich die Regulierungsbehörde im Telekommunikationsrecht besser als die Datenschutzbehörde in der Materie auskenne und somit diese die Überwachung dieser Bestimmungen übernehmen sollte¹⁴⁴. Des Weiteren wird in Abs 1ab klargestellt, dass die zuständigen Behörden die rechtliche

¹⁴¹ § 18 Abs 1 DSG: Die Datenschutzbehörde wird als nationale Aufsichtsbehörde gemäß Art 51 DSGVO eingerichtet.

¹⁴² Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über die Achtung des Privatlebens und den Schutz personenbezogener Daten in der elektronischen Kommunikation und zur Aufhebung der Richtlinie 2002/58/EG (Verordnung über Privatsphäre und elektronische Kommunikation), Brüssel, 10.01.2017, Art 18 Abs 1.

¹⁴³ Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) – Examination of the Presidency discussion paper, Brussels, 12. June 2018, 9958/18, 68 f.

¹⁴⁴ Illibauer, Ursula, Positionspapier zum Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über die Achtung des Privatlebens und den Schutz personenbezogener Daten in der elektronischen Kommunikation und zur Aufhebung der Richtlinie 2002/58/EG (Verordnung über Privatsphäre und elektronische Kommunikation), 5.3.2018, 7.

Befugnis haben müssen, Abhilfe gegen Missstände sowie Geldbußen zu erlassen. Sollten mehrere Aufsichtsbehörden zuständig sein, so sollen diese gemäß Abs 1b miteinander kooperieren.

Die Behörden haben gemäß Art 18 Abs 2, wenn es zweckmäßig ist, auch mit anderen nationalen Aufsichtsbehörden zusammenzuarbeiten, die nach dem EECC für die Betreiber der Kommunikationsdienste zuständig sind. In Österreich ist dies in der Regel die Telekom-Control-Kommission, kurz TKK.

Würde der neue Änderungsentwurf von den Mitgliedstaaten übernommen werden, würde Österreich entscheiden müssen, für die Überwachung des Kapitels III die Datenschutzbehörde oder die TKK zuständig werden. Nach der derzeitigen österreichischen Rechtslage ist das Fernmeldebüro, das vom Bundesministerium für Verkehr, Innovation und Technologie (Sektion III) wahrgenommen wird, für Verstöße gegen die unerbetene Kommunikation gemäß § 107 TKG zuständig. Es wird abzuwarten sein, ob sich hier die Zuständigkeit der Behörden ändern wird.

8.2 Rechtsbehelfe

Art 21 Abs 1 e-Privacy Verordnung räumt den Endnutzern elektronischer Kommunikationsdienste dieselben Rechte ein, die in den Artikeln 77, 78 und 79 DSGVO vorgesehen sind.

Art 77 DSGVO regelt das Recht auf Beschwerde bei einer Aufsichtsbehörde für die betroffene Person. Wichtig für die betroffene Person ist, dass die Beschwerde im Mitgliedstaat des Aufenthaltsortes oder des Arbeitsplatzes der betroffenen Person bzw. des Ortes des mutmaßlichen Verstoßes erhoben werden darf. So muss die Beschwerde nicht am Sitz des Verantwortlichen bzw. des Betreibers des Kommunikationsdienstes erhoben werden.

Art 78 DSGVO bestimmt, dass „jede natürliche oder juristische Person das Recht auf einen wirksamen gerichtlichen Rechtsbehelf gegen einen sie betreffenden rechtverbindlichen Beschluss einer Aufsichtsbehörde“ hat. Des Weiteren wird das Recht eingeräumt sich zu beschweren, wenn sich die Aufsichtsbehörde nicht mit einer Beschwerde befasst oder die betroffene Person nicht innerhalb von drei Monaten in Kenntnis über den Stand oder das Ergebnis der Beschwerde setzt.

Zuletzt räumt Art 79 DSGVO das Recht auf einen wirksamen gerichtlichen Rechtsbehelf gegen den Verantwortlichen oder den Auftragsverarbeiter ein. Im Sinne der e-Privacy Verordnung ist der Betreiber des Kommunikationsdienstes dem Verantwortlichen gleichzusetzen. Bedient er sich eines Auftragsverarbeiters, so kann der Endnutzer auch direkt gegen den Auftragsverarbeiter vorgehen. Für Klagen sind die Gerichte des Mitgliedstaates zuständig, in denen der Verantwortliche oder der Auftragsverarbeiter eine Niederlassung hat¹⁴⁵. Die betroffene Person kann aber auch entscheiden in jenem Mitgliedstaat gerichtlich vorzugehen, in dem sie ihren gewöhnlichen Aufenthalt hat¹⁴⁶.

Art 1a e-Privacy Verordnung bestimmt zusätzlich, dass für Endnutzer, die natürliche Personen sind, auch das Recht der Vertretung nach Art 80 DSGVO anwendbar ist¹⁴⁷. Demnach hat die betroffene Person das Recht, sich durch eine Einrichtung, Organisation oder Vereinigung ohne Gewinnerzielungsabsicht, die nach dem Recht des Mitgliedstaates gegründet wurde, vertreten zu lassen. Die von der betroffenen Person gewählte Organisation kann in dessen Namen eine Beschwerde einreichen sowie in den Art 77, 78 und 79 genannten Rechte wahrnehmen und des Weiteren Schadenersatz gemäß Art 82 DSGVO in Anspruch nehmen, sofern dies im Recht der Mitgliedstaaten vorgesehen ist. Dies ist im österreichischen DSG nicht vorgesehen¹⁴⁸. Aus Sicht der österreichischen Wirtschaftskammer sollte dieser Absatz gestrichen werden¹⁴⁹.

Art 21 Abs 2 e-Privacy Verordnung räumt auch Personen das Recht ein, die keine Endnutzer sind, gerichtlich vorzugehen, wenn sie durch einen Verstoß der e-Privacy Verordnung beeinträchtigt wurden.

¹⁴⁵ Art 79 Abs 2 Satz 1 DSGVO.

¹⁴⁶ Art 79 Abs 2 Satz 2 DSGVO.

¹⁴⁷ Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) – Examination of the Presidency discussion paper, Brussels, 12. June 2018, 9958/18, 73.

¹⁴⁸ § 28 DSG

¹⁴⁹ Illibauer, Ursula, Positionspapier zum Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über die Achtung des Privatlebens und den Schutz personenbezogener Daten in der elektronischen Kommunikation und zur Aufhebung der Richtlinie 2002/58/EG (Verordnung über Privatsphäre und elektronische Kommunikation), 5.3.2018, 7.

8.3 Haftung und Recht auf Schadenersatz

Art 22 e-Privacy Verordnung räumt jedem Endnutzer elektronischer Kommunikationsdienste das Recht auf Schadenersatz ein. Hierbei kann der Endnutzer Schadenersatz von materiellen und immateriellen Schäden gegen den Rechtsverletzer geltend machen, wenn dieser gegen die e-Privacy Verordnung verstoßen hat. Hier verweist Art 22 e-Privacy Verordnung auf Art 82 DSGVO. So wird auch nach der e-Privacy Verordnung die in Art 82 Abs 3 DSGVO vorgesehene Haftungsbefreiung anwendbar sein, die bestimmt, dass der Rechtsverletzer nicht haftet, wenn er nachweisen kann, dass er für den Umstand, dass der Schaden eingetreten ist, nicht verantwortlich ist.

8.4 Geldbußen und Sanktionen

Die derzeit noch in Kraft stehende e-Privacy Richtlinie hatte keine Bestimmungen zu den Geldbußen, die einzuhoben sind, wenn gegen die Richtlinie verstoßen wird. Somit wurden bis jetzt die Art der Sanktionen, die Höhe der Geldbußen sowie die Art der Verfahren von den Mitgliedstaaten selbst bestimmt. Der erste Entwurf der e-Privacy Verordnung verweist in Art 23 Abs 1 auf die Anwendung des Kapitel VII der DSGVO bei der Verhängung von Geldbußen, die aufgrund von Verstößen der e-Privacy Verordnung verhängt werden sollen¹⁵⁰. Kapitel VII der DSGVO regelt im ersten Abschnitt die Zusammenarbeit zwischen den Aufsichtsbehörden. Hier wird die prozessuale Vorgehensweise zwischen der federführenden Aufsichtsbehörde und den anderen betroffenen Aufsichtsbehörden sowie die Amtshilfe geregelt. Im zweiten Abschnitt wird das Kohärenzverfahren beschrieben. Um innerhalb der Mitgliedstaaten eine einheitliche Umsetzung der DSGVO zu gewährleisten, beschreibt die DSGVO sehr genau, wie das Kohärenzverfahren zwischen den Aufsichtsbehörden und gegebenenfalls mit der Kommission stattzufinden hat. Der dritte Abschnitt beschreibt den Europäischen Datenschutzausschuss. Dieser löste am 24. Mai 2018 die Artikel 29 Gruppe ab, die ein Zusammenschluss aller Datenschutzbehörden der Mitgliedstaaten war und Stellungnahmen sowie Leitlinien zu datenschutzrechtlichen Themen erlassen hat. Nun erhält der Europäische Datenschutzausschuss eine eigene Rechtspersönlichkeit und wird unabhängig. Mit dem Verweis in Art 23 Abs 1 e-Privacy Verordnung auf das Kapitel VII DSGVO ist der Europäische Datenschutzausschuss

¹⁵⁰ Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über die Achtung des Privatlebens und den Schutz personenbezogener Daten in der elektronischen Kommunikation und zur Aufhebung der Richtlinie 2002/58/EG (Verordnung über Privatsphäre und elektronische Kommunikation), Brüssel, 10.01.2017, Art 18 Abs 1.

ebenfalls für Themen der elektronischen Kommunikation zuständig und die Aufsichtsbehörden haben sich bei Verfahren gemäß der e-Privacy Verordnung an die selben prozessualen Vorschriften wie in der DSGVO zu halten. Dies erleichtert selbstverständlich die Umsetzung der e-Privacy Verordnung, da keine neuen Aufsichtsbehörden oder Ausschüsse eingerichtet werden müssen.

Dies wurde in den weiteren Entwürfen zur e-Privacy Verordnung geändert. Der Änderungsvorschlag der bulgarischen Präsidentschaft bestimmt in Art 19 e-Privacy Verordnung zusätzliche Aufgaben für den Europäischen Datenschutzausschuss in Bezug auf die e-Privacy Verordnung, nämlich die Beratung der Europäischen Kommission zu Änderungen dieser Verordnung, die Begutachtung sämtlicher Fragen und Erstellung von Leitlinien zu Kapitel II der e-Privacy Verordnung, die Erstellung von Leitlinien für die zuständigen Aufsichtsbehörden nach Art 18 e-Privacy Verordnung und 54 DSGVO. Des Weiteren soll der Europäische Datenschutzausschuss Kooperationen und internationalen Informationsaustausch, Schulungsprogramme sowie Erfahrungen und Gesetzesentwürfe zwischen den Aufsichtsbehörden fördern. Er soll soweit wie möglich sämtliche Meinungen, Leitlinien, Empfehlungen und Erfahrungen veröffentlichen und an die Europäische Kommission weiterleiten¹⁵¹.

Hingegen verweist Art 23 Abs 1 e-Privacy Verordnung nun mehr auf die Anwendbarkeit des Kapitel VIII der DSGVO. In diesem Kapitel sind die Bestimmungen zu Rechtsbehelfen, Haftung und Sanktionen geregelt.

Die e-Privacy Verordnung orientiert sich auch bei der Höhe der Geldbußen an der DSGVO. So unterscheidet sie ebenfalls zwischen leichteren und schweren Verstößen. Leichte Verstöße werden mit Geldbußen von bis zu EUR 10 Millionen oder im Fall eines Unternehmens von bis zu 2% seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahres, je nachdem was höher ist, geahndet. Bei schweren Verstößen können Geldbußen in einer Höhe von bis zu EUR 20 Millionen oder 4% des weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahres verhängt werden.

¹⁵¹ Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) – Examination of the Presidency discussion paper, Brussels, 12. June 2018, 9958/18, 69 ff.

In Art 23 Abs 2 werden sogenannte leichte Verstöße aufgezählt:

- a) Verstöße der Verpflichtungen einer juristischen oder natürlichen Person, die elektronische Kommunikation nach Art 8 verarbeitet;
- b) Verstöße der Verpflichtungen des Anbieters der Software, die eine elektronische Kommunikation nach Art 10 ermöglicht;
- c) Verstöße der Verpflichtungen des Betreibers öffentlich zugänglicher Verzeichnisse nach Art 15;
- d) Verstöße der Verpflichtungen einer juristischen oder natürlichen Person, die elektronische Kommunikationsdienste nach Art 16 nutzt.

Die höheren Geldbußen von bis zu 20 Millionen EURO bzw. 4% des weltweiten Jahresumsatzes des vergangenen Jahres, je nach dem was höher ist, sollen jedenfalls bei schweren Verstößen verhängt werden. Diese sind jene, die gegen die Vertraulichkeit der Kommunikation gemäß Art 5 e-Privacy Verordnung sowie jene, die gegen die erlaubte Verarbeitung elektronischer Kommunikationsdaten gemäß Art 6 und ihre Löschung gemäß Art 7 e-Privacy Verordnung verstoßen¹⁵². Diese Geldbußen kommen auch dann zur Anwendung, wenn eine Anweisung einer Aufsichtsbehörde nicht befolgt wird¹⁵³.

Über Vorschriften der Sanktionen für Verstöße der Art 12, 13 und 14 sollen die Mitgliedstaaten selbst entscheiden¹⁵⁴. Dies gilt aber auch für jene Verstöße, deren Sanktionen nicht in Art 23 e-Privacy VO geregelt sind¹⁵⁵. Die Mitgliedstaaten können des Weiteren darüber entscheiden, „ob und in welchem Umfang gegen Behörden und öffentliche Stellen“ Geldbußen verhängt werden können¹⁵⁶. Diese Bestimmung entspricht Art 83 Abs 6 DSGVO. Österreich hat von dieser Regelung Gebrauch gemacht und in § 30 Abs 5 DSG¹⁵⁷ geregelt, dass „gegen Behörden und öffentliche Stellen, wie insbesondere in Formen des öffentlichen Rechts sowie des Privatrechts eingerichtete Stellen, die im gesetzlichen Auftrag handeln, und gegen Körperschaften des öffentlichen Rechts“ keine Geldbußen verhängt werden. Aufgrund dieser

¹⁵² Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über die Achtung des Privatlebens und den Schutz personenbezogener Daten in der elektronischen Kommunikation und zur Aufhebung der Richtlinie 2002/58/EG (Verordnung über Privatsphäre und elektronische Kommunikation), Brüssel, 10.01.2017, Art 23 Abs 3.

¹⁵³ aaO, Art 23 Abs 5.

¹⁵⁴ aaO, Art 23 Abs 4.

¹⁵⁵ aaO, Art 24 Abs 1.

¹⁵⁶ aaO, Art 23 Abs 6.

¹⁵⁷ Bundesgesetz zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten (Datenschutzgesetz – DSG).

Bestimmung ist davon auszugehen, dass dies auch bei der Umsetzung der e-Privacy Verordnung der Fall sein wird.

9. Schlussbetrachtung

Die e-Privacy Verordnung sollte ursprünglich gemeinsam mit der DSGVO mit 25. Mai 2018 in Kraft treten. Die Verhandlungen für die DSGVO haben insgesamt vier Jahre andauert, es wird sich noch herausstellen, ob dies auch hier zutreffen wird. Aus den Änderungsvorschlägen während der einzelnen Ratspräsidentschaften ist ersichtlich, dass der Europäische Rat die Befürchtungen und Vorschläge der Unternehmen berücksichtigt. Im Vergleich zum ursprünglichen Entwurf sind bereits einige Erleichterungen erkennbar. Dennoch vertreten viele Unternehmen immer noch die Meinung, dass die DSGVO auch zum Schutz des Kommunikationsgeheimnisses vollkommen ausreicht und daher keine weitere Regulierung notwendig ist. Hingegen befürworten selbstverständlich Vertreter von Datenschutzorganisationen weiterhin die strengeren Bestimmungen für die elektronische Kommunikation. Es stellt sich jedoch die Frage, ob die e-Privacy Verordnung nicht obsolet wird, wenn der Zeitraum bis zu ihrem Inkrafttreten immer länger andauert. Unternehmen werden in dieser Zeit die DSGVO und die bereits bestehende e-Privacy Richtlinie umsetzen aber keine zusätzlichen datenschutzrechtlichen Schutzmaßnahmen etablieren.

Die Zukunft wird uns zeigen, ob die e-Privacy Verordnung in Zukunft tatsächlich erlassen wird oder ob aufgrund der vielen Meinungsverschiedenheiten zwischen den Unternehmen und Datenschutzorganisationen noch mehr Änderungsvorschläge ausgearbeitet werden und sich damit die Fertigstellung der Verordnung noch weiterhin verzögert. Experten gehen mittlerweile davon aus, dass die e-Privacy Verordnung im Jahr 2020/2021 in Kraft treten könnte¹⁵⁸.

Diese Situation ist von den Betreibern der elektronischen Kommunikationsdienste nicht erwünscht, da die bestehende e-Privacy Richtlinie kein level playing field zwischen den Anbietern der elektronischen Kommunikation schafft und diese eine Gleichberechtigung zwischen den Technologien anstreben.

Aus der Sicht der Endnutzer sind die Bestimmungen der e-Privacy Verordnung vorteilhafter, da diese sich in vielen Fällen in die Verarbeitung von personenbezogenen Daten einwilligen müssen. Damit wird die Verarbeitung von Kommunikationsdaten für den Endnutzer nachvollziehbarer als sie heute ist und erfüllt gerade bei dieser komplizierten Materie das in der

¹⁵⁸ Bundesverband Digitale Wirtschaft (BVDW) e.V., aktuelle Informationen zur ePrivacy Verordnung. Onlinedokument: <https://www.bvdw.org/themen/recht/kommunikationsrecht-eprivacy/>; Download am 26.08.2018.

DSGVO vorgesehene Grundprinzip der Transparenz. Der Datenschutz im Rahmen der e-Privacy Verordnung reicht oft weiter als in der DSGVO. So kann in manchen Fällen der Endnutzer gar nicht in eine Datenverarbeitung einwilligen, wenn die Dienstleistung auch mit anonymisierten Daten erbracht werden kann.

Wie bereits erwähnt, wird sich noch herausstellen, inwieweit die in dieser Arbeit beschriebenen Bestimmungen tatsächlich in Kraft treten werden.

9. Abstract

9.1 Abstract in Deutsch

In der Strategie für einen digitalen Binnenmarkt in Europa¹⁵⁹, stellt der Europäische Rat fest, dass sich die europäischen Unternehmen auf die neuen technischen Innovationen und die damit verbundene digitale Zukunft vorbereiten müssen. Nur so kann der hohe Lebensstandard für die europäischen Bürger gewährleistet werden. So ist dem Europäischen Rat auch bewusst, dass Big Data, Cloud-Dienste und das Internet der Dinge wichtige Voraussetzungen für die Wettbewerbsfähigkeit von europäischen Unternehmen auf dem internationalen Markt sind.¹⁶⁰

Gleichzeitig soll auch die Privatsphäre der einzelnen Nutzer dieser neuen Dienste nach dem hohen europäischen Standard weiterhin geschützt werden. Die Europäische Union geht davon aus, dass die allgemeinen Datenschutzbestimmungen nach der DSGVO für den Schutz der Privatsphäre der elektronischen Kommunikation nicht ausreichen, da die Unternehmen durch die Kommunikationsinhalte und –metadaten sehr großen Einblick in persönliche Vorlieben der einzelnen Nutzer bekommen.

Aus diesem Grund wurde geplant, dass gleichzeitig mit dem Inkrafttreten der DSGVO am 25. Mai 2018 auch die Verordnung des Europäischen Parlaments und des Rates über die Achtung des Privatlebens und den Schutz personenbezogener Daten in der elektronischen Kommunikation und zur Aufhebung der Richtlinie 2002/58/EG, kurz e-privacy Verordnung, in Kraft tritt.

¹⁵⁹ Rat der Europäischen Union, Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen – Strategie für einen digitalen Binnenmarkt für Europa, Brüssel, 06.Mai 2015, 8672/15

¹⁶⁰ aaO, 16.

Gleichzeitig sollte die veraltete Richtlinie 2002/58/EG abgelöst und die Prinzipien der DSGVO übernommen werden.¹⁶¹ Dieses Ziel konnte aufgrund von Meinungsverschiedenheiten der unterschiedlichen Positionen in den europäischen Gremien nicht erreicht werden. Es stellt sich nun die Frage, wann und mit welchem Inhalt die e-Privacy Verordnung in Kraft treten wird. Die von diesen Bestimmungen betroffenen Unternehmen bringen ihre Standpunkte beim Entstehungsprozess dieser Verordnung ein, da sie durch die e-Privacy Verordnung große Einschränkungen bei der Verarbeitung von Daten im Vergleich zu den Bestimmungen der DSGVO befürchten.

Diese Master Thesis behandelt in ihrem ersten Kapitel die Rechtsgrundlage, auf die sich die Europäische Kommission stützt, die e-privacy Verordnung zu erlassen sowie die Ausdehnung der bestehenden Regulierung und den Versuch der europäischen Kommission ein level playing field für die elektronische Kommunikation zu schaffen. Im zweiten Kapitel werden das Kommunikationsgeheimnis sowie die Verarbeitung der elektronischen Kommunikation und die damit verbundenen Einschränkungen im Verhältnis zur DSGVO dargestellt. Das dritte Kapitel beschäftigt sich mit der neuen Bestimmung für Webtracking und Cookies und die damit verbundenen Befürchtungen, vor allem der Werbevermarkter. Das vierte Kapitel beschäftigt sich mit dem Recht jedes Nutzers seine Rufnummer zu unterdrücken aber auch der Fangschaltung und der Beauskunftung der Notrufdienste. Im fünften Kapitel wird die neue Regelung für öffentliche Verzeichnisse sowie die damit verbundenen Argumente von betroffenen Unternehmen beleuchtet. Das sechste Kapitel widmet sich den Bestimmungen über die unerbetene Kommunikation bzw. der Direktwerbung. Diese Bestimmung betrifft jedes Unternehmen, das seine Werbung über E-Mail, SMS, Telefonie oder Messaging-Dienste¹⁶² an seine bestehenden oder potentiellen Kunden übermitteln möchte. Mit dieser Bestimmung kommt es zu einer deutlichen Schlechterstellung gegenüber der sehr liberalen Regelung in Art 21 DSGVO und führt dazu, dass die Unternehmen noch viel mehr von Einwilligungserklärungen der Nutzer abhängig sind. Das siebte Kapitel geht auf die Sanktionen ein, die bei einem Verstoß gegen diese Verordnung drohen. Die e-Privacy Verordnung lehnt sich an der Struktur der DSGVO an und regelt Geldbußen in einer Höhe von bis zu 20 Millionen Euro bzw. 4% des

¹⁶¹ 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 2002/201, 37ff.

¹⁶² Unter Messaging Dienste sind Nachrichten über WhatsApp, Facebook, etc. zu verstehen.

gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahres, je nachdem welcher Betrag höher ist.

In dieser Master Thesis wird der Entwurfstext sowie die Änderungsvorschläge der Ratspräsidentschaften analysiert, auf strittige Punkte eingegangen und die verschiedenen Standpunkte von der Interessenverbänden sowie der Art 29 Gruppe¹⁶³, dargestellt. Die Zukunft wird zeigen, welche dieser Positionen sich im Europäischen Parlament und Rat durchsetzen wird und wie der Schutz der elektronischen Kommunikation in Hinblick auf die neuen Technologien gestaltet werden wird.

¹⁶³ Mit der DSGVO wurde die Art 29 Gruppe zum Europäischen Datenschutzausschuss. Hierbei handelt es sich um den Zusammenschluss aller Datenschutzbehörden in der Europäischen Union.

9.2 Abstract in English

The European Council notes in the European Digital Single Market Strategy¹⁶⁴ that European companies must prepare for the new technological innovations and the digital future that goes with them. Only in this way the high standard of living for European citizens can be guaranteed. The European Council also recognizes that big data, cloud services and the internet of things are important preconditions for the competitiveness of European companies on the international market¹⁶⁵.

At the same time, the privacy of the individual users of these new services should continue to be protected according to the high European standards. The European Union believes that the general data protection provisions under the GDPR are insufficient to protect the privacy of electronic communications, as companies' communications content and metadata give them a great deal of insight into the personal preferences of individual users.

For this reason, it was planned that, at the same time as the GDPR entered into force on 25 May 2018, the Regulation of the European Parliament and of the Council on the protection of privacy and confidentiality in relation to electronic communications and repealing Directive 2002/58/EC (in short e-Privacy Regulation) would come into force. At the same time, the obsolete Directive 2002/58/EC¹⁶⁶ should be replaced and the principles of the GDPR adopted. This target could not be achieved due to disagreements between the different positions in the European committees. The question now arises when and with which content the e-Privacy Regulation will enter into force. The companies affected by these provisions express their views on the drafting process of this Regulation, as they fear that the e-Privacy Regulation will impose major restrictions on the processing of data in comparison with the provisions of the GDPR.

In its first chapter, this master's thesis deals with the legal basis upon which the European Commission bases its adoption of the e-privacy regulation, the extension of existing regulation and the attempt by the European Commission to establish a level playing field for electronic communications. The second chapter presents the privacy of communication as well as the

¹⁶⁴ Rat der Europäischen Union, Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen – Strategie für einen digitalen Binnenmarkt für Europa, Brüssel, 06.Mai 2015, 8672/15

¹⁶⁵ aaO, 16.

¹⁶⁶ Directive 2002/58/EC of the European Parliament and the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications).

processing of electronic communications and the associated restrictions in relation to the GDPR. The third chapter deals with the new provisions for web tracking and cookies and the associated fears, especially of the advertising marketers. The fourth chapter deals with the right of every user preventing the presentation of the calling line identification but also the call tracing and the obligation to provide access to emergency services. The fifth chapter looks at the new regime for public directories and related arguments of affected companies. The sixth chapter deals with the provisions on unsolicited and direct marketing. These provisions apply to any company advertising via e-mail, SMS, call or messaging services¹⁶⁷ to its existing or potential customers. This entails a clear disadvantage compared to the more liberal regulation in Art 21 GDPR and results in companies being more dependent on consent from the end-users. The seventh chapter deals with the sanctions in case of a breach of this regulation. The e-Privacy Regulation is based on the structure of the GDPR and impose fines of up to € 20 million or 4% of the total worldwide annual turnover of the previous financial year, whichever is higher.

This Master Thesis analyzes the draft text as well as the proposed amendments of the Council Presidencies. It also presents different positions of the stakeholders and the Art 29 Party¹⁶⁸. The future will show which of these positions will prevail in the European Parliament and the Council and how the protection of electronic communications will be shaped in the light of new technologies.

¹⁶⁷ Messaging Services are e.g. WhatsApp, Facebook.

¹⁶⁸ The Art 29 Party was replaced by the European Data Protection Board according to Art 68 GDPR.

Literaturverzeichnis

Europarecht

- 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 1995/281, 31ff.
- 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 2002/201, 37ff.
- Verordnung (EU) 611/2013 der Kommission vom 24. Juni 2013 über die Maßnahmen für die Benachrichtigung von Verletzungen des Schutzes personenbezogener Daten gemäß der Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates (Datenschutzrichtlinie für elektronische Kommunikation), ABl. L 2013/173, 2ff.
- Verordnung (EU) 2015/2120 des Europäischen Parlaments und des Rates vom 25. November 2015 über Maßnahmen zum Zugang zum offenen Internet und zur Änderung der Richtlinie 2002/22/EG über den Universaldienst und Nutzerrechte bei elektronischer Kommunikationsnetzen und -diensten sowie der Verordnung (EU) Nr. 531/2012 über das Roaming in öffentlichen Mobilfunknetzen in der Union, ABl. L 2015/310, 1ff.
- 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), kurz DSGVO), ABl. L 2016/119, 1ff.

Dokumente der Europäischen Union

- Arbeitsunterlage der Kommissionsdienststellen, Zusammenfassung der Folgenabschätzung, 2017.
- Europäische Kommission, Commission Staff Working Document, SWD, 2017, 3 final.
- European Commission, Commission Staff Working Document, Impact Assessment, Accompanying the document Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications), Brussels, 10.01.2017.
- Rat der Europäischen Union, Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen - Strategie für einen digitalen Binnenmarkt für Europa, Brüssel, 06. Mai 2015, 8672/15.

- Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über den europäischen Kodex für die elektronische Kommunikation, kurz EECC, Brüssel, 12.10.2016.
- Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über die Achtung des Privatlebens und den Schutz personenbezogener Daten in der elektronischen Kommunikation und zur Aufhebung der Richtlinie 2002/58/EG (Verordnung über Privatsphäre und elektronische Kommunikation), Brüssel, 10.01.2017.
- Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) – Examination of the Presidency text; Brussels, 08. September 2017, 11995/17.
- Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) – Examination of the Presidency text (Art 1-5 and related recitals; Brussels, 06. October 2017, 12955/17.
- Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) – Examination of the Presidency text (Articles 12 to 20 and related recitals; Brussels, 16. October 2017, 13217/17.
- Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) – Examination of the Presidency discussion paper; Brussels, 11. January 2018, 5165/18.
- Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) – Examination of the Presidency discussion paper; Brussels, 22. March 2018, 7207/18.
- Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) – Examination of the Presidency text; Brussels, 12. June 2018, 9958/18.
- Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) – Examination of the Presidency text; Brussels, 10. July 2018, 10975/18.

Österreichisches Recht

- DSG = Bundesgesetz zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten (Datenschutzgesetz), BGBl I Nr. 165/1999 i.d.F. BGBl I Nr. 24/2018.
- TKG = Telekommunikationsgesetz 2003, BGBl. I Nr. 70/2003 i.d.F. BGBl I Nr. 29/2018.

Umfragen

- European Commission, Flash Eurobarometer 443, Briefing note on e-Privacy (July 2016).
Onlinedokument:
<http://ec.europa.eu/commfrontoffice/publicopinion/index.cfm/ResultDoc/download/DocumentKy/76378>; Download am 19.06.2018.
- RTR, Die Konkurrenz aus dem Netz, OTT-Dienste in Medien und Telekommunikation, Wien, Juni 2017.

Stellungnahmen

- Article 29 Data Protection Working Party, Opinion 01/2017 on the Proposed Regulation for the ePrivacy Regulation (2002/58/EC), 2017.
- EuroISPA, Mai 2017: Position about ePrivacy Regulation concerning the respect of private life and the protection of personal data in electronic communications.
- Illibauer, Ursula, Positionspapier zum Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über die Achtung des Privatlebens und den Schutz personenbezogener Daten in der elektronischen Kommunikation und zur Aufhebung der Richtlinie 2002/58/EG (Verordnung über Privatsphäre und elektronische Kommunikation), 5.3.2018.
- Pöchersdorfer, Winfried, Vorschlag der Europäischen Kommission für die Überarbeitung der Richtlinie über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation – Richtlinie 2002/58/EG, COM (2017) 10 final v 10.01.2017 [Vorschlag EK-DSVO] – Stellungnahme, 10.04.2017.
- Schrefler, Lorna, Review of the ePrivacy Directive, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector, 2017.

Schubert, Maximilian (2017): ISPA Stellungnahme betreffend den Entwurf der Verordnung über Privatsphäre und elektronische Kommunikation (e-Privacy-VO).
Onlinedokument:
https://www.ispa.at/filed/0/0/1498408297/530f4cf428655c3a6477cca77f252c970e16925f/fileadmin/content/5_Wissenspool/Stellungnahmen/2017/20170317_BMvit_E-Privacy/201703013_ISPA_Stellungnahme_E-Privacy_final.pdf;
Download am 15.07.2017.

Literatur

- Ernst (2017): Kapitel I. Allgemeine Bestimmungen. B. Grundrechte (Abs 2) in Paal – Pauly (Hrsg): Datenschutz-Grundverordnung.
- Schwartmann / Weiß (Hrsg.), 2017: Whitepaper zur Pseudonymisierung der Fokusgruppe Datenschutz der Plattform Sicherheit, Schutz und Vertrauen für Gesellschaft und Wirtschaft im Rahmen des Digital-Gipfels 2017 – Leitlinien für die rechtssichere Nutzung von Pseudonymisierungslösungen unter Berücksichtigung der Datenschutz-Grundverordnung, Kölner Forschungsstelle für Medienrecht, Köln.

Entscheidungen

- Rechtssache C-450/06 Varec SA, ECLI:EU:C:2008:91.

Onlinedokument

- Article 29 Data Protection Working Party, Andrea Jelinek, (11. April 2018), Statement of the WP29 on encryption and their impact on the protection of individuals with regard to the processing of their personal data in the EU. Onlinedokument: [https://iapp.org/media/pdf/resource_center/20180413_Article29WPStatementonencryptionnePrivacypdf%20\(1\).pdf](https://iapp.org/media/pdf/resource_center/20180413_Article29WPStatementonencryptionnePrivacypdf%20(1).pdf); Download am 31.07.2018.
- Bundesverband Digitale Wirtschaft (BVDW) e.V., aktuelle Informationen zur ePrivacy Verordnung. Onlinedokument: <https://www.bvdw.org/themen/recht/kommunikationsrecht-epriacy/>; Download am 26.08.2018.
- CHIP Digital GmbH (12.07.2015), Cookies akzeptieren oder nicht? Das sollten sie tun. Onlinedokument: https://praxistipps.chip.de/cookies-akzeptieren-oder-nicht-das-sollten-sie-tun_42136; Download am 18.02.2018.
- Datenschutzkonferenz (26. April 2018), Positionsbestimmung der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder, Zur Anwendbarkeit des TMG für nicht-öffentliche Stellen ab dem 25. Mai 2018. Onlinedokument: https://www.ldi.nrw.de/mainmenu_Datenschutz/submenu_Technik/Inhalt/TechnikundOrganisation/Inhalt/Zur-Anwendbarkeit-des-TMG-fuer-nicht-oeffentliche-Stellen-ab-dem-25_-Mai-2018/Positionsbestimmung-TMG.pdf; Download am 08.08.2018.
- Epicenter.Works, (10.07.2017), Österreich steht vor beispielloser Ausweitung des Überwachungsstaats. Onlinedokument: <https://epicenter.works/content/oesterreich-steht-vor-beispielloser-ausweitung-des-ueberwachungsstaats>; Download am 18.07.2017.
- European Publishers Council (29.05.2017), Open letter to the European Parliament/Council, Trust, privacy and news – the need to rethink ePrivacy proposals. Onlinedokument: <http://epceurope.eu/wp-content/uploads/2017/05/FNL-ePrivacy-letter-1.pdf>; Download am 18.02.2018.
- Lechien, Oliver, GSMA (2018); GSMA comments on the Agreement on EECC: Europe passes up opportunity to demonstrate 5G Leadership. Onlinedokument: <https://www.gsma.com/gsmaeurope/whats-new/gsma-comments-on-the-agreement-on-eecc/>; Download am 23.07.2018.

- Flade, Florian, Welt (19.06.2017); Bei WhatsApp und Co. muss der Staat selbst zum Hacker werden. Onlinedokument: <https://www.welt.de/politik/deutschland/article165688690/Bei-WhatsApp-und-Co-muss-der-Staat-selbst-zum-Hacker-werden.html>; Download am 18.07.2018
- golem.de (3. Juli 2018) Drittfirmen lesen massenweise Gmail-Postfächer. Onlinedokument: <https://www.golem.de/news/datenschutz-drittfirmen-lesen-massenweise-gmail-postfaecher-1807-135289.html>; Download am 07.08.2018.
- Standard (06.07.2017), Doppelmord in Linz: Sobotka fordert erneut Whatsapp-Überwachung. Onlinedokument: <http://derstandard.at/2000060900352/Doppelmord-in-Linz-Sobotka-fordert-erneut-WhatsApp-Ueberwachung?ref=rec>; Download am 18.07.2017.
- Der Standard (28. Oktober 2017), „Wanna Cry“: Mindestmaß an IT-Security hätte Chaos verhindert. Onlinedokument: <https://derstandard.at/2000066778145/WannaCry-Mindestmass-an-IT-Security-haette-Chaos-verhindert>; Download am 31.07.2018.
- Stern.de (21.09.2009), Der Terror der Geisteranrufe. Onlinedokument: <https://www.stern.de/digital/smartphones/automatische-waehlcomputer-der-terror-der-geisteranrufe-3532052.html>; Download am 01.05.2018.
- VATM (2015), The OTT-challenge – OTTs verändern die Märkte. Onlinedokument: http://www.vatm.de/724.0.html?&tx_ttnews%5Btt_news%5D=2071&cHash=1721966e9bff7327487d1aa755cc1d34; Download am 17.07.2018.

Abbildungsverzeichnis

Abbildung 1: Entwicklung von Gesprächsminuten, SMS und mobilem Datenverbrauch 2012 bis 2016, Die Konkurrenz aus dem Netz, 30.	12
Abbildung 2: Anteil der OTT-Nutzer/Innen für Kommunikation an Bevölkerung ab 16 Jahren, Die Konkurrenz aus dem Netz, OTT-Dienste in Medien und Telekommunikation, 32.....	12
Abbildung 4: Nutzungshäufigkeit von OTT-Nachrichten und OTT-Telefonie, Die Konkurrenz aus dem Netz, OTT-Dienste in Medien und Telekommunikation, 35.....	13
Abbildung 3: Beliebteste Anbieter für OTT-Kommunikation nach Alter, Die Konkurrenz aus dem Netz, OTT-Dienste in Medien und Telekommunikation, 39.....	13
Abbildung 6: Cookie - Einwilligung auf www.derstandard.at seit 25.08.2018	40
Abbildung 7: Ergebnis der Eurobarometer – Studie 2016: Belästigung durch zu viele Direktwerbeanrufe nach EU-Mitgliedstaaten.....	55
Abbildung 8: Ergebnis der Eurobarometer Studie 2016: Erkennung von Direktwerbeanrufen ...	55