Rat der
Europäischen Union

Brüssel, den 16. Januar 2017
(OR. en)

5358/17

Interinstitutionelles Dossier:
2017/0003 (COD)

TELECOM 12
COMPET 32
MI 45
DATAPROTECT 4
CONSOM 19
JAI 40
DIGIT 10
FREMP 3
CYBER 10
IA 12
CODEC 52

VORSCHLAG

Absender:	Herr Jordi AYET PUIGARNAU, Direktor, im Auftrag des Generalsekretärs der Europäischen Kommission
Eingangsdatum:	12. Januar 2017
Empfänger:	Herr Jeppe TRANHOLM-MIKKELSEN, Generalsekretär des Rates der Europäischen Union
Nr. Komm.dok.:	COM(2017) 10 final
Betr.:	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)

Die Delegationen erhalten in der Anlage das Dokument COM(2017) 10 final.

Anl.: COM(2017) 10 final

EUROPÄISCHE
KOMMISSION

Brüssel, den 10.1.2017
COM(2017) 10 final

2017/0003 (COD)

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)

(Text von Bedeutung für den EWR)

{SWD(2017) 3 final}
{SWD(2017) 4 final}
{SWD(2017) 5 final}
{SWD(2017) 6 final}

BEGRÜNDUNG

1. KONTEXT DES VORSCHLAGS

1.1. Gründe und Ziele des Vorschlags

Eines der Ziele der Strategie für einen digitalen Binnenmarkt („**DBM-Strategie**“)[1] ist es, das Vertrauen in digitale Dienste und deren Sicherheit zu erhöhen. Eine wichtige Maßnahme war in dieser Hinsicht die Reform des Datenschutzrechtsrahmens und insbesondere der Erlass der Verordnung (EU) 2016/679 (Datenschutz-Grundverordnung, „**DS-GVO**“)[2]. Ferner wurde in der DBM-Strategie die Überprüfung der Richtlinie 2002/58/EG („**e-Datenschutz-Richtlinie**“)[3] angekündigt, um ein hohes Niveau des Schutzes der Privatsphäre für die Nutzer elektronischer Kommunikationsdienste und gleiche Wettbewerbsbedingungen für alle Marktteilnehmer zu gewährleisten. Der vorliegende Vorschlag dient der Überarbeitung der e-Datenschutz-Richtlinie entsprechend den Zielen der DBM-Strategie und in Übereinstimmung mit der DS-GVO.

Die e-Datenschutz-Richtlinie gewährleistet den Schutz von Grundrechten und Grundfreiheiten, insbesondere die Achtung des Privatlebens, die Wahrung der Vertraulichkeit der Kommunikation und den Schutz personenbezogener Daten im Bereich der elektronischen Kommunikation. Außerdem gewährleistet sie den freien Verkehr von elektronischen Kommunikationsdaten, -geräten und -diensten in der Union. Sie bewirkt hinsichtlich der Kommunikation die Umsetzung des in Artikel 7 der Charta der Grundrechte der Europäischen Union („**Charta**“) verankerten Grundrechts auf Achtung des Privatlebens im Sekundärrecht der Union.

Im Einklang mit den Anforderungen an eine „bessere Rechtsetzung“ nahm die Kommission im Rahmen des Programms zur Gewährleistung der Effizienz und Leistungsfähigkeit der Rechtsetzung (REFIT) eine Ex-Post-Bewertung („**REFIT-Evaluierung**“) der e-Datenschutz-Richtlinie vor. Diese Evaluierung ergab, dass die Ziele und Grundsätze des gegenwärtigen Rahmens weiterhin Gültigkeit haben. Seit der letzten Überprüfung der e-Datenschutz-Richtlinie im Jahr 2009 haben sich jedoch wichtige technische und wirtschaftliche Entwicklungen auf dem Markt vollzogen. Anstatt herkömmliche Kommunikationsdienste zu nutzen, verlassen sich Verbraucher und Unternehmen zunehmend auf neue Internetdienste, die eine interpersonelle Kommunikation ermöglichen, z. B. VoIP-Telefonie, Sofortnachrichtenübermittlung (*Instant-Messaging*) und webgestützte E-Mail-Dienste. Solche *Over-the-Top*-Kommunikationsdienste („**OTT-Dienste**“) werden aber im Allgemeinen vom gegenwärtigen Rechtsrahmen der Union für die elektronische Kommunikation, einschließlich der e-Datenschutz-Richtlinie, nicht erfasst. Folglich hat die Richtlinie mit der technischen

---

[1] 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, COM(2015) 192 final.

[2] Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (ABl. L 119 vom 4.5.2016, S. 1).

[3] Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation) (ABl. L 201 vom 31.7.2002, S. 37).

Entwicklung nicht Schritt gehalten, was zu einem mangelnden Schutz der über solche neuen Dienste abgewickelten Kommunikation führt.

1.2. Kohärenz mit den bestehenden Vorschriften in diesem Bereich

Dieser Vorschlag stellt eine *Lex specialis* zur DS-GVO dar und wird diese im Hinblick auf elektronische Kommunikationsdaten, die als personenbezogene Daten einzustufen sind, präzisieren und ergänzen. Alle Fragen der Verarbeitung personenbezogener Daten, die in diesem Vorschlag nicht spezifisch geregelt sind, werden von der DS-GVO erfasst. Die Angleichung an die DS-GVO führte zur Aufhebung einiger Bestimmungen, z. B. der Sicherheitspflichten in Artikel 4 der e-Datenschutz-Richtlinie.

1.3. Kohärenz mit der Politik der Union in anderen Bereichen

Die e-Datenschutz-Richtlinie ist Teil des Rechtsrahmens für die elektronische Kommunikation. Im Jahr 2016 nahm die Kommission den Vorschlag für eine Richtlinie über den europäischen Kodex für die elektronische Kommunikation („**Kodex**“)[4] an, mit dem der Rechtsrahmen überarbeitet wird. Der vorliegende Vorschlag ist zwar kein Bestandteil des Kodex, er beruht aber teilweise auf darin enthaltenen Begriffsbestimmungen wie der für „elektronische Kommunikationsdienste“. Wie der Kodex erfasst auch der vorliegende Vorschlag OTT-Anbieter in seinem Anwendungsbereich, um der Marktwirklichkeit Rechnung zu tragen. Überdies ergänzt der Kodex diesen Vorschlag, indem er die Sicherheit elektronischer Kommunikationsdienste gewährleistet.

Die Funkanlagenrichtlinie 2014/53/EU („**FA-RL**“)[5] gewährleistet einen Binnenmarkt für Funkanlagen und -ausrüstungen. Sie schreibt insbesondere vor, dass Funkanlagen, bevor sie in Verkehr gebracht werden dürfen, über Sicherheitsvorrichtungen verfügen müssen, die sicherstellen, dass personenbezogene Daten und die Privatsphäre der Nutzer geschützt werden. Nach Maßgabe der FA-RL und der Verordnung (EU) Nr. 1025/2012 über die europäische Normung[6] ist die Kommission ermächtigt, Maßnahmen zu ergreifen. Der vorliegende Vorschlag lässt die FA-RL unberührt.

Der vorliegende Vorschlag enthält keine besonderen Bestimmungen in Bezug auf die Vorratsdatenspeicherung. Er behält den wesentlichen Inhalt des Artikels 15 der e-Datenschutz-Richtlinie bei und passt ihn an den besonderen Wortlaut des Artikel 23 der DS-GVO an, der Gründe vorsieht, aus denen die Mitgliedstaaten den Umfang der aus bestimmten Artikeln der e-Datenschutz-Richtlinie erwachsenden Rechte und Pflichten einschränken können. Daher steht es den Mitgliedstaaten frei, nationale Rahmen für die Vorratsdatenspeicherung zu schaffen oder beizubehalten, die u. a. gezielte

---

4 Vorschlag der Kommission für eine Richtlinie des Europäischen Parlaments und des Rates über den europäischen Kodex für die elektronische Kommunikation (Neufassung), COM(2016) 590 final – 2016/0288 (COD).

5 Richtlinie 2014/53/EU des Europäischen Parlaments und des Rates vom 16. April 2014 über die Harmonisierung der Rechtsvorschriften der Mitgliedstaaten über die Bereitstellung von Funkanlagen auf dem Markt und zur Aufhebung der Richtlinie 1999/5/EG (ABl. L 153 vom 22.5.2014, S. 62).

6 Verordnung (EU) Nr. 1025/2012 des Europäischen Parlaments und des Rates vom 25. Oktober 2012 zur europäischen Normung, zur Änderung der Richtlinien 89/686/EWG und 93/15/EWG des Rates sowie der Richtlinien 94/9/EG, 94/25/EG, 95/16/EG, 97/23/EG, 98/34/EG, 2004/22/EG, 2007/23/EG, 2009/23/EG und 2009/105/EG des Europäischen Parlaments und des Rates und zur Aufhebung des Beschlusses 87/95/EWG des Rates und des Beschlusses Nr. 1673/2006/EG des Europäischen Parlaments und des Rates (ABl. L 316 vom 14.11.2012. S. 12).

Vorratsspeicherungen vorsehen, sofern solche Rahmen unter Beachtung der Rechtsprechung des Gerichtshofs der Europäischen Union zur Auslegung der e-Datenschutz-Richtlinie und der Charta der Grundrechte[7] mit dem Unionsrecht vereinbar sind.

Schließlich gilt der Vorschlag nicht für die Tätigkeiten der Organe, Einrichtungen und sonstigen Stellen der Europäischen Union. Seine Grundsätze und einschlägigen Verpflichtungen bezüglich des Rechts auf Achtung des Privatlebens und der privaten Kommunikation bei der Verarbeitung elektronischer Kommunikationsdaten wurden jedoch in den Vorschlag für eine Verordnung zur Aufhebung der Verordnung (EG) Nr. 45/2001[8] aufgenommen.

2. RECHTSGRUNDLAGE, SUBSIDIARITÄT UND VERHÄLTNISMÄSSIGKEIT

2.1. Rechtsgrundlage

Die einschlägigen Rechtsgrundlagen für diesen Vorschlag sind Artikel 16 und Artikel 114 des Vertrags über die Arbeitsweise der Europäischen Union („**AEUV**“).

Artikel 16 AEUV bildet eine besondere Rechtsgrundlage für den Erlass von Vorschriften über den Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe der Union sowie durch die Mitgliedstaaten im Rahmen der Ausübung von Tätigkeiten, die in den Anwendungsbereich des Unionsrechts fallen, und über den freien Datenverkehr. Da elektronische Kommunikationsvorgänge, an denen natürliche Personen beteiligt sind, normalerweise als personenbezogene Daten einzustufen sind, sollte der Schutz natürlicher Personen im Hinblick auf ihre Privatsphäre in der Kommunikation und die Verarbeitung solcher Daten auf Artikel 16 gestützt werden.

Überdies soll der Vorschlag auch dem Schutz der Kommunikation und damit zusammenhängender rechtmäßiger Interessen juristischer Personen dienen. Die Bedeutung und der Umfang der in Artikel 7 der Charta verankerten Rechte stimmen – im Einklang mit Artikel 52 Absatz 3 der Charta – mit denen in Artikel 8 Absatz 1 der Europäischen Konvention zum Schutz der Menschenrechte und Grundfreiheiten („**EMRK**“) überein. Hinsichtlich des Anwendungsbereichs des Artikels 7 der Charta wurde durch die Rechtsprechung des Gerichtshofs der Europäischen Union („**EuGH**“)[9] und des Europäischen Gerichtshofs für Menschenrechte[10] bestätigt, dass berufliche Tätigkeiten juristischer Personen vom Schutz des durch Artikel 7 der Charta und Artikel 8 der EMRK gewährleisteten Rechts nicht ausgeschlossen werden können.

---

7 Siehe verbundene Rechtssachen C-293/12 und C-594/12 *Digital Rights Ireland und Seitlinger und andere*, ECLI:EU:C:2014:238; verbundene Rechtssachen C-203/15 und C-698/15 *Tele2 Sverige AB und Secretary of State for the Home Department*, ECLI:EU:C:2016:970.

8 Verordnung (EG) Nr. 45/2001 des Europäischen Parlaments und des Rates vom 18. Dezember 2000 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe und Einrichtungen der Gemeinschaft und zum freien Datenverkehr (ABl. L 8 vom 12.1.2001, S. 1).

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

10 Siehe u. a. EMRK, Urteile *Niemietz/Deutschland* vom 16. Dezember 1992, Serie A Nr. 251-B, § 29; *Société Colas Est u. a./Frankreich*, Nr. 37971/97, § 41, ECHR 2002-III; *Peck/Vereinigtes Königreich* Nr. 44647/98, § 57, ECHR 2003-I; sowie *Vinci Construction und GTM Génie Civil et Services/Frankreich*, Nr. 63629/10 und 60567/10, § 63, 2. April 2015.

Da mit der Initiative ein zweifacher Zweck verfolgt wird und der Aspekt des Schutzes der Kommunikation juristischer Personen und das Ziel, einen Binnenmarkt für diese Art der elektronischen Kommunikation zu schaffen und dessen Funktionieren in dieser Hinsicht zu sichern, nicht als nur nebensächlich betrachtet werden können, sollte die Initiative auch auf Artikel 114 AEUV gestützt werden.

2.2. Subsidiarität

Die Achtung der Kommunikation ist ein mit der Charta anerkanntes Grundrecht. Inhalte der elektronischen Kommunikation können hochsensible Informationen über die daran beteiligten Endnutzer offenlegen. Ebenso können Metadaten der elektronischen Kommunikation – wie vom EuGH ausdrücklich festgestellt[11] – sehr sensible und persönliche Informationen offenlegen. Die Mehrheit der Mitgliedstaaten erkennt auch die Notwendigkeit an, die Kommunikation als eigenständiges verfassungsmäßiges Recht zu schützen. Es ist zwar möglich, dass die Mitgliedstaaten Vorgaben in Kraft setzen, die gewährleisten, dass dieses Recht nicht verletzt wird, ohne Unionsvorschriften wäre dies allerdings nicht in einheitlicher Weise zu erreichen und würde im Zusammenhang mit der Nutzung elektronischer Kommunikationsdienste zu Beschränkungen beim grenzüberschreitenden Verkehr personenbezogener und nicht personenbezogener Daten führen. Um die Kohärenz mit der DS-GVO zu wahren, ist es schließlich notwendig, die e-Datenschutz-Richtlinie zu überarbeiten und Maßnahmen zur Angleichung beider Rechtsinstrumente zu treffen.

Die technischen Entwicklungen und die ehrgeizigen Ziele der Strategie für einen digitalen Binnenmarkt sprechen für ein Vorgehen auf Unionsebene. Der Erfolg des digitalen Binnenmarkts der EU hängt davon ab, wie wirksam die EU nationale Abschottungen und Schranken beseitigen und sich die Vorteile und Einsparungen eines europäischen digitalen Binnenmarkts zunutze machen kann. Überdies geht die Dimension des Problems weit über das Gebiet eines einzelnen Mitgliedstaats hinaus, denn das Internet und die digitale Technik kennen keine Grenzen. Die Mitgliedstaaten können die Probleme in der derzeitigen Lage im Alleingang nicht wirksam lösen. Gleiche Wettbewerbsbedingungen für alle Wirtschaftsteilnehmer, die substituierbare Dienste bereitstellen, und ein gleicher Schutz der Endnutzer auf Unionsebene sind Voraussetzungen, damit der digitale Binnenmarkt ordnungsgemäß funktionieren kann.

2.3. Verhältnismäßigkeit

Zur Gewährleistung eines wirksamen rechtlichen Schutzes bezüglich der Achtung der Privatsphäre und der Kommunikation ist es erforderlich, den Anwendungsbereich auf OTT-Anbieter auszudehnen. Mehrere große OTT-Anbieter halten den Grundsatz der Vertraulichkeit der Kommunikation zwar schon ganz oder teilweise ein, dennoch kann der Schutz von Grundrechten nicht allein der Selbstregulierung der Branche überlassen werden. Außerdem wird es immer wichtiger, die Privatsphäre auch in Bezug auf Endeinrichtungen wirksam zu schützen, da solche Geräte im persönlichen und beruflichen Leben für das Speichern sensibler Informationen unentbehrlich geworden sind. Die Umsetzung der e-Datenschutz-Richtlinie hat sich bezüglich der Verfügungsbefugnis des Endnutzers über seine Daten als unwirksam erwiesen. Deshalb ist die Umsetzung dieses Grundsatzes durch eine zentrale Einholung der Nutzereinwilligung über die Software mit Anzeige der Informationen über die Einstellungen zur Privatsphäre erforderlich, damit das angestrebte Ziel erreicht

[11] Siehe Fußnote 7.

werden kann. Die Durchsetzung dieser Verordnung ist Aufgabe der Aufsichtsbehörden und unterliegt dem Kohärenzverfahren der DS-GVO. Darüber hinaus ermöglicht es der Vorschlag den Mitgliedstaaten, für bestimmte rechtmäßige Zwecke nationale Ausnahmeregelungen zu treffen. Somit geht der Vorschlag nicht über das für die Erreichung der Ziele erforderliche Maß hinaus und entspricht dem in Artikel 5 des Vertrags über die Europäische Union verankerten Grundsatz der Verhältnismäßigkeit. Die den betroffenen Diensten auferlegten Verpflichtungen werden so gering wie möglich gehalten, ohne dass dadurch in die betreffenden Grundrechte eingegriffen wird.

2.4. Wahl des Instruments

Die Kommission legt einen Vorschlag für eine Verordnung vor, um die Kohärenz mit der DS-GVO sowie Rechtssicherheit gleichermaßen für Nutzer und Unternehmen dadurch zu gewährleisten, dass eine unterschiedliche Auslegung in den Mitgliedstaaten vermieden wird. Eine Verordnung kann in der gesamten Union ein gleiches Schutzniveau für die Nutzer und niedrige Einhaltungskosten für grenzüberschreitend tätige Unternehmen sicherstellen.

3. ERGEBNISSE DER EX-POST-BEWERTUNG, DER KONSULTATION DER INTERESSENTRÄGER UND DER FOLGENABSCHÄTZUNG

3.1. Ex-post-Bewertung/Eignungsprüfungen bestehender Rechtsvorschriften

Im Zuge der REFIT-Evaluierung wurde geprüft, wie wirksam die e-Datenschutz-Richtlinie zu einem angemessenen Schutz der Achtung des Privatlebens und der Wahrung der Vertraulichkeit der Kommunikation in der EU beigetragen hat. Außerdem wurde geprüft, ob Redundanzen bestehen.

Wie die REFIT-Evaluierung ergab, sind die obigen Ziele der Richtlinie weiterhin **gültig**. Während die DS-GVO den Schutz personenbezogener Daten gewährleistet, sichert die e-Datenschutz-Richtlinie die Vertraulichkeit der Kommunikation, die auch nicht personenbezogene Daten und Daten in Bezug auf juristische Personen enthalten kann. Deshalb sollte ein getrenntes Rechtsinstrument den wirksamen Schutz der in Artikel 7 der Charta verankerten Rechte gewährleisten. Auch andere Bestimmungen, wie die Vorschriften über unerbetene Werbung, haben sich als weiterhin wichtig erwiesen.

In Bezug auf die **Wirksamkeit und Effizienz** hat die REFIT-Evaluierung ergeben, dass die mit der Richtlinie verfolgten Ziele nicht vollständig erreicht worden sind. Eine Harmonisierung wurde durch die mangelnde Klarheit gewisser Bestimmungen und die Mehrdeutigkeit von Rechtsbegriffen erschwert, was grenzüberschreitend tätigen Unternehmen Probleme bereitete. Ferner zeigte die REFIT-Evaluierung, dass einige Bestimmungen zu unnötigen Belastungen für Unternehmen und Verbraucher geführt haben. So hat beispielsweise die Einwilligungsvorschrift zum Schutz der Vertraulichkeit von Endeinrichtungen ihr Ziel verfehlt, denn Endnutzer werden aufgefordert, Verfolgungs-Cookies (*Tracking-Cookies*) zu akzeptieren, ohne dass sie deren Sinn verstehen, und in einigen Fällen werden Cookies sogar ohne ihre Einwilligung gespeichert. Die Einwilligungsvorschrift ist einerseits zu umfassend, weil sie auch Verfahren einschließt, die gar keine Gefahr für die Privatsphäre darstellen, und andererseits zu eng, weil sie einige Verfolgungstechniken (z. B. Verfolgung von Gerätekennungen), die ohne Zugriff/Speicherung im Gerät auskommen, nicht erfasst. Schließlich kann auch ihre Umsetzung für Unternehmen teuer sein.

Die Evaluierung führte zu dem Schluss, dass **der EU-Mehrwert** im Falle der e-Datenschutz-Vorschriften nach wie vor gegeben ist, da das Ziel der Gewährleistung der Privatsphäre im Online-Umfeld angesichts eines zunehmend transnationalen Marktes der elektronischen Kommunikation durch ein Tätigwerden der EU besser erreicht werden kann. Überdies zeigte sie, dass die Vorschriften insgesamt mit anderen einschlägigen Rechtsvorschriften **im Einklang stehen**, wenn auch einige Redundanzen in Bezug auf die neue DS-GVO festgestellt wurden (siehe Abschnitt 1.2).

3.2. Konsultation der Interessenträger

Die Kommission führte vom 12. April bis um 5. Juli 2016 eine öffentliche Konsultation durch, zu der sie 421 Antworten erhielt[12]. Die wichtigsten Erkenntnisse sind Folgende[13]:

– **Notwendigkeit besonderer Vorschriften für den Sektor der elektronischen Kommunikation über die Vertraulichkeit der elektronischen Kommunikation:** 83,4 % der teilnehmenden Bürger, Verbraucherschutzverbände und Organisationen der Zivilgesellschaft und 88,9 % der Behörden stimmen dem zu, während 63,4 % der antwortenden Unternehmen nicht zustimmen.

– **Ausweitung des Anwendungsbereichs auf neue Kommunikationsdienste (OTT):** 76 % der Bürger und der Vertreter der Zivilgesellschaft sowie 93,1 % der Behörden stimmen zu, während nur 36,2 % der antwortenden Unternehmen eine solche Ausweitung befürworten.

– **Änderung der Ausnahmen für die Einwilligung in die Verarbeitung von Verkehrs- und Standortdaten:** 49,1 % der Bürger, Verbraucher und Organisationen der Zivilgesellschaft sowie 36 % der Behörden sprechen sich gegen eine Ausweitung der Ausnahmen aus, wogegen 36 % der Unternehmen erweiterte Ausnahmen befürworten und zwei Drittel der Unternehmen für eine schlichte Aufhebung der Vorschriften sind.

– **Unterstützung für vorgeschlagene Lösungen des Problems der Einwilligung in die Verwendung von Cookies:** 81,2 % der Bürger und 63 % der Behörden sind dafür, den Herstellern von Endeinrichtungen Verpflichtungen aufzuerlegen, damit sie Produkte mit Standardeinstellungen zugunsten des Schutzes der Privatsphäre auf den Markt bringen, wogegen 58,3 % der Unternehmen sich für die Unterstützung einer Selbst-/oder Koregulierung aussprechen.

Des Weiteren veranstaltete die Europäische Kommission im April 2016 zwei Workshops zu den Hauptfragen der öffentlichen Konsultation, den einen für alle Interessenträger und den anderen für die zuständigen nationalen Behörden. Die während der Workshops geäußerten Meinungen spiegelten die Ergebnisse der öffentlichen Konsultation wider.

[12] 162 Beiträge von Bürgern, 33 von Organisationen der Zivilgesellschaft und Verbraucherschutzverbänden; 186 Beiträge von Unternehmen und 40 von Behörden, darunter von solchen, die für die Durchsetzung der e-Datenschutz-Richtlinie zuständig sind.

[13] Der vollständige Bericht ist abrufbar unter: https://ec.europa.eu/digital-single-market/news-redirect/37204.

Zur Einholung von Meinungen der Bürger wurde eine EU-weite Eurobarometer-Umfrage zum Thema Privatsphäre in der elektronischen Kommunikation[14] durchgeführt. Die wichtigsten Erkenntnisse sind Folgende[15]:

– 78 % der Befragten erklärten, dass sie es für sehr wichtig halten, dass auf persönliche Daten auf ihrem Computer, Smartphone oder Tablet nur mit ihrer Einwilligung zugegriffen werden kann.

– 72 % halten es für sehr wichtig, dass die Vertraulichkeit ihrer E-Mails und Online-Sofortnachrichten gewährleistet ist.

– 89 % stimmen der vorgeschlagenen Option zu, dass die Standardeinstellungen ihres Browsers eine Weitergabe ihrer Informationen verhindern sollten.

3.3. Einholung und Nutzung von Expertenwissen

Die Kommission hat den folgenden externen fachlichen Rat eingeholt:

– gezielte Anhörungen von EU-Sachverständigengruppen: Stellungnahme der Artikel-29-Datenschutzgruppe; Stellungnahme des Europäischen Datenschutzbeauftragten; Stellungnahme der REFIT-Plattform; Standpunkte des GEREK; Standpunkte der ENISA und Äußerungen von Mitgliedern des Netzes für die Zusammenarbeit im Verbraucherschutz;

– externe Fachkompetenz, insbesondere die beiden folgenden Untersuchungen:

  – Studie „*ePrivacy Directive: assessment of transposition, effectiveness and compatibility with proposed Data Protection Regulation*“ (e-Datenschutz-Richtlinie: Bewertung der Umsetzung, der Wirksamkeit und der Vereinbarkeit mit der vorgeschlagenen Datenschutzverordnung) (SMART 2013/007116);

  – Studie „*Evaluation and review of Directive 2002/58 on privacy and the electronic communication sector*“ (Bewertung und Überprüfung der Richtlinie 2002/58/EG über den Schutz der Privatsphäre in der elektronischen Kommunikation) (SMART 2016/0080).

3.4. Folgenabschätzung

Zu diesem Vorschlag wurde eine Folgenabschätzung durchgeführt, zu welcher der Ausschuss für Regulierungskontrolle am 28. September 2016 eine befürwortende Stellungnahme[16] abgab. Auf Empfehlung des Ausschusses werden der Umfang der Initiative und ihre Kohärenz mit anderen Rechtsinstrumenten (DS-GVO, Kodex, FA-RL) sowie die Notwendigkeit eines getrennten Rechtsinstruments in der Folgenabschätzung besser erläutert. Zudem wird das Basisszenario ausführlicher dargelegt und verdeutlicht. Die Analyse der Auswirkungen wird vertieft und ausgewogener dargestellt, wodurch die Beschreibung der erwarteten Kosten und Vorteile klarer und ausführlicher wird.

---

14 Eurobarometer-Umfrage 443 zum Thema „e-Privacy“ (SMART 2016/079).

15 Der vollständige Bericht ist abrufbar unter: https://ec.europa.eu/digital-single-market/news-redirect/37205.

16 http://ec.europa.eu/transparency/regdoc/?fuseaction=ia.

Die folgenden Politikoptionen wurde anhand der Kriterien der Wirksamkeit, Effizienz und Kohärenz geprüft:

– **Option 1:** Nichtlegislative (nicht zwingende) Maßnahmen;

– **Option 2:** Begrenzte Stärkung der Privatsphäre/Vertraulichkeit und Vereinfachung;

– **Option 3:** Maßvolle Stärkung der Privatsphäre/Vertraulichkeit und Vereinfachung;

– **Option 4:** Weitreichende Stärkung der Privatsphäre/Vertraulichkeit und Vereinfachung;

– **Option 5:** Aufhebung der e-Datenschutz-Richtlinie.

Die **Option 3** stellte sich unter den meisten Aspekten als die **bevorzugte Option** heraus, um die Ziele unter Berücksichtigung der Effizienz und Kohärenz zu erreichen. Die Hauptvorteile sind:

– Erweiterter Schutz der Vertraulichkeit der elektronischen Kommunikation durch Ausdehnung des Anwendungsbereichs des Rechtsinstruments auf neue funktional gleichwertige elektronische Kommunikationsdienste. Außerdem ermöglicht die Verordnung den Endnutzern eine bessere Kontrolle, indem sie klarstellt, dass die Einwilligung auch durch geeignete technische Einstellungen gegeben werden kann.

– Verbesserter Schutz vor unerbetener Kommunikation mit Einführung einer Verpflichtung zur Anzeige der Rufnummer des Anrufers oder einer obligatorischen Vorwahl für Werbeanrufe sowie mit den erweiterten Möglichkeiten, Anrufe von unerwünschten Rufnummern zu sperren.

– Vereinfachung und Klarstellung des Regulierungsumfelds durch Einengung des Handlungsspielraums der Mitgliedstaaten, Aufhebung überholter Bestimmungen und Ausweitung der Ausnahmen zu den Einwilligungsvorschriften.

Die wirtschaftlichen Folgen der Option 3 werden voraussichtlich in einem angemessenen Verhältnis zu den Zielen des Vorschlags stehen. Für herkömmliche elektronische Kommunikationsdienste ergeben sich neue Geschäftsmöglichkeiten im Zusammenhang mit der Verarbeitung von Kommunikationsdaten, wogegen OTT-Anbieter nunmehr denselben Vorschriften unterworfen werden. Für Letztere ist dies mit zusätzlichen Einhaltungskosten verbunden. Diese Änderungen werden sich aber nicht wesentlich auf jene OTT-Anbieter auswirken, die bereits auf der Grundlage einer Einwilligung arbeiten. Schließlich wären in all jenen Mitgliedstaaten, die diese Vorschriften bereits auf OTT-Anbieter ausgeweitet haben, keine Auswirkungen dieser Option spürbar.

Dank der Zentralisierung der Einwilligung in einer Software wie den Internet-Browsern und der Aufforderung an die Nutzer, ihre Einstellungen zur Privatsphäre zu wählen, sowie dank erweiterter Ausnahmen zu den Einwilligungsvorschriften in Bezug auf Cookies könnte ein beträchtlicher Anteil der Unternehmen auf Cookie-Banner und -Hinweise verzichten, was möglicherweise erhebliche Kosteneinsparungen und Vereinfachungen mit sich bringen würde. Für Anbieter gezielter Online-Werbung könnte es jedoch schwieriger werden, die Einwilligung zu erlangen, wenn ein großer Teil der Nutzer Einstellungen wählt, bei denen Cookies von Dritten abgewiesen werden. Gleichzeitig wird den Website-Betreibern durch eine Zentralisierung der Einwilligung aber nicht die Möglichkeit genommen, die Einwilligung

mit einer individuellen Anfrage beim Endnutzer einzuholen und auf diese Weise ihr Geschäftsmodell fortzuführen. Einigen Anbietern von Browsern oder ähnlicher Software entstünden zusätzliche Kosten, weil sie für datenschutzfreundliche Einstellungen sorgen müssten.

In der externen Studie wurden drei unterschiedliche Einführungsszenarios für die Option 3 ermittelt, die davon abhängen, wer das Dialogfenster anzeigen soll, mit dem ein Nutzer, der Einstellungen wie „Cookies von Dritten ablehnen“ oder „Nicht verfolgen“ gewählt hat, später von besuchten Websites aufgefordert werden kann, seine Cookie-Einstellungen zu ändern. Mit dieser technischen Aufgabe könnten folgende Stellen betraut werden: 1) Software wie Internet-Browser; 2) der Dritte, der die Verfolgung vornimmt; 3) die einzelnen Websites (d. h. die vom Nutzer gewünschten Dienste der Informationsgesellschaft). Beim ersten Szenario (Browser-Lösung), das in diesem Vorschlag umgesetzt wurde, würde die Option 3 insgesamt gegenüber dem Basisszenario zu Einsparungen in Höhe von 70 % (948,8 Mio. EUR) bei den Einhaltungskosten führen. Bei den anderen beiden Szenarios würden die Kosteneinsparungen geringer ausfallen. Da sich die Gesamteinsparungen weitgehend daraus ergeben, dass die Zahl der betroffenen Unternehmen ganz erheblich gesenkt wird, dürften die Einhaltungskosten, mit denen ein einzelnes Unternehmen zu rechnen hätte, im Durchschnitt höher als heute ausfallen.

3.5. Effizienz der Rechtsetzung und Vereinfachung

Im Einklang mit den Ergebnissen der REFIT-Evaluierung und der Stellungnahme der REFIT-Plattform[17] dienen die im Rahmen der bevorzugten Option vorgeschlagenen Maßnahmen dem Ziel der Vereinfachung und der Verringerung des Verwaltungsaufwands.

Die REFIT-Plattform gab der Kommission drei Grundempfehlungen:

– Der Schutz des Privatlebens der Bürger sollte durch eine Angleichung der e-Datenschutz-Richtlinie an die Datenschutz-Grundverordnung gestärkt werden.

– Die Wirksamkeit des Schutzes der Bürger vor unerbetener Werbung sollte verbessert werden, indem weitere Ausnahmen von der Einwilligungsvorschrift in Bezug auf Cookies zugelassen werden.

– Die Kommission sollte sich mit nationalen Umsetzungsproblemen befassen und den Austausch bewährter Verfahren zwischen den Mitgliedstaaten erleichtern.

Konkret sieht der Vorschlag Folgendes vor:

– Verwendung technologieneutraler Begriffsbestimmungen, damit auch neue Dienste und Technologien erfasst werden, um die Verordnung somit zukunftssicher zu machen;

– Aufhebung der Sicherheitsvorschriften, um doppelte rechtliche Vorgaben zu beseitigen;

– Klarstellung des Anwendungsbereichs, um die Gefahr einer abweichenden Umsetzung in den Mitgliedstaaten zu verringern bzw. zu beseitigen (Punkt 3 der Stellungnahme);

[17] http://ec.europa.eu/smart-regulation/refit/refit-platform/docs/recommendations/opinion_comm_net.pdf.

– Klarstellung und Vereinfachung der Einwilligungsvorschrift in Bezug auf die Verwendung von Cookies und anderen Kennungen, wie in den Abschnitten 3.1 und 3.4 erläutert (Punkt 2 der Stellungnahme);

– die Aufsichtsbehörden entsprechen denen, die für die Durchsetzung der Datenschutz-Grundverordnung zuständig sind, und Anwendung des Kohärenzverfahrens der Datenschutz-Grundverordnung.

3.6. Auswirkungen auf die Grundrechte

Der Vorschlag dient einem wirksameren und besseren Schutz der Privatsphäre und der verarbeiteten personenbezogenen Daten im Zusammenhang mit der elektronischen Kommunikation im Einklang mit den Artikeln 7 und 8 der Charta sowie einer größeren Rechtssicherheit. Der Vorschlag ergänzt und präzisiert die DS-GVO. Ein wirksamer Schutz der Vertraulichkeit der Kommunikation ist unverzichtbar für die Ausübung der Rechte auf freie Meinungsäußerung und Informationsfreiheit sowie andere damit verbundene Rechte wie derjenigen auf Schutz personenbezogener Daten oder auf Gedanken-, Gewissens- und Religionsfreiheit.

4. AUSWIRKUNGEN AUF DEN HAUSHALT

Der Vorschlag hat keine Auswirkungen auf den Unionshaushalt.

5. WEITERE ANGABEN

5.1. Durchführungspläne sowie Monitoring-, Bewertungs- und Berichterstattungsmodalitäten

Die Kommission wird die Anwendung der Verordnung überwachen und dem Europäischen Parlament, dem Rat und dem Europäischen Wirtschafts- und Sozialausschuss alle drei Jahre einen Bewertungsbericht vorlegen. Diese Berichte werden veröffentlicht und geben detailliert Auskunft über die tatsächliche Anwendung und Durchsetzung dieser Verordnung.

5.2. Ausführliche Erläuterung einzelner Bestimmungen des Vorschlags

Kapitel I enthält die allgemeinen Bestimmungen: den Gegenstand (Artikel 1), den Anwendungsbereich (Artikel 2 und 3) und die Begriffsbestimmungen mit Verweisen auf einschlägige Begriffsbestimmungen in anderen EU-Rechtsinstrumenten wie der DS-GVO.

Kapitel II enthält die wesentlichen Bestimmungen zur Gewährleistung der Vertraulichkeit der elektronischen Kommunikation (Artikel 5) und über die begrenzten zulässigen Zwecke und die Bedingungen der Verarbeitung solcher Kommunikationsdaten (Artikel 6 und 7). Geregelt wird ferner der Schutz von Endeinrichtungen, indem i) die Integrität der darin gespeicherten Informationen gewährleistet und ii) die von Endeinrichtungen ausgehenden Informationen geschützt werden, da sich Endnutzer anhand dieser Daten identifizieren lassen (Artikel 8). Artikel 9 regelt schließlich die Einwilligung des Endnutzers, die in dieser Verordnung als Grundlage für die rechtmäßige Verarbeitung im Mittelpunkt steht, mit ausdrücklicher Bezugnahme auf die in der DS-GVO festgelegten Begriffsbestimmungen und Voraussetzungen, während in Artikel 10 die Anbieter von Software, die elektronische Kommunikation ermöglicht, dazu verpflichtet werden, den Endnutzern bei der wirksamen

Auswahl der Einstellungen zur Privatsphäre behilflich zu sein. Artikel 11 regelt, zu welchen Zwecken und unter welchen Bedingungen die Mitgliedstaaten die obigen Bestimmungen einschränken können.

In Kapitel III geht es um die Rechte der Endnutzer auf die Kontrolle über ihre ausgehende und eingehende elektronische Kommunikation zum Schutz ihrer Privatsphäre: i) das Recht der Endnutzer auf Verhinderung der Anzeige der Rufnummer des Anrufers, um die Anonymität zu wahren (Artikel 12) mit seinen Einschränkungen (Artikel 13); ii) die Verpflichtung der Betreiber öffentlich zugänglicher nummerngebundener interpersoneller Kommunikationsdienste, Endnutzern die Möglichkeit zu geben, den Erhalt unerwünschter Anrufe zu begrenzen (Artikel 14). Außerdem regelt dieses Kapitel die Bedingungen, unter denen Endnutzer in öffentlich zugängliche Verzeichnisse aufgenommen werden können (Artikel 15), und die Bedingungen, unter denen unerbetene Direktwerbung erlaubt ist (Artikel 17). Ferner behandelt es Sicherheitsrisiken und erlegt Betreibern elektronischer Kommunikationsdienste die Verpflichtung auf, Endnutzer vor einem besonderen Risiko zu warnen, das die Sicherheit von Netzen und elektronischen Kommunikationsdiensten beeinträchtigen könnte. Die Sicherheitsverpflichtungen in der DS-GVO und im europäischen Kodex für die elektronische Kommunikation werden für die Betreiber elektronischer Kommunikationsdienste gelten.

Kapitel IV regelt die Beaufsichtigung und Durchsetzung dieser Verordnung und betraut damit die für die DS-GVO zuständigen Aufsichtsbehörden wegen der großen Synergien zwischen dem allgemeinen Datenschutz und der Vertraulichkeit der Kommunikation (Artikel 18). Die Befugnisse des Europäischen Datenschutzausschusses werden erweitert (Artikel 19), und das Verfahren der Zusammenarbeit sowie das Kohärenzverfahren der DS-GVO werden auf grenzübergreifende Fragen in Zusammenhang mit der vorliegenden Verordnung Anwendung finden (Artikel 20).

In Kapitel V werden die verschiedenen Rechtsbehelfe aufgeführt, die Endnutzern zur Verfügung stehen (Artikel 21 und 22), und mögliche Sanktionen (Artikel 24) sowie allgemeine Bedingungen für die Verhängung von Geldbußen (Artikel 23) festgelegt.

Kapitel VI betrifft den Erlass von delegierten Rechtsakten und Durchführungsrechtsakten im Einklang mit den Artikeln 290 und 291 AEUV.

Schließlich enthält Kapitel VII die Schlussbestimmungen dieser Verordnung: Aufhebung der e-Datenschutz-Richtlinie, Überwachung und Überprüfung, Inkrafttreten und Anwendung. Bezüglich der Überprüfung beabsichtigt die Kommission, u. a. zu prüfen, ob in Anbetracht rechtlicher, technischer oder wirtschaftlicher Entwicklungen und unter Berücksichtigung der ersten Bewertung der Verordnung (EU) 2016/679, die zum 25. Mai 2020 vorzulegen ist, ein getrennter Rechtsakt noch immer notwendig ist.

2017/0003 (COD)

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)

(Text von Bedeutung für den EWR)

DAS EUROPÄISCHE PARLAMENT UND DER RAT DER EUROPÄISCHEN UNION –

gestützt auf den Vertrag über die Arbeitsweise der Europäischen Union, insbesondere auf die Artikel 16 und 114,

auf Vorschlag der Europäischen Kommission,

nach Zuleitung des Entwurfs des Gesetzgebungsakts an die nationalen Parlamente,

nach Stellungnahme des Europäischen Wirtschafts- und Sozialausschusses[1],

nach Stellungnahme des Ausschusses der Regionen[2],

nach Stellungnahme des Europäischen Datenschutzbeauftragten[3],

gemäß dem ordentlichen Gesetzgebungsverfahren,

in Erwägung nachstehender Gründe:

(1) Artikel 7 der Charta der Grundrechte der Europäischen Union (im Folgenden „Charta“) schützt das Grundrecht aller Menschen auf Achtung ihres Privat- und Familienlebens, ihrer Wohnung und ihrer Kommunikation. Die Achtung der Privatsphäre in der Kommunikation ist ein wesentlicher Aspekt dieses Rechts. Vertraulichkeit der elektronischen Kommunikation bedeutet, dass Informationen, die zwischen Beteiligten ausgetauscht werden, wie auch die externen Elemente dieser Kommunikation (unter anderem wann, woher und an wen) niemandem außer den an der Kommunikation Beteiligten offengelegt werden. Der Grundsatz der Vertraulichkeit sollte für gegenwärtige und künftige Kommunikationsmittel gelten, darunter Anrufe, Internetzugang, Sofortnachrichtenanwendungen, E-Mail, Internettelefonie und Übermittlung persönlicher Nachrichten über soziale Medien.

---

1 ABl. C […] vom […], S. […].
2 ABl. C […] vom […], S. […].
3 ABl. C […] vom […], S. […].

(2) Inhalte der elektronischen Kommunikation können hochsensible Informationen über die daran beteiligten natürlichen Personen offenlegen, von persönlichen Erlebnissen und Gefühlen oder Erkrankungen bis hin zu sexuellen Vorlieben und politischen Überzeugungen, was zu schweren Folgen im persönlichen und gesellschaftlichen Leben, zu wirtschaftlichen Einbußen oder Schamgefühl führen kann. Auch durch Metadaten elektronischer Kommunikation können sehr sensible und persönliche Informationen offengelegt werden. Zu solchen Metadaten gehören beispielsweise angerufene Nummern, besuchte Websites, der geografische Standort, Uhrzeit, Datum und Dauer eines von einer Person getätigten Anrufs, aus denen sich präzise Schlussfolgerungen über das Privatleben der an der elektronischen Kommunikation beteiligten Personen ziehen lassen, z. B. in Bezug auf ihre sozialen Beziehungen, Gewohnheiten und ihren Lebensalltag, ihre Interessen, ihren Geschmack usw.

(3) Elektronische Kommunikationsdaten können zudem Informationen über juristische Personen wie Geschäftsgeheimnisse oder andere sensible Informationen offenlegen, die einen wirtschaftlichen Wert haben. Deshalb sollten die Bestimmungen dieser Verordnung sowohl für natürliche als auch für juristische Personen gelten. Außerdem sollte diese Verordnung sicherstellen, dass die Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates[4] auch für Endnutzer gilt, die juristische Personen sind. Dies bezieht sich auch auf die Begriffsbestimmung für „Einwilligung“ in der Verordnung (EU) 2016/679. Bei Bezugnahmen auf die Einwilligung von Endnutzern, einschließlich juristischer Personen, sollte diese Begriffsbestimmung gelten. Außerdem sollten juristische Personen gegenüber den Aufsichtsbehörden dieselben Rechte haben wie Endnutzer, die natürliche Personen sind; die nach dieser Verordnung zuständigen Aufsichtsbehörden sollten zudem auch für die Überwachung der Anwendung dieser Verordnung im Hinblick auf juristische Personen zuständig sein.

(4) Nach Artikel 8 Absatz 1 der Charta und Artikel 16 Absatz 1 des Vertrags über die Arbeitsweise der Europäischen Union hat jede Person das Recht auf Schutz der sie betreffenden personenbezogenen Daten. Die Verordnung (EU) 2016/679 enthält Vorschriften zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Verkehr solcher Daten. Elektronische Kommunikationsdaten können auch personenbezogene Daten im Sinne der Verordnung (EU) 2016/679 enthalten.

(5) Die Bestimmungen dieser Verordnung präzisieren und ergänzen die in der Verordnung (EU) 2016/679 festgelegten allgemeinen Vorschriften über den Schutz personenbezogener Daten im Hinblick auf elektronische Kommunikationsdaten, die als personenbezogene Daten einzustufen sind. Diese Verordnung führt daher zu keiner Absenkung des Schutzniveaus, das natürliche Personen nach der Verordnung (EU) 2016/679 genießen. Eine Verarbeitung elektronischer Kommunikationsdaten durch Betreiber elektronischer Kommunikationsdienste sollte nur im Einklang mit der vorliegenden Verordnung erlaubt sein.

---

[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) (ABl. L 119 vom 4.5.2016, S. 1).

(6) Die Grundsätze und wichtigsten Bestimmungen der Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates[5] haben sich im Allgemeinen zwar bewährt, jedoch hat diese Richtlinie mit der Entwicklung der Wirklichkeit der Technik und der Märkte nicht vollständig Schritt gehalten, weshalb der Schutz der Privatsphäre und der Vertraulichkeit im Zusammenhang mit der elektronischen Kommunikation uneinheitlich bzw. nicht wirksam genug ist. Zu solchen Entwicklungen zählt beispielsweise der Markteintritt von elektronischen Kommunikationsdiensten, die aus Sicht des Verbrauchers herkömmliche Dienste ersetzen, für die aber nicht dieselben Vorschriften gelten. Eine andere solche Entwicklung ist das Aufkommen neuer Techniken für die Verfolgung des Online-Verhaltens der Endnutzer, die von der Richtlinie 2002/58/EG nicht erfasst werden. Die Richtlinie 2002/58/EG sollte daher aufgehoben und durch diese Verordnung ersetzt werden.

(7) Die Mitgliedstaaten sollten die Möglichkeit haben, innerhalb des von dieser Verordnung vorgegebenen Rahmens nationale Bestimmungen beizubehalten oder einzuführen, mit denen die Anwendung der Vorschriften dieser Verordnung genauer und klarer festgelegt wird, um eine wirksame Anwendung und Auslegung dieser Vorschriften sicherzustellen. Deshalb sollte der Ermessenspielraum, den die Mitgliedstaaten in dieser Hinsicht haben, so wahrgenommen werden, dass ein ausgewogenes Verhältnis zwischen dem Schutz des Privatlebens und personenbezogener Daten und dem freien Verkehr elektronischer Kommunikationsdaten gewährleistet bleibt.

(8) Diese Verordnung sollte für Betreiber elektronischer Kommunikationsdienste, für Betreiber öffentlich zugänglicher Verzeichnisse und für Anbieter von Software, die elektronische Kommunikation ermöglicht, einschließlich Abruf und Darstellung von Informationen aus dem Internet, gelten. Diese Verordnung sollte ferner für natürliche und juristische Personen gelten, die mithilfe elektronischer Kommunikationsdienste an Endnutzer gerichtete gewerbliche Direktwerbung betreiben oder Informationen sammeln, die in Endeinrichtungen der Endnutzer gespeichert sind oder sich auf diese beziehen.

(9) Diese Verordnung sollte für elektronische Kommunikationsdaten gelten, die in Verbindung mit der Bereitstellung und Nutzung elektronischer Kommunikationsdienste in der Union verarbeitet werden, unabhängig davon, ob die Verarbeitung in der Union stattfindet. Damit den Endnutzern in der Union ein wirksamer Schutz nicht vorenthalten wird, sollte diese Verordnung darüber hinaus auch für elektronische Kommunikationsdaten gelten, die im Zusammenhang mit der Bereitstellung elektronischer Kommunikationsdienste von außerhalb der Union für Endnutzer in der Union verarbeitet werden.

(10) Funkanlagen und zugehörige Software, die auf dem Binnenmarkt der Union in Verkehr gebracht werden, müssen den Anforderungen der Richtlinie 2014/53/EU des

[5] Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation) (ABl. L 201 vom 31.7.2002, S. 37).

Europäischen Parlaments und des Rates[6] entsprechen. Die Anwendbarkeit der Anforderungen der Richtlinie 2014/53/EU und die Befugnis der Kommission zum Erlass delegierter Rechtsakte nach der Richtlinie 2014/53/EU zum Zweck der Festlegung von Sicherheitsvorrichtungen für bestimmte Kategorien oder Klassen von Funkanlagen, die dem Schutz der personenbezogenen Daten und der Privatsphäre der Endnutzer dienen, sollten von dieser Verordnung unberührt bleiben.

(11) Die für Kommunikationszwecke genutzten Dienste und die technischen Mittel für ihre Bereitstellung haben sich beträchtlich weiterentwickelt. Anstelle herkömmlicher Übermittlungsdienste für Sprachtelefonie, Textnachrichten (SMS) und E-Mail verwenden die Endnutzer zunehmend funktional gleichwertige Online-Dienste wie VoIP-Telefonie, Nachrichtenübermittlung (Messaging) und webgestützte E-Mail-Dienste. Zur Gewährleistung eines wirksamen und einheitlichen Schutzes der Endnutzer bei der Benutzung funktional gleichwertiger Dienste wird in dieser Verordnung die in der [Richtlinie des Europäischen Parlaments und des Rates über den europäischen Kodex für die elektronische Kommunikation[7]] festgelegte Begriffsbestimmung für elektronische Kommunikationsdienste verwendet. Diese Begriffsbestimmung erfasst nicht nur Internetzugangsdienste und Dienste, die ganz oder teilweise in der Übertragung von Signalen bestehen, sondern auch interpersonelle Kommunikationsdienste, die nummerngebunden oder nummernunabhängig sein können, beispielsweise VoIP-Telefonie, Nachrichtenübermittlung und webgestützte E-Mail-Dienste. Der Schutz der Vertraulichkeit der Kommunikation ist auch im Hinblick auf interpersonelle Kommunikationsdienste, die nur eine untergeordnete Nebenfunktion eines anderen Dienstes darstellen, unverzichtbar; deshalb sollten derartige Dienste, die auch eine Kommunikationsfunktion aufweisen, ebenfalls unter diese Verordnung fallen.

(12) Vernetzte Geräte und Maschinen kommunizieren zunehmend über elektronische Kommunikationsnetze untereinander (Internet der Dinge). Auch bei der Übermittlung von Kommunikationsvorgängen zwischen Maschinen werden Signale über ein Netz übertragen, sodass es sich dabei in der Regel um einen elektronischen Kommunikationsdienst handelt. Um den vollständigen Schutz der Rechte auf Privatsphäre und Vertraulichkeit der Kommunikation zu gewährleisten und ein vertrauenswürdiges und sicheres Internet der Dinge im digitalen Binnenmarkt zu gewährleisten, ist es notwendig klarzustellen, dass diese Verordnung auch für die Übermittlung von Maschine-Maschine-Kommunikation gelten sollte. Dementsprechend sollte der in dieser Verordnung festgelegte Grundsatz der Vertraulichkeit auch für die die Übermittlung von Maschine-Maschine-Kommunikation gelten. Besondere Sicherheitsvorrichtungen könnten auch im Rahmen sektorspezifischer Rechtsvorschriften wie beispielsweise der Richtlinie 2014/53/EU getroffen werden.

(13) Die Entwicklung schneller und effizienter Drahtlostechnik hat dazu beigetragen, dass der öffentliche Internetzugang über drahtlose Netze zunehmend in öffentlichen und

---

6 Richtlinie 2014/53/EU des Europäischen Parlaments und des Rates vom 16. April 2014 über die Harmonisierung der Rechtsvorschriften der Mitgliedstaaten über die Bereitstellung von Funkanlagen auf dem Markt und zur Aufhebung der Richtlinie 1999/5/EG (ABl. L 153 vom 22.5.2014, S. 62).

7 Vorschlag der Kommission für eine Richtlinie des Europäischen Parlaments und des Rates über den europäischen Kodex für die elektronische Kommunikation (Neufassung), COM(2016) 590 final – 2016/0288 (COD).

halbprivaten Räumen für jedermann zur Verfügung steht, beispielsweise an sogenannten „Hotspots“, die sich an verschiedenen Orten in einer Stadt wie in Kaufhäusern, Einkaufszentren und Krankenhäusern befinden können. Insoweit solche Kommunikationsnetze für eine unbestimmte Gruppe von Endnutzern bereitgestellt werden, sollte die Vertraulichkeit der über solche Netze übermittelten Kommunikation geschützt werden. Die Tatsache, dass drahtlose elektronische Kommunikationsdienste eine Nebenfunktion anderer Dienste darstellen können, sollte dem Schutz der Vertraulichkeit der Kommunikationsdaten und der Anwendung dieser Verordnung nicht entgegenstehen. Deshalb sollte diese Verordnung für elektronische Kommunikationsdaten gelten, die mithilfe elektronischer Kommunikationsdienste und öffentlicher Kommunikationsnetze übertragen werden. Diese Verordnung sollte dagegen keine Anwendung auf geschlossene Gruppen von Endnutzern (z. B. Unternehmensnetze) finden, bei denen der Zugang auf die Angehörigen des Unternehmens beschränkt ist.

(14) Der Ausdruck „elektronische Kommunikationsdaten“ sollte hinreichend breit und technologieneutral definiert werden, damit er alle Informationen bezüglich der übermittelten oder ausgetauschten Inhalte (elektronische Kommunikationsinhalte) und die Informationen bezüglich der Endnutzer von elektronischen Kommunikationsdiensten erfasst, die zum Zwecke der Übermittlung, Verbreitung oder Ermöglichung des Austauschs elektronischer Kommunikationsinhalte verarbeitet werden; dazu zählen die zur Verfolgung und Identifizierung des Ausgangs- und Zielpunkts eines Kommunikationsvorgangs verwendeten Daten, des geografischen Standorts sowie von Datum, Uhrzeit, Dauer und Art der Kommunikation. Unabhängig davon, ob solche Signale über Kabel, Funk, optische oder elektromagnetische Medien, einschließlich Satellitennetze, Kabelnetze, Festnetze (leitungs- und paketvermittelte, einschließlich Internet) und terrestrische Mobilfunknetze oder Stromleitungssysteme, übertragen werden, sollten die auf solche Signale bezogenen Daten als elektronische Kommunikationsmetadaten betrachtet und somit von dieser Verordnung erfasst werden. Elektronische Kommunikationsmetadaten können Informationen enthalten, die Teil des Vertrags mit bzw. der Anmeldung bei dem Dienst sind, sofern diese Informationen zu Zwecken der Übermittlung, der Verbreitung oder des Austauschs elektronischer Kommunikationsinhalte verarbeitet werden.

(15) Elektronische Kommunikationsdaten sollten vertraulich behandelt werden. Das bedeutet, dass Eingriffe in die Übermittlung elektronischer Kommunikationsdaten, ob unmittelbar durch menschliches Zutun oder mittelbar durch eine automatische Verarbeitung durch Maschinen, ohne Einwilligung aller an der Kommunikation Beteiligten untersagt sein sollten. Das Verbot des Abfangens von Kommunikationsdaten sollte während ihrer Übertragung gelten, d. h. bis zum Empfang der Inhalte der elektronischen Kommunikation durch den bestimmungsgemäßen Empfänger. Ein Abfangen der elektronischen Kommunikation kann dann vorliegen, wenn beispielsweise andere als die an der Kommunikation Beteiligten Anrufe mithören oder den Inhalt der elektronischen Kommunikation oder die damit zusammenhängenden Metadaten zu anderen Zwecken als dem Kommunikationsaustausch lesen, scannen oder speichern. Ein Abfangen liegt auch vor, wenn Dritte ohne Einwilligung des betreffenden Endnutzers besuchte Websites, den Zeitpunkt der Besuche, die Interaktion mit anderen usw. beobachten. Mit der technischen Entwicklung haben auch die technischen Abfangmöglichkeiten zugenommen. Diese Möglichkeiten reichen von der Installation von Einrichtungen, die in ganzen Zielgebieten Daten von Endeinrichtungen erfassen, z. B. IMSI-Catcher

(zum Abgreifen der internationalen Mobilfunk-Teilnehmerkennung), bis hin zu Programmen und Techniken, die beispielsweise die Surfgewohnheiten heimlich beobachten, um daraus Endnutzerprofile zu erstellen. Weitere Beispiele für ein Abfangen sind das Erfassen von Nutzdaten oder Inhaltsdaten aus unverschlüsselten drahtlosen Netzen und Routern, z. B. von Surfgewohnheiten ohne Einwilligung der Endnutzer.

(16) Mit dem Verbot der Speicherung der Kommunikation soll nicht jede automatische, einstweilige und vorübergehende Speicherung dieser Informationen untersagt werden, soweit diese zum alleinigen Zweck der Durchführung der Übermittlung über das elektronische Kommunikationsnetz erfolgt. Untersagt werden soll ebenfalls nicht die Verarbeitung elektronischer Kommunikationsdaten zur Gewährleistung der Sicherheit und Kontinuität der elektronischen Kommunikationsdienste, darunter die Prüfung auf Sicherheitsbedrohungen wie Vorhandensein von Schadsoftware oder die Verarbeitung von Metadaten zur Sicherung der Einhaltung der erforderlichen Dienstqualitätsanforderungen wie Latenz, Verzögerungsschwankung (*Jitter*) usw.

(17) Die Verarbeitung elektronischer Kommunikationsdaten kann für Unternehmen, für die Verbraucher und für die gesamte Gesellschaft nützlich sein. Gegenüber der Richtlinie 2002/58/EG erweitert diese Verordnung die Möglichkeiten der Betreiber elektronischer Kommunikationsdienste, elektronische Kommunikationsmetadaten mit Einwilligung der Endnutzer zu verarbeiten. Die Endnutzer messen jedoch der Vertraulichkeit ihrer Kommunikation, einschließlich ihrer Online-Aktivitäten, eine große Bedeutung bei und wollen die Kontrolle über die Verwendung ihrer elektronischen Kommunikationsdaten für andere Zwecke als die Übertragung der Kommunikation haben. Deshalb sollte diese Verordnung den Betreibern elektronischer Kommunikationsdienste vorschreiben, dass sie die Einwilligung der Endnutzer in die Verarbeitung elektronischer Kommunikationsmetadaten einholen, zu denen auch Daten über den Standort des Gerätes gehören, welche zwecks Gewährung und Aufrechterhaltung des Zugangs und der Verbindung zu dem jeweiligen Dienst erzeugt werden. Standortdaten, die in einem anderen Zusammenhang als dem der Bereitstellung elektronischer Kommunikationsdienste erzeugt werden, sollten nicht als Metadaten betrachtet werden. Ein Beispiel für eine gewerbliche Verwendung elektronischer Kommunikationsmetadaten durch Betreiber elektronischer Kommunikationsdienste wäre die Erstellung von *Heatmaps*, also grafischen Darstellungen von Daten über die Anwesenheit von Personen anhand von Farben. Zur Anzeige von Verkehrsbewegungen in bestimmte Richtungen über einen bestimmten Zeitraum wird eine Kennung benötigt, damit die Positionen von Einzelpersonen in bestimmten Zeitabständen miteinander verknüpft werden können. Bei Verwendung anonymisierter Daten würde diese Kennung fehlen, sodass solche Bewegungen nicht dargestellt werden könnten. Aus einer solchen Nutzung elektronischer Kommunikationsmetadaten könnten beispielsweise Behörden und öffentliche Verkehrsbetriebe Nutzen ziehen, wenn sie ausgehend von der Benutzung und Belastung bestehender Anlagen festlegen, wo neue Infrastrukturen gebaut werden sollten. Hat eine Form der Verarbeitung elektronischer Kommunikationsmetadaten, insbesondere bei Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge, so sollte vor der Verarbeitung eine Datenschutz-Folgenabschätzung und gegebenenfalls eine Konsultation der Aufsichtsbehörde nach den Artikeln 35 und 36 der Verordnung (EU) 2016/679 durchgeführt werden.

(18) Endnutzer können in die Verarbeitung ihrer Metadaten einwilligen, um bestimmte Dienstleistungen nutzen zu können, beispielsweise Dienste zum Schutz vor betrügerischen Aktivitäten (indem Nutzungsdaten, Standort und Kundenkonto in Echtzeit geprüft werden). In der digitalen Wirtschaft werden Dienstleistungen häufig für eine andere Gegenleistung als Geld erbracht, beispielsweise indem Endnutzern Werbung angezeigt wird. Für die Zwecke dieser Verordnung sollte der Ausdruck „Einwilligung“ des Endnutzers unabhängig davon, ob es sich um eine natürliche oder eine juristische Person handelt, dieselbe Bedeutung haben und denselben Voraussetzungen unterliegen wie der in der Verordnung (EU) 2016/679 festgelegte Begriff „Einwilligung der betroffenen Person“. Grundlegende breitbandige Internetzugangs- und Sprachkommunikationsdienste gelten als unverzichtbare Dienste, damit Personen kommunizieren und an den Vorteilen der digitalen Wirtschaft teilhaben können. Eine Einwilligung in die Verarbeitung von Daten aus der Benutzung von Internet- oder Sprachkommunikationsdiensten ist unwirksam, wenn die betroffene Person keine echte und freie Wahl hat oder ihre Einwilligung nicht verweigern oder widerrufen kann, ohne Nachteile zu erleiden.

(19) Der Inhalt der elektronischen Kommunikation fällt in den Wesensgehalt des nach Artikel 7 der Charta geschützten Grundrechts auf Achtung des Privat- und Familienlebens, der Wohnung und der Kommunikation. Eingriffe in die Inhalte der elektronischen Kommunikation sollten nur unter eindeutig festgelegten Voraussetzungen, zu ganz bestimmten Zwecken und unter Einhaltung angemessener Schutzvorkehrungen gegen Missbrauch erlaubt werden. Diese Verordnung sieht die Möglichkeit vor, dass die Betreiber elektronischer Kommunikationsdienste mit einer in Kenntnis der Sachlage gegebenen Einwilligung aller betroffenen Endnutzer die in Übertragung befindlichen elektronischen Kommunikationsdaten verarbeiten können. Beispielsweise können so Betreiber Dienstleistungen anbieten, die das Scannen aller E-Mail-Nachrichten zur Entfernung von bestimmtem, zuvor festgelegten Material umfassen. Angesichts der Sensibilität der Kommunikationsinhalte wird in dieser Verordnung von der Annahme ausgegangen, dass die Verarbeitung solcher Inhaltsdaten hohe Risiken für die Rechte und Freiheiten natürlicher Personen mit sich bringt. Betreiber elektronischer Kommunikationsdienste, die beabsichtigen, solche Arten von Daten zu verarbeiten, sollten vor der Verarbeitung stets die Aufsichtsbehörde konsultieren. Eine solche Konsultation sollte nach Artikel 36 Absätze 2 und 3 der Verordnung (EU) 2016/679 erfolgen. Diese Annahme bezieht sich nicht auf die Verarbeitung von Inhaltsdaten zur Bereitstellung eines vom Endnutzer gewünschten Dienstes, wenn der Endnutzer darin eingewilligt hat und die Verarbeitung nur zu den Zwecken und für die Dauer erfolgt, die für den Dienst unbedingt notwendig und verhältnismäßig sind. Nachdem elektronische Kommunikationsinhalte vom Endnutzer verschickt und von dem bzw. den bestimmungsgemäßen Endnutzern empfangen wurden, können sie von den Endnutzern oder von einem Dritten, der von den Endnutzern mit der Aufzeichnung oder Speicherung solcher Daten beauftragt wurde, aufgezeichnet oder gespeichert werden. Eine solche Verarbeitung der Daten muss im Einklang mit der Verordnung (EU) 2016/679 stehen.

(20) Die Endeinrichtungen der Endnutzer elektronischer Kommunikationsnetze und alle Informationen im Zusammenhang mit der Nutzung dieser Endeinrichtungen, ob sie nun von solchen Geräten gespeichert oder ausgesendet, von ihnen angefordert oder verarbeitet werden, um sich mit anderen Geräten oder mit Netzanlagen verbinden zu können, sind Teil der Privatsphäre der Endnutzer, die dem Schutz aufgrund der Charta

der Grundrechte der Europäischen Union und der Europäischen Konvention zum Schutz der Menschenrechte und Grundfreiheiten unterliegt. Die Informationen im Zusammenhang mit solchen Endeinrichtungen erfordern einen erhöhten Schutz der Privatsphäre, da solche Endeinrichtungen Informationen enthalten oder verarbeiten, die einen tiefen Einblick in komplexe emotionale, politische und soziale Aspekte der Persönlichkeit einer Person geben können, darunter Nachrichteninhalte, Bilder, Aufenthaltsorte durch Zugriff auf die GPS-Funktionen der Geräte sowie Kontaktlisten und andere bereits in dem Gerät gespeicherte Informationen. Darüber hinaus können unerwünschte Verfolgungswerkzeuge wie z. B. Spyware, Webbugs, versteckte Kennungen und Verfolgungs-Cookies ohne das Wissen des Endnutzers in dessen Endeinrichtung eindringen, um Zugang zu Informationen zu erlangen, versteckte Informationen zu speichern oder die Nutzeraktivität zu verfolgen. Informationen in Bezug auf das Gerät des Endnutzers können auch im Fernzugang zu Identifizierungs- und Verfolgungszwecken erhoben werden, mit Techniken wie der Verfolgung von Gerätekennungen, was oft ohne Wissen des Endnutzers geschieht, und können eine ernsthafte Verletzung der Privatsphäre dieser Endnutzer darstellen. Techniken, mit denen die Aktivitäten der Endnutzer heimlich beobachtet werden, indem z. B. ihre Online-Aktivitäten oder die Standorte ihrer Endeinrichtungen verfolgt werden, oder mit denen die Funktionsweise der Endeinrichtungen der Endnutzer unbemerkt manipuliert wird, stellen eine ernste Bedrohung der Privatsphäre der Endnutzer dar. Deshalb sollten derartige Eingriffe in die Endeinrichtungen der Endnutzer nur mit Einwilligung des Endnutzers und für bestimmte transparente Zwecke erlaubt sein.

(21) Ausnahmen von der Verpflichtung, die Einwilligung in die Nutzung der Verarbeitungs- und Speicherfunktionen von Endeinrichtungen oder den Zugriff auf in Endeinrichtungen gespeicherte Informationen einzuholen, sollten auf Situationen beschränkt sein, in denen kein oder nur ein geringfügiger Eingriff in die Privatsphäre stattfindet. Beispielsweise sollte keine Einwilligung eingeholt werden für ein technisches Speichern oder Zugreifen, das zu dem rechtmäßigen Zweck, die vom Endnutzer ausdrücklich gewünschte Nutzung eines bestimmten Dienstes zu ermöglichen, unbedingt notwendig und verhältnismäßig ist. Dazu gehört auch das Speichern von Cookies für die Dauer einer für den Besuch einer Website einmal aufgebauten Sitzung, um die Eingaben des Endnutzers beim Ausfüllen von Online-Formularen, die sich über mehrere Seiten erstrecken, mitverfolgen zu können. Cookies können auch ein legitimes und nützliches Hilfsmittel sein, um beispielsweise den Webdatenverkehr zu einer Website zu messen. Konfigurationsprüfungen, die Anbieter von Diensten der Informationsgesellschaft vornehmen, um ihren Dienst entsprechend den Einstellungen des Endnutzers bereitstellen zu können, wie auch das bloße Feststellen der Tatsache, dass das Gerät des Endnutzers die vom Endnutzer angeforderten Inhalte nicht empfangen kann, sollten nicht als Zugriff auf ein Gerät oder als Nutzung der Verarbeitungsfunktionen des Geräts betrachtet werden.

(22) Die Methoden zur Bereitstellung von Informationen und die Einholung der Einwilligung des Endnutzers sollten so benutzerfreundlich wie möglich sein. Wegen der allgegenwärtigen Verwendung von Verfolgungs-Cookies und anderer Verfolgungstechniken werden die Endnutzer immer häufiger aufgefordert, ihre Einwilligung in die Speicherung solcher Verfolgungs-Cookies in ihren Endeinrichtungen zu geben. Infolge dessen werden die Endnutzer mit Einwilligungsanfragen überhäuft. Mit Hilfe technischer Mittel für die Erteilung der Einwilligung, z. B. durch transparente und benutzerfreundliche Einstellungen, könnte dieses Problem behoben werden. Deshalb sollte diese Verordnung die Möglichkeit

vorsehen, dass die Einwilligung durch die entsprechenden Einstellungen in einem Browser oder einer anderen Anwendung erteilt werden kann. Die Auswahl, die Endnutzer bei der Festlegung ihrer allgemeinen Einstellungen zur Privatsphäre in einem Browser oder einer anderen Anwendung getroffen haben, sollte für Dritte verbindlich und ihnen gegenüber auch durchsetzbar sein. Webbrowser sind eine Art von Softwareanwendung, die es ermöglicht, Informationen aus dem Internet abzurufen und darzustellen. Andere Arten von Anwendungen wie solche, die Anrufe und die Nachrichtenübermittlung ermöglichen oder Navigationshilfe bieten, sind dazu ebenfalls in der Lage. Ein Großteil der Vorgänge, die zwischen dem Endnutzer und der Website ablaufen, werden von Webbrowsern abgewickelt. Aus dieser Sicht kommt ihnen eine Sonderstellung zu, wenn es darum geht, den Endnutzern die Kontrolle über den Informationsfluss zu und von ihrer Endeinrichtung zu erleichtern. So können Webbrowser insbesondere als Torwächter dienen und den Endnutzern helfen, ein Speichern von Informationen in ihren Endeinrichtungen (wie Smartphones, Tablets oder Computer) bzw. den Zugriff darauf zu verhindern.

(23) Die Grundsätze des Datenschutzes durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen wurden in Artikel 25 der Verordnung (EU) 2016/679 festgeschrieben. Gegenwärtig haben die meisten weitverbreiteten Browser für Cookies die Standardeinstellung „Alle Cookies annehmen“. Deshalb sollten Anbieter von Software, die das Abrufen und Darstellen von Informationen aus dem Internet erlaubt, dazu verpflichtet sein, die Software so zu konfigurieren, dass sie die Möglichkeit bietet zu verhindern, dass Dritte Informationen in der Endeinrichtung speichern; diese Einstellung wird häufig als „Cookies von Drittanbietern zurückweisen“ bezeichnet. Den Endnutzern sollte eine Reihe von Einstellungsmöglichkeiten zur Privatsphäre angeboten werden, die vom höheren Schutz (z. B. „Cookies niemals annehmen“) über einen mittleren Schutz (z. B. „Cookies von Drittanbietern zurückweisen“ oder „Nur Cookies von Erstanbietern annehmen“) bis zum niedrigeren Schutz (z. B. „Cookies immer annehmen“) reicht. Solche Einstellungen zur Privatsphäre sollten in leicht sichtbarer und verständlicher Weise dargestellt werden.

(24) Damit Webbrowser die in der Verordnung (EU) 2016/679 vorgeschriebene Einwilligung der Endnutzer, z. B. in die Speicherung von Verfolgungs-Cookies von Drittanbietern, einholen können, sollten sie unter anderem eine eindeutige bestätigende Handlung von der Endeinrichtung des Endnutzers verlangen, mit der dieser seine freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich erklärte Zustimmung zur Speicherung solcher Cookies in seiner Endeinrichtung und zum Zugriff darauf bekundet. Eine solche Handlung kann als bestätigend verstanden werden, wenn Endnutzer zur Einwilligung beispielsweise die Option „Cookies von Drittanbietern annehmen“ aktiv auswählen müssen und ihnen die dazu notwendigen Informationen gegeben werden. Hierzu müssen die Anbieter von Software, die den Zugang zum Internet ermöglicht, verpflichtet werden, die Endnutzer zum Zeitpunkt der Installation darauf hinzuweisen, dass die Einstellungen zur Privatsphäre unter den verschiedenen Möglichkeiten ausgewählt werden können, und sie aufzufordern, eine Wahl zu treffen. Die gegebenen Informationen sollten die Endnutzer nicht davon abschrecken, höhere Einstellungen zur Privatsphäre zu wählen, und sie sollten alle wichtigen Informationen über die mit der Annahme von Cookies von Drittanbietern verbundenen Risiken enthalten, wozu auch das Anlegen langfristiger Aufzeichnungen über die Browserverläufe des Betroffenen und die Verwendung solcher Aufzeichnungen zur Übermittlung gezielter Werbung gehören.

Es sollte gefördert werden, dass Webbrowser den Endnutzern einfache Möglichkeiten bieten, die Einstellungen zur Privatsphäre während der Benutzung jederzeit zu ändern, und dem Nutzer erlauben, Ausnahmen für bestimmte Websites zu machen oder in Listen festzulegen oder anzugeben, von welchen Websites Cookies (auch von Drittanbietern) immer oder niemals angenommen werden sollen.

(25) Für den Zugang zu elektronischen Kommunikationsnetzen ist es erforderlich, dass regelmäßig bestimmte Datenpakete ausgesendet werden, um eine Verbindung zum Netz oder mit anderen Geräten im Netz zu erkennen oder aufrecht zu erhalten. Darüber hinaus muss den Geräten eine eindeutige Adresse zugewiesen sein, damit sie in diesem Netz identifizierbar sind. In ähnlicher Weise sehen auch die Normen für auf Drahtlos- und Funkzellentechnik beruhende Telefonie ein Aussenden aktiver Signale vor, die eindeutige Kennungen wie eine MAC-Adresse, die IMEI (internationale Mobilfunkgerätekennung), die IMSI (internationale Mobilfunk-Teilnehmerkennung) usw. enthalten. Eine einzelne Drahtlos-Basisstation (d. h. ein Sender und Empfänger) wie beispielsweise ein Drahtlos-Zugangspunkt deckt einen bestimmten Bereich ab, in dem solche Informationen erfasst werden können. Es gibt inzwischen Diensteanbieter, die aufgrund gescannter gerätebezogener Informationen Verfolgungsdienste mit verschiedenartigen Funktionsmerkmalen anbieten, darunter die Zählung von Personen, die Bereitstellung von Daten über die Zahl der in einer Schlange wartenden Personen, die Ermittlung der Personenzahl in einem bestimmten Gebiet usw. Diese Informationen können zu Zwecken verwendet werden, die stärker in die Privatsphäre eingreifen, wie das Übermitteln gewerblicher Werbenachrichten mit persönlich angepassten Angeboten an Endnutzer, wenn diese beispielsweise ein Ladengeschäft betreten. Während einige dieser Funktionsmerkmale keine große Gefahr für die Privatsphäre mit sich bringen, sind andere durchaus bedenklich, z. B. solche, die mit der Verfolgung einzelner Personen über einen längeren Zeitraum verbunden sind (u. a. wiederholte Besuche an bestimmten Orten). Anwender solcher Praktiken sollten am Rand des betroffenen Bereichs in hervorgehobener Weise Hinweise anzeigen, mit denen die Endnutzer vor Betreten des Bereichs darüber aufgeklärt werden, dass entsprechende Technik in einem bestimmten Umkreis im Einsatz ist, aber auch über den Zweck der Verfolgung, die dafür verantwortliche Person und darüber, was der Endnutzer der Endeinrichtung tun kann, um die Datenerhebung zu beenden oder auf ein Minimum zu beschränken. Werden personenbezogene Daten nach Artikel 13 der Verordnung (EU) 2016/679 erhoben, so sollten zusätzlich weitere Informationen bereitgestellt werden.

(26) Soweit diese Verordnung für die Verarbeitung elektronischer Kommunikationsdaten durch Betreiber elektronischer Kommunikationsdienste gilt, sollte sie vorsehen, dass die Mitgliedstaaten einige Pflichten und Rechte unter bestimmten Voraussetzungen mittels Rechtsvorschriften beschränken können, wenn diese Beschränkung in einer demokratischen Gesellschaft eine notwendige und verhältnismäßige Maßnahme zum Schutz bestimmter wichtiger öffentlicher Interessen darstellt, wozu die nationale Sicherheit, die Verteidigung, die öffentliche Sicherheit und die Verhütung, Ermittlung, Aufdeckung und Verfolgung von Straftaten oder die Strafvollstreckung zählen, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit und sonstiger wichtiger Ziele des allgemeinen öffentlichen Interesses der Union oder eines Mitgliedstaats, insbesondere wichtiger wirtschaftlicher oder finanzieller Interessen der Union oder eines Mitgliedstaats, oder Kontroll-, Überwachungs- und Ordnungsfunktionen, die dauernd oder zeitweise mit der Ausübung öffentlicher Gewalt in Bezug auf solche Interessen verbunden sind. Deshalb

sollte diese Verordnung die Möglichkeit der Mitgliedstaaten zum rechtmäßigen Abfangen elektronischer Kommunikation oder zum Ergreifen anderer Maßnahmen nicht beeinträchtigen, sofern dies notwendig und verhältnismäßig ist, um die oben genannten öffentlichen Interessen zu schützen, und im Einklang mit der Charta der Grundrechte der Europäischen Union und der Europäischen Konvention zum Schutz der Menschenrechte und Grundfreiheiten in ihrer Auslegung durch den Gerichtshof der Europäischen Union und den Europäischen Gerichtshof für Menschenrechte erfolgt. Die Betreiber elektronischer Kommunikationsdienste sollten geeignete Verfahren zur leichteren Beantwortung berechtigter Anfragen der zuständigen Behörden schaffen und dabei gegebenenfalls auch die Rolle des nach Artikel 3 Absatz 3 benannten Vertreters berücksichtigen.

(27) Im Hinblick auf die Rufnummernanzeige ist es erforderlich, das Recht des Anrufers zu wahren, die Anzeige der Rufnummer des Anschlusses, von dem aus der Anruf erfolgt, zu unterdrücken, ebenso wie das Recht des Angerufenen, Anrufe von nicht identifizierten Anschlüssen abzuweisen. Bestimmte Endnutzer, insbesondere telefonische Beratungsdienste und ähnliche Einrichtungen, haben ein Interesse daran, die Anonymität ihrer Anrufer zu gewährleisten. Im Hinblick auf die Anzeige der Rufnummer des Angerufenen ist es erforderlich, das Recht und das berechtigte Interesse des Angerufenen zu wahren, die Anzeige der Rufnummer des Anschlusses, mit dem der Anrufer tatsächlich verbunden ist, zu unterdrücken.

(28) In Sonderfällen ist es gerechtfertigt, die Unterdrückung der Rufnummernanzeige aufzuheben. Die Rechte der Endnutzer auf Privatsphäre in Bezug auf die Rufnummernanzeige sollten eingeschränkt werden, wenn dies erforderlich ist, um belästigende Anrufe zurückzuverfolgen, sowie in Bezug auf die Rufnummernanzeige und Standortdaten, wenn dies erforderlich ist, damit Notdienste wie *e*Call ihre Aufgaben so effektiv wie möglich erfüllen können.

(29) Es gibt technische Möglichkeiten, mit denen Anbieter elektronischer Kommunikationsdienste den Erhalt unerwünschter Anrufe durch die Endnutzer auf unterschiedliche Weisen begrenzen können, z. B. durch Sperren stiller Anrufe und anderer betrügerischer und belästigender Anrufe. Die Betreiber öffentlich zugänglicher nummerngebundener interpersoneller Kommunikationsdienste sollten solche Technik einsetzen und Endnutzer vor belästigenden Anrufen kostenlos schützen. Die Betreiber sollten dafür sorgen, dass die Endnutzer vom Vorhandensein solcher Funktionen Kenntnis haben, indem sie beispielsweise auf ihrer Website darauf hinweisen.

(30) Öffentlich zugängliche Verzeichnisse der Endnutzer elektronischer Kommunikationsdienste finden eine weite Verbreitung. Öffentlich zugängliche Verzeichnisse sind Verzeichnisse oder Dienste, die Informationen über Endnutzer wie deren Telefonnummer (auch Mobiltelefonnummer), E-Mail-Adresse oder andere Kontaktangaben enthalten und Auskunftsdienste umfassen. Das Recht natürlicher Personen auf Privatsphäre und den Schutz personenbezogener Daten erfordert, dass Endnutzer, die natürliche Personen sind, um ihre Einwilligung gebeten werden, bevor ihre personenbezogenen Daten in ein Verzeichnis aufgenommen werden. Das berechtigte Interesse juristischer Personen erfordert, dass Endnutzer, die juristische Personen sind, das Recht haben, der Aufnahme der auf sie bezogenen Daten in ein Verzeichnis zu widersprechen.

(31) Wenn Endnutzer, die natürliche Personen sind, ihre Einwilligung zur Aufnahme ihrer Daten in ein solches Verzeichnis geben, sollten sie mit ihrer Einwilligung auch bestimmen können, welche Kategorien personenbezogener Daten in das Verzeichnis aufgenommen werden (z. B. Name, E-Mail-Adresse, Wohnanschrift, Benutzername, Telefonnummer). Außerdem sollten die Betreiber öffentlicher Verzeichnisse die Endnutzer über die Zwecke des Verzeichnisses und die Suchfunktionen informieren, bevor sie sie in das Verzeichnis aufnehmen. Die Endnutzer sollten mit ihrer Einwilligung auch bestimmen können, anhand welcher Kategorien personenbezogener Daten ihre Kontaktangaben durchsucht werden können. Die Kategorien personenbezogener Daten, die in das Verzeichnis aufgenommen werden, und die Kategorien personenbezogener Daten, anhand deren die Kontaktangaben der Endnutzer durchsucht werden können, müssen nicht notwendigerweise dieselben sein.

(32) In dieser Verordnung wird unter Direktwerbung jede Art von Werbung verstanden, mittels derer eine natürliche oder juristische Person Direktwerbung über elektronische Kommunikationsdienste unmittelbar an einen oder mehrere bestimmte oder bestimmbare Endnutzer richtet. Dies umfasst neben dem zu gewerblichen Zwecken erfolgenden Anbieten von Produkten und Dienstleistungen auch Nachrichten von politischen Parteien, die sich über elektronische Kommunikationsdienste an natürliche Personen wenden, um für ihre Parteien zu werben. Dasselbe sollte für Nachrichten gelten, die von anderen Organisationen ohne Erwerbszweck übermittelt werden, um die Zwecke ihrer Organisation zu fördern.

(33) Es sollten Vorkehrungen getroffen werden, um die Endnutzer vor unerbetener Direktwerbung zu schützen, die in das Privatleben der Endnutzer eingreift. Der Grad des Eingriffs in die Privatsphäre und der Belästigung wird unabhängig von der großen Vielfalt der zur Durchführung dieser elektronischen Kommunikation genutzten Techniken und Kanäle wie automatischer Anruf- und Kommunikationssysteme, Sofortnachrichtenanwendungen, E-Mail, SMS, MMS, Bluetooth usw. als relativ ähnlich betrachtet. Daher ist es gerechtfertigt zu verlangen, dass die Einwilligung des Endnutzers eingeholt wird, bevor gewerbliche elektronische Direktwerbung an Endnutzer gerichtet wird, um so den Schutz natürlicher Personen vor Eingriffen in ihr Privatleben und den Schutz der berechtigten Interessen juristischer Personen wirksam zu gewährleisten. Aus Gründen der Rechtssicherheit und wegen der Notwendigkeit, dafür zu sorgen, dass die Vorschriften zum Schutz vor unerbetener elektronischer Kommunikation zukunftssicher bleiben, ist es erforderlich, einheitliche Vorschriften zu schaffen, die nicht danach unterscheiden, mit welcher Technik diese unerbetene Kommunikation erfolgt, und zugleich einen gleichwertigen Schutz aller Bürger in der gesamten Union zu gewährleisten. Es ist jedoch vertretbar, im Rahmen einer bestehenden Kundenbeziehung die Nutzung von E-Mail-Kontaktangaben zu erlauben, damit ähnliche Produkte oder Dienstleistungen angeboten werden können. Diese Möglichkeit sollte jedoch nur für dasselbe Unternehmen gelten, das die elektronischen Kontaktangaben im Einklang mit der Verordnung (EU) 2016/679 erlangt hat.

(34) Wenn Endnutzer in den Empfang unerbetener Direktwerbung eingewilligt haben, sollten sie dennoch in der Lage sein, ihre Einwilligung jederzeit auf einfache Weise zu wiederrufen. Zur Erleichterung der wirksamen Durchsetzung der Unionsvorschriften über unerbetene Direktwerbung ist es notwendig, die Verschleierung der Identität und die Verwendung falscher Identitäten, falscher Rücksendeadressen oder Rückrufnummern bei der Durchführung unerbetener gewerblicher Direktwerbung zu untersagen. Unerbetene Werbung sollte daher eindeutig als solche erkennbar sein, die

Identität der übermittelnden juristischen oder natürlichen Person offenlegen oder angeben, in wessen Namen die Nachricht übermittelt wird, und die nötigen Informationen geben, damit die Empfänger ihr Recht ausüben können, dem weiteren Empfang von schriftlichen und mündlichen Werbenachrichten zu widersprechen.

(35) Um einen einfachen Widerruf der Einwilligung zu ermöglichen, sollten juristische oder natürliche Personen, die Direktwerbung per E-Mail betreiben, einen Link oder eine gültige E-Mail-Adresse angeben, mit deren Hilfe Endnutzer ihre Einwilligung auf einfache Weise widerrufen können. Juristische oder natürliche Personen, die Direktwerbung mittels persönlicher Anrufe und mittels Anrufen über automatische Anruf- und Kommunikationssysteme betreiben, sollten ihre Anschlussrufnummer, unter der das Unternehmen angerufen werden kann, oder einen besonderen Kode angeben, der kenntlich macht, dass es sich um einen Werbeanruf handelt.

(36) Persönliche Direktwerbeanrufe, die ohne Verwendung automatischer Anruf- und Kommunikationssysteme ausgeführt werden, sind für den Absender kostspieliger und bringen für Endnutzer keine finanziellen Kosten mit sich. Deshalb sollten die Mitgliedstaaten hierfür nationale Systeme einrichten oder beibehalten können, die solche Anrufe nur an Endnutzer erlauben, die dem nicht widersprochen haben.

(37) Anbieter elektronischer Kommunikationsdienste sollten die Endnutzer darüber informieren, welche Maßnahmen diese ergreifen können, um die Sicherheit ihrer Kommunikation, z. B. durch den Einsatz bestimmter Software oder Verschlüsselungstechniken, zu schützen. Die Anforderung, die Endnutzer über besondere Sicherheitsrisiken aufzuklären, entbindet einen Diensteanbieter nicht von der Verpflichtung, auf eigene Kosten unverzüglich geeignete Maßnahmen zu treffen, um einem neuen, unvorhergesehenen Sicherheitsrisiko vorzubeugen und den normalen Sicherheitsstandard des Dienstes wiederherzustellen. Die Bereitstellung von Informationen über Sicherheitsrisiken für die Endnutzer sollte kostenlos sein. Die Bewertung der Sicherheit erfolgt unter Berücksichtigung des Artikels 32 der Verordnung (EU) 2016/679.

(38) Um die vollständige Kohärenz mit der Verordnung (EU) 2016/679 zu gewährleisten, sollte die Durchsetzung der Bestimmungen dieser Verordnung denselben Behörden übertragen werden, die auch für die Durchsetzung der Bestimmungen der Verordnung (EU) 2016/679 zuständig sind; außerdem sollte diese Verordnung dem Kohärenzverfahren der Verordnung (EU) 2016/679 unterliegen. Die Mitgliedstaaten sollten mehr als eine Aufsichtsbehörde haben können, wenn dies ihrer verfassungsmäßigen, organisatorischen und administrativen Struktur entspricht. Die Aufsichtsbehörden sollten auch für die Überwachung der Anwendung dieser Verordnung im Hinblick auf elektronische Kommunikationsdaten für juristische Personen zuständig sein. Diese zusätzlichen Aufgaben sollten die Fähigkeit der Aufsichtsbehörde, ihre Aufgaben in Bezug auf den Schutz personenbezogener Daten nach der Verordnung (EU) 2016/679 und dieser Verordnung wahrzunehmen, nicht beeinträchtigen. Jede Aufsichtsbehörde sollte zusätzlich mit Finanzmitteln, Personal, Räumlichkeiten und Infrastruktur ausgestattet werden, die für die wirksame Wahrnehmung ihrer Aufgaben nach dieser Verordnung notwendig sind.

(39) Jede Aufsichtsbehörde sollte dafür zuständig sein, im Hoheitsgebiet ihres Mitgliedstaats die Befugnisse auszuüben und die Aufgaben zu erfüllen, die in dieser Verordnung festgelegt sind. Um die einheitliche Überwachung und Durchsetzung

dieser Verordnung in der gesamten Union sicherzustellen, sollten die Aufsichtsbehörden in jedem Mitgliedstaat dieselben Aufgaben und wirksamen Befugnisse haben, darunter – unbeschadet der Befugnisse der Strafverfolgungsbehörden nach dem Recht der Mitgliedstaaten – die Befugnis, Verstöße gegen diese Verordnung den Justizbehörden zur Kenntnis zu bringen und Gerichtsverfahren anzustrengen. Die Mitgliedstaaten und deren Aufsichtsbehörden werden dazu angehalten, bei der Anwendung dieser Verordnung die besonderen Bedürfnisse von Kleinstunternehmen sowie von kleinen und mittleren Unternehmen zu berücksichtigen.

(40) Im Interesse einer konsequenteren Durchsetzung der Vorschriften dieser Verordnung sollte jede Aufsichtsbehörde befugt sein, zusätzlich zu oder anstelle von anderen geeigneten Maßnahmen nach dieser Verordnung bei Verstößen gegen diese Verordnung Sanktionen einschließlich Geldbußen zu verhängen. In dieser Verordnung sollten die Verstöße sowie die Obergrenze der entsprechenden Geldbußen und die Kriterien für ihre Festsetzung genannt werden, wobei diese Geldbußen von der zuständigen Aufsichtsbehörde in jedem Einzelfall unter Berücksichtigung aller besonderen Umstände und insbesondere der Art, Schwere und Dauer des Verstoßes und seiner Folgen sowie der Maßnahmen festzusetzen sind, die ergriffen wurden, um die Einhaltung der aus dieser Verordnung erwachsenden Verpflichtungen zu gewährleisten und die Folgen des Verstoßes abzuwenden oder abzumildern. Zum Zweck der Festsetzung einer Geldbuße sollte der Begriff „Unternehmen“ im Sinne der Artikel 101 und 102 AEUV verstanden werden.

(41) Um die Zielvorgaben dieser Verordnung zu erfüllen, d. h. die Grundrechte und Grundfreiheiten natürlicher Personen und insbesondere ihr Recht auf Schutz ihrer personenbezogenen Daten zu schützen und den freien Verkehr personenbezogener Daten innerhalb der Union zu gewährleisten, sollte der Kommission die Befugnis übertragen werden, gemäß Artikel 290 AEUV Rechtsakte zur Ergänzung dieser Verordnung zu erlassen. Delegierte Rechtsakte sollten insbesondere erlassen werden in Bezug auf die bereitzustellenden Informationen, auch mittels standardisierter Bildsymbole, um einen leicht wahrnehmbaren und verständlichen Überblick über die Erhebung der von der Endeinrichtung ausgesendeten Informationen zu vermitteln, sowie den Zweck, die dafür verantwortliche Person und die Maßnahmen, die der Endnutzer der Endeinrichtung treffen kann, um die Erhebung zu beenden oder auf ein Minimum zu beschränken. Delegierte Rechtsakte sind ebenfalls erforderlich, um einen Kode festzulegen, der Direktwerbeanrufe kenntlich macht, auch solche, die mithilfe automatischer Anruf- und Kommunikationssysteme getätigt werden. Es ist von besonderer Bedeutung, dass die Kommission angemessene Konsultationen durchführt, und dass diese Konsultationen mit den Grundsätzen im Einklang stehen, die in der Interinstitutionellen Vereinbarung über bessere Rechtsetzung vom 13. April 2016[8] niedergelegt wurden. Um insbesondere für eine gleichberechtigte Beteiligung an der Ausarbeitung delegierter Rechtsakte zu sorgen, erhalten das Europäische Parlament und der Rat alle Dokumente zur gleichen Zeit wie die Sachverständigen der Mitgliedstaaten, und ihre Sachverständigen haben systematisch Zugang zu den Sitzungen der Sachverständigengruppen der Kommission, die mit der Ausarbeitung

[8] Interinstitutionelle Vereinbarung zwischen dem Europäischen Parlament, dem Rat der Europäischen Union und der Europäischen Kommission vom 13. April 2016 über bessere Rechtsetzung (ABl. L 123 vom 12.5.2016, S. 1).

der delegierten Rechtsakte befasst sind. Überdies sollten der Kommission zur Gewährleistung einheitlicher Bedingungen für die Durchführung dieser Verordnung Durchführungsbefugnisse übertragen werden, wenn dies in dieser Verordnung vorgesehen ist. Diese Befugnisse sollten nach Maßgabe der Verordnung (EU) Nr. 182/2011 des Europäischen Parlaments und des Rates ausgeübt werden.

(42) Da das Ziel dieser Verordnung, nämlich die Gewährleistung eines gleichwertigen Datenschutzniveaus für natürliche und juristische Personen und des freien Verkehrs elektronischer Kommunikationsdaten in der Union, von den Mitgliedstaaten nicht ausreichend verwirklicht werden kann, sondern vielmehr wegen des Umfangs oder der Wirkungen der Maßnahme auf Unionsebene besser zu verwirklichen ist, kann die Union im Einklang mit dem in Artikel 5 des Vertrags über die Europäische Union verankerten Subsidiaritätsprinzip tätig werden. Entsprechend dem in demselben Artikel genannten Grundsatz der Verhältnismäßigkeit geht diese Verordnung nicht über das für die Verwirklichung dieses Ziels erforderliche Maß hinaus.

(43) Die Richtlinie 2002/58/EG sollte aufgehoben werden –

HABEN FOLGENDE VERORDNUNG ERLASSEN:

KAPITEL I
ALLGEMEINE BESTIMMUNGEN

Artikel 1
Gegenstand

(1) Diese Verordnung legt Vorschriften zum Schutz von Grundrechten und Grundfreiheiten natürlicher und juristischer Personen bei der Bereitstellung und Nutzung elektronischer Kommunikationsdienste fest und regelt insbesondere die Rechte auf Achtung des Privatlebens und der Kommunikation und den Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten.

(2) Diese Verordnung gewährleistet den freien Verkehr elektronischer Kommunikationsdaten und elektronischer Kommunikationsdienste in der Union, der aus Gründen der Achtung des Privatlebens und der Kommunikation natürlicher und juristischer Personen und des Schutzes natürlicher Personen bei der Verarbeitung personenbezogener Daten weder beschränkt noch untersagt werden darf.

(3) Die Bestimmungen dieser Verordnung präzisieren und ergänzen die Verordnung (EU) 2016/679 durch die Festlegung besonderer Vorschriften für die in den Absätzen 1 und 2 genannten Zwecke.

Artikel 2
Sachlicher Anwendungsbereich

(1) Diese Verordnung gilt für die Verarbeitung elektronischer Kommunikationsdaten, die in Verbindung mit der Bereitstellung und Nutzung elektronischer Kommunikationsdienste erfolgt, und für Informationen in Bezug auf die Endeinrichtungen der Endnutzer.

(2) Diese Verordnung gilt nicht für:

a) Tätigkeiten, die nicht in den Anwendungsbereich des Unionsrechts fallen;

b) Tätigkeiten der Mitgliedstaaten, die in den Anwendungsbereich von Titel V Kapitel 2 des Vertrags über die Europäische Union fallen;

c) elektronische Kommunikationsdienste, die nicht öffentlich zugänglich sind;

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.

(3) Für die Verarbeitung elektronischer Kommunikationsdaten durch die Organe, Einrichtungen und sonstigen Stellen der Europäischen Union gilt die Verordnung (EU) 00/0000 [neue Verordnung zur Ersetzung der Verordnung 45/2001].

(4) Die vorliegende Verordnung lässt die Anwendung der Richtlinie 2000/31/EG[9] und insbesondere der Vorschriften zur Verantwortlichkeit der Anbieter reiner Vermittlungsdienste in den Artikeln 12 bis 15 dieser Richtlinie unberührt.

(5) Die Bestimmungen der Richtlinie 2014/53/EU bleiben von dieser Verordnung unberührt.

Artikel 3
Räumlicher Anwendungsbereich und Vertreter

(1) Diese Verordnung gilt für:

a) die Bereitstellung elektronischer Kommunikationsdienste für Endnutzer in der Union, unabhängig davon, ob vom Endnutzer eine Bezahlung verlangt wird;

b) die Nutzung solcher Dienste;

c) den Schutz von Informationen in Bezug auf die Endeinrichtungen der Endnutzer in der Union.

(2) Ist der Betreiber eines elektronischen Kommunikationsdienstes nicht in der Union niedergelassen, so muss er schriftlich einen Vertreter in der Union benennen.

(3) Der Vertreter muss in einem der Mitgliedstaaten niedergelassen sein, in denen sich die Endnutzer dieser elektronischen Kommunikationsdienste befinden.

(4) Der Vertreter muss für die Zwecke der Gewährleistung der Einhaltung dieser Verordnung befugt sein, zusätzlich zu dem von ihm vertretenen Betreiber oder an

[9] Richtlinie 2000/31/EG des Europäischen Parlaments und des Rates vom 8. Juni 2000 über bestimmte rechtliche Aspekte der Dienste der Informationsgesellschaft, insbesondere des elektronischen Geschäftsverkehrs, im Binnenmarkt („Richtlinie über den elektronischen Geschäftsverkehr“) (ABl. L 178 vom 17.7.2000, S. 1).

dessen Stelle Fragen zu beantworten und Auskünfte zu erteilen, und zwar insbesondere gegenüber Aufsichtsbehörden und Endnutzern in Bezug auf alle Belange im Zusammenhang mit der Verarbeitung elektronischer Kommunikationsdaten.

(5) Die Benennung eines Vertreters nach Absatz 2 erfolgt unbeschadet etwaiger rechtlicher Schritte gegen eine natürliche oder juristische Person, die elektronische Kommunikationsdaten in Verbindung mit der Bereitstellung elektronischer Kommunikationsdienste von außerhalb der Union für Endnutzer in der Union verarbeitet.

Artikel 4
Begriffsbestimmungen

(1) Für die Zwecke dieser Verordnung gelten folgende Begriffsbestimmungen:

a) die Begriffsbestimmungen der Verordnung (EU) 2016/679;

b) die Begriffsbestimmungen für „elektronisches Kommunikationsnetz“, „elektronischer Kommunikationsdienst“, „interpersoneller Kommunikationsdienst“, „nummerngebundener interpersoneller Kommunikationsdienst“, „nummernunabhängiger interpersoneller Kommunikationsdienst“, „Endnutzer“ und „Anruf“ in Artikel 2 Nummern 1, 4, 5, 6, 7, 14 bzw. 21 der [Richtlinie über den europäischen Kodex für die elektronische Kommunikation];

c) die Begriffsbestimmung für „Endeinrichtungen“ in Artikel 1 Nummer 1 der Richtlinie 2008/63/EG der Kommission[10].

(2) Für die Zwecke des Absatzes 1 Buchstabe b schließt die Begriffsbestimmung für „interpersoneller Kommunikationsdienst“ auch Dienste ein, die eine interpersonelle und interaktive Kommunikation lediglich als untrennbar mit einem anderen Dienst verbundene untergeordnete Nebenfunktion ermöglichen.

(3) Für die Zwecke dieser Verordnung gelten zusätzlich folgende Begriffsbestimmungen:

a) „elektronische Kommunikationsdaten“: elektronische Kommunikationsinhalte und elektronische Kommunikationsmetadaten;

b) „elektronische Kommunikationsinhalte“: Inhalte, die mittels elektronischer Kommunikationsdienste übermittelt werden, z. B. Textnachrichten, Sprache, Videos, Bilder und Ton;

c) „elektronische Kommunikationsmetadaten“: Daten, die in einem elektronischen Kommunikationsnetz zu Zwecken der Übermittlung, der Verbreitung oder des Austauschs elektronischer Kommunikationsinhalte

[10] Richtlinie 2008/63/EG der Kommission vom 20. Juni 2008 über den Wettbewerb auf dem Markt für Telekommunikationsendeinrichtungen (ABl. L 162 vom 21.6.2008, S. 20).

verarbeitet werden; dazu zählen die zur Verfolgung und Identifizierung des Ausgangs- und Zielpunkts einer Kommunikation verwendeten Daten, die im Zusammenhang mit der Bereitstellung elektronischer Kommunikationsdienste erzeugten Daten über den Standort des Geräts sowie Datum, Uhrzeit, Dauer und Art der Kommunikation;

d) „öffentlich zugängliches Verzeichnis“: ein Verzeichnis der Endnutzer elektronischer Kommunikationsdienste in gedruckter oder elektronischer Form, das veröffentlicht oder der Öffentlichkeit bzw. einem Teil der Öffentlichkeit zugänglich gemacht wird, auch mithilfe eines Verzeichnisauskunftsdienstes;

e) „E-Mail“ (elektronische Post): jede über ein elektronisches Kommunikationsnetz verschickte elektronische Nachricht, die Informationen in Text-, Sprach-, Video-, Ton- oder Bildform enthält und die im Netz oder in zugehörigen Rechneranlagen oder in Endeinrichtungen ihres Empfängers gespeichert werden kann;

f) „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.;

g) „persönliche Direktwerbeanrufe“: direkt persönlich und ohne Verwendung automatischer Anruf- und Kommunikationssysteme ausgeführte Anrufe;

h) „automatische Anruf- und Kommunikationssysteme“: Systeme, die automatisch Anrufe zu einem oder mehreren Empfängern entsprechend den für das System gemachten Einstellungen aufbauen und Ton übertragen können, der keine live gesprochene Rede darstellt, einschließlich Anrufen unter Verwendung automatischer Anruf- und Kommunikationssysteme, die die angerufene Person mit einer einzelnen Person verbinden.

KAPITEL II
SCHUTZ DER ELEKTRONISCHEN KOMMUNIKATION NATÜRLICHER UND JURISTISCHER PERSONEN UND DER IN IHREN ENDEINRICHTUNGEN GESPEICHERTEN INFORMATIONEN

Artikel 5
Vertraulichkeit elektronischer Kommunikationsdaten

Elektronische Kommunikationsdaten sind vertraulich. Eingriffe in elektronische Kommunikationsdaten wie Mithören, Abhören, Speichern, Beobachten, Scannen oder andere Arten des Abfangens oder Überwachens oder Verarbeitens elektronischer Kommunikationsdaten durch andere Personen als die Endnutzer sind untersagt, sofern sie nicht durch diese Verordnung erlaubt werden.

Artikel 6
Erlaubte Verarbeitung elektronischer Kommunikationsdaten

(1) Betreiber elektronischer Kommunikationsnetze und -dienste dürfen elektronische Kommunikationsdaten verarbeiten, wenn

a) dies zur Durchführung der Übermittlung der Kommunikation nötig ist, für die dazu erforderliche Dauer, oder

b) dies zur Aufrechterhaltung oder Wiederherstellung der Sicherheit elektronischer Kommunikationsnetze und -dienste oder zur Erkennung von technischen Defekten und Fehlern bei der Übermittlung der elektronischen Kommunikation nötig ist, für die dazu erforderliche Dauer.

(2) Betreiber elektronischer Kommunikationsdienste dürfen elektronische Kommunikationsmetadaten verarbeiten, wenn

a) dies zur Einhaltung verbindlicher Dienstqualitätsanforderungen nach der [Richtlinie über den europäischen Kodex für die elektronische Kommunikation] oder der Verordnung (EU) 2015/2120[11] nötig ist, für die dazu erforderliche Dauer, oder

b) dies zur Rechnungstellung, zur Berechnung von Zusammenschaltungszahlungen, zur Erkennung oder Beendigung betrügerischer oder missbräuchlicher Nutzungen elektronischer Kommunikationsdienste oder der diesbezüglichen Verträge nötig ist, oder

c) der betreffende Endnutzer seine Einwilligung zur Verarbeitung seiner Kommunikationsmetadaten für einen oder mehrere bestimmte Zwecke gegeben hat, so auch für die Bereitstellung bestimmter Dienste für diese Endnutzer, sofern die betreffenden Zwecke durch eine Verarbeitung anonymisierter Informationen nicht erreicht werden können.

(3) Betreiber elektronischer Kommunikationsdienste dürfen elektronische Kommunikationsinhalte nur verarbeiten:

a) zum alleinigen Zweck der Bereitstellung eines bestimmten Dienstes für einen Endnutzer, wenn der bzw. die betreffenden Endnutzer ihre Einwilligung zur Verarbeitung ihrer elektronischen Kommunikationsinhalte gegeben haben und die Dienstleistung ohne Verarbeitung dieser Inhalte nicht erbracht werden kann, oder

b) wenn alle betreffenden Endnutzer ihre Einwilligung zur Verarbeitung ihrer elektronischen Kommunikationsinhalte für einen oder mehrere bestimmte Zwecke gegeben haben, die durch eine Verarbeitung anonymisierter Informationen nicht erreicht werden können, und wenn der Betreiber hierzu die

[11] 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 310 vom 26.11.2015, S. 1).

Aufsichtsbehörde konsultiert hat. Artikel 36 Absätze 2 und 3 der Verordnung (EU) 2016/679 findet auf die Konsultation der Aufsichtsbehörde Anwendung.

Artikel 7
Speicherung und Löschung elektronischer Kommunikationsdaten

(1) Unbeschadet des Artikels 6 Absatz 1 Buchstabe b und des Artikels 6 Absatz 3 Buchstaben a und b löscht der Betreiber des elektronischen Kommunikationsdienstes elektronische Kommunikationsinhalte oder anonymisiert diese Daten, sobald der bzw. die vorgesehenen Empfänger die elektronischen Kommunikationsinhalte erhalten haben. Diese Daten können von den Endnutzern oder von Dritten, die von den Endnutzern mit der Aufzeichnung, Speicherung oder anderweitigen Verarbeitung dieser Daten beauftragt werden, im Einklang mit der Verordnung (EU) 2016/679 aufgezeichnet oder gespeichert werden.

(2) Unbeschadet des Artikels 6 Absatz 1 Buchstabe b und des Artikels 6 Absatz 2 Buchstaben a und c löscht der Betreiber des elektronischen Kommunikationsdienstes elektronische Kommunikationsmetadaten oder anonymisiert diese Daten, sobald sie für die Übermittlung einer Kommunikation nicht mehr benötigt werden.

(3) Erfolgt die Verarbeitung elektronischer Kommunikationsmetadaten zu Abrechnungszwecken im Einklang mit Artikel 6 Absatz 2 Buchstabe b, so dürfen die betreffenden Metadaten bis zum Ablauf der Frist aufbewahrt werden, innerhalb deren nach nationalem Recht die Rechnung rechtmäßig angefochten oder der Anspruch auf Zahlung geltend gemacht werden kann.

Artikel 8
Schutz der in Endeinrichtungen der Endnutzer gespeicherten oder sich auf diese beziehenden Informationen

(1) Jede vom betreffenden Endnutzer nicht selbst vorgenommene Nutzung der Verarbeitungs- und Speicherfunktionen von Endeinrichtungen und jede Erhebung von Informationen aus Endeinrichtungen der Endnutzer, auch über deren Software und Hardware, ist untersagt, außer sie erfolgt aus folgenden Gründen:

a) sie ist für den alleinigen Zweck der Durchführung eines elektronischen Kommunikationsvorgangs über ein elektronisches Kommunikationsnetz nötig oder

b) der Endnutzer hat seine Einwilligung gegeben oder

c) sie ist für die Bereitstellung eines vom Endnutzer gewünschten Dienstes der Informationsgesellschaft nötig oder

d) sie ist für die Messung des Webpublikums nötig, sofern der Betreiber des vom Endnutzer gewünschten Dienstes der Informationsgesellschaft diese Messung durchführt.

(2) Die Erhebung von Informationen, die von Endeinrichtungen ausgesendet werden, um sich mit anderen Geräten oder mit Netzanlagen verbinden zu können, ist untersagt, außer

a) sie erfolgt ausschließlich zum Zwecke der Herstellung einer Verbindung und für die dazu erforderliche Dauer oder

b) es wird in hervorgehobener Weise ein deutlicher Hinweis angezeigt, der zumindest Auskunft gibt über die Modalitäten der Erhebung, ihren Zweck, die dafür verantwortliche Person und die anderen nach Artikel 13 der Verordnung (EU) 2016/679 verlangten Informationen, soweit personenbezogene Daten erfasst werden, sowie darüber, was der Endnutzer der Endeinrichtung tun kann, um die Erhebung zu beenden oder auf ein Minimum zu beschränken.

Voraussetzung für die Erhebung solcher Informationen ist die Anwendung geeigneter technischer und organisatorischer Maßnahmen, die ein dem Risiko angemessenes Schutzniveau nach Artikel 32 der Verordnung (EU) 2016/679 gewährleisten.

(3) Die nach Absatz 2 Buchstabe b zu gebenden Informationen können in Kombination mit standardisierten Bildsymbolen bereitgestellt werden, um in leicht wahrnehmbarer, verständlicher und klar nachvollziehbarer Form einen aussagekräftigen Überblick über die Erhebung zu vermitteln.

(4) Der Kommission wird die Befugnis übertragen, nach Artikel 27 delegierte Rechtsakte zur Bestimmung der Informationen, die durch standardisierte Bildsymbole darzustellen sind, und der Verfahren für die Bereitstellung standardisierter Bildsymbole zu erlassen.

Artikel 9
Einwilligung

(1) Für die Einwilligung gelten die Begriffsbestimmung und die Voraussetzungen, die in Artikel 4 Nummer 11 und Artikel 7 der Verordnung (EU) 2016/679 festgelegt sind.

(2) Unbeschadet des Absatzes 1 kann die Einwilligung für die Zwecke des Artikels 8 Absatz 1 Buchstabe b – soweit dies technisch möglich und machbar ist – in den passenden technischen Einstellungen einer Software, die den Zugang zum Internet ermöglicht, gegeben werden.

(3) Endnutzern, die ihre Einwilligung zur Verarbeitung elektronischer Kommunikationsdaten nach Artikel 6 Absatz 2 Buchstabe c und Artikel 6 Absatz 3 Buchstaben a und b gegeben haben, wird nach Artikel 7 Absatz 3 der Verordnung (EU) 2016/679 die Möglichkeit eingeräumt, ihre Einwilligung jederzeit zu widerrufen; sie werden in regelmäßigen Abständen von sechs Monaten an diese Möglichkeit erinnert, solange die Verarbeitung andauert.

Artikel 10
Bereitzustellende Informationen und Einstellungsmöglichkeiten zur Privatsphäre

(1) In Verkehr gebrachte Software, die eine elektronische Kommunikation erlaubt, darunter auch das Abrufen und Darstellen von Informationen aus dem Internet, muss die Möglichkeit bieten zu verhindern, dass Dritte Informationen in der Endeinrichtung eines Endnutzers speichern oder bereits in der Endeinrichtung gespeicherte Informationen verarbeiten.

(2) Bei der Installation muss die Software den Endnutzer über die Einstellungsmöglichkeiten zur Privatsphäre informieren und zur Fortsetzung der Installation vom Endnutzer die Einwilligung zu einer Einstellung verlangen.

(3) Bei Software, die am 25. Mai 2018 bereits installiert ist, müssen die Anforderungen der Absätze 1 und 2 zum Zeitpunkt der ersten Aktualisierung der Software, jedoch spätestens ab dem 25. August 2018 erfüllt werden.

Artikel 11
Beschränkungen

(1) Die Union oder die Mitgliedstaaten können im Wege von Gesetzgebungsmaßnahmen den Umfang der in den Artikeln 5 bis 8 festgelegten Pflichten und Rechte beschränken, sofern eine solche Beschränkung den Wesensgehalt der Grundrechte und Grundfreiheiten achtet und in einer demokratischen Gesellschaft eine notwendige, geeignete und verhältnismäßige Maßnahme darstellt, um ein oder mehrere der in Artikel 23 Absatz 1 Buchstaben a bis e der Verordnung (EU) 2016/679 genannten allgemeinen öffentlichen Interessen zu wahren oder Überwachungs-, Kontroll- oder Regulierungsaufgaben, die mit der Ausübung öffentlicher Gewalt verbunden sind, wahrzunehmen.

(2) Die Betreiber elektronischer Kommunikationsdienste richten auf der Grundlage einer nach Absatz 1 erlassenen Gesetzgebungsmaßnahme interne Verfahren zur Beantwortung von Anfragen auf Zugang zu elektronischen Kommunikationsdaten von Endnutzern ein. Sie stellen der zuständigen Aufsichtsbehörde auf Anfrage Informationen über diese Verfahren, die Zahl der eingegangenen Anfragen, die vorgebrachten rechtlichen Begründungen und ihre Antworten zur Verfügung.

KAPITEL III
RECHTE NATÜRLICHER UND JURISTISCHER PERSONEN IN BEZUG AUF DIE KONTROLLE ÜBER IHRE ELEKTRONISCHE KOMMUNIKATION

Artikel 12
Anzeige der Rufnummer des Anrufers und des Angerufenen und deren Unterdrückung

(1) Wird die Anzeige der Rufnummer des Anrufers und des Angerufenen im Einklang mit Artikel [107] der [Richtlinie über den europäischen Kodex für die elektronische

Kommunikation] angeboten, stellen die Betreiber öffentlich zugänglicher nummerngebundener interpersoneller Kommunikationsdienste Folgendes bereit:

a) für den anrufenden Endnutzer die Möglichkeit, die Anzeige seiner Rufnummer für einen einzelnen Anruf, für eine bestimmte Verbindung oder dauerhaft zu verhindern;

b) für den angerufenen Endnutzer die Möglichkeit, die Rufnummernanzeige für eingehende Anrufe zu verhindern;

c) für den angerufenen Endnutzer die Möglichkeit, eingehende Anrufe, bei denen die Rufnummernanzeige durch den anrufenden Endnutzer verhindert wurde, abzuweisen;

d) für den angerufenen Endnutzer die Möglichkeit, die Anzeige seiner Rufnummer beim anrufenden Endnutzer zu verhindern.

(2) Die in Absatz 1 Buchstaben a, b, c und d genannten Möglichkeiten werden Endnutzern auf einfache Weise und kostenlos bereitgestellt.

(3) Absatz 1 Buchstabe a gilt auch für aus der Union abgehende Anrufe in Drittländer. Absatz 1 Buchstaben b, c und d gelten auch für aus Drittländern eingehende Anrufe.

(4) Wird die Anzeige der Rufnummer des Anrufers oder des Angerufenen angeboten, geben die Betreiber öffentlich zugänglicher nummerngebundener interpersoneller Kommunikationsdienste der Öffentlichkeit Informationen über die in Absatz 1 Buchstaben a, b, c und d genannten Möglichkeiten.

Artikel 13

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

(1) Ungeachtet dessen, ob der anrufende Endnutzer die Anzeige seiner Rufnummer verhindert hat, übergehen die Betreiber öffentlich zugänglicher nummerngebundener interpersoneller Kommunikationsdienste bei Anrufen bei Notdiensten die Unterdrückung der Rufnummernanzeige und eine verweigerte oder fehlende Einwilligung eines Endnutzers in die Verarbeitung von Metadaten anschlussbezogen für Einrichtungen, die Notrufe bearbeiten, einschließlich der Notrufabfragestellen, zum Zwecke der Beantwortung dieser Anrufe.

(2) Die Mitgliedstaaten legen spezifischere Bestimmungen in Bezug auf die Einrichtung von Verfahren und die Umstände fest, unter denen Betreiber öffentlich zugänglicher nummerngebundener interpersoneller Kommunikationsdienste die Unterdrückung der Anzeige der Rufnummer des Anrufers vorrübergehend aufheben sollen, wenn Endnutzer beantragen, dass böswillige oder belästigende Anrufe zurückverfolgt werden.

Artikel 14
Sperrung eingehender Anrufe

Die Betreiber öffentlich zugänglicher nummerngebundener interpersoneller Kommunikationsdienste treffen Maßnahmen, die dem Stand der Technik entsprechen, um den Erhalt unerwünschter Anrufe durch Endnutzer zu beschränken, und stellen den angerufenen Endnutzern außerdem folgende Möglichkeiten kostenlos zur Verfügung:

a) Sperrung eingehender Anrufe von bestimmten Rufnummern oder von anonymen Quellen;

b) Abstellung einer von einem Dritten veranlassten automatischen Anrufweiterschaltung zur Endeinrichtung des Endnutzers.

Artikel 15
Öffentlich zugängliche Verzeichnisse

(1) Die Betreiber öffentlich zugänglicher Verzeichnisse holen die Einwilligung der Endnutzer, die natürliche Personen sind, in die Aufnahme ihrer personenbezogenen Daten in das Verzeichnis und folglich die Einwilligung dieser Endnutzer in die Aufnahme von Daten nach Kategorien personenbezogener Daten ein, soweit diese Daten für den vom Anbieter des Verzeichnisses angegebenen Zweck relevant sind. Die Betreiber geben Endnutzern, die natürliche Personen sind, die Möglichkeit, die Daten zu überprüfen, zu berichtigen und zu löschen.

(2) Die Betreiber öffentlich zugänglicher Verzeichnisse informieren Endnutzer, die natürliche Personen sind und deren personenbezogene Daten in das Verzeichnis aufgenommen worden sind, über die verfügbaren Suchfunktionen des Verzeichnisses und holen die Einwilligung der Endnutzer ein, bevor sie diese Suchfunktionen in Bezug auf deren Daten aktivieren.

(3) Die Betreiber öffentlich zugänglicher Verzeichnisse räumen Endnutzern, die juristische Personen sind, die Möglichkeit ein, der Aufnahme von auf sie bezogenen Daten in das Verzeichnis zu widersprechen. Die Betreiber geben solchen Endnutzern, die juristische Personen sind, die Möglichkeit, die Daten zu überprüfen, zu berichtigen und zu löschen.

(4) Die Möglichkeit der Endnutzer, nicht in ein öffentlich zugängliches Verzeichnis aufgenommen zu werden und alle Daten, die sich auf sie beziehen, zu überprüfen, zu berichtigen und zu löschen, wird kostenlos zur Verfügung gestellt.

Artikel 16
Unerbetene Kommunikation

(1) Natürliche oder juristische Personen können Direktwerbung über elektronische Kommunikationsdienste an Endnutzer richten, die natürliche Personen sind und hierzu ihre Einwilligung gegeben haben.

(2) Hat eine natürliche oder juristische Person von ihren Kunden im Zusammenhang mit dem Verkauf eines Produkts oder einer Dienstleistung im Einklang mit der

Verordnung (EU) 2016/679 deren elektronische Kontaktangaben für E-Mail erhalten, darf sie diese zur Direktwerbung für eigene ähnliche Produkte oder Dienstleistungen nur dann verwenden, wenn die Kunden klar und deutlich die Möglichkeit haben, einer solchen Nutzung kostenlos und auf einfache Weise zu widersprechen. Das Widerspruchsrecht wird bei Erlangung der Angaben und bei jedem Versand einer Nachricht eingeräumt.

(3) Unbeschadet der Absätze 1 und 2 müssen natürliche oder juristische Personen, die Direktwerbeanrufe mittels elektronischer Kommunikationsdienste tätigen,

a) eine Rufnummer angeben, unter der sie erreichbar sind, oder

b) einen besonderen Kode/eine Vorwahl angeben, der/die kenntlich macht, dass es sich um einen Werbeanruf handelt.

(4) Ungeachtet des Absatzes 1 können Mitgliedstaaten durch Rechtsvorschriften vorsehen, dass die Tätigung persönlicher Direktwerbeanrufe an Endnutzer, die natürliche Personen sind, nur bei Endnutzern erlaubt ist, die natürliche Personen sind und dem Erhalt solcher Kommunikation nicht widersprochen haben.

(5) Die Mitgliedstaaten stellen im Rahmen des Unionsrechts und des geltenden nationalen Rechts sicher, dass die berechtigten Interessen von Endnutzern, die juristische Personen sind, in Bezug auf unerbetene Kommunikation, die in der in Absatz 1 genannten Weise übermittelt wird, ausreichend geschützt werden.

(6) Natürliche oder juristische Personen, die Direktwerbung mittels elektronischer Kommunikationsdienste übermitteln, informieren die Endnutzer über den Werbecharakter der Nachricht und die Identität der juristischen oder natürlichen Person, in deren Namen die Nachricht übermittelt wird, und stellen die nötigen Informationen bereit, damit die Empfänger in einfacher Weise ihr Recht ausüben können, die Einwilligung in den weiteren Empfang von Werbenachrichten zu widerrufen.

(7) Der Kommission wird die Befugnis übertragen, nach Artikel 26 Absatz 2 Durchführungsmaßnahmen zu erlassen, in denen der Kode/die Vorwahl zur Kennzeichnung von Werbeanrufen nach Absatz 3 Buchstabe b festgelegt wird.

Artikel 17
Information über erkannte Sicherheitsrisiken

Besteht ein besonderes Risiko, dass die Sicherheit von Netzen und elektronischen Kommunikationsdiensten beeinträchtigt werden könnte, informiert der Betreiber eines elektronischen Kommunikationsdienstes die Endnutzer über dieses Risiko und – wenn das Risiko außerhalb des Anwendungsbereichs der vom Diensteanbieter zu treffenden Maßnahmen liegt – über mögliche Abhilfen, einschließlich voraussichtlich entstehender Kosten.

KAPITEL IV
UNABHÄNGIGE AUFSICHTSBEHÖRDEN UND DURCHSETZUNG

Artikel 18
Unabhängige Aufsichtsbehörden

(1) Die für die Überwachung der Anwendung der Verordnung (EU) 2016/679 zuständigen unabhängigen Aufsichtsbehörden sind auch für die Überwachung der Anwendung der vorliegenden Verordnung zuständig. Die Kapitel VI und VII der Verordnung (EU) 2016/679 finden sinngemäß Anwendung. Die Aufgaben und Befugnisse der Aufsichtsbehörden werden in Bezug auf die Endnutzer wahrgenommen.

(2) Die in Absatz 1 genannten Aufsichtsbehörden arbeiten mit den nach der [Richtlinie über den europäischen Kodex für die elektronische Kommunikation] geschaffenen nationalen Regulierungsbehörden zusammen, wenn dies zweckmäßig ist.

Artikel 19
Europäischer Datenschutzausschuss

Der durch Artikel 68 der Verordnung (EU) 2016/679 eingesetzte Europäische Datenschutzausschuss ist für die Gewährleistung der einheitlichen Anwendung dieser Verordnung zuständig. Dazu nimmt der Europäische Datenschutzausschuss die in Artikel 70 der Verordnung (EU) 2016/679 festgelegten Aufgaben wahr. Außerdem hat der Ausschuss folgende Aufgaben:

a) Beratung der Kommission bezüglich etwaiger Vorschläge zur Änderung dieser Verordnung;

b) Prüfung – von sich aus, auf Antrag eines seiner Mitglieder oder auf Ersuchen der Kommission – von die Anwendung dieser Verordnung betreffenden Fragen und Bereitstellung von Leitlinien, Empfehlungen und bewährten Verfahren zwecks Sicherstellung einer einheitlichen Anwendung dieser Verordnung.

Artikel 20
Zusammenarbeit und Kohärenzverfahren

Jede Aufsichtsbehörde leistet einen Beitrag zur einheitlichen Anwendung dieser Verordnung in der gesamten Union. Zu diesem Zweck arbeiten die Aufsichtsbehörden untereinander sowie mit der Kommission nach Kapitel VII der Verordnung (EU) 2016/679 in den unter diese Verordnung fallenden Angelegenheiten zusammen.

KAPITEL V
RECHTSBEHELFE, HAFTUNG UND SANKTIONEN

Artikel 21
Rechtsbehelfe

(1) Jeder Endnutzer elektronischer Kommunikationsdienste hat unbeschadet anderweitiger verwaltungsrechtlicher oder gerichtlicher Rechtsbehelfe dieselben Rechte, die in den Artikeln 77, 78 und 79 der Verordnung (EU) 2016/679 vorgesehen sind.

(2) Jede natürliche oder juristische Person, die kein Endnutzer ist, die durch Verstöße gegen die vorliegende Verordnung beeinträchtigt wird und ein berechtigtes Interesse an der Einstellung oder dem Verbot solcher Verstöße hat, einschließlich der Betreiber elektronischer Kommunikationsdienste, die ihre berechtigten Geschäftsinteressen schützen wollen, hat das Recht, gegen solche Verstöße gerichtlich vorzugehen.

Artikel 22
Haftung und Recht auf Schadenersatz

Jeder Endnutzer elektronischer Kommunikationsdienste, dem wegen eines Verstoßes gegen diese Verordnung ein materieller oder immaterieller Schaden entstanden ist, hat Anspruch auf Schadenersatz gegen den Rechtsverletzer, es sei denn der Rechtsverletzer weist im Einklang mit Artikel 82 der Verordnung (EU) 2016/679 nach, dass er in keinerlei Hinsicht für den Umstand, durch den der Schaden eingetreten ist, verantwortlich ist.

Artikel 23
Allgemeine Voraussetzungen für die Verhängung von Geldbußen

(1) Für die Zwecke dieses Artikels findet Kapitel VII der Verordnung (EU) 2016/679 auf Verstöße gegen die vorliegende Verordnung Anwendung.

(2) Bei Verstößen gegen die folgenden Bestimmungen der vorliegenden Verordnung werden im Einklang mit Absatz 1 Geldbußen von bis zu 10 000 000 EUR oder im Fall eines Unternehmens von bis zu 2 % seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs verhängt, je nachdem, welcher der Beträge höher ist:

a) die Verpflichtungen einer juristischen oder natürlichen Person, die elektronische Kommunikationsdaten nach Artikel 8 verarbeitet;

b) die Verpflichtungen des Anbieters der Software, die eine elektronische Kommunikation nach Artikel 10 ermöglicht;

c) die Verpflichtungen des Betreibers öffentlich zugänglicher Verzeichnisse nach Artikel 15;

d) die Verpflichtungen einer juristischen oder natürlichen Person, die elektronische Kommunikationsdienste nach Artikel 16 nutzt.

(3) Bei Verstößen gegen den Grundsatz der Vertraulichkeit der Kommunikation, die erlaubte Verarbeitung elektronischer Kommunikationsdaten und Löschungsfristen nach den Artikeln 5, 6 und 7 werden im Einklang mit Absatz 1 des vorliegenden Artikels Geldbußen von bis zu 20 000 000 EUR oder im Fall eines Unternehmens von bis zu 4 % seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs verhängt, je nachdem, welcher der Beträge höher ist.

(4) Die Mitgliedstaaten legen Vorschriften über Sanktionen für die in den Artikeln 12, 13, 14 und 17 genannten Verstöße fest.

(5) Bei Nichtbefolgung einer Anweisung der Aufsichtsbehörde nach Artikel 18 werden Geldbußen von bis zu 20 000 000 EUR oder im Fall eines Unternehmens von bis zu 4 % seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs verhängt, je nachdem, welcher der Beträge höher ist.

(6) Unbeschadet der Abhilfebefugnisse der Aufsichtsbehörden nach Artikel 18 kann jeder Mitgliedstaat Vorschriften dafür festlegen, ob und in welchem Umfang gegen Behörden und öffentliche Stellen, die in dem betreffenden Mitgliedstaat niedergelassen sind, Geldbußen verhängt werden können.

(7) Die Ausübung der eigenen Befugnisse durch eine Aufsichtsbehörde nach diesem Artikel muss angemessenen Verfahrensgarantien gemäß dem Unionsrecht und dem Recht der Mitgliedstaaten, einschließlich wirksamer gerichtlicher Rechtsbehelfe und ordnungsgemäßer Verfahren, unterliegen.

(8) Sieht die Rechtsordnung eines Mitgliedstaats keine Geldbußen vor, kann dieser Artikel so angewandt werden, dass die Geldbuße von der zuständigen Aufsichtsbehörde in die Wege geleitet und von den zuständigen nationalen Gerichten verhängt wird, wobei sicherzustellen ist, dass diese Rechtsbehelfe wirksam sind und die gleiche Wirkung wie von Aufsichtsbehörden verhängte Geldbußen haben. In jeden Fall müssen die verhängten Geldbußen wirksam, verhältnismäßig und abschreckend sein. Die betreffenden Mitgliedstaaten teilen der Kommission bis zum [xxx] die Rechtsvorschriften, die sie aufgrund dieses Absatzes erlassen, sowie unverzüglich alle späteren Änderungsgesetze oder Änderungen dieser Vorschriften mit.

Artikel 24
Sanktionen

(1) Die Mitgliedstaaten legen die Vorschriften über andere Sanktionen für Verstöße gegen diese Verordnung – insbesondere für Verstöße, die keiner Geldbuße nach Artikel 23 unterliegen – fest und treffen alle zu deren Anwendung erforderlichen Maßnahmen. Diese Sanktionen müssen wirksam, verhältnismäßig und abschreckend sein.

(2) Jeder Mitgliedstaat teilt der Kommission spätestens 18 Monate nach dem in Artikel 29 Absatz 2 festgelegten Termin die Rechtsvorschriften, die er nach Absatz 1 erlässt, sowie unverzüglich alle späteren Änderungen dieser Vorschriften mit.

KAPITEL VI
DELEGIERTE RECHTSAKTE UND DURCHFÜHRUNGSRECHTSAKTE

Artikel 25
Ausübung der Befugnisübertragung

(1) Die Befugnis zum Erlass delegierter Rechtsakte wird der Kommission unter den in diesem Artikel festgelegten Bedingungen übertragen.

(2) Die Befugnis zum Erlass delegierter Rechtsakte nach Artikel 8 Absatz 4 wird der Kommission auf unbestimmte Zeit ab dem [Tag des Inkrafttretens dieser Verordnung] übertragen.

(3) Die Befugnisübertragung nach Artikel 8 Absatz 4 kann vom Europäischen Parlament oder vom Rat jederzeit widerrufen werden. Der Beschluss über den Widerruf beendet die Übertragung der in diesem Beschluss angegebenen Befugnis. Er wird am Tag nach seiner Veröffentlichung im *Amtsblatt der Europäischen Union* oder zu einem im Beschluss über den Widerruf angegebenen späteren Zeitpunkt wirksam. Die Gültigkeit von delegierten Rechtsakten, die bereits in Kraft sind, wird von dem Beschluss über den Widerruf nicht berührt.

(4) Vor dem Erlass eines delegierten Rechtsakts konsultiert die Kommission die von den einzelnen Mitgliedstaaten benannten Sachverständigen im Einklang mit den in der Interinstitutionellen Vereinbarung über bessere Rechtsetzung vom 13. April 2016 niedergelegten Grundsätzen.

(5) Sobald die Kommission einen delegierten Rechtsakt erlässt, übermittelt sie ihn gleichzeitig dem Europäischen Parlament und dem Rat.

(6) Ein delegierter Rechtsakt, der nach Artikel 8 Absatz 4 erlassen wurde, tritt nur in Kraft, wenn weder das Europäische Parlament noch der Rat innerhalb einer Frist von zwei Monaten nach Übermittlung dieses Rechtsakts an das Europäische Parlament und den Rat Einwände erhoben haben oder wenn vor Ablauf dieser Frist das Europäische Parlament und der Rat beide der Kommission mitgeteilt haben, dass sie keine Einwände erheben werden. Auf Initiative des Europäischen Parlaments oder des Rates wird diese Frist um zwei Monate verlängert.

Artikel 26
Ausschuss

(1) Die Kommission wird von dem durch Artikel 110 der [Richtlinie über den europäischen Kodex für die elektronische Kommunikation] eingesetzten

Kommunikationsausschuss unterstützt. Dieser Ausschuss ist ein Ausschuss im Sinne der Verordnung (EU) Nr. 182/2011[12].

(2) Wird auf diesen Absatz Bezug genommen, so gilt Artikel 5 der Verordnung (EU) Nr. 182/2011.

KAPITEL VII
SCHLUSSBESTIMMUNGEN

Artikel 27
Aufhebung

(1) Die Richtlinie 2002/58/EG wird mit Wirkung vom 25. Mai 2018 aufgehoben.

(2) Bezugnahmen auf die aufgehobene Richtlinie gelten als Bezugnahmen auf die vorliegende Verordnung.

Artikel 28
Überwachung und Bewertung

Die Kommission stellt spätestens zum 1. Januar 2018 ein detailliertes Programm für die Überwachung der Wirksamkeit dieser Verordnung auf.

Spätestens drei Jahre nach dem Geltungsbeginn dieser Verordnung und danach alle drei Jahre führt die Kommission eine Bewertung dieser Verordnung durch und legt die wichtigsten Erkenntnisse daraus dem Europäischen Parlament, dem Rat und dem Europäischen Wirtschafts- und Sozialausschuss vor. In Anbetracht rechtlicher, technischer oder wirtschaftlicher Entwicklungen dient die Bewertung gegebenenfalls als Grundlage für einen Vorschlag zur Änderung oder Aufhebung dieser Verordnung.

Artikel 29
Inkrafttreten und Anwendung

(1) Diese Verordnung tritt am zwanzigsten Tag nach ihrer Veröffentlichung im *Amtsblatt der Europäischen Union* in Kraft.

(2) Sie gilt ab dem 25. Mai 2018.

Diese Verordnung ist in allen ihren Teilen verbindlich und gilt unmittelbar in jedem Mitgliedstaat.

[12] Verordnung (EU) Nr. 182/2011 des Europäischen Parlaments und des Rates vom 16. Februar 2011 zur Festlegung der allgemeinen Regeln und Grundsätze, nach denen die Mitgliedstaaten die Wahrnehmung der Durchführungsbefugnisse durch die Kommission kontrollieren (ABl. L 55 vom 28.2.2011, S. 13).

Geschehen zu Brüssel am

Im Namen des Europäischen Parlaments	*Im Namen des Rates*
Der Präsident	*Der Präsident*