



## 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)



# Synopse der ePrivacy-VO

folgender Fassungen:

- Vorschlag der **Europäischen Kommission** vom 10. Januar 2017, (COM(2017) final 2017/0003 (COD))
- Entwurf einer legislativen Entschließung des **Europäischen Parlaments** vom 23.10.2017, A8-0324/2017
- **Rats der Europäischen Union** vom .... (noch offen)

**Redaktionelle Bearbeitung:**

Bayerisches Landesamt für Datenschutzaufsicht (BayLDA)

Promenade 27, 91522 Ansbach

E-Mail: [poststelle@lda.bayern.de](mailto:poststelle@lda.bayern.de)

Web: [www.lda.bayern.de](http://www.lda.bayern.de)

## Inhalt

Erwägungsgründe.....	4
Kapitel I ALLGEMEINE BESTIMMUNGEN .....	39
Kapitel II SCHUTZ DER ELEKTRONISCHEN KOMMUNIKATION NATÜRLICHER UND JURISTISCHER PERSONEN UND DER IN IHREN ENDEINRICHTUNGEN GESPEICHERTEN INFORMATIONEN .....	49
Kapitel III RECHTE NATÜRLICHER UND JURISTISCHER PERSONEN IN BEZUG AUF DIE KONTROLLE ÜBER IHRE ELEKTRONISCHE KOMMUNIKATION.....	67
Kapitel IV UNABHÄNGIGE AUFSICHTSBEHÖRDEN UND DURCHSETZUNG.....	75
Kapitel V RECHTSBEHELFE, HAFTUNG UND SANKTIONEN.....	78
Kapitel VI DELEGIERTE RECHTSAKTE UND DURCHFÜHRUNGSRECHTSAKTE.....	84
Kapitel VII SCHLUSSBESTIMMUNGEN .....	86

EU-Kommission	EU-Parlament	EU-Rat
<p><b>VERORDNUNG DES EUROPÄISCHEN PARLAMENTS UND DES RATES</b></p> <p>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)</p> <p>(Text von Bedeutung für den EWR)</p> <p>DAS EUROPÄISCHE PARLAMENT UND DER RAT DER EUROPÄISCHEN UNION –</p> <p>gestützt auf den Vertrag über die Arbeitsweise der Europäischen Union, insbesondere auf die Artikel 16 und 114,</p> <p>auf Vorschlag der Europäischen Kommission,</p> <p>nach Zuleitung des Entwurfs des Gesetzgebungsakts an die nationalen Parlamente,</p> <p>nach Stellungnahme des Europäischen Wirtschafts- und Sozialausschusses<sup>1</sup>,</p> <p>nach Stellungnahme des Ausschusses der Regionen<sup>2</sup>,</p> <p>nach Stellungnahme des Europäischen Datenschutzbeauftragten<sup>3</sup>,</p> <p>gemäß dem ordentlichen Gesetzgebungsverfahren,</p>		
<p><b>Erwägungsgründe</b></p>		
<p>(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 <b>an der Kommunikation Beteiligten</b> offengelegt werden. Der Grundsatz der Vertraulichkeit sollte für gegenwärtige und künftige Kommunikationsmittel gelten, darunter Anrufe, Internetzugang, Sofortnachrichtenwendungen, E-Mail, Internettelefonie und Übermittlung <b>persönlicher</b> Nachrichten über soziale Medien.</p>	<p>(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 <b>miteinander kommunizierenden Parteien</b> offengelegt werden. Der Grundsatz der Vertraulichkeit sollte für gegenwärtige und künftige Kommunikationsmittel gelten, darunter Anrufe, Internetzugang, Sofortnachrichtenwendungen, E-Mail, Internettelefonie und Übermittlung <b>interpersoneller</b> Nachrichten über soziale Medien. <b>Er sollte auch gelten, wenn die Vertraulichkeit der elektronischen Kommunikation und die Privatsphäre in der physischen Umwelt in engem Zusammenhang stehen, d. h. wenn mit Endgeräten für die elektronische Kommunikation auch die physische Umwelt abgehört werden kann oder andere Eingangskanäle, etwa Bluetooth-Signale oder Bewegungssensoren, genutzt werden können.</b></p>	

EU-Kommission	EU-Parlament	EU-Rat
<p>2) <b>Inhalte</b> der elektronischen Kommunikation können hochsensible Informationen über die daran beteiligten natürlichen Personen <b>offenlegen</b>, 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.</p>	<p>(2) <b>In Inhalten</b> der elektronischen Kommunikation können hochsensible Informationen über die daran beteiligten natürlichen Personen <b>offengelegt werden</b>, 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. <b>Metadaten sind zudem – da sie bereits in ein strukturiertes und standardisiertes Format überführt wurden – viel einfacher zu verarbeiten und zu analysieren als Inhalte. Der Schutz der Vertraulichkeit der Kommunikation ist eine Grundvoraussetzung für die Wahrung anderer damit verbundener Grundrechte und -freiheiten, etwa den Schutz der Gedanken-, Gewissens- und Religionsfreiheit, der Versammlungsfreiheit sowie des Rechts auf freie Meinungsäußerung und Informationsfreiheit.</b></p>	
<p>(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 auch für Endnutzer gilt, die juristische Personen sind. Dies be-</p>	<p>(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 auch für Endnutzer gilt, die juristische Personen sind. Dies be-</p>	

EU-Kommission	EU-Parlament	EU-Rat
<p>zieht 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.</p>	<p>zieht 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.</p>	
<p>(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. <b>Elektronische</b> Kommunikationsdaten <b>können auch</b> personenbezogene Daten im Sinne der Verordnung (EU) 2016/679 <b>enthalten</b>.</p>	<p>(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. <b>Bei elektronischen</b> Kommunikationsdaten <b>handelt es sich im Allgemeinen um</b> personenbezogene Daten im Sinne der Verordnung (EU) 2016/679.</p>	
<p>(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. <b>Eine</b> Verarbeitung elektronischer Kommunikationsdaten <b>durch Betreiber elektronischer Kommunikationsdienste</b> sollte nur im Einklang mit der vorliegenden Verordnung <b>erlaubt</b> sein.</p>	<p>(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. <b>Vielmehr sollen durch diese Verordnung zusätzliche und ergänzende Sicherheitsvorkehrungen getroffen werden, da die Vertraulichkeit der Kommunikation über das bisherige Maß hinaus geschützt werden muss.</b> Die Verarbeitung elektronischer Kommunikationsdaten sollte nur im Einklang mit der vorliegenden Verordnung <b>zulässig</b> sein.</p>	

EU-Kommission	EU-Parlament	EU-Rat
<p>(6) Die Grundsätze und wichtigsten Bestimmungen der Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates<sup>22</sup> 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 <b>andere solche</b> Entwicklung ist das Aufkommen neuer Techniken für die Verfolgung des Online-Verhaltens der <b>Endnutzer, die von der Richtlinie 2002/58/EG nicht erfasst werden</b>. Die Richtlinie 2002/58/EG sollte daher aufgehoben und durch diese Verordnung ersetzt werden.</p>	<p>(6) Die Grundsätze und wichtigsten Bestimmungen der Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates<sup>22</sup> 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 <b>weitere derartige</b> Entwicklung ist das Aufkommen neuer Techniken für die Verfolgung des Online-Verhaltens der <b>Nutzer</b>. Die Richtlinie 2002/58/EG sollte daher aufgehoben und durch diese Verordnung ersetzt werden.</p>	
<p>_____</p> <p><sup>22</sup> 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).</p>	<p>_____</p> <p><sup>22</sup> 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).</p>	
<p>(7) <b>Die Mitgliedstaaten sollten die Möglichkeit haben</b>, 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, <b>um eine wirksame Anwendung und Auslegung dieser Vorschriften sicherzustellen. Deshalb sollte der Ermessensspielraum, den die Mitgliedstaaten in dieser Hinsicht haben, so wahrgenommen werden, dass</b> ein ausgewogenes Verhältnis zwischen dem Schutz des Privatlebens und personenbezogener Daten und dem freien Verkehr elektronischer Kommu-</p>	<p>(7) <b>Der Europäische Datenschutzausschuss sollte, soweit erforderlich</b>, innerhalb des von dieser Verordnung vorgegebenen Rahmens <b>Leitlinien und Stellungnahmen dazu veröffentlichen, ob</b> nationale Bestimmungen beizubehalten oder einzuführen <b>sind</b>, mit denen die Anwendung der Vorschriften dieser Verordnung genauer und klarer festgelegt wird, <b>damit diese Vorschriften wirksam angewandt und ausgelegt werden. Zusammenarbeit und Kohärenz zwischen den Mitgliedstaaten, insbesondere zwischen den nationalen Datenschutzbehörden, sind von entscheidender Bedeutung, damit</b> ein ausgewogenes</p>	

EU-Kommission	EU-Parlament	EU-Rat
<p>nikationsdaten <b>gewährleistet bleibt</b>.</p>	<p>Verhältnis zwischen dem Schutz des Privatlebens und personenbezogener Daten und dem freien Verkehr elektronischer Kommunikationsdaten <b>in der Union gewahrt wird</b>.</p>	
<p>(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 <b>an Endnutzer gerichtete</b> gewerbliche Direktwerbung betreiben oder Informationen sammeln, die <b>in</b> Endeinrichtungen der <b>Endnutzer</b> gespeichert sind <b>oder</b> sich <b>auf diese</b> beziehen.</p>	<p>(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 gewerbliche Direktwerbung betreiben oder Informationen sammeln, die <b>an</b> Endeinrichtungen der <b>Nutzer übertragen werden, dort</b> gespeichert sind, sich <b>darauf</b> beziehen <b>oder davon verarbeitet werden</b>.</p>	
<p>(9) Diese Verordnung sollte für elektronische Kommunikationsdaten gelten, die in Verbindung mit <b>der Bereitstellung</b> 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.</p>	<p>(9) Diese Verordnung sollte für elektronische Kommunikationsdaten gelten, die in Verbindung mit <b>dem Anbieten</b> und <b>der</b> 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. <b>Dies sollte ungeachtet dessen gelten, ob die elektronische Kommunikation mit einer Zahlung verbunden ist. Für die Zwecke dieser Verordnung sollte ein nicht in der Union niedergelassener Betreiber eines elektronischen Kommunikationsdienstes schriftlich einen Vertreter in der Union benennen.</b></p>	
<p>(10) Funkanlagen und zugehörige Software, die auf dem Binnenmarkt der Union in Verkehr gebracht werden,</p>	<p>(10) Funkanlagen und zugehörige Software, die auf dem Binnenmarkt der Union in Verkehr gebracht werden,</p>	



EU-Kommission	EU-Parlament	EU-Rat
<p>müssen den Anforderungen der Richtlinie 2014/53/EU des Europäischen Parlaments und des Rates<sup>6</sup> 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.</p>	<p>müssen den Anforderungen der Richtlinie 2014/53/EU des Europäischen Parlaments und des Rates<sup>6</sup> 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.</p>	
<p>_____</p> <p><sup>6</sup> 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).</p>	<p>_____</p> <p><sup>6</sup> Richtlinie 2014/53/EU des Europäischen Parlaments und des Rates vom 16. April 2014 über die Harmonisierung der</p>	
<p>(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, <b>Nachrichtenübermittlung (Messaging)</b> und webgestützte E-Mail-Dienste. <b>Zur Gewährleistung eines wirksamen und einheitlichen Schutzes</b> der Endnutzer bei der Benutzung funktional gleichwertiger Dienste <b>wird in dieser Verordnung die in der [Richtlinie des Europäischen Parlaments und des Rates über den europäischen Kodex für die elektronische Kommunikation<sup>24</sup>] festgelegte Begriffsbestimmung für elektronische Kommunikationsdienste verwendet.</b> Diese <b>Begriffsbestimmung erfasst</b> 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,</p>	<p>(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, <b>Nachrichtenübermittlungsdienste</b> und webgestützte E-Mail-Dienste, <b>die auch „Over-the-top-Dienste“ (OTT-Dienste) genannt werden. Mit dieser Verordnung soll ein wirksamer und einheitlicher Schutz</b> der Endnutzer bei der Benutzung funktional gleichwertiger Dienste <b>gewährleistet werden, damit – unabhängig vom gewählten technischen Mittel – die Vertraulichkeit ihrer Kommunikation gewahrt wird.</b> Diese <b>Verordnung betrifft</b> 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, <b>Nachrichtenübermittlungsdienste</b> und</p>	

EU-Kommission	EU-Parlament	EU-Rat
<p><b>Nachrichtenübermittlung</b> und webgestützte E-Mail-Dienste. <b>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.</b></p>	<p>webgestützte E-Mail-Dienste.</p>	
<p>_____</p> <p><sup>24</sup> Vorschlag der Kommission für eine Richtlinie des Europäischen Parlaments und des Rates über den europäischen Kodex für die elektronische Kommunikation (Neufassung), COM(2016)0590 – 2016/0288 (COD).</p>		
<p><b>(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 Übermittlung von Maschine-Maschine-Kommunikation gelten. Besondere Sicherheitsvorrichtungen könnten auch im Rahmen sektorspezifischer Rechtsvorschriften wie beispielsweise der Richtlinie 2014/53/EU getroffen werden.</b></p>	<p><b>entfällt</b></p>	

EU-Kommission	EU-Parlament	EU-Rat
<p>(13) Die Entwicklung schneller und effizienter Drahtlostechnik hat dazu beigetragen, dass der öffentliche Internetzugang über drahtlose Netze zunehmend in öffentlichen und halbprivaten Räumen für <b>jedermann</b> zur Verfügung steht, beispielsweise an <b>so genannten „Hotspots“</b>, die sich an verschiedenen Orten in einer Stadt wie in Kaufhäusern, Einkaufszentren <b>und</b> Krankenhäusern befinden können. Insofern solche Kommunikationsnetze <b>für eine unbestimmte Gruppe von Endnutzern</b> bereitgestellt werden, sollte die Vertraulichkeit der über solche Netze übermittelten Kommunikation geschützt werden. <b>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.</b> Deshalb sollte diese Verordnung für elektronische Kommunikationsdaten gelten, die mithilfe elektronischer Kommunikationsdienste und öffentlicher Kommunikationsnetze übertragen werden. Diese Verordnung <b>sollte dagegen keine</b> Anwendung auf geschlossene Gruppen von Endnutzern (z. B. <b>Unternehmensnetze</b>) <b>finden</b>, bei denen der Zugang auf die Angehörigen <b>des Unternehmens</b> beschränkt ist.</p>	<p>(13) Die Entwicklung schneller und effizienter Drahtlostechnik hat dazu beigetragen, dass der öffentliche Internetzugang über drahtlose Netze zunehmend in öffentlichen und halbprivaten Räumen für <b>alle</b> zur Verfügung steht, beispielsweise an <b>drahtlosen Internetzugangspunkten</b>, die sich an verschiedenen Orten in einer Stadt wie in Kaufhäusern, Einkaufszentren, Krankenhäusern, <b>Flughäfen, Hotels und Restaurants</b> befinden können. <b>Diese Zugangspunkte erfordern möglicherweise eine Anmeldung oder die Eingabe eines Kennworts und werden unter Umständen auch von der öffentlichen Verwaltung, z. B. von Einrichtungen und sonstigen Stellen der Union, bereitgestellt.</b> Insofern <b>den Nutzern</b> solche Kommunikationsnetze bereitgestellt werden, sollte die Vertraulichkeit der über solche Netze übermittelten Kommunikation geschützt werden. Deshalb sollte diese Verordnung für elektronische Kommunikationsdaten gelten, die mithilfe elektronischer Kommunikationsdienste und öffentlicher Kommunikationsnetze übertragen werden. <b>Diese Verordnung sollte auch auf geschlossene Profile und Gruppen in sozialen Medien, die die Nutzer als eingeschränkt zugänglich oder privat festgelegt haben, Anwendung finden. Hingegen sollte</b> diese Verordnung auf geschlossene Gruppen von Endnutzern (z. B. <b>das Intranet von Unternehmen</b>), bei denen der Zugang auf die Angehörigen <b>einer Organisation</b> beschränkt ist, <b>keine Anwendung finden. Wird der Zugang zu einem Dienst als Ganzes für eine unbestimmte Gruppe von Endnutzern bereitgestellt und für den Zugang lediglich die Eingabe eines Kennworts verlangt, so sollte für diesen Vorgang nicht gelten, dass damit der Zugang zu einer geschlossenen Gruppe von Endnutzern erlangt wird.</b></p>	
<p>(14) Der Ausdruck „elektronische Kommunikationsdaten“ sollte hinreichend breit und technologieunabhängig definiert werden, damit er alle Informationen bezüglich der übermittelten oder ausgetauschten Inhalte (elektronische</p>	<p>(14) Der Ausdruck „elektronische Kommunikationsdaten“ sollte hinreichend breit und technologieunabhängig definiert werden, damit er alle Informationen bezüglich der übermittelten oder ausgetauschten Inhalte (elektronische</p>	

EU-Kommission	EU-Parlament	EU-Rat
<p>Kommunikationsinhalte) und die Informationen bezüglich <b>der Endnutzer</b> 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, <b>des geografischen Standorts</b> sowie <b>von</b> Datum, Uhrzeit, Dauer und Art der Kommunikation. Unabhängig davon, ob solche Signale über Kabel, Funk, optische oder elektromagnetische Medien, <b>einschließlich</b> 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.</p>	<p>Kommunikationsinhalte) und die Informationen bezüglich <b>eines Nutzers</b> 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, <b>der geografische Standort</b> sowie Datum, Uhrzeit, Dauer und Art der Kommunikation. <b>Ferner sollten dazu Daten zählen, die erforderlich sind, um die Endeinrichtungen von Nutzern zu identifizieren, und Daten, die von Endeinrichtungen bei der Suche nach Zugangspunkten oder anderen Einrichtungen ausgesendet werden.</b> Unabhängig davon, ob solche Signale über Kabel, Funk, optische oder elektromagnetische Medien, <b>darunter</b> 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. <b>Die Ausnahme von Diensten, die „Inhalte, die mittels elektronischer Kommunikationsdienste übermittelt [...] werden“, anbieten, von der Begriffsbestimmung „elektronischer Kommunikationsdienst“ in Artikel 4 dieser Verordnung bedeutet nicht, dass Anbieter, die sowohl elektronische Kommunikationsdienste als auch Inheldienste anbieten, nicht in den Geltungsbereich dieser Verordnung fallen, die für Anbieter von elektronischen Kommunikationsdiensten gilt.</b></p>	
<p><b>nicht vorhanden</b></p>	<p><b>(14a) Moderne elektronische Kommunikationsdienste, auch das Inter-</b></p>	

EU-Kommission	EU-Parlament	EU-Rat
	<p><b>net und die darauf aufbauenden OTT-Dienste, funktionieren auf der Grundlage eines Protokollstapels. In jedem Protokoll sind der Inhalt (auch „Nutzdaten“), die Kopfdaten und bisweilen ein Nachspann definiert. In einem Stapel sind alle Protokolle einer höheren Ebene im Inhaltsteil eines Protokolls einer niedrigeren Ebene eingeschlossen. Beispielsweise ist ein TCP-Segment im Inhaltsteil eines IP-Pakets enthalten, dessen Kopfdaten die Quell- und Ziel-IP-Adressen enthalten, zwischen denen das IP-Paket versandt wird. TCP-Segmente können in ihrem Inhaltsteil eine SMTP-Nachricht enthalten, z. B. eine E-Mail. Auf der Ebene des SMTP-Protokolls enthalten die Kopfdaten vor allem die E-Mail-Adressen des Absenders und des Empfängers, während der Inhaltsteil aus der E-Mail selbst besteht. In der Praxis entsprechen die Kopfdaten und der Nachspann einer Protokollmeldung den Metadaten des jeweiligen Protokolls. Das heißt, dass das, was in einer Protokollschicht Metadaten sind, für die unterhalb davon befindlichen Schichten Inhaltsdaten sind. Die in dieser Verordnung festgelegten unterschiedlichen Vorschriften für die Verarbeitung von Inhalts- und Metadaten sollten entsprechend so verstanden werden, dass sie sich auf den jeweiligen elektronischen Kommunikationsdienst und auf die Protokollschicht, auf der dieser Dienst betrieben wird, beziehen. Beispielsweise betrachtet ein Internetdienstanbieter den Betreff, den Absender, den Empfänger und den Text einer E-Mail zusammen als Inhalt der von ihm weitergeleiteten IP-Pakete. Hingegen betrachtet ein E-Mail-Anbieter lediglich den Betreff und den Text der E-Mail als Inhalt, den Absender und den Empfänger der E-Mail aber als Metadaten. Diese Trennung der Protokollschichten ist entscheidend, damit die im Rahmen der Verordnung (EU) 2015/2120 geschützte Neutralität der elektronischen Kommunikationsdienste (Netzneutralität) gewahrt wird.</b></p>	

EU-Kommission	EU-Parlament	EU-Rat
<p>(15) Elektronische <b>Kommunikationsdaten sollten</b> vertraulich behandelt werden. Das bedeutet, dass Eingriffe in die Übermittlung elektronischer <b>Kommunikationsdaten</b>, 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 <b>Kommunikationsdaten</b> sollte während ihrer Übertragung gelten, <b>d. h. bis zum</b> Empfang der Inhalte der elektronischen Kommunikation durch den bestimmungsgemäßen <b>Empfänger</b>. 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, <b>scannen</b> oder speichern. Ein Abfangen liegt auch vor, wenn Dritte ohne Einwilligung des <b>betreffenden Endnutzers</b> 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 <b>Endnutzerprofile</b> 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 <b>Endnutzer</b>.</p>	<p>(15) Elektronische <b>Kommunikation sollte</b> vertraulich behandelt werden. Das bedeutet, dass Eingriffe in die Übermittlung elektronischer <b>Kommunikation</b>, ob unmittelbar durch menschliches Zutun oder mittelbar durch eine automatische Verarbeitung durch Maschinen, ohne Einwilligung aller an der Kommunikation Beteiligten untersagt sein sollten. <b>Ist die Verarbeitung aufgrund einer Ausnahme von den in dieser Verordnung festgelegten Verboten zulässig, so sollte jede sonstige Verarbeitung auf der Grundlage von Artikel 6 der Verordnung (EU) 2016/679 als untersagt gelten, wozu auch die Verarbeitung zu einem anderen Zweck auf der Grundlage von Artikel 6 Absatz 4 der genannten Verordnung zählt. Dadurch sollte jedoch nicht verhindert werden, dass für neue Verarbeitungsvorgänge eine zusätzliche Einwilligung eingeholt wird.</b> Das Verbot des Abfangens von <b>Kommunikation</b> sollte <b>auch</b> während ihrer Übertragung gelten. <b>Bei elektronischer Kommunikation, die nicht in Echtzeit stattfindet, wie E-Mail- oder Nachrichtenübermittlung, beginnt die Übertragung mit dem Abschicken der zuzustellenden Inhalte und endet mit dem</b> Empfang der Inhalte der elektronischen Kommunikation durch den <b>Diensteanbieter des bestimmungsgemäßen Empfängers</b>. 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, <b>durchleuchten</b> oder speichern. Ein Abfangen liegt auch vor, wenn Dritte ohne Einwilligung des <b>jeweiligen Nutzers</b> 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 internatio-</p>	

EU-Kommission	EU-Parlament	EU-Rat
	<p>nenalen Mobilfunk-Teilnehmerkennung), bis hin zu Programmen und Techniken, die beispielsweise die Surfgewohnheiten heimlich beobachten, um daraus <b>Nutzerprofile</b> zu erstellen. Weitere Beispiele für ein Abfangen sind das Erfassen von Nutzdaten oder Inhaltsdaten aus unverschlüsselten drahtlosen Netzen und Routern <b>sowie die Analyse der Datenverkehrsdaten von Nutzern</b>, z. B. von Surfgewohnheiten, ohne Einwilligung der <b>Nutzer</b>.</p>	
<p>(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 <b>über das elektronische Kommunikationsnetz</b> erfolgt. Untersagt werden soll <b>ebenfalls nicht</b> die Verarbeitung elektronischer Kommunikationsdaten <b>zur Gewährleistung der Sicherheit und Kontinuität der elektronischen Kommunikationsdienste, darunter die Prüfung</b> auf Sicherheitsbedrohungen wie Vorhandensein von Schadsoftware oder <b>die Verarbeitung von Metadaten zur Sicherung der</b> Einhaltung der erforderlichen Dienstqualitätsanforderungen wie Latenz, Verzögerungsschwankung (Jitter) usw.</p>	<p>(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 erfolgt. <b>Nicht</b> untersagt werden soll die Verarbeitung elektronischer Kommunikationsdaten <b>durch Behörden, Computer-Notfallteams (Computer Emergency Response Teams – CERT bzw. Computer Security Incident Response Teams – CSIRT), Betreiber elektronischer Kommunikationsnetze und -dienste sowie Anbieter von Sicherheitstechnologien und -diensten gemäß der Verordnung (EU) 2016/679 und, soweit dies unbedingt notwendig und verhältnismäßig ist, die Verarbeitung, mit der einzig und allein die Netz- und Informationssicherheit[, d. h. die Aufrechterhaltung der Verfügbarkeit, Integrität] und die Vertraulichkeit von Informationen sowie die Sicherheit damit zusammenhängender Dienste, die über diese Netze und Informationssysteme angeboten werden bzw. zugänglich sind, gewährleistet werden soll. Dies könnte beispielsweise umfassen, den Zugang Unbefugter zu elektronischen Kommunikationsnetzen und die Verbreitung von Schadcode zu verhindern sowie Angriffe in Form der gezielten Überlastung von Servern („Denial of service“-Angriffe, Dienstverweigerungsangriffe) und Schädigungen von Computersystemen und elektronischen Kommunikationssystemen abzuwehren, auf Sicherheitsbedrohungen wie <b>das</b> Vorhandensein von Schadsoftware oder <b>unverlangten E-Mails („Spam“) oder</b></b></p>	

EU-Kommission	EU-Parlament	EU-Rat
	<p><b>DDoS-Angriffe (Distributed Denial of Service, verteilte –d. h. von vielen Rechnern ausgehende – Dienstverweigerungsangriffe) zu prüfen</b> oder Metadaten <b>zu verarbeiten, um die</b> Einhaltung der erforderlichen Dienstqualitätsanforderungen wie Latenz, Verzögerungsschwankung (Jitter) usw. <b>sicherzustellen. Eine solche Verarbeitung könnte auch von einer anderen Partei vorgenommen werden, die für den Diensteanbieter als Datenverarbeiter im Sinne der Verordnung (EU) 2016/679 fungiert.</b></p>	
<p>(17) Die Verarbeitung elektronischer Kommunikationsdaten kann für Unternehmen, für die Verbraucher und für die gesamte Gesellschaft nützlich sein. <b>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</b> 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. <b>Deshalb sollte diese</b> Verordnung den Betreibern elektronischer Kommunikationsdienste <b>vorschreiben</b>, dass sie die Einwilligung der <b>Endnutzer</b> in die Verarbeitung elektronischer Kommunikationsmetadaten einholen, zu denen auch Daten über den Standort des Gerätes gehören, <b>welche</b> 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. <b>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.</b></p>	<p>(17) Die Verarbeitung elektronischer Kommunikationsdaten kann für Unternehmen, für die Verbraucher und für die gesamte Gesellschaft nützlich sein. Die <b>Nutzer</b> 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. <b>Mit dieser</b> Verordnung <b>sollte</b> den Betreibern elektronischer Kommunikationsdienste <b>vorgeschrieben werden</b>, dass sie die Einwilligung der <b>Nutzer</b> in die Verarbeitung elektronischer Kommunikationsmetadaten einholen, zu denen auch Daten über den Standort des Gerätes gehören, <b>die</b> 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. 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, <b>falls angezeigt</b>, eine Konsultation der Aufsichtsbehörde nach den Artikeln 35 und 36 der Verordnung (EU) 2016/679 durch-</p>	



EU-Kommission	EU-Parlament	EU-Rat
<p><b>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.</b> 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 <b>gegebenenfalls</b> eine Konsultation der Aufsichtsbehörde nach den Artikeln 35 und 36 der Verordnung (EU) 2016/679 durchgeführt werden.</p>	<p>geführt werden.</p>	
<p><b>nicht vorhanden</b></p>	<p><b>(17a) Ein Beispiel für die 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 zie-</b></p>	

EU-Kommission	EU-Parlament	EU-Rat
	<p><b>hen, wenn sie ausgehend von der Benutzung und Belastung bestehender Anlagen festlegen, wo neue Infrastruktur gebaut werden sollte.</b></p>	
<p>(18) Endnutzer <b>können</b> in die Verarbeitung <b>ihrer</b> 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“ <b>des Endnutzers unabhängig davon, ob es sich um eine natürliche oder eine juristische Person handelt</b>, dieselbe Bedeutung haben und denselben Voraussetzungen unterliegen wie der in der Verordnung (EU) 2016/679 festgelegte Begriff „Einwilligung der betroffenen Person“. Grundlegende breitbandige Internetzugangsdienste 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.</p>	<p>(18) <b>Der Nutzer oder der</b> Endnutzer <b>kann</b> in die Verarbeitung <b>seiner</b> 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“ <b>des Nutzers</b> dieselbe Bedeutung haben und denselben Voraussetzungen unterliegen wie der in der Verordnung (EU) 2016/679 festgelegte Begriff „Einwilligung der betroffenen Person“. Grundlegende breitbandige Internetzugangsdienste 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. <b>Die Einwilligung sollte nicht als freiwillig gelten, wenn sie erforderlich ist, um Zugang zu einer Dienstleistung zu erhalten, oder wenn sie durch wiederholte Aufforderungen erwirkt wird. Um solche missbräuchlichen Aufforderungen zu verhindern, sollten die Nutzer in der Lage sein, Diensteanbieter anzuweisen, ihre Entscheidung, nicht einzuwilligen, zu speichern und sich nach technischen Spezifikationen zu richten, durch die eine nicht erteilte Einwilligung, ein Widerruf der Einwilligung oder ein Widerspruch angezeigt wird.</b></p>	
<p>(19) Der Inhalt der elektronischen Kommunikation fällt in den Wesens-</p>	<p>(19) Der Inhalt der elektronischen Kommunikation fällt in den Wesens-</p>	

EU-Kommission	EU-Parlament	EU-Rat
<p>gehalt des nach Artikel 7 der Charta geschützten Grundrechts auf Achtung des Privat- und Familienlebens, der Wohnung und der Kommunikation.</p> <p><b>Eingriffe in die Inhalte</b> der elektronischen Kommunikation <b>sollten</b> nur unter eindeutig festgelegten Voraussetzungen, zu <b>ganz</b> bestimmten Zwecken und unter Einhaltung angemessener Schutzvorkehrungen gegen Missbrauch <b>erlaubt</b> werden. Diese Verordnung sieht die Möglichkeit vor, dass die Betreiber elektronischer Kommunikationsdienste mit einer in Kenntnis der Sachlage gegebenen Einwilligung aller betroffenen <b>Endnutzer</b> die in Übertragung befindlichen elektronischen Kommunikationsdaten verarbeiten können. Beispielsweise können so Betreiber Dienstleistungen anbieten, die das <b>Scannen</b> aller E-Mail-Nachrichten zur Entfernung von bestimmtem, zuvor <b>festgelegtem</b> 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 <b>stets</b> die Aufsichtsbehörde konsultieren. <b>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.</b> Nachdem elektronische Kommunikationsinhalte <b>vom Endnutzer</b> verschickt und von dem bzw. den bestimmungsgemäßen <b>Endnutzern</b> empfangen <b>wurden, können sie</b> von den <b>Endnutzern</b> oder von einem Dritten, der von <b>den Endnutzern</b> mit der Aufzeichnung oder Speicherung solcher Daten beauftragt wurde, aufgezeichnet oder gespeichert werden. Eine <b>solche</b> Verarbeitung der Daten muss <b>im Einklang mit der</b> Verordnung (EU) 2016/679 <b>stehen.</b></p>	<p>gehalt des nach Artikel 7 der Charta geschützten Grundrechts auf Achtung des Privat- und Familienlebens, der Wohnung und der Kommunikation.</p> <p><b>Die Verarbeitung von Inhaltsdaten</b> der elektronischen Kommunikation <b>sollte</b> nur unter eindeutig festgelegten Voraussetzungen, zu <b>sehr genau</b> bestimmten Zwecken und unter Einhaltung angemessener Schutzvorkehrungen gegen Missbrauch <b>gestattet</b> werden. Diese Verordnung sieht die Möglichkeit vor, dass die Betreiber elektronischer Kommunikationsdienste mit einer in Kenntnis der Sachlage gegebenen Einwilligung aller betroffenen <b>Nutzer</b> die in Übertragung befindlichen elektronischen Kommunikationsdaten verarbeiten können. Beispielsweise können so Betreiber Dienstleistungen anbieten, die das <b>Durchleuchten</b> aller E-Mail-Nachrichten zur Entfernung von bestimmtem, zuvor <b>festgelegtem</b> 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 <b>stets eine Folgenabschätzung gemäß Verordnung (EU) 2016/679 durchführen und, soweit die Verordnung dies erfordert,</b> vor der Verarbeitung die Aufsichtsbehörde konsultieren. Nachdem elektronische Kommunikationsinhalte <b>von einem Nutzer</b> verschickt und von dem <b>bestimmungsgemäßen Nutzer</b> bzw. den bestimmungsgemäßen <b>Nutzern</b> empfangen <b>worden sind, dürfen diese Inhalte</b> von <b>dem Nutzer bzw. den Nutzern</b> oder von einem Dritten, der von <b>ihm bzw. ihnen</b> mit der Aufzeichnung oder Speicherung solcher Daten beauftragt wurde <b>und bei dem es sich um den Anbieter elektronischer Kommunikation handeln könnte,</b> aufgezeichnet oder gespeichert werden. Eine Verarbeitung <b>solcher gespeicherter Kommunikationsdaten, bei der die Daten im Auftrag des Nutzers gespeichert werden, muss mit der vorliegenden Verordnung im Einklang stehen. Der Nutzer darf die Daten weiterverarbeiten, und wenn sich personenbe-</b></p>	

EU-Kommission	EU-Parlament	EU-Rat
	<p><b>zogene Daten darunter befinden, muss er dabei die</b> Verordnung (EU) 2016/679 <b>einhalten.</b></p>	
<p><b>nicht vorhanden</b></p>	<p><b>(19a) Es sollte möglich sein, elektronische Kommunikationsdaten zur Erbringung von Dienstleistungen zu verarbeiten, die von einem Nutzer ausdrücklich für persönliche oder persönliche arbeitsbezogene Zwecke angefordert werden, etwa eine Such- oder Verschlagwortungsfunktion, virtuelle Assistenten, Text-Sprach-Module und Übersetzungsdienste, einschließlich der Umwandlung von Bild zu Stimme oder sonstiger automatisierter Verarbeitung von Inhalten, die von Menschen mit Behinderungen als Barrierefreiheitswerkzeuge verwendet werden. Dies sollte ohne die Einwilligung aller Nutzer möglich sein, darf jedoch mit der Einwilligung des Nutzers, der die Dienstleistung anfordert, erfolgen. Diese Einwilligung schließt ferner aus, dass der Betreiber die Daten für andere Zwecke verarbeitet.</b></p>	
<p><b>nicht vorhanden</b></p>	<p><b>(19b) Eingriffe in die Vertraulichkeit von Metadaten oder in den Schutz der in Endeinrichtungen der Endnutzer gespeicherten oder sich auf diese beziehenden Informationen können nur dann als rechtmäßig angesehen werden, wenn sie unbedingt notwendig und verhältnismäßig sind, um ein lebenswichtiges Interesse der betroffenen Person oder einer anderen natürlichen Person zu schützen. Solche Eingriffe, die auf einem lebenswichtigen Interesse einer anderen natürlichen Person beruhen, sollten nur in Sonderfällen erfolgen, wenn es für die Verarbeitung offensichtlich keine andere Rechtsgrundlage gibt.</b></p>	
<p>(20) Die Endeinrichtungen der <b>Endnutzer</b> 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</p>	<p>(20) Die Endeinrichtungen der <b>Nutzer</b> 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</p>	

EU-Kommission	EU-Parlament	EU-Rat
<p>verarbeitet werden, um sich mit anderen Geräten oder mit Netzanlagen verbinden zu können, sind Teil der Privatsphäre der <b>Endnutzer</b>, 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 <b>Informationen</b> enthalten oder verarbeiten, die einen tiefen Einblick in <b>komplexe</b> emotionale, politische und soziale <b>Aspekte der Persönlichkeit</b> 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. <b>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.</b> Informationen in Bezug auf das Gerät des <b>Endnutzers</b> 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 <b>ernsthafte</b> Verletzung der Privatsphäre dieser <b>Endnutzer</b> darstellen. Techniken, mit denen die Aktivitäten der <b>Endnutzer</b> heimlich beobachtet werden, indem z. B. ihre Online-Aktivitäten oder die Standorte ihrer Endeinrichtungen verfolgt werden, oder mit denen die Funktionsweise der Endeinrichtungen der <b>Endnutzer</b> unbemerkt manipuliert wird, stellen eine <b>ernste</b> Bedrohung der Privatsphäre der <b>Endnutzer</b> dar. Deshalb sollten derartige Eingriffe in die Endeinrichtungen der <b>Endnutzer</b> nur mit Einwilligung des <b>Endnutzers</b> und für bestimmte transparente Zwecke erlaubt sein.</p>	<p>verarbeitet werden, um sich mit anderen Geräten oder mit Netzanlagen verbinden zu können, sind Teil der Privatsphäre der <b>Nutzer</b>, 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 <b>hochsensible Daten</b> enthalten oder verarbeiten, die einen tiefen Einblick in <b>das Verhalten, psychologische Eigenschaften, die emotionale Verfassung und</b> politische und soziale <b>Präferenzen</b> 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. Informationen in Bezug auf das Gerät des <b>Nutzers</b> 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 <b>erhebliche</b> Verletzung dieser <b>Nutzer</b> darstellen. <b>Darüber hinaus ist es möglich, z. B. mit Spyware, Webbugs, versteckten Kennungen und unerwünschten Verfolgungswerkzeugen ohne das Wissen des Nutzers in dessen Endeinrichtung einzudringen, um Zugang zu Informationen zu erlangen, versteckte Informationen zu speichern, Daten zu verarbeiten, Ein- und Ausgabefunktionen wie Sensoren zu verwenden oder die Nutzeraktivität zu verfolgen.</b> Techniken, mit denen die Aktivitäten der <b>Nutzer</b> heimlich beobachtet werden, indem z. B. ihre Online-Aktivitäten oder die Standorte ihrer Endeinrichtungen verfolgt werden, oder mit denen die Funktionsweise der Endeinrichtungen der <b>Nutzer</b> unbemerkt manipuliert wird, stellen eine <b>erhebliche</b> Bedrohung der Privatsphäre der <b>Nutzer</b> dar. Deshalb sollten derartige Eingriffe in die Endeinrichtungen <b>eines Nutzers</b> nur mit Einwilligung des <b>Nutzers</b> und für bestimmte transparente Zwecke erlaubt sein. <b>Die Nutzer sollten alle wichtigen Informationen zu der beabsichtigten Verarbeitung</b></p>	

EU-Kommission	EU-Parlament	EU-Rat
	<p><b><i>in klarer und leicht verständlicher Sprache erhalten. Diese Informationen sollten gesondert von den Bedingungen des Dienstes bereitgestellt werden.</i></b></p>	
<p>(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 <b>keine Einwilligung eingeholt werden</b> für ein technisches Speichern oder Zugreifen, das zu dem rechtmäßigen Zweck, die vom <b>Endnutzer</b> 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. <b>Cookies</b> 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 <b>Endnutzers</b> bereitstellen zu können, wie auch <b>das bloße Feststellen der Tatsache</b>, dass das Gerät des <b>Endnutzers</b> die vom <b>Endnutzer</b> angeforderten Inhalte nicht empfangen kann, sollten nicht als Zugriff auf ein Gerät oder als Nutzung der Verarbeitungs-funktionen des Geräts betrachtet werden.</p>	<p>(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 für ein technisches Speichern oder Zugreifen, das zu dem rechtmäßigen Zweck, die vom <b>Nutzer</b> ausdrücklich gewünschte Nutzung eines bestimmten Dienstes zu ermöglichen, unbedingt notwendig und verhältnismäßig ist, <b>keine Einwilligung eingeholt werden</b>. Dazu gehört auch das Speichern von <b>Informationen (wie Cookies und sonstigen Kennungen)</b> 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. <b>Solche Verfahren</b> können, <b>sofern sie mit geeigneten Datenschutzvorkehrungen einhergehen</b>, auch ein legitimes und nützliches Hilfsmittel sein, um beispielsweise den Webdatenverkehr zu einer Website zu messen. <b>Im Zusammenhang mit solchen Messungen wird vorausgesetzt, dass die Ergebnisse der Verarbeitung keine personenbezogenen, sondern aggregierte Daten sind und dass diese Ergebnisse oder die personenbezogenen Daten nicht für Maßnahmen oder Entscheidungen gegenüber einzelnen natürlichen Personen verwendet werden.</b> Konfigurationsprüfungen, die Anbieter von Diensten der Informationsgesellschaft vornehmen, um ihren Dienst entsprechend den Einstellungen des <b>Nutzers</b> bereitstellen zu können, wie auch <b>bloße Abfragen, bei denen festgestellt wird</b>, dass das Gerät des <b>Nutzers</b> die vom <b>Nutzer</b> angeforderten Inhalte nicht empfangen kann, sollten nicht als <b>unrechtmäßiger</b> Zugriff auf ein Gerät oder als Nutzung der Verar-</p>	

EU-Kommission	EU-Parlament	EU-Rat
	<p>beitungsfunktionen des Geräts – <b>wofür es einer Einwilligung bedarf</b> – betrachtet werden.</p>	
<p>(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 <b>Endnutzer</b> immer häufiger aufgefordert, ihre Einwilligung in die Speicherung solcher Verfolgungs-Cookies in ihren Endeinrichtungen zu geben. <b>Infolge dessen</b> werden die <b>Endnutzer</b> mit Einwilligungsanfragen überhäuft. <b>Mit Hilfe</b> 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 <b>Endnutzer</b> bei der Festlegung <b>ihrer</b> 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 <b>Endnutzer</b> und der Website ablaufen, <b>werden</b> von Webbrowsern abgewickelt. Aus dieser Sicht kommt ihnen eine Sonderstellung zu, wenn es darum geht, den <b>Endnutzern</b> die Kontrolle über den Informationsfluss zu und von ihrer Endeinrichtung zu erleichtern. So können Webbrowser <b>insbesondere als Torwächter</b> dienen und den Endnutzern helfen, ein Speichern von Informationen in ihren Endeinrichtungen (wie Smartphones, Tablets oder <b>Computer</b>) bzw. den Zugriff darauf zu verhindern.</p>	<p>(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 <b>Nutzer</b> immer häufiger aufgefordert, ihre Einwilligung in die Speicherung solcher Verfolgungs-Cookies in ihren Endeinrichtungen zu geben. <b>Infolgedessen</b> werden die <b>Nutzer</b> mit Einwilligungsanfragen überhäuft. <b>Die Verwendung von sogenannten Cookie-Mauern und Cookie-Bannern, die Nutzern nicht helfen, die Kontrolle über ihre personenbezogenen Daten und ihre Privatsphäre zu behalten oder sich über ihre Rechte zu informieren, sollte durch diese Verordnung verhindert werden.</b> <b>Mithilfe</b> 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 <b>technische Spezifikationen, etwa durch</b> die entsprechenden Einstellungen in einem Browser oder einer anderen Anwendung, erteilt werden kann. <b>Diese Einstellungen sollten Auswahlmöglichkeiten bezüglich der Speicherung von Informationen auf den Endeinrichtungen des Nutzers sowie einen vom Browser oder von einer anderen Anwendung gesendeten Hinweis umfassen, durch den anderen Parteien die Präferenzen des Nutzers mitgeteilt werden.</b> Die Auswahl, die <b>Nutzer</b> bei der Festlegung <b>der</b> 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 Na-</p>	

EU-Kommission	EU-Parlament	EU-Rat
	<p>vigationshilfe bieten, sind dazu ebenfalls in der Lage. Ein Großteil der Vorgänge, die zwischen dem <b>Nutzer</b> und der Website ablaufen, <b>wird</b> von Webbrowsern abgewickelt. Aus dieser Sicht kommt ihnen eine Sonderstellung zu, wenn es darum geht, den <b>Nutzern</b> die Kontrolle über den Informationsfluss zu und von ihrer Endeinrichtung zu erleichtern. So können Webbrowser, <b>Anwendungen oder Betriebssysteme insbesondere dazu dienen, die vom Nutzer getroffene Auswahl auszuführen</b>, und den Endnutzern helfen, ein Speichern von Informationen in ihren Endeinrichtungen (wie Smartphones, Tablets oder <b>Computern</b>) bzw. den Zugriff darauf zu verhindern.</p>	
<p>(23) Die Grundsätze des Datenschutzes durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen <b>wurden</b> in Artikel 25 der Verordnung (EU) 2016/679 festgeschrieben. Gegenwärtig haben die meisten weitverbreiteten Browser für Cookies die Standardeinstellung „Alle Cookies annehmen“. Deshalb <b>sollten</b> Anbieter von Software, die <b>das Abrufen und Darstellen von Informationen aus dem Internet erlaubt, dazu verpflichtet sein</b>, die Software so <b>zu konfigurieren</b>, dass <b>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</b>. Solche Einstellungen zur Privatsphäre sollten in leicht sichtbarer und verständlicher Weise dargestellt werden.</p>	<p>(23) Die Grundsätze des Datenschutzes durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen <b>sind</b> in Artikel 25 der Verordnung (EU) 2016/679 festgeschrieben. Gegenwärtig haben die meisten weitverbreiteten Browser für Cookies die Standardeinstellung „Alle Cookies annehmen“. Deshalb <b>müssen</b> Anbieter von Software, die <b>elektronische Kommunikation ermöglicht (wie etwa Browser, Betriebssysteme und Kommunikationsanwendungen)</b> die Software <b>unabhängig davon, ob sie getrennt oder im Paket mit Hardware erworben wurde</b>, so konfigurieren, dass <b>die Privatsphäre in der Voreinstellung geschützt ist und dass die domänenübergreifende Verfolgung und Speicherung von Daten auf der Endeinrichtung durch Dritte in der Voreinstellung untersagt ist. Zudem sind die Anbieter dieser Software verpflichtet, ausreichend detaillierte Einstellungsmöglichkeiten bereitzustellen, damit für jede einzelne Zweckkategorie die Einwilligung erteilt werden kann. Dabei handelt es sich mindestens um folgende Kategorien: i) Verfolgung zu kommerziellen Zwecken oder für Direktwerbung zu nichtkommerziellen Zwecken (verhaltensorientierte Werbung), ii) Verfolgung personalisierter Inhalte, iii) Verfolgung zu analytischen Zwecken, iv) Verfolgung von Standortdaten, v) Weitergabe personenbezogener Daten an Dritte (ein-</b></p>	



EU-Kommission	EU-Parlament	EU-Rat
	<p><i>schließlich der Weitergabe eindeutiger Kennungen, die sich mit den im Besitz von Dritten befindlichen personenbezogenen Daten in Verbindung bringen lassen). Bei Informationen, die aus den Endeinrichtungen der Endnutzer erhoben werden, bedarf es keiner Einwilligung, wenn diese Informationen für die Erbringung einer vom Endnutzer angeforderten Dienstleistung der Informationsgesellschaft unbedingt erforderlich sind, etwa um die Bildschirmgröße an das Gerät anzupassen oder zu vermerken, dass Artikel in einem Einkaufswagen abgelegt wurden. Webbrowser, Betriebssysteme und Kommunikationsanwendungen sollten dem Endnutzer die Möglichkeit bieten, in das Speichern von Cookies oder anderen Informationen in Endeinrichtungen (einschließlich des Browsers in dem jeweiligen Gerät) bzw. ihr Auslesen daraus durch eine bestimmte Website oder Quelle einzuwilligen, auch wenn dieser Vorgang aufgrund der allgemeinen Einstellungen verhindert bzw. zugelassen wird. Was bestimmte Parteien betrifft, sollten Webbrowser und Kommunikationsanwendungen den Nutzern außerdem die Möglichkeit bieten, gesondert in die internetweite Verfolgung einzuwilligen. Die Einstellungen zur Privatsphäre sollten zudem Optionen umfassen, anhand deren der Nutzer beispielsweise auswählen kann, ob Multimedia-Player, interaktive Programme zur Betrachtung von Programmiersprachen oder ähnliche Anwendungen ausgeführt werden sollen oder ob eine Website Standortdaten des Nutzers erfassen oder auf bestimmte Hardware wie Webcam oder Mikrofon zugreifen darf. Solche Einstellungen zur Privatsphäre sollten in leicht sichtbarer und verständlicher Weise dargestellt werden, und die Nutzer sollten zum Zeitpunkt der Installation bzw. der ersten Verwendung über die Möglichkeit informiert werden, unter den verschiedenen verfügbaren Optionen auch die Voreinstellungen zur Privatsphäre zu ändern. Die bereitgestellten Informationen sollten die Nutzer nicht davon abbringen, strengere Einstellungen zur Privatsphäre auszuwählen, und diese</i></p>	

EU-Kommission	EU-Parlament	EU-Rat
	<p><i>Informationen sollten einschlägige Hinweise auf die mit der Annahme von domänenübergreifenden Trackern verbundenen Risiken enthalten, wozu auch das Anlegen langfristiger Aufzeichnungen über die Browserverläufe des Betroffenen und die Verwendung solcher Aufzeichnungen zur Übermittlung gezielter Werbung oder zur Weitergabe an Drittanbieter gehören. Softwarehersteller sollten verpflichtet werden, den Nutzern einfache Möglichkeiten dafür zu bieten, die Einstellungen zur Privatsphäre während der Benutzung jederzeit zu ändern, und dem Nutzer zu gestatten, Ausnahmen für bestimmte Websites festzulegen oder anzugeben, von welchen Websites dieser Dienste Tracker und Cookies immer oder niemals angenommen werden sollen.</i></p>	
<p><b>(24)</b> <i>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</i></p>	<p>entfällt</p>	

EU-Kommission	EU-Parlament	EU-Rat
<p><i>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.</i></p>		
<p>(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 <b>aufrecht zu erhalten</b>. 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 <b>Drahtlos-Zugangspunkt</b> deckt einen bestimmten Bereich ab, in dem solche Informationen erfasst werden können. Es gibt inzwischen Diensteanbieter, die aufgrund <b>gescannter</b> 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 kön-</p>	<p>(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 <b>aufrechtzuerhalten</b>. 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 <b>Drahtloszugangspunkt</b> deckt einen bestimmten Bereich ab, in dem solche Informationen erfasst werden können. Es gibt inzwischen Diensteanbieter, die aufgrund <b>ausgelesener</b> 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</p>	

EU-Kommission	EU-Parlament	EU-Rat
<p>nen zu Zwecken verwendet werden, <b>die</b> stärker in die Privatsphäre <b>eingreifen</b>, wie das Übermitteln gewerblicher Werbenachrichten mit persönlich angepassten Angeboten an <b>Endnutzer</b>, wenn <b>diese</b> 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). <b>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.</b></p>	<p>Gebiet usw. Diese Informationen können zu Zwecken verwendet werden, <b>mit denen</b> stärker in die Privatsphäre <b>eingegriffen wird</b>, wie das Übermitteln gewerblicher Werbenachrichten mit persönlich angepassten Angeboten an <b>Nutzer</b>, wenn <b>sie</b> 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). <b>Die Anbieter derartiger Verfahren sollten entweder die Einwilligung des Nutzers einholen oder die Daten unverzüglich anonymisieren und dabei den Zweck ausschließlich auf zeitlich und örtlich begrenzte statistische Zählungen beschränken und überdies wirksame Abschaltmöglichkeiten bieten.</b></p>	
<p>(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 <b>und sonstiger wichtiger Ziele des allgemeinen öffentlichen Interesses der Union oder eines Mitgliedstaats, insbesondere wichtiger</b></p>	<p>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. Deshalb sollte diese Verordnung die Möglichkeit der Mitgliedstaaten zum rechtmäßigen Abfangen elektronischer Kommunikation o-</p>	

EU-Kommission	EU-Parlament	EU-Rat
<p><b>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.</b> 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 <b>oben</b> 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. <b>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.</b></p>	<p>der zum Ergreifen anderer Maßnahmen nicht beeinträchtigen, sofern dies notwendig und verhältnismäßig ist, um die genannten öffentlichen Interessen zu schützen, und <b>sofern dies</b> 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.</p>	
<p><b>nicht vorhanden</b></p>	<p><b>(26a) Die Ende-zu-Ende-Verschlüsselung sollte gefördert werden, damit Sicherheit und Integrität der Netze und Dienste gewahrt werden, und nötigenfalls sollte diese Verschlüsselung im Einklang mit den Grundsätzen der Sicherheit durch Technikgestaltung und des Datenschutzes durch Technikgestaltung vorgeschrieben sein. Die Mitgliedstaaten sollten Anbietern von Verschlüsselungsdiensten, Anbietern elektronischer Kommunikationsdienste und allen anderen Organisationen (auf allen Ebenen der Lieferkette) keine Verpflichtungen auferlegen, die der Sicherheit der Netze und Dienste dieser Anbieter und Organisationen abträglich wären, was etwa der Fall wäre, wenn „Hintertüren“ geschaffen würden oder möglich wären.</b></p>	

EU-Kommission	EU-Parlament	EU-Rat
<p>(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 berechnigte Interesse des Angerufenen zu wahren, die Anzeige der Rufnummer des Anschlusses, mit dem der Anrufer tatsächlich verbunden ist, zu unterdrücken.</p>	<p>(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 berechnigte Interesse des Angerufenen zu wahren, die Anzeige der Rufnummer des Anschlusses, mit dem der Anrufer tatsächlich verbunden ist, zu unterdrücken.</p>	
<p>(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 eCall ihre Aufgaben so effektiv wie möglich erfüllen können.</p>	<p>(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 eCall ihre Aufgaben so effektiv wie möglich erfüllen können.</p>	
<p>(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 nummergebundener 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.</p>	<p>(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 nummergebundener 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.</p>	

EU-Kommission	EU-Parlament	EU-Rat
<p>(30) Öffentlich zugängliche Verzeichnisse der Endnutzer elektronischer Kommunikationsdienste finden <b>eine</b> 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 <b>Endnutzer, die natürliche Personen sind</b>, um ihre Einwilligung gebeten werden, bevor ihre personenbezogenen Daten in ein Verzeichnis aufgenommen werden. Das berechnigte 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.</p>	<p>(30) Öffentlich zugängliche Verzeichnisse der Endnutzer elektronischer Kommunikationsdienste finden 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 die <b>Nutzer</b> um ihre Einwilligung gebeten werden, bevor ihre personenbezogenen Daten in ein Verzeichnis aufgenommen werden. Das berechnigte 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. <b>Die Einwilligung sollte von dem Anbieter elektronischer Kommunikationsdienste zum Zeitpunkt der Unterzeichnung des Vertrags für diesen Dienst eingeholt werden. Natürliche Personen, die in beruflicher Eigenschaft handeln, beispielsweise Freiberufler, Kleingewerbetreibende oder freie Mitarbeiter, sind hinsichtlich ihrer Daten über ihre berufliche Eigenschaft juristischen Personen gleichgestellt.</b></p>	
<p>(31) Wenn <b>Endnutzer, die natürliche Personen sind</b>, 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, <b>Benutzername</b>, Telefonnummer). Außerdem sollten die Betreiber <b>öffentlicher Verzeichnisse</b> die <b>Endnutzer</b> über die Zwecke <b>des Verzeichnisses</b> und die Suchfunktionen informieren, bevor sie sie in das Verzeichnis aufnehmen. Die <b>Endnutzer</b> sollten mit ihrer Einwilligung auch bestimmen können, anhand welcher Kategorien personenbezogener Daten ihre Kontaktangaben durchsucht werden können. Die Kategorien personenbezogener Daten, die in das Ver-</p>	<p>(31) Wenn <b>Nutzer</b> 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, <b>Nutzername</b>, Telefonnummer). Außerdem sollten die Betreiber <b>elektronischer Kommunikationsdienste</b> die <b>Nutzer</b> über die Zwecke und die Suchfunktionen <b>des Verzeichnisses</b> informieren, bevor sie sie in das Verzeichnis aufnehmen. Die <b>Nutzer</b> 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 wer-</p>	

EU-Kommission	EU-Parlament	EU-Rat
<p>zeichnis aufgenommen werden, und die Kategorien personenbezogener Daten, anhand deren die Kontaktangaben der <b>Endnutzer</b> durchsucht werden können, müssen nicht <b>notwendigerweise</b> dieselben sein.</p>	<p>den, und die Kategorien personenbezogener Daten, anhand deren die Kontaktangaben der <b>Nutzer</b> durchsucht werden können, müssen nicht <b>unbedingt</b> dieselben sein. <b>Die Betreiber öffentlich zugänglicher Verzeichnisse sind gehalten, Informationen über die Suchfunktionen und darüber bereitzustellen, dass in den öffentlich zugänglichen Verzeichnissen neue Optionen und Funktionen zur Verfügung stehen, und zudem den Nutzern die Möglichkeit bieten, diese Funktionen zu deaktivieren.</b></p>	
<p>(32) In dieser Verordnung wird unter Direktwerbung jede Art von Werbung verstanden, mittels <b>derer</b> 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.</p>	<p>(32) In dieser Verordnung wird unter Direktwerbung jede Art von Werbung <b>unabhängig von ihrer Form</b> verstanden, mittels <b>deren</b> 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.</p>	
<p>(33) Es sollten Vorkehrungen getroffen werden, um die Endnutzer vor unerbetener Direktwerbung zu schützen, <b>die</b> in das Privatleben der Endnutzer <b>eingreift</b>. 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, Sofortnachrichtenwendungen, <b>E-Mail</b>, SMS, MMS, Bluetooth <b>usw.</b> 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</p>	<p>(33) Es sollten Vorkehrungen getroffen werden, um die Endnutzer vor unerbetener <b>Kommunikation oder</b> Direktwerbung zu schützen, <b>mit der</b> in das Privatleben der Endnutzer <b>eingegriffen wird</b>. 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, <b>halbautomatischer Systeme</b>, Sofortnachrichtenwendungen, <b>Faxe, E-Mails</b>, SMS, MMS, Bluetooth als relativ ähnlich betrachtet. Daher ist es gerechtfertigt, zu verlangen, dass die Einwilligung des Endnutzers eingeholt wird, bevor gewerbliche elektronische Direktwerbung an Endnutzer gerichtet</p>	



EU-Kommission	EU-Parlament	EU-Rat
<p>und den Schutz der berechtigten Interessen juristischer Personen wirksam zu gewährleisten. Aus Gründen der Rechtssicherheit und <b>wegen der Notwendigkeit, dafür zu sorgen, dass</b> die Vorschriften zum Schutz vor unerbetener elektronischer Kommunikation zukunftsicher bleiben, ist es <b>erforderlich, die</b> nicht danach <b>unterscheiden</b>, mit welcher Technik <b>diese</b> unerbetene Kommunikation erfolgt, und zugleich <b>einen gleichwertigen</b> Schutz aller <b>Bürger</b> in der gesamten Union <b>zu gewährleisten</b>. Es ist jedoch vertretbar, im Rahmen einer bestehenden Kundenbeziehung die Nutzung von E-Mail-Kontaktangaben zu <b>erlauben</b>, damit <b>ähnliche</b> 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.</p>	<p>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 <b>weil</b> die Vorschriften zum Schutz vor unerbetener elektronischer Kommunikation zukunftsicher bleiben <b>müssen</b>, ist es <b>gerechtfertigt</b>, einheitliche Vorschriften zu schaffen, <b>bei denen</b> nicht danach <b>unterschieden wird</b>, mit welcher Technik <b>die</b> unerbetene Kommunikation erfolgt, und <b>durch die</b> zugleich <b>ein hochwertiger</b> Schutz aller <b>Endnutzer ist</b>. Es ist jedoch vertretbar, im Rahmen einer bestehenden Kundenbeziehung die Nutzung von E-Mail-Kontaktangaben zu <b>gestatten</b>, damit <b>andere</b> 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.</p>	
<p>(34) Wenn Endnutzer in den Empfang unerbetener Direktwerbung eingewilligt haben, sollten sie dennoch in der Lage sein, ihre Einwilligung jederzeit auf einfache Weise zu widerrufen. 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.</p>	<p>(34) Wenn Endnutzer in den Empfang unerbetener Direktwerbung eingewilligt haben, sollten sie dennoch in der Lage sein, ihre Einwilligung jederzeit auf einfache Weise zu widerrufen. 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.</p>	
<p>(35) Um einen einfachen Widerruf der Einwilligung zu ermöglichen,</p>	<p>(35) Um einen einfachen Widerruf der Einwilligung zu ermöglichen,</p>	

EU-Kommission	EU-Parlament	EU-Rat
<p>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.</p>	<p>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.</p>	
<p>(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. <b>Deshalb sollten</b> die Mitgliedstaaten hierfür nationale Systeme einrichten oder beibehalten <b>können, die</b> solche Anrufe nur an Endnutzer <b>erlauben</b>, die dem nicht widersprochen haben.</p>	<p>(36) Persönliche Direktwerbeanrufe, die ohne Verwendung automatischer Anruf- und Kommunikationssysteme ausgeführt werden, sind für den Absender kostspieliger und bringen für <b>die</b> Endnutzer keine finanziellen Kosten mit sich, <b>weshalb es gerechtfertigt ist, dass</b> die Mitgliedstaaten hierfür nationale Systeme einrichten oder beibehalten <b>müssen, in denen</b> solche Anrufe nur an Endnutzer <b>zulässig sind</b>, die dem nicht widersprochen haben.</p>	
<p>(37) Anbieter elektronischer Kommunikationsdienste sollten die <b>Endnutzer</b> 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 <b>Dienstanbieter</b> 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.</p>	<p>(37) <b>Die Anbieter elektronischer Kommunikationsdienste sollten elektronische Kommunikationsdaten so verarbeiten, dass eine unerlaubte Verarbeitung – einschließlich Zugriff oder Änderung – verhindert wird. Sie sollten dafür Sorge tragen, dass solche Fälle unerlaubten Zugriffs oder unerlaubter Änderung festgestellt werden können, und sollten außerdem sicherstellen, dass solche elektronischen Kommunikationsdaten durch die Verwendung modernster Software und Verschlüsselungsverfahren, einschließlich Verschlüsselungstechniken, geschützt werden.</b> Die Anbieter elektronischer Kommunikationsdienste sollten die <b>Nutzer</b> auch 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 Sicherheitsrisi-</p>	

EU-Kommission	EU-Parlament	EU-Rat
	<p>ken aufzuklären, entbindet einen <b>Anbieter elektronischer Kommunikationsdienste</b> 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. <b>Die in Artikel 40 des [europäischen Kodex für die elektronische Kommunikation] dargelegten Verpflichtungen sollten für alle Dienste dieser Verordnung mit Blick auf die Sicherheit von Netzen und elektronischen Kommunikationsdiensten sowie den damit verbundenen Sicherheitsverpflichtungen Anwendung finden.</b></p>	
<p>(38) Um die vollständige Kohärenz mit der Verordnung (EU) 2016/679 zu <b>gewährleisten</b>, 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 <b>sollten</b> die Fähigkeit <b>der Aufsichtsbehörde</b>, ihre Aufgaben in Bezug auf den Schutz personenbezogener Daten nach der Verordnung (EU) 2016/679 und dieser Verordnung wahrzunehmen, <b>nicht beeinträchtigen</b>. Jede Aufsichtsbehörde sollte zusätzlich mit Finanzmitteln, Personal, Räumlichkeiten und Infrastruktur ausgestattet werden, die für die wirksame Wahrnehmung ihrer Aufgaben nach</p>	<p>(38) Um die vollständige Kohärenz mit der Verordnung (EU) 2016/679 zu <b>wahren</b>, 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. <b>Gibt es in einem Mitgliedstaat mehr als eine Aufsichtsbehörde, so sollten die Behörden zusammenarbeiten. Sie sollten auch mit den für die Durchsetzung des europäischen Kodex für die elektronische Kommunikation beauftragten Behörden und weiteren einschlägigen Durchsetzungsbehörden wie Verbraucherschutzbehörden zusammenarbeiten. Durch</b> diese zusätzlichen Aufgaben <b>sollte</b> die <b>Aufsichts-</b></p>	

EU-Kommission	EU-Parlament	EU-Rat
<p>dieser Verordnung notwendig sind.</p>	<p><b>behörde nicht in ihrer Fähigkeit beeinträchtigt werden</b>, ihre Aufgaben in Bezug auf den Schutz personenbezogener Daten nach der Verordnung (EU) 2016/679 und dieser Verordnung wahrzunehmen. Jede Aufsichtsbehörde sollte zusätzlich mit Finanzmitteln, Personal, Räumlichkeiten und Infrastruktur ausgestattet werden, die für die wirksame Wahrnehmung ihrer Aufgaben nach dieser Verordnung notwendig sind.</p>	
<p><b>nicht vorhanden</b></p>	<p><b>(38a) Zur Durchsetzung der Bestimmungen dieser Verordnung ist es oftmals notwendig, dass die nationalen Aufsichtsbehörden zweier oder mehrerer Mitgliedstaaten zusammenarbeiten, zum Beispiel, um gegen unrechtmäßige Eingriffe in die Vertraulichkeit von Endeinrichtungen vorzugehen. Um in solchen Fällen eine reibungslose und schnelle Zusammenarbeit zu garantieren, sollten die Verfahren der Zusammenarbeit und der einheitlichen Rechtsanwendung gemäß der Verordnung (EU) 2016/679 auf Kapitel II dieser Verordnung Anwendung finden. Deshalb sollte der Europäische Datenschutzausschuss einen Beitrag zur einheitlichen Anwendung dieser Verordnung in der gesamten Union leisten, insbesondere indem er Stellungnahmen mit Blick auf das Kohärenzverfahren abgibt oder in Bezug auf Kapitel II dieser Verordnung verbindliche Beschlüsse im Rahmen der Streitbeilegung gemäß Artikel 65 der Verordnung 2016/679/EU erlässt.</b></p>	
<p>(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</p>	<p>(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, <b>darunter den Erlass verbindlicher Beschlüsse</b>. 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 <b>Untersuchungsbefugnisse, Abhilfe- und Sanktionsbefugnisse und Genehmi-</b></p>	

EU-Kommission	EU-Parlament	EU-Rat
<p>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 Kleinunternehmen sowie von kleinen und mittleren Unternehmen zu berücksichtigen.</p>	<p><b>gungs- und Beratungsbefugnisse, sowie</b> – 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 Kleinunternehmen sowie von kleinen und mittleren Unternehmen zu berücksichtigen.</p>	
<p>(40) Im Interesse einer konsequenten 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.</p>	<p>(40) Im Interesse einer konsequenten 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.</p>	
<p>(41) Um die Zielvorgaben dieser Verordnung zu erfüllen, d. h. die Grundrechte und Grundfreiheiten natürlicher Personen und insbesondere ihr Recht auf <b>Schutz ihrer personenbezogenen</b> 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</p>	<p>(41) Um die Zielvorgaben dieser Verordnung zu erfüllen, d. h. die Grundrechte und Grundfreiheiten natürlicher Personen <b>bei der Bereitstellung und Nutzung elektronischer Kommunikationsdienste</b> und insbesondere ihr Recht auf <b>Achtung des Privatlebens und der Kommunikation bei der Verarbeitung personenbezogener</b> Daten zu schützen und den freien Verkehr personenbezogener Daten innerhalb der Union zu gewährleis-</p>	

EU-Kommission	EU-Parlament	EU-Rat
<p>Rechtsakte sollten insbesondere <b>erlassen werden</b> in Bezug <b>auf die bereitzustellenden</b> 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 <b>Endnutzer</b> der Endeinrichtung treffen kann, um die Erhebung zu beenden oder auf ein Minimum zu beschränken. <b>Delegierte Rechtsakte sind ebenfalls erforderlich, um einen Code festzulegen, der Direktwerbeanrufer kenntlich macht, auch solche, die mithilfe automatischer Anruf- und Kommunikationssysteme getätigt werden.</b> 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<sup>25</sup> vom 13. April 2016 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 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.</p>	<p>ten, sollte der Kommission die Befugnis übertragen werden, gemäß Artikel 290 AEUV Rechtsakte zur Ergänzung dieser Verordnung zu erlassen. Delegierte Rechtsakte sollten insbesondere in Bezug <b>darauf erlassen werden, welche Informationen bereitzustellen sind</b>, auch mittels standardisierter Bildsymbole, um einen leicht wahrnehmbaren und verständlichen Überblick über die Erhebung der von der Endeinrichtung ausgesendeten Informationen zu vermitteln, sowie <b>in Bezug auf</b> den Zweck, die dafür verantwortliche Person und die Maßnahmen, die der <b>Nutzer</b> der Endeinrichtung treffen kann, um die Erhebung zu beenden oder auf ein Minimum zu beschränken. 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<sup>25</sup> vom 13. April 2016 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 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. <b>So sind zum Beispiel Durchführungsmaßnahmen erforderlich, um einen Code festzulegen, der Direktwerbeanrufer kenntlich macht, auch solche, die mithilfe automatischer Anruf- und Kommunikationssysteme getätigt werden. Durchführungsmaßnahmen sind außerdem erforderlich, um die Verfahren einzurichten und die Umstände festzustellen, nach bzw. unter denen die Unterdrückung der Anzeige der Rufnummer des Anrufers vorübergehend aufzuheben ist, wenn Nutzer beantragen, dass böswillige oder belästigende Anrufe zurückverfolgt werden.</b> Diese Befugnisse sollten</p>	

EU-Kommission	EU-Parlament	EU-Rat
	nach Maßgabe der Verordnung (EU) Nr. 182/2011 des Europäischen Parlaments und des Rates ausgeübt werden.	
<p>_____</p> <p><sup>25</sup> 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).</p>	<p>_____</p> <p><sup>25</sup> 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).</p>	
<p>(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.</p>	<p>(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.</p>	
<p>(43) Die Richtlinie 2002/58/EG sollte aufgehoben werden –</p>	<p>(43) Die Richtlinie 2002/58/EG sollte aufgehoben werden –</p>	
<p>HABEN FOLGENDE VERORDNUNG ERLASSEN:</p>		
<p><b>Kapitel I</b> <b>ALLGEMEINE BESTIMMUNGEN</b></p>		
<p><i>Artikel 1</i></p> <p><i>Gegenstand</i></p> <p>(1) Diese Verordnung legt Vorschriften zum Schutz von Grundrechten und Grundfreiheiten natürlicher und juris-</p>	<p><i>Artikel 1</i></p> <p><i>Gegenstand</i></p> <p>(1) Diese Verordnung legt Vorschriften zum Schutz von Grundrechten und Grundfreiheiten natürlicher und juris-</p>	

EU-Kommission	EU-Parlament	EU-Rat
<p>tischer 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.</p>	<p>tischer 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.</p>	
<p><i>Artikel 2</i></p> <p><i>Sachlicher Anwendungsbereich</i></p> <p>(1) Diese Verordnung gilt für <b>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.</b></p>	<p><i>Artikel 2</i></p> <p><i>Sachlicher Anwendungsbereich</i></p> <p>(1) Diese Verordnung gilt für</p>	
<p><b>nicht vorhanden</b></p>	<p><b>a) die Verarbeitung elektronischer Kommunikationsdaten, die in Verbindung mit der Bereitstellung und Nutzung elektronischer Kommunikationsdienste erfolgt, unabhängig davon, ob eine Bezahlung verlangt wird,</b></p>	
<p><b>nicht vorhanden</b></p>	<p><b>b) die Verarbeitung von Informationen, die sich auf die Endeinrichtungen der Endnutzer beziehen oder von den Endeinrichtungen der Endnutzer verarbeitet werden,</b></p>	
<p><b>nicht vorhanden</b></p>	<p><b>c) das Inverkehrbringen von Software, die elektronische Kommunikation ermöglicht, darunter das Abrufen und Darstellen von Informationen aus dem Internet,</b></p>	
<p><b>nicht vorhanden</b></p>	<p><b>d) die Bereitstellung öffentlich zugänglicher Verzeichnisse der Nutzer elektronischer Kommunikation,</b></p>	
<p><b>nicht vorhanden</b></p>	<p><b>e) die Übermittlung von Direktwerbung an Endnutzer mittels elektro-</b></p>	



EU-Kommission	EU-Parlament	EU-Rat
	<b>nischer Kommunikation.</b>	
(2) Diese Verordnung gilt nicht für:	(2) Diese Verordnung gilt nicht für:	
a) Tätigkeiten, die nicht in den Anwendungsbereich des Unionsrechts fallen;	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;	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;	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.	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].	(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 <sup>9</sup> und insbesondere der Vorschriften zur Verantwortlichkeit der Anbieter reiner Vermittlungsdienste in den Artikeln 12 bis 15 dieser Richtlinie unberührt.	(4) Die vorliegende Verordnung lässt die Anwendung der Richtlinie 2000/31/EG <sup>9</sup> und insbesondere der Vorschriften zur Verantwortlichkeit der Anbieter reiner Vermittlungsdienste in den Artikeln 12 bis 15 dieser Richtlinie unberührt.	
<p>_____</p> <p><sup>9</sup> Richtlinie 2000/31/EG des Europäischen Parlaments und des Rates vom 8. Juni</p>	<p>_____</p> <p><sup>9</sup> Richtlinie 2000/31/EG des Europäischen Parlaments und des Rates vom 8. Juni</p>	

EU-Kommission	EU-Parlament	EU-Rat
<p>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).</p>	<p>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).</p>	
<p>(5) Die Bestimmungen der Richtlinie 2014/53/EU bleiben von dieser Verordnung unberührt.</p>	<p>(5) Die Bestimmungen der Richtlinie 2014/53/EU bleiben von dieser Verordnung unberührt.</p>	
<p><i>Artikel 3</i></p> <p><i>Räumlicher Anwendungsbereich und Vertreter</i></p> <p>(1) Diese Verordnung gilt für:</p>	<p><i>Artikel 3</i></p> <p><i>Räumlicher Anwendungsbereich und Vertreter</i></p> <p>(1) Diese Verordnung gilt für:</p>	
<p>a) <b>die Bereitstellung</b> elektronischer Kommunikationsdienste für Endnutzer in der Union, unabhängig davon, ob vom Endnutzer eine Bezahlung verlangt wird;</p>	<p>a) <b>das Anbieten</b> elektronischer Kommunikationsdienste, <b>Software und öffentlich zugänglicher Verzeichnisse</b> für Endnutzer in der Union <b>und das Übermitteln von Direktwerbung an Endnutzer in der Union mittels elektronischer Kommunikation</b>, unabhängig davon, ob vom Endnutzer eine Bezahlung verlangt wird;</p>	
<p>b) die <b>Nutzung solcher Dienste</b>;</p>	<p>b) die <b>in Artikel 2 genannten Tätigkeiten, die vom Gebiet der Union aus erbracht werden</b>;</p>	
<p>c) <b>den Schutz</b> von Informationen <b>in Bezug auf die</b> Endeinrichtungen <b>der Endnutzer</b> in der Union.</p>	<p>c) <b>die Verarbeitung</b> von Informationen, <b>die sich</b> auf Endeinrichtungen <b>von Endnutzern</b> in der Union <b>beziehen oder in solchen Endeinrichtungen verarbeitet werden</b>.</p>	
<p>(2) Ist der Betreiber eines elektronischen Kommunikationsdienstes nicht in der Union niedergelassen, so muss er schriftlich einen Vertreter in der Union benennen.</p>	<p>(2) Ist der Betreiber eines elektronischen Kommunikationsdienstes, <b>der Anbieter von Software, die elektronische Kommunikation ermöglicht, eine Person, die Informationen verarbeitet, die sich auf Endeinrichtungen von Nutzern oder Endnutzern</b></p>	

EU-Kommission	EU-Parlament	EU-Rat
	<p><b>beziehen oder dort verarbeitet werden, der Betreiber eines öffentlich zugänglichen Verzeichnisses oder eine Person, die Direktwerbung mittels elektronischer Kommunikationsdienste übermittelt,</b> nicht in der Union niedergelassen, so muss er <b>bzw. sie</b> schriftlich einen Vertreter in der Union benennen.</p>	
<p>(3) Der Vertreter muss in einem der Mitgliedstaaten niedergelassen sein, in denen sich die Endnutzer dieser elektronischen Kommunikationsdienste befinden.</p>	<p>(3) Der Vertreter muss in einem der Mitgliedstaaten niedergelassen sein, in denen sich die Endnutzer dieser elektronischen Kommunikationsdienste befinden.</p>	
<p>(4) Der Vertreter muss <b>für die Zwecke der Gewährleistung der Einhaltung dieser Verordnung</b> befugt sein, zusätzlich zu dem von ihm vertretenen Betreiber oder an dessen Stelle Fragen zu beantworten und Auskünfte zu erteilen, und zwar insbesondere gegenüber Aufsichtsbehörden und Endnutzern <b>in Bezug auf alle Belange im Zusammenhang mit der Verarbeitung elektronischer Kommunikationsdaten.</b></p>	<p>(4) Der Vertreter muss befugt sein, <b>in Bezug auf alle Belange im Zusammenhang mit Tätigkeiten nach Artikel 2</b> zusätzlich zu dem von ihm vertretenen Betreiber oder an dessen Stelle Fragen zu beantworten und Auskünfte zu erteilen, und zwar insbesondere gegenüber Aufsichtsbehörden, <b>Gerichten</b> und Endnutzern, <b>damit er die Einhaltung dieser Verordnung gewährleisten kann.</b></p>	
<p>(5) Die Benennung eines Vertreters nach Absatz 2 erfolgt unbeschadet etwaiger rechtlicher Schritte gegen eine natürliche oder juristische Person, die <b>elektronische Kommunikationsdaten in Verbindung mit der Bereitstellung elektronischer Kommunikationsdienste</b> von außerhalb der Union <b>für Endnutzer in der Union verarbeitet.</b></p>	<p>(5) Die Benennung eines Vertreters nach Absatz 2 erfolgt unbeschadet etwaiger rechtlicher Schritte gegen eine natürliche oder juristische Person, die <b>Tätigkeiten nach Artikel 2</b> von außerhalb der Union <b>ausübt.</b></p>	
<p><i>Artikel 4</i> <i>Begriffsbestimmungen</i></p> <p>(1) Für die Zwecke dieser Verordnung gelten folgende Begriffsbestimmungen:</p>	<p><i>Artikel 4</i> <i>Begriffsbestimmungen</i></p> <p>(1) Für die Zwecke dieser Verordnung gelten folgende Begriffsbestimmungen:</p>	
<p>a) die Begriffsbestimmungen der Verordnung (EU) 2016/679;</p>	<p>a) die Begriffsbestimmungen der Verordnung (EU) 2016/679;</p>	

EU-Kommission	EU-Parlament	EU-Rat
<p>b) die <b>Begriffsbestimmungen</b> für „<b>elektronisches Kommunikationsnetz</b>“, „<b>elektronischer Kommunikationsdienst</b>“, „<b>interpersoneller Kommunikationsdienst</b>“, „<b>nummerngebundener interpersoneller Kommunikationsdienst</b>“, „<b>nummernunabhängiger interpersoneller Kommunikationsdienst</b>“, „<b>Endnutzer</b>“ und „Anruf“ in Artikel 2 <b>Nummern 1, 4, 5, 6, 7, 14 bzw. 21</b> der [Richtlinie über den europäischen Kodex für die elektronische Kommunikation];</p>	<p>b) die <b>Begriffsbestimmung</b> für „Anruf“ in Artikel 2 <b>Nummer 21</b> der [Richtlinie über den europäischen Kodex für die elektronische Kommunikation];</p>	
<p>c) die Begriffsbestimmung für „Endeinrichtungen“ in Artikel 1 Nummer 1 der Richtlinie 2008/63/EG der Kommission<sup>10</sup>.</p>	<p>c) die Begriffsbestimmung für „Endeinrichtungen“ in Artikel 1 Nummer 1 der Richtlinie 2008/63/EG der Kommission<sup>10</sup>.</p>	
<p>_____</p> <p><sup>10</sup> Richtlinie 2008/63/EG der Kommission vom 20. Juni 2008 über den Wettbewerb auf dem Markt für Telekommunikationsend-einrichtungen (ABl. L 162 vom 21.6.2008, S. 20).</p>	<p>_____</p> <p><sup>10</sup> Richtlinie 2008/63/EG der Kommission vom 20. Juni 2008 über den Wettbewerb auf dem Markt für Telekommunikationsend-einrichtungen (ABl. L 162 vom 21.6.2008, S. 20).</p>	
<p><b>(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.</b></p>	<p><b>entfällt</b></p>	
<p>(3) Für die Zwecke dieser Verordnung gelten zusätzlich folgende Begriffsbestimmungen:</p>	<p>(3) Für die Zwecke dieser Verordnung gelten zusätzlich folgende Begriffsbestimmungen:</p>	
<p>a) „elektronische Kommunikationsdaten“: elektronische Kommunikationsinhalte und elektronische Kommunikationsmetadaten;</p>	<p>a) „elektronisches Kommunikationsnetz“: ein Übertragungssystem, ungeachtet dessen, ob es auf einer permanenten Infrastruktur oder einer zentralen Verwaltungskapazität beruht, und, falls vorhanden, Vermitt-</p>	

EU-Kommission	EU-Parlament	EU-Rat
	<p><i>lungs- und Leitweeinrichtungen sowie anderweitige Ressourcen – einschließlich der nicht aktiven Netzbestandteile –, die die Übertragung von Signalen über Kabel, Funk, optische oder andere elektromagnetische Einrichtungen ermöglichen, einschließlich Satellitennetzen, fester (leitungs- und paketvermittelter, einschließlich des Internets) und mobiler terrestrischer Netze, Stromleitungssystemen, soweit sie zur Signalübertragung genutzt werden, Netzen für Hör- und Fernsehfunk sowie Kabelfernsehnetzen, unabhängig von der Art der übertragenen Informationen;</i></p> <p><i>aa) „elektronischer Kommunikationsdienst“: ein über elektronische Kommunikationsnetze gegen Entgelt oder unentgeltlich erbrachter Dienst, der einen oder mehrere der folgenden Punkte umfasst: einen „Internetzugangsdienst“ gemäß der Begriffsbestimmung in Artikel 2 Nummer 2 der Verordnung (EU) 2015/2120; einen interpersonellen Kommunikationsdienst; einen Dienst, der ganz oder überwiegend in der Übertragung von Signalen besteht, beispielsweise ein Übertragungsdienst, der zur Bereitstellung eines Maschine-Maschine-Dienstes und als Rundfunkdienst genutzt wird, wobei dies keine Informationen einschließt, die als Teil eines Rundfunkdienstes über ein elektronisches Kommunikationsnetz oder einen elektronischen Kommunikationsdienst öffentlich übertragen werden, soweit die Informationen nicht mit dem identifizierbaren Endnutzer, der sie empfängt, in Verbindung gebracht werden können; dazu zählen auch Dienste, die zwar nicht öffentlich zugänglich sind, aber über die der Zugang zu einem öffentlich zugänglichen elektronischen Kommunikationsnetz bereitgestellt wird;</i></p>	

EU-Kommission	EU-Parlament	EU-Rat
	<p><b>ab) „interpersoneller Kommunikationsdienst“: gegen Entgelt oder unentgeltlich erbrachter Dienst, der einen direkten interpersonellen und interaktiven Informationsaustausch zwischen einer endlichen Zahl von Personen ermöglicht, wobei die Empfänger von den Personen bestimmt werden, die die Kommunikation veranlassen oder daran beteiligt sind;</b></p> <p><b>ac) „nummerngebundener interpersoneller Kommunikationsdienst“: ein interpersoneller Kommunikationsdienst, der an das öffentliche Fernsprechnetz angebunden ist, entweder mittels zugeteilter Nummerierungsressourcen, d. h. Nummern nationaler oder internationaler Telefonnummernpläne, oder durch Ermöglichung der Kommunikation über Nummern nationaler oder internationaler Telefonnummernpläne;</b></p> <p><b>ad) „nummernunabhängiger interpersoneller Kommunikationsdienst“: ein interpersoneller Kommunikationsdienst, der nicht an das öffentliche Fernsprechnetz angebunden ist, weder mittels zugeteilter Nummerierungsressourcen, d. h. Nummern nationaler oder internationaler Telefonnummernpläne, noch durch Ermöglichung der Kommunikation über Nummern nationaler oder internationaler Telefonnummernpläne;</b></p> <p><b>ae) „Endnutzer“: eine juristische oder natürliche Person, die einen öffentlich zugänglichen elektronischen Kommunikationsdienst in Anspruch nimmt oder beantragt;</b></p> <p><b>af) „Nutzer“: eine natürliche Person, die einen öffentlich zugänglichen elektronischen Kommunikationsdienst für private oder geschäftliche Zwecke in Anspruch nimmt, ohne diesen Dienst zwangsläufig abonniert zu haben;</b></p>	

EU-Kommission	EU-Parlament	EU-Rat
<p>b) „elektronische Kommunikationsinhalte“: Inhalte, die mittels elektronischer Kommunikationsdienste übermittelt werden, z. B. Textnachrichten, Sprache, Videos, Bilder und Ton;</p>	<p>b) „elektronische Kommunikationsinhalte“: Inhalte, die mittels elektronischer Kommunikationsdienste übermittelt, <b>verbreitet oder ausgetauscht</b> werden, z. B. Textnachrichten, Sprache, Videos, Bilder und Ton; <b>werden Metadaten anderer elektronischer Kommunikationsdienste oder -protokolle durch Nutzung des jeweiligen Dienstes übermittelt, verbreitet oder ausgetauscht, gelten sie für den jeweiligen Dienst als elektronische Kommunikationsinhalte;</b></p>	
<p>c) „elektronische Kommunikationsmetadaten“: Daten, die in einem elektronischen Kommunikationsnetz zu Zwecken der Übermittlung, der Verbreitung oder des Austauschs elektronischer Kommunikationsinhalte 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 <b>erzeugten</b> Daten über den Standort <b>des Geräts</b> sowie Datum, Uhrzeit, Dauer und Art der Kommunikation;</p>	<p>c) „elektronische Kommunikationsmetadaten“: Daten, die in einem elektronischen Kommunikationsnetz zu Zwecken der Übermittlung, der Verbreitung oder des Austauschs elektronischer Kommunikationsinhalte 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 <b>verarbeiteten</b> Daten über den Standort <b>der Endeinrichtung</b> sowie Datum, Uhrzeit, Dauer und Art der Kommunikation;</p>	
<p>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;</p>	<p>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;</p>	
<p>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</p>	<p>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</p>	

EU-Kommission	EU-Parlament	EU-Rat
<p>Rechneranlagen oder in Endrichtungen ihres Empfängers gespeichert werden kann;</p>	<p>Rechneranlagen oder in Endrichtungen ihres Empfängers gespeichert werden kann;</p>	
<p>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 <b>menschliche(r) Beteiligung</b>, mittels E-Mail, SMS-Nachrichten usw.;</p>	<p>f) „Direktwerbung“: jede Art der Werbung in schriftlicher oder mündlicher Form <b>oder als Videoformat</b>, die an einen oder mehrere bestimmte oder bestimmbare Endnutzer elektronischer Kommunikationsdienste gerichtet, <b>für sie bereitgestellt oder ihnen angezeigt</b> wird, auch mittels automatischer Anruf- und Kommunikationssysteme mit oder ohne <b>Beteiligung eines Menschen</b>, mittels E-Mail, SMS-Nachrichten, <b>Faxgeräten</b> usw.;</p>	
<p>g) „persönliche Direktwerbeanrufe“: direkt persönlich und ohne Verwendung automatischer Anruf- und Kommunikationssysteme ausgeführte Anrufe;</p>	<p>g) „persönliche Direktwerbeanrufe“: direkt persönlich und ohne Verwendung automatischer Anruf- und Kommunikationssysteme ausgeführte Anrufe, <b>einschließlich Anrufen unter Verwendung automatischer Anruf- und Kommunikationssysteme, die die angerufene Person mit einer einzelnen Person verbinden</b>;</p>	
<p>h) „automatische Anruf- und Kommunikationssysteme“: Systeme, die automatisch Anrufe zu einem oder mehreren Empfängern entsprechend den <b>für das</b> System <b>gemachten</b> Einstellungen aufbauen und Ton übertragen können, der keine live gesprochene Rede darstellt, <b>einschließlich Anrufen unter Verwendung automatischer Anruf- und Kommunikationssysteme, die die angerufene Person mit einer einzelnen Person verbinden</b>.</p>	<p>h) „automatische Anruf- und Kommunikationssysteme“: Systeme, die automatisch Anrufe zu einem oder mehreren Empfängern entsprechend den <b>im</b> System <b>festgelegten</b> Einstellungen aufbauen und Ton übertragen können, der keine live gesprochene Rede darstellt.</p>	



EU-Kommission	EU-Parlament	EU-Rat
<p><b>Kapitel II</b>  <b>SCHUTZ DER ELEKTRONISCHEN KOMMUNIKATION NATÜRLICHER UND JURISTISCHER PERSONEN UND DER IN IHREN ENDEINRICHTUNGEN GESPEICHERTEN INFORMATIONEN</b></p>		
<p>Änderung der Überschrift für KAPITEL II</p> <p>SCHUTZ DER ELEKTRONISCHEN KOMMUNIKATION NATÜRLICHER <b>UND JURISTISCHER</b> PERSONEN UND DER <b>IN</b> IHREN ENDEINRICHTUNGEN <b>GESPEICHERTEN</b> INFORMATIONEN</p>	<p>Änderung der Überschrift für KAPITEL II</p> <p>SCHUTZ DER ELEKTRONISCHEN KOMMUNIKATION NATÜRLICHER PERSONEN UND DER <b>VON</b> IHREN ENDEINRICHTUNGEN <b>VERARBEITETEN UND DAMIT ZUSAMMENHÄNGENDEN</b> INFORMATIONEN</p>	
<p><i>Artikel 5</i></p> <p>Änderung der Überschrift für Artikel 5</p> <p>Vertraulichkeit elektronischer <b>Kommunikationsdaten</b></p>	<p><i>Artikel 5</i></p> <p>Änderung der Überschrift für Artikel 5</p> <p>Vertraulichkeit elektronischer <b>Kommunikation</b></p>	
<p><i>Artikel 5</i></p> <p>Elektronische <b>Kommunikationsdaten sind</b> vertraulich. Eingriffe in elektronische <b>Kommunikationsdaten</b> wie Mithören, Abhören, Speichern, Beobachten, <b>Scannen</b> oder andere Arten des Abfangens oder Überwachens oder <b>Verarbeitens</b> elektronischer <b>Kommunikationsdaten</b> durch andere Personen als die Endnutzer sind untersagt, <b>sofern sie nicht durch diese Verordnung erlaubt werden.</b></p>	<p><i>Artikel 5</i></p> <p><b>(1)</b> Elektronische <b>Kommunikation ist</b> vertraulich. Eingriffe in elektronische <b>Kommunikation</b> wie Mithören, Abhören, Speichern, Beobachten, <b>Durchleuchten</b> oder andere Arten des Abfangens oder Überwachens oder <b>jegliche Verarbeitung</b> elektronischer <b>Kommunikation</b> durch andere Personen als die Endnutzer sind untersagt.</p>	
<p><b>nicht vorhanden</b></p>	<p><b>(1a)</b> <b>Die Vertraulichkeit elektronischer Kommunikation gilt auch für Daten, die sich auf Endeinrichtungen beziehen oder in ihnen verarbeitet werden.</b></p>	
<p><i>Artikel 6</i></p> <p>Änderung der Überschrift für Artikel 6</p>	<p><i>Artikel 6</i></p> <p>Änderung der Überschrift für Artikel 6</p>	

EU-Kommission	EU-Parlament	EU-Rat
<b>Erlaubte</b> Verarbeitung elektronischer Kommunikationsdaten	<b>Rechtmäßige</b> Verarbeitung elektronischer Kommunikationsdaten	
<p>Artikel 6</p> <p>(1) Betreiber elektronischer Kommunikationsnetze und -dienste dürfen elektronische Kommunikationsdaten <b>verarbeiten</b>, wenn</p>	<p>Artikel 6</p> <p>(1) Betreiber elektronischer Kommunikationsnetze und -dienste dürfen elektronische Kommunikationsdaten <b>nur dann verarbeiten</b>, wenn <b>dies zur Durchführung der Übermittlung der Kommunikation technisch nötig ist, und auch nur für den hierfür erforderlichen Zeitraum.</b></p>	
<p>a) dies zur Durchführung der Übermittlung der Kommunikation nötig ist, für die dazu erforderliche Dauer, oder</p>	<p>a) dies zur Durchführung der Übermittlung der Kommunikation nötig ist, für die dazu erforderliche Dauer, oder</p>	
<p><b>nicht vorhanden</b></p>	<p><b>(1b) Betreiber elektronischer Kommunikationsnetze und -dienste und andere im Auftrag des Betreibers oder Endnutzers handelnde Parteien dürfen elektronische Kommunikationsdaten nur dann verarbeiten, wenn dies technisch nötig ist, um die Verfügbarkeit, Integrität, Vertraulichkeit und Sicherheit des jeweiligen elektronischen Kommunikationsnetzes oder -dienstes aufrechtzuerhalten oder wiederherzustellen, oder um technische Defekte und Fehler bei der Übermittlung der elektronischen Kommunikation zu erkennen, und auch nur für den hierfür erforderlichen Zeitraum.</b></p>	
<p>(2) Betreiber elektronischer Kommunikationsdienste dürfen elektronische Kommunikationsmetadaten verarbeiten, wenn</p>	<p>(2) Betreiber elektronischer Kommunikationsdienste <b>und -netze</b> dürfen elektronische Kommunikationsmetadaten <b>nur</b> verarbeiten, wenn</p>	
<p>a) dies zur Einhaltung verbindlicher Dienstqualitätsanforderungen nach der [Richtlinie über den europäischen Kodex für die elektronische Kommunikation] oder der Verordnung (EU) 2015/2120<sup>28</sup> nötig ist, für <b>die dazu erforderliche</b></p>	<p>a) dies zur Einhaltung verbindlicher Dienstqualitätsanforderungen nach der [Richtlinie über den europäischen Kodex für die elektronische Kommunikation] oder der Verordnung (EU) 2015/2120<sup>28</sup> <b>unbedingt</b> nötig ist, <b>und auch nur</b> für <b>den hierfür technisch er-</b></p>	

EU-Kommission	EU-Parlament	EU-Rat
<b>Dauer</b> , oder	<b>forderlichen Zeitraum</b> , oder	
<p>_____</p> <p><sup>28</sup> 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. 1–18).</p>	<p>_____</p> <p><sup>28</sup> 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. 1–18).</p>	
<p>b) dies zur Rechnungstellung, zur <b>Berechnung</b> von Zusammenschaltungszahlungen, zur Erkennung oder Beendigung <b>betrügerischer oder missbräuchlicher Nutzungen</b> elektronischer Kommunikationsdienste oder der diesbezüglichen Verträge nötig ist, oder</p>	<p>b) dies zur Rechnungstellung, zur <b>Festlegung</b> von Zusammenschaltungszahlungen, zur Erkennung oder Beendigung <b>der betrügerischen Nutzung</b> elektronischer Kommunikationsdienste oder der diesbezüglichen Verträge <b>unbedingt</b> nötig ist, oder</p>	
<p>c) der <b>betreffende Endnutzer</b> seine Einwilligung zur Verarbeitung seiner Kommunikationsmetadaten für einen oder mehrere bestimmte Zwecke gegeben hat, so auch für die Bereitstellung bestimmter Dienste für diese <b>Endnutzer</b>, sofern die <b>betreffenden Zwecke durch eine Verarbeitung anonymisierter Informationen</b> nicht erreicht werden können.</p>	<p>c) der <b>jeweilige Nutzer</b> seine Einwilligung zur Verarbeitung seiner Kommunikationsmetadaten für einen oder mehrere bestimmte Zwecke gegeben hat, so auch für die Bereitstellung bestimmter Dienste für diese <b>Nutzer</b>, sofern die <b>jeweiligen Zwecke ohne die Verarbeitung dieser Metadaten</b> nicht erreicht werden können.</p>	
<p><b>nicht vorhanden</b></p>	<p><b>(2a) Hat eine Form der Verarbeitung elektronischer Kommunikationsmetadaten, insbesondere bei Verwendung neuer Technologien, unter Berücksichtigung der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge, finden für die Zwecke von Absatz 2 Buchstabe c die Artikel 35 und 36 der Verordnung (EU) 2016/679 Anwendung.</b></p>	

EU-Kommission	EU-Parlament	EU-Rat
<p>(3) Betreiber elektronischer Kommunikationsdienste dürfen elektronische Kommunikationsinhalte nur verarbeiten:</p>	<p>(3) Betreiber elektronischer Kommunikationsdienste dürfen elektronische Kommunikationsinhalte nur verarbeiten:</p>	
<p>a) zum alleinigen Zweck der Bereitstellung eines bestimmten <b>Diens-tes für einen Endnutzer</b>, wenn der <b>bzw. die betreffenden Endnutzer ihre</b> Einwilligung zur Verarbeitung <b>ihrer</b> elektronischen Kommunikationsinhalte gegeben <b>haben</b> und die Dienstleistung ohne Verarbeitung dieser Inhalte nicht erbracht werden kann, oder</p>	<p>a) zum alleinigen Zweck der Bereitstellung eines bestimmten, <b>vom Nutzer angeforderten Dienstes</b>, wenn der <b>jeweilige Nutzer seine</b> Einwilligung zur Verarbeitung <b>seiner</b> elektronischen Kommunikationsinhalte gegeben <b>hat</b> und die Dienstleistung ohne Verarbeitung dieser Inhalte <b>vom Anbieter</b> nicht erbracht werden kann, oder</p>	
<p>b) wenn alle <b>betreffenden Endnutzer</b> 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 Aufsichtsbehörde konsultiert hat. Artikel 36 Absätze 2 und 3 der Verordnung (EU) 2016/679 findet auf die Konsultation der Aufsichtsbehörde Anwendung.</p>	<p>b) wenn alle <b>jeweiligen Nutzer</b> 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 Aufsichtsbehörde konsultiert hat; Artikel 36 Absätze 2 und 3 der Verordnung (EU) 2016/679 findet auf die Konsultation der Aufsichtsbehörde Anwendung.</p>	
<p><b>nicht vorhanden</b></p>	<p><b>(3a) Die Betreiber elektronischer Kommunikationsdienste dürfen elektronische Kommunikationsdaten nur für die Bereitstellung eines ausdrücklich angeforderten Dienstes, zum alleinigen Zweck der persönlichen Nutzung, ausschließlich für den hierfür erforderlichen Zeitraum und ohne die Einwilligung aller Nutzer nur dann verarbeiten, wenn durch die angeforderte Verarbeitung die Grundrechte und Interessen eines anderen Nutzers oder mehrerer anderer Nutzer nicht beeinträchtigt werden.</b></p>	
<p>Artikel 7 Speicherung und Löschung elektronischer</p>	<p>Artikel 7 Speicherung und Löschung elektronischer</p>	

EU-Kommission	EU-Parlament	EU-Rat
<p><i>Kommunikationsdaten</i></p> <p>(1) Unbeschadet des Artikels 6 Absatz <b>1 Buchstabe b</b> und des Artikels 6 Absatz 3 Buchstaben a und b löscht der Betreiber des elektronischen Kommunikationsdienstes elektronische Kommunikationsinhalte <b>oder anonymisiert diese Daten</b>, sobald <b>der bzw. die vorgesehenen Empfänger die elektronischen Kommunikationsinhalte erhalten haben</b>. Diese Daten können von den <b>Endnutzern</b> oder von Dritten, die von den <b>Endnutzern</b> mit der Aufzeichnung, Speicherung oder anderweitigen Verarbeitung dieser Daten beauftragt werden, <b>im Einklang mit der Verordnung (EU) 2016/679</b> aufgezeichnet oder gespeichert werden.</p>	<p><i>Kommunikationsdaten</i></p> <p>(1) Unbeschadet des Artikels 6 Absatz <b>1b</b> und des Artikels 6 Absatz 3 Buchstaben a und b löscht der Betreiber des elektronischen Kommunikationsdienstes elektronische Kommunikationsinhalte, sobald <b>sie für die Bereitstellung eines vom Nutzer angeforderten Dienstes nicht mehr benötigt werden</b>. Diese Daten können von den <b>Nutzern</b> oder von Dritten, die von den <b>Nutzern</b> mit der Aufzeichnung, Speicherung oder anderweitigen Verarbeitung dieser Daten beauftragt werden, aufgezeichnet oder gespeichert werden. <b>Die Nutzer dürfen die Daten im Einklang mit der Verordnung (EU) 2016/679 verarbeiten.</b></p>	
<p>(2) Unbeschadet des Artikels 6 Absatz <b>1 Buchstabe b</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 <b>Übermittlung einer Kommunikation</b> nicht mehr benötigt werden.</p>	<p>(2) Unbeschadet des Artikels 6 Absatz <b>1b</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 <b>Bereitstellung eines vom Nutzer angeforderten Dienstes</b> nicht mehr benötigt werden.</p>	
<p>(3) Erfolgt die Verarbeitung elektronischer Kommunikationsmetadaten zu Abrechnungszwecken im Einklang mit Artikel 6 Absatz 2 Buchstabe b, so dürfen die <b>betreffenden</b> 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.</p>	<p>(3) Erfolgt die Verarbeitung elektronischer Kommunikationsmetadaten zu Abrechnungszwecken im Einklang mit Artikel 6 Absatz 2 Buchstabe b, so dürfen die <b>zwingend notwendigen</b> 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.</p>	
<p><i>Artikel 8</i></p> <p>Änderung der Überschrift für Artikel 8</p> <p>Schutz <b>der in</b> Endeinrichtungen der <b>Endnutzer gespeicherten oder sich</b></p>	<p><i>Artikel 8</i></p> <p>Änderung der Überschrift für Artikel 8</p> <p>Schutz <b>von Informationen, die an</b> Endeinrichtungen der <b>Nutzer über-</b></p>	

EU-Kommission	EU-Parlament	EU-Rat
<p><b>auf diese beziehenden Informationen</b></p>	<p><b>tragen werden, dort gespeichert werden, sich darauf beziehen, dort verarbeitet werden oder daraus erhoben werden</b></p>	
<p>Artikel 8</p> <p>(1) Jede vom <b>betreffenden Endnutzer</b> 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:</p>	<p>Artikel 8</p> <p>(1) Jede vom <b>jeweiligen Nutzer</b> 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:</p>	
<p>a) sie ist für den alleinigen Zweck der Durchführung eines elektronischen Kommunikationsvorgangs über ein elektronisches Kommunikationsnetz nötig oder</p>	<p>a) sie ist für den alleinigen Zweck der Durchführung eines elektronischen Kommunikationsvorgangs über ein elektronisches Kommunikationsnetz <b>unbedingt</b> nötig oder</p>	
<p>b) der <b>Endnutzer</b> hat seine Einwilligung gegeben oder</p>	<p>b) der <b>Nutzer</b> hat seine <b>ausdrückliche</b> Einwilligung gegeben oder</p>	
<p>c) sie ist für die Bereitstellung eines vom <b>Endnutzer gewünschten</b> Dienstes der Informationsgesellschaft nötig oder</p>	<p>c) sie ist für die Bereitstellung eines vom <b>Nutzer ausdrücklich angeforderten</b> Dienstes der Informationsgesellschaft <b>technisch zwingend</b> nötig oder</p>	
<p>d) sie ist für die Messung des <b>Webpublikums</b> nötig, sofern <b>der</b> Betreiber <b>des vom Endnutzer gewünschten Dienstes der Informationsgesellschaft diese Messung durchführt.</b></p>	<p>d) sie ist für die Messung <b>der Reichweite</b> des <b>vom Nutzer angeforderten Dienstes der Informationsgesellschaft technisch</b> nötig, sofern <b>diese Messung vom Betreiber oder in seinem Namen oder von einer unabhängigen Webanalyseagentur durchgeführt wird, die im öffentlichen Interesse – auch für wissenschaftliche Zwecke – tätig ist, sofern die Daten aggregiert sind und der Nutzer die Möglichkeit hat, der Nutzung zu widersprechen, und sofern personenbezogene Daten keinem</b></p>	

EU-Kommission	EU-Parlament	EU-Rat
	<p><i>Dritten zugänglich gemacht und die Grundrechte des Nutzers durch diese Messung nicht beeinträchtigt werden, und falls eine Publikumsmessung im Namen eines Betreibers von Diensten der Informationsgesellschaft durchgeführt wird, dürfen die erhobenen Daten nur von diesem Betreiber verarbeitet werden und müssen getrennt von den Daten aufbewahrt werden, die bei Publikumsmessungen erhoben wurden, die im Namen anderer Betreiber durchgeführt werden, oder</i></p>	
<p><i>nicht vorhanden</i></p>	<p><i>da) sie ist nötig, um Sicherheit, Vertraulichkeit, Integrität, Verfügbarkeit und Authentizität der Endeinrichtungen des Endnutzers zu wahren, und zwar durch Aktualisierungen und für den hierfür erforderlichen Zeitraum, sofern</i></p> <ul style="list-style-type: none"> <li><i>i) dadurch in keiner Weise die Funktionsweise der Hardware oder Software geändert wird oder die vom Nutzer festgelegten Einstellungen zum Schutz der Privatsphäre geändert werden,</i></li> <li><i>ii) der Nutzer bei jeder Installation einer Aktualisierung im Voraus informiert wird und</i></li> <li><i>iii) der Nutzer die Möglichkeit hat, die automatische Installation dieser Aktualisierungen zu verschieben oder auszuschalten,</i></li> </ul>	
<p><i>nicht vorhanden</i></p>	<p><i>db) sie ist im Rahmen von Arbeitsverhältnissen für die Erfüllung einer von einem Arbeitnehmer wahrzunehmenden Aufgabe technisch zwingend nötig, sofern</i></p> <ul style="list-style-type: none"> <li><i>i) der Arbeitgeber die Endeinrichtung bereitstellt bzw. deren Nutzer ist,</i></li> <li><i>ii) der Arbeitnehmer der Nutzer der</i></li> </ul>	

EU-Kommission	EU-Parlament	EU-Rat
	<p><b>Endeinrichtung ist und</b></p> <p><b>iii) sie überdies nicht der Überwachung des Arbeitnehmers dient.</b></p>	
<p><b>nicht vorhanden</b></p>	<p><b>(1a) Unabhängig davon, ob es sich um einen vergüteten Dienst handelt, darf keinem Nutzer der Zugang zu einem Dienst oder einem Funktionselement der Informationsgesellschaft mit der Begründung verweigert werden, er habe seine Einwilligung in die Verarbeitung personenbezogener Daten bzw. in die zur Bereitstellung dieses Dienstes oder dieses Funktionselements nicht erforderliche Nutzung von Verarbeitungs- oder Speicherkapazitäten seiner Endeinrichtung nach Artikel 8 Absatz 1 Buchstabe b nicht gegeben.</b></p>	
<p>(2) Die <b>Erhebung</b> von Informationen, die von Endeinrichtungen ausgesendet werden, um sich mit anderen Geräten oder mit Netzanlagen verbinden zu können, ist untersagt, außer</p>	<p>(2) Die <b>Verarbeitung</b> von Informationen, die von Endeinrichtungen ausgesendet werden, um sich mit anderen Geräten oder mit Netzanlagen verbinden zu können, ist untersagt, außer</p>	
<p>a) sie erfolgt ausschließlich zum Zwecke der Herstellung einer Verbindung und für <b>die dazu erforderliche Dauer</b> oder</p>	<p>a) sie erfolgt ausschließlich <b>und</b> zum <b>alleinigen</b> Zwecke der Herstellung einer <b>vom Nutzer angeforderten</b> Verbindung, und <b>auch nur</b> für <b>den hierfür erforderlichen Zeitraum</b>, oder</p>	
<p><b>nicht vorhanden</b></p>	<p><b>aa) der Nutzer wurde informiert und hat seine Einwilligung gegeben oder</b></p>	
<p><b>nicht vorhanden</b></p>	<p><b>ab) die Risiken werden eingedämmt.</b></p>	
<p><b>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</b></p>	<p><b>entfällt</b></p>	



EU-Kommission	EU-Parlament	EU-Rat
<p><b>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.</b></p> <p><b>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.</b></p>		
<p><b>nicht vorhanden</b></p>	<p><b>(2a) Für die Zwecke von Absatz 1 Buchstabe d und Absatz 2 Buchstabe ab werden zur Eindämmung der Risiken die folgenden Vorkehrungen getroffen:</b></p> <ul style="list-style-type: none"> <li><b>a) Daten aus der Endeinrichtung werden ausschließlich für statistische Zählungen erhoben,</b></li> <li><b>b) die Verarbeitung ist zeitlich und örtlich auf das für diesen Zweck ausdrücklich notwendige Maß beschränkt,</b></li> <li><b>c) die Daten werden unverzüglich nach Erfüllung des Zwecks gelöscht oder anonymisiert, und</b></li> <li><b>d) die Nutzer erhalten wirksame Widerspruchsmöglichkeiten, durch die das Funktionieren der Endeinrichtungen nicht beeinträchtigt wird.</b></li> </ul>	
<p><b>nicht vorhanden</b></p>	<p><b>(2b) Die Informationen nach Absatz 2 Buchstaben aa und ab werden in einer klaren und auffälligen Mitteilung vermittelt, in der mindestens näher beschrieben wird, wie die Informationen erhoben werden, zu welchem Zweck die Verarbeitung erfolgt und welche Person dafür zuständig ist, und in der weitere Angaben gemacht werden, die nach Artikel 13 der Verordnung (EU) 2016/679 in Fäl-</b></p>	

EU-Kommission	EU-Parlament	EU-Rat
	<p><i>len erforderlich sind, in denen personenbezogene Daten erhoben werden. Voraussetzung für die Erhebung solcher Informationen ist die Anwendung geeigneter technischer und organisatorischer Maßnahmen, mit denen ein dem Risiko angemessenes Schutzniveau nach Artikel 32 der Verordnung (EU) 2016/679 sichergestellt wird.</i></p>	
<p>(3) Die nach Absatz <b>2 Buchstabe b</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.</p>	<p>(3) Die nach Absatz <b>2b</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.</p>	
<p>(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.</p>	<p>(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.</p>	
<p><i>Artikel 9</i> <i>Einwilligung</i></p> <p>(1) Für die Einwilligung gelten die Begriffsbestimmung und die Voraussetzungen, die in <b>Artikel 4 Nummer 11 und Artikel 7</b> der Verordnung (EU) 2016/679 festgelegt sind.</p>	<p><i>Artikel 9</i> <i>Einwilligung</i></p> <p>(1) Für die Einwilligung gelten die Begriffsbestimmung und die Voraussetzungen, die in der Verordnung (EU) 2016/679 festgelegt sind.</p>	
<p>(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 – <b>in den passenden</b> technischen <b>Einstellungen einer Software, die den Zugang zum Internet ermöglicht</b>, gegeben werden.</p>	<p>(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 – <b>unter Verwendung der</b> technischen <b>Spezifikationen für elektronische Kommunikationsdienste oder Dienste der Informationsgesellschaft, die eine bestimmte Einwilligung zu bestimmten Zwecken ermöglichen, sowie in</b></p>	

EU-Kommission	EU-Parlament	EU-Rat
	<p><b>Bezug auf bestimmte Diensteanbieter, die gemäß Absatz 1 von den Nutzern in allen Fällen aktiv ausgewählt wurden, gegeben oder widerrufen werden. Wenn diese technischen Spezifikationen von der Endeinrichtung des Nutzers oder der dort installierten Software verwendet werden, können sie auf der Grundlage der vorherigen aktiven Entscheidungen des Nutzers auf seine Auswahl hinweisen. Diese Hinweise sind für alle anderen Parteien verbindlich und ihnen gegenüber durchsetzbar.</b></p>	
<p>(3) <b>Endnutzern</b>, 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; <b>sie werden in regelmäßigen Abständen von sechs Monaten an diese Möglichkeit erinnert</b>, solange die Verarbeitung andauert.</p>	<p>(3) <b>Nutzern</b>, die ihre Einwilligung zur Verarbeitung elektronischer Kommunikationsdaten nach Artikel 6 Absatz 2 Buchstabe c und Artikel 6 Absatz 3 Buchstaben a und b, <b>Artikel 8 Absatz 1 Buchstabe b und Artikel 8 Absatz 2 Buchstabe aa</b> gegeben haben, wird nach Artikel 7 Absatz 3 der Verordnung (EU) 2016/679 die Möglichkeit eingeräumt, ihre Einwilligung jederzeit zu widerrufen, solange die Verarbeitung andauert.</p>	
<p><b>nicht vorhanden</b></p>	<p><b>(3a) Die auf einer Einwilligung beruhende Verarbeitung darf sich nicht nachteilig auf die Rechte und Freiheiten von Einzelpersonen – insbesondere ihr Recht auf Privatsphäre und auf Schutz personenbezogener Daten – auswirken, deren personenbezogene Daten mit einer Kommunikation in Verbindung stehen oder in ihrem Rahmen übermittelt werden.</b></p>	
<p>Artikel 10</p> <p>Bereitzustellende Informationen und Einstellungsmöglichkeiten zur Privatsphäre</p> <p>(1) In Verkehr gebrachte Software, die <b>eine</b> elektronische Kommunikation <b>erlaubt</b>, darunter auch das Abrufen und Darstellen von Informationen aus</p>	<p>Artikel 10</p> <p>Bereitzustellende Informationen und Einstellungsmöglichkeiten zur Privatsphäre</p> <p>(1) In Verkehr gebrachte Software, die elektronische Kommunikation <b>ermöglicht</b>, darunter auch das Abrufen und Darstellen von Informationen</p>	

EU-Kommission	EU-Parlament	EU-Rat
<p>dem Internet, muss <b>die Möglichkeit bieten zu verhindern, dass Dritte Informationen in der Endeinrichtung eines Endnutzers speichern oder bereits in der Endeinrichtung gespeicherte Informationen verarbeiten.</b></p>	<p>aus dem Internet, muss</p>	
<p><b>nicht vorhanden</b></p>	<p><b>a) in der Voreinstellung aktivierte Einstellungen zum Schutz der Privatsphäre aufweisen, durch die verhindert wird, dass andere Parteien außer zu den in Artikel 8 Absatz 1 Buchstaben a und c genannten Zwecken Informationen an die Endeinrichtung eines Nutzers übermitteln, dort speichern oder bereits dort gespeicherte oder von dort erhobene Informationen verarbeiten,</b></p>	
<p><b>nicht vorhanden</b></p>	<p><b>b) nach der Installation den Nutzer informieren und ihm die Möglichkeit bieten, die nach Buchstabe a festgelegten Einstellungen zum Schutz der Privatsphäre zu ändern oder zu bestätigen, indem er aufgefordert wird, in eine Einstellung einzuwilligen, und indem ihm die Möglichkeit geboten wird, zu verhindern, dass andere Parteien zu den in Artikel 8 Absatz 1 Buchstaben a, c, d und da genannten Zwecken Informationen verarbeiten, die an die Endeinrichtung übermittelt werden, bereits dort gespeichert sind oder von dort erhoben werden,</b></p>	
<p><b>nicht vorhanden</b></p>	<p><b>c) dem Nutzer die Möglichkeit bieten, nach der Installation der Software mittels der Einstellungen eine ausdrückliche Einwilligung zu geben.</b></p>	
<p><b>nicht vorhanden</b></p>	<p><b>Artikel 10 – Absatz 1 – Unterabsatz 1</b>  <b>Vor der ersten Verwendung der Software muss der Nutzer von der Software über die Privatsphäre ein-</b></p>	

EU-Kommission	EU-Parlament	EU-Rat
	<p><i>stellungen und die je nach dem aufgerufenen Dienst der Informationsgesellschaft verfügbaren detaillierten Einstellungsoptionen informiert werden. Bei der Verwendung der Software müssen die Einstellungen leicht zugänglich und so gestaltet sein, dass die Nutzer in der Lage sind, eine fundierte Entscheidung zu treffen.</i></p>	
<b>nicht vorhanden</b>	<b>(1a) Für die Zwecke</b>	
<b>nicht vorhanden</b>	<b>a) des Absatzes 1 Buchstaben a und b,</b>	
<b>nicht vorhanden</b>	<b>b) der Erteilung oder des Widerrufs der Einwilligung nach Artikel 9 Absatz 2 dieser Verordnung und</b>	
<b>nicht vorhanden</b>	<b>c) des Widerspruchs gegen die Verarbeitung personenbezogener Daten nach Artikel 21 Absatz 5 der Verordnung (EU) 2016/679</b>	
<b>nicht vorhanden</b>	<p><b>Artikel 10 – Absatz 1 a – Unterabsatz 1</b></p> <p><i>wird aufgrund der Einstellungen ein auf den technischen Spezifikationen beruhender Hinweis ausgelöst, der den anderen Parteien übermittelt wird, damit sie über die Absicht des Nutzers, einzuwilligen oder Widerspruch einzulegen, informiert werden, wobei dieser Hinweis für alle anderen Parteien gilt und für sie verbindlich und ihnen gegenüber durchsetzbar ist.</i></p>	
<b>nicht vorhanden</b>	<b>(1b) Im Einklang mit Artikel 9 Absatz 2 muss in der Software sichergestellt sein, dass es dem Nutzer von einem bestimmten Dienst der Informationsgesellschaft ermöglicht wird, seine ausdrückliche Einwilligung zu geben. Die ausdrückliche Einwilligung eines Nutzers im Sinne von Artikel 8 Ab-</b>	

EU-Kommission	EU-Parlament	EU-Rat
	<p><i>satz 1 Buchstabe b hat für diesen bestimmten Dienst der Informationsgesellschaft Vorrang vor den vorhandenen Einstellungen zum Schutz der Privatsphäre. Unbeschadet des Absatzes 1 kann, sofern der Datenschutzausschuss eine bestimmte Technologie zugelassen hat, für die Zwecke des Artikels 8 Absatz 1 Buchstabe b die Einwilligung jederzeit – sowohl in der Endeinrichtung als auch mittels von dem bestimmten Dienst der Informationsgesellschaft bereitgestellter Verfahren – erteilt oder widerrufen werden.</i></p>	
<p><i>(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.</i></p>	<p><i>entfällt</i></p>	
<p><i>(3) Bei Software, die am <b>25. Mai 2018</b> bereits installiert ist, müssen die Anforderungen der Absätze 1 und 2 zum Zeitpunkt der ersten Aktualisierung der Software, jedoch spätestens <b>ab dem 25. August 2018</b> erfüllt werden.</i></p>	<p><i>(3) Bei Software, die am <b>[xx.xx.xxxx]</b> bereits installiert ist, müssen die Anforderungen der Absätze 1, <b>1a</b> und <b>1b</b> zum Zeitpunkt der ersten Aktualisierung der Software, jedoch spätestens <b>sechs Monate nach dem [Datum des Inkrafttretens dieser Verordnung]</b> erfüllt werden.</i></p>	
<p><i>Artikel 11</i></p> <p><i>Beschränkungen</i></p> <p><i>(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)</i></p>	<p><i>entfällt</i></p>	

EU-Kommission	EU-Parlament	EU-Rat
<p><b>2016/679 genannten allgemeinen öffentlichen Interessen zu wahren oder Überwachungs-, Kontroll- oder Regulierungsaufgaben, die mit der Ausübung öffentlicher Gewalt verbunden sind, wahrzunehmen.</b></p> <p><b>(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.</b></p>		
<p><b>nicht vorhanden</b></p>	<p>Artikel 11a</p> <p>Beschränkungen der Nutzerrechte</p> <p><b>(1) Durch die von der Union oder von den Mitgliedstaaten erlassenen Rechtsvorschriften, denen der Betreiber unterliegt, können im Wege einer Gesetzgebungsmaßnahme der Umfang der Pflichten und Grundsätze in Bezug auf die Verarbeitung elektronischer Kommunikationsdaten nach den Artikeln 6, 7 und 8 dieser Verordnung beschränkt werden, soweit die Bestimmungen den Rechten und Pflichten nach der Verordnung (EU) 2016/679 entsprechen und sofern im Rahmen einer solchen Beschränkung der Wesensgehalt der Grundrechte und Grundfreiheiten uneingeschränkt geachtet wird und die Beschränkung in einer demokratischen Gesellschaft eine notwendige, angemessene und verhältnismäßige Maßnahme ist, mit der ein oder mehrere der allgemeinen öffentlichen Interessen nach Artikel 23 Absatz 1 Buchstaben a bis d der Verordnung (EU) 2016/679 geschützt werden.</b></p> <p><b>(2) Insbesondere müssen Gesetzge-</b></p>	

EU-Kommission	EU-Parlament	EU-Rat
	<p><b>Maßnahmen im Sinne von Absatz 1 im Bedarfsfall zumindest Vorschriften nach Artikel 23 Absatz 2 der Verordnung (EU) 2016/679 enthalten.</b></p>	
<p><b>nicht vorhanden</b></p>	<p>Artikel 11b</p> <p>Beschränkungen der Vertraulichkeit von Mitteilungen</p> <p><b>(1) Die Union oder die Mitgliedstaaten können im Wege von Gesetzgebungsmaßnahmen den Umfang der in Artikel 5 festgelegten Rechte beschränken, sofern im Rahmen einer solchen Beschränkung der Wesensgehalt der Grundrechte und Grundfreiheiten uneingeschränkt geachtet wird und die Beschränkung in einer demokratischen Gesellschaft eine notwendige, angemessene und verhältnismäßige Maßnahme ist, mit der ein oder mehrere der folgenden allgemeinen öffentlichen Interessen geschützt werden:</b></p> <ul style="list-style-type: none"> <li><b>a) die nationale Sicherheit,</b></li> <li><b>b) die Verteidigung,</b></li> <li><b>c) die öffentliche Sicherheit,</b></li> <li><b>d) die Verhütung, Ermittlung, Aufdeckung oder Verfolgung schwerer Straftaten oder des unzulässigen Gebrauchs von elektronischen Kommunikationssystemen oder die Strafverfolgung, was den Schutz vor und die Abwehr von Gefahren für die öffentliche Sicherheit umfasst.</b></li> </ul> <p><b>(2) Insbesondere müssen Gesetzgebungsmaßnahmen im Sinne von Absatz 1 im Bedarfsfall zumindest Vorschriften nach Artikel 23 Absatz 2 der Verordnung (EU) 2016/679 enthalten.</b></p>	
<p><b>nicht vorhanden</b></p>	<p>Artikel 11c</p> <p>Dokumentations- und Berichterstattungspflichten bei Beschränkungen</p>	



EU-Kommission	EU-Parlament	EU-Rat
	<p><b>(1) Die Anbieter elektronischer Kommunikationsdienste bewahren Unterlagen im Zusammenhang mit Anträgen von zuständigen Behörden auf Zugang zu Kommunikationsinhalten gemäß Artikel 11b Absatz 2 auf. Diese Unterlagen umfassen bei jedem Antrag Angaben zu</b></p> <ul style="list-style-type: none"> <li><b>a) den internen Mitarbeitern, die den Antrag bearbeitet haben,</b></li> <li><b>b) der Bezeichnung der Stelle, die den Antrag stellt,</b></li> <li><b>c) dem Zweck, zu dem die Informationen angefordert wurden,</b></li> <li><b>d) Datum und Uhrzeit des Antrags,</b></li> <li><b>e) der Rechtsgrundlage und der Befugnis für den Antrag, einschließlich der Identität und der Stellung oder Funktion des Beamten, der den Antrag übermittelt hat,</b></li> <li><b>f) der richterlichen Genehmigung des Antrags,</b></li> <li><b>g) der Anzahl der Nutzer, auf deren Daten sich der Antrag bezieht,</b></li> <li><b>h) den Daten, die der antragstellenden Behörde zur Verfügung gestellt werden, und</b></li> <li><b>i) dem von den Daten erfassten Zeitraum.</b></li> </ul> <p><b>Die Unterlagen werden der zuständigen Aufsichtsbehörde auf Antrag zur Verfügung gestellt.</b></p> <p><b>(2) Anbieter elektronischer Kommunikationsdienste veröffentlichen einmal jährlich einen Bericht mit statistischen Angaben zu Anträgen auf Zugang zu Daten durch Strafverfolgungsbehörden gemäß den Artikeln 11a und 11b. Der Bericht enthält zumindest folgende Angaben:</b></p> <ul style="list-style-type: none"> <li><b>a) die Zahl der Anträge,</b></li> <li><b>b) die Zweckkategorien der Anträge,</b></li> </ul>	

EU-Kommission	EU-Parlament	EU-Rat
	<p><i>ge,</i></p> <p><i>c) die Kategorien der angeforderten Daten,</i></p> <p><i>d) die Rechtsgrundlage und die Befugnis für die Anträge,</i></p> <p><i>e) die Anzahl der Nutzer, auf deren Daten sich die Anträge beziehen,</i></p> <p><i>f) den von den Daten erfassten Zeitraum,</i></p> <p><i>g) die Anzahl negativer und positiver Antworten auf die Anträge.</i></p> <p><b>(3) Die zuständigen Behörden der Mitgliedstaaten veröffentlichen einmal jährlich einen Bericht mit monatlichen statistischen Angaben zu Anträgen auf Zugang zu Daten gemäß den Artikeln 11a und 11b, darunter zu Anträgen, für die keine richterliche Genehmigung erteilt wurde, und zwar unter anderem zu folgenden Elementen:</b></p> <p><i>a) der Zahl der Anträge,</i></p> <p><i>b) den Zweckkategorien der Anträge,</i></p> <p><i>c) den Kategorien der angeforderten Daten,</i></p> <p><i>d) der Rechtsgrundlage und der Befugnis für die Anträge,</i></p> <p><i>e) der Anzahl der Nutzer, auf deren Daten sich die Anträge beziehen,</i></p> <p><i>f) dem von den Daten erfassten Zeitraum,</i></p> <p><i>g) der Anzahl abgelehnter und genehmigter Anträge.</i></p> <p><b>Außerdem enthält der Bericht monatliche statistische Angaben zu etwaigen weiteren Beschränkungen gemäß den Artikeln 11a und 11b.</b></p>	

EU-Kommission	EU-Parlament	EU-Rat
<h3 style="margin: 0;">Kapitel III</h3> <h2 style="margin: 0;">RECHTE NATÜRLICHER UND JURISTISCHER PERSONEN IN BEZUG AUF DIE KONTROLLE ÜBER IHRE ELEKTRONISCHE KOMMUNIKATION</h2>		
<p><i>Artikel 12</i></p> <p><i>Anzeige der Rufnummer des Anrufers und des Angerufenen und deren Unterdrückung</i></p> <p>(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:</p> <ul style="list-style-type: none"> <li>a) für den anrufenden Endnutzer die Möglichkeit, die Anzeige seiner Rufnummer für einen einzelnen Anruf, für eine bestimmte Verbindung oder dauerhaft zu verhindern;</li> <li>b) für den angerufenen Endnutzer die Möglichkeit, die Rufnummernanzeige für eingehende Anrufe zu verhindern;</li> <li>c) für den angerufenen Endnutzer die Möglichkeit, eingehende Anrufe, bei denen die Rufnummernanzeige durch den anrufenden Endnutzer verhindert wurde, abzuweisen;</li> <li>d) für den angerufenen Endnutzer die Möglichkeit, die Anzeige seiner Rufnummer beim anrufenden Endnutzer zu verhindern.</li> </ul> <p>(2) Die in Absatz 1 Buchstaben a, b, c und d genannten Möglichkeiten werden Endnutzern auf einfache Weise und kostenlos bereitgestellt.</p> <p>(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</p>	<p><i>Artikel 12</i></p> <p><i>Anzeige der Rufnummer des Anrufers und des Angerufenen und deren Unterdrückung</i></p> <p>(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:</p> <ul style="list-style-type: none"> <li>a) für den anrufenden Endnutzer die Möglichkeit, die Anzeige seiner Rufnummer für einen einzelnen Anruf, für eine bestimmte Verbindung oder dauerhaft zu verhindern;</li> <li>b) für den angerufenen Endnutzer die Möglichkeit, die Rufnummernanzeige für eingehende Anrufe zu verhindern;</li> <li>c) für den angerufenen Endnutzer die Möglichkeit, eingehende Anrufe, bei denen die Rufnummernanzeige durch den anrufenden Endnutzer verhindert wurde, abzuweisen;</li> <li>d) für den angerufenen Endnutzer die Möglichkeit, die Anzeige seiner Rufnummer beim anrufenden Endnutzer zu verhindern.</li> </ul> <p>(2) Die in Absatz 1 Buchstaben a, b, c und d genannten Möglichkeiten werden Endnutzern auf einfache Weise und kostenlos bereitgestellt.</p> <p>(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</p>	

EU-Kommission	EU-Parlament	EU-Rat
<p>eingehende Anrufe.</p> <p>(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.</p>	<p>dem eingehende Anrufe.</p> <p>(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.</p>	
<p><i>Artikel 13</i></p> <p><i>Ausnahmen für die Anzeige der Rufnummer des Anrufers und des Angerufenen und deren Unterdrückung</i></p> <p>(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.</p>	<p><i>Artikel 13</i></p> <p><i>Ausnahmen für die Anzeige der Rufnummer des Anrufers und des Angerufenen und deren Unterdrückung</i></p> <p>(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.</p>	
<p>(2) <b>Die Mitgliedstaaten legen spezifische Bestimmungen</b> in Bezug auf die Einrichtung von Verfahren und die Umstände <b>fest</b>, unter denen Betreiber öffentlich zugänglicher nummerngebundener interpersoneller Kommunikationsdienste die Unterdrückung der Anzeige der Rufnummer des Anrufers vorübergehend aufheben <b>sollen</b>, wenn <b>Endnutzer</b> beantragen, dass böswillige oder belästigende Anrufe zurückverfolgt werden.</p>	<p>(2) <b>Der Kommission wird die Befugnis übertragen, nach Artikel 26 Absatz 1 Durchführungsmaßnahmen</b> in Bezug auf die Einrichtung von Verfahren und die Umstände <b>zu erlassen</b>, unter denen Betreiber öffentlich zugänglicher nummerngebundener interpersoneller Kommunikationsdienste die Unterdrückung der Anzeige der Rufnummer des Anrufers vorübergehend aufheben <b>müssen</b>, wenn <b>Nutzer</b> beantragen, dass böswillige oder belästigende Anrufe zurückverfolgt werden.</p>	

EU-Kommission	EU-Parlament	EU-Rat
<p><i>Artikel 14</i></p> <p><i>Sperrung eingehender Anrufe</i></p> <p>Die Betreiber öffentlich zugänglicher nummergebundener interpersoneller Kommunikationsdienste <b>treffen Maßnahmen, die dem Stand der Technik entsprechen, um den Erhalt unerwünschter Anrufe durch Endnutzer zu beschränken, und</b> stellen den angerufenen Endnutzern <b>außerdem</b> folgende Möglichkeiten kostenlos zur Verfügung:</p>	<p><i>Artikel 14</i></p> <p><i>Sperrung eingehender Anrufe</i></p> <p>Die Betreiber öffentlich zugänglicher nummergebundener interpersoneller Kommunikationsdienste stellen den angerufenen Endnutzern folgende Möglichkeiten kostenlos zur Verfügung:</p>	
<p>a) Sperrung eingehender Anrufe von bestimmten Rufnummern oder von anonymen Quellen;</p>	<p>a) Sperrung eingehender Anrufe von bestimmten Rufnummern, <b>Rufnummern mit einem bestimmten Code oder einer bestimmten Vorwahl, an dem bzw. der sich erkennen lässt, dass es sich um einen Werbeanruf nach Artikel 16 Absatz 3 Buchstabe b handelt</b>, oder von anonymen Quellen;</p>	
<p>b) Abstellung einer von einem Dritten veranlassten automatischen Anrufweitschaltung zur Endrichtung des <b>Endnutzers</b>.</p>	<p>b) Abstellung einer von einem Dritten veranlassten automatischen Anrufweitschaltung zur Endrichtung des <b>Nutzers</b>.</p>	
<p><i>Artikel 15</i></p> <p><i>Öffentlich zugängliche Verzeichnisse</i></p> <p>(1) <b>Die Betreiber öffentlich zugänglicher Verzeichnisse</b> holen die Einwilligung der <b>Endnutzer, die natürliche Personen sind</b>, in die Aufnahme ihrer personenbezogenen Daten in das Verzeichnis und folglich die Einwilligung dieser <b>Endnutzer</b> in die Aufnahme von Daten nach Kategorien personenbezogener Daten ein, soweit diese Daten für den <b>vom Anbieter des Verzeichnisses angegebenen Zweck</b> relevant sind. Die <b>Betreiber geben Endnutzern, die natürliche Personen sind</b>, die Möglichkeit, die</p>	<p><i>Artikel 15</i></p> <p><i>Öffentlich zugängliche Verzeichnisse</i></p> <p>(1) <b>Unbeschadet der Artikel 12 bis 22 der Verordnung (EU) 2016/679</b> holen die <b>Anbieter eines elektronischen Kommunikationsdienstes</b> die Einwilligung der <b>Nutzer</b> in die Aufnahme ihrer personenbezogenen Daten in das <b>öffentlich zugängliche</b> Verzeichnis und folglich die Einwilligung dieser <b>Nutzer</b> in die Aufnahme von Daten nach Kategorien personenbezogener Daten ein, soweit diese Daten für den <b>Zweck</b> des Verzeichnisses relevant sind. Die <b>Anbieter elektronischer Kommunikati-</b></p>	

EU-Kommission	EU-Parlament	EU-Rat
<p>Daten zu überprüfen, zu berichtigen und zu löschen.</p>	<p><b>onsdienste geben den Nutzern</b> die Möglichkeit, die Daten zu überprüfen, zu berichtigen, <b>zu aktualisieren, zu ergänzen</b> und zu löschen. <b>Erhalten Anbieter elektronischer Kommunikationsdienste die Einwilligung der Nutzer, so stellen sie Anbietern öffentlicher Verzeichnisse die Nutzerdaten unverzüglich, diskriminierungsfrei und in fairer Weise zur Verfügung</b></p>	
<p>(2) Die Betreiber öffentlich zugänglicher Verzeichnisse informieren <b>Endnutzer, die natürliche Personen sind</b> und deren personenbezogene Daten in das Verzeichnis aufgenommen worden sind, über die verfügbaren Suchfunktionen des Verzeichnisses und <b>holen die Einwilligung der Endnutzer ein, bevor sie</b> diese Suchfunktionen in Bezug auf <b>deren</b> Daten <b>aktivieren</b>.</p>	<p>(2) Die Betreiber öffentlich zugänglicher Verzeichnisse informieren <b>Nutzer</b>, deren personenbezogene Daten in das Verzeichnis aufgenommen worden sind, über die verfügbaren Suchfunktionen des Verzeichnisses und <b>geben ihnen die Möglichkeit</b>, diese Suchfunktionen in Bezug auf <b>ihre</b> Daten <b>zu deaktivieren</b>.</p>	
<p>(3) Die Betreiber <b>öffentlich zugänglicher Verzeichnisse</b> 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.</p>	<p>(3) Die Betreiber <b>elektronischer Kommunikationsdienste</b> räumen Endnutzern, die juristische Personen sind, die Möglichkeit ein, der Aufnahme von auf sie bezogenen Daten in das Verzeichnis zu widersprechen. Die Betreiber <b>elektronischer Kommunikationsdienste</b> geben solchen Endnutzern, die juristische Personen sind, die Möglichkeit, die Daten zu überprüfen, zu berichtigen und zu löschen. <b>Für die Zwecke dieses Artikels sind natürliche Personen, die in beruflicher Eigenschaft handeln, beispielsweise Freiberufler, Klein- und gewerbetreibende oder freie Mitarbeiter, hinsichtlich ihrer Daten über ihre berufliche Eigenschaft juristischen Personen gleichgestellt.</b></p>	
<p>(4) <b>Die</b> Möglichkeit der <b>Endnutzer</b>, nicht in ein öffentlich zugängliches Verzeichnis aufgenommen zu werden und alle Daten, die sich auf sie beziehen, zu überprüfen, zu berichtigen und zu löschen, <b>wird</b> kostenlos zur Verfügung gestellt.</p>	<p>(4) <b>Unbeschadet des Artikels 12 Absatz 5 der Verordnung (EU) 2016/679 werden den Nutzern die Informationen und die</b> Möglichkeit der <b>Nutzer</b>, nicht in ein öffentlich zugängliches Verzeichnis aufgenommen zu werden, und alle Daten, die sich auf sie beziehen, zu überprüfen, zu berichtigen, <b>zu aktualisieren, zu ergänzen</b> und zu löschen, <b>von den</b></p>	

EU-Kommission	EU-Parlament	EU-Rat
	<p><b>Anbietern elektronischer Kommunikationsdienste</b> kostenlos <b>und in leicht zugänglicher Weise</b> zur Verfügung gestellt.</p>	
<p>nicht vorhanden</p>	<p><b>(4a) Wurden personenbezogene Daten von Nutzern nummerngebundener interpersoneller Kommunikationsdienste vor dem Inkrafttreten der vorliegenden Verordnung in ein öffentlich zugängliches Verzeichnis aufgenommen, so dürfen die personenbezogenen Daten solcher Nutzer in einem öffentlich zugänglichen Verzeichnis, auch in Versionen mit Suchfunktionen, verbleiben, es sei denn, die Nutzer haben der Aufnahme ihrer Daten in das Verzeichnis oder ihre Daten betreffenden Suchfunktionen widersprochen.</b></p>	
<p>Artikel 16</p> <p><i>Unerbetene Kommunikation</i></p> <p>(1) Natürliche oder juristische Personen <b>können Direktwerbung über elektronische Kommunikationsdienste an Endnutzer richten, die natürliche Personen sind und hierzu</b> ihre Einwilligung gegeben haben.</p>	<p>Artikel 16</p> <p><i>Unerbetene Kommunikation</i></p> <p>(1) <b>Die Nutzung elektronischer Kommunikationsdienste durch</b> natürliche oder juristische Personen, <b>beispielsweise automatische Anrufe, Kommunikationssysteme, halbautomatische Systeme, die den Anrufer mit einer Person verbinden, Faxe, E-Mails oder eine sonstige Nutzung elektronischer Kommunikationsdienste für das Anbieten oder Übermitteln von Direktwerbung an Nutzer ist nur bei Nutzern zulässig, die zuvor</b> ihre Einwilligung gegeben haben.</p>	
<p>(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 <b>ähnliche</b> Produkte oder Dienstleistungen nur dann verwenden, wenn die Kunden klar und deutlich</p>	<p>(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 Produkte oder Dienstleistungen nur dann verwenden, wenn die Kunden klar und deutlich die Möglichkeit</p>	

EU-Kommission	EU-Parlament	EU-Rat
<p>die Möglichkeit haben, einer solchen Nutzung kostenlos und auf einfache Weise zu widersprechen. <b>Das</b> Widerspruchsrecht <b>wird</b> bei Erlangung der Angaben und bei jedem Versand einer Nachricht <b>eingeräumt</b>.</p>	<p>haben, einer solchen Nutzung kostenlos und auf einfache Weise zu widersprechen. <b>Der Kunde wird über sein</b> Widerspruchsrecht <b>belehrt und kann es</b> bei Erlangung der Angaben und bei jedem Versand einer Nachricht <b>auf einfache Weise ausüben</b>.</p>	
<p>(3) Unbeschadet der Absätze 1 und 2 müssen natürliche oder juristische Personen, die Direktwerbeanrufer mittels elektronischer Kommunikationsdienste tätigen,</p>	<p>(3) Unbeschadet der Absätze 1 und 2 müssen natürliche oder juristische Personen, die Direktwerbeanrufer mittels elektronischer Kommunikationsdienste tätigen,</p>	
<p>a) eine Rufnummer angeben, unter der sie erreichbar sind, oder</p>	<p>a) eine Rufnummer angeben, unter der sie erreichbar sind, oder</p>	
<p>b) einen besonderen Code/eine Vorwahl angeben, der/die kenntlich macht, dass es sich um einen Werbeanrufer handelt.</p>	<p>b) einen besonderen Code/eine Vorwahl angeben, der/die kenntlich macht, dass es sich um einen Werbeanrufer handelt.</p>	
<p><b>nicht vorhanden</b></p>	<p><b>(3a) Die Verschleierung der Identität und die Verwendung falscher Identitäten, falscher Rücksendeadressen oder Rückrufnummern beim Versand unerbetener Direktwerbung ist verboten.</b></p>	
<p>(4) Ungeachtet des Absatzes 1 <b>können Mitgliedstaaten durch Rechtsvorschriften vorsehen, dass</b> die Tätigkeit persönlicher Direktwerbeanrufer an <b>Endnutzer, die natürliche Personen sind</b>, nur bei <b>Endnutzern erlaubt ist</b>, die <b>natürliche Personen sind und</b> dem Erhalt solcher Kommunikation nicht widersprochen haben.</p>	<p>(4) Ungeachtet des Absatzes 1 <b>ist</b> die Tätigkeit persönlicher Direktwerbeanrufer an <b>Nutzer</b> nur bei <b>Nutzern zulässig</b>, die dem Erhalt solcher Kommunikation nicht widersprochen haben. <b>Die Mitgliedstaaten legen fest, dass die Nutzer dem Empfang persönlicher Direktwerbeanrufer über eine Robinsonliste widersprechen können, wodurch auch sichergestellt wird, dass sich die Nutzer nur ein einziges Mal abmelden müssen.</b></p>	
<p>(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 genannt</p>	<p>(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 genannt</p>	



EU-Kommission	EU-Parlament	EU-Rat
<p>ten Weise übermittelt wird, ausreichend geschützt werden.</p>	<p>ten Weise übermittelt wird, ausreichend geschützt werden.</p>	
<p>(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.</p>	<p>(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 <b>und kostenlos</b> ihr Recht ausüben können, die Einwilligung in den weiteren Empfang von Werbenachrichten zu widerrufen.</p>	
<p>(7) Der Kommission wird die Befugnis übertragen, nach Artikel 26 Absatz 2 Durchführungsmaßnahmen zu erlassen, in denen der <b>Kode</b>/die Vorwahl zur Kennzeichnung von Werbeanrufen nach Absatz 3 Buchstabe b festgelegt wird.</p>	<p>(7) Der Kommission wird die Befugnis übertragen, nach Artikel 26 Absatz 1 Durchführungsmaßnahmen zu erlassen, in denen der <b>Code</b> / die Vorwahl zur Kennzeichnung von Werbeanrufen nach Absatz 3 Buchstabe b festgelegt wird.</p>	
<p>Artikel 17</p> <p>Information über erkannte Sicherheitsrisiken</p> <p><b>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.</b></p>	<p>Artikel 17</p> <p>Information über erkannte Sicherheitsrisiken</p> <p><b>Die Betreiber elektronischer Kommunikationsdienste erfüllen die Sicherheitsvorschriften, die in der Verordnung (EU) 2016/679 und im [Europäischen Kodex für elektronische Kommunikation] vorgesehen sind. Im Hinblick auf die Sicherheit der Netze und Dienste und die damit verbundenen Sicherheitspflichten gelten die Pflichten nach Artikel 40 des [Europäischen Kodex für die elektronische Kommunikation] sinngemäß für alle Dienste im Anwendungsbereich dieser Verordnung. Dieser Artikel gilt unbeschadet der Pflichten gemäß den Artikeln 32 bis 34 der Verordnung (EU) 2016/679 und der Pflichten gemäß der Richtlinie (EU) 2016/1148.</b></p>	
<p>nicht vorhanden</p>	<p>(1a) <b>Die Betreiber elektronischer Kommunikationsdienste tragen da-</b></p>	

EU-Kommission	EU-Parlament	EU-Rat
	<p><i>für Sorge, dass elektronische Kommunikationsdaten ausreichend vor unbefugten Zugriffen oder Änderungen geschützt sind und dass die Vertraulichkeit und die Integrität der Kommunikation während der Übertragung oder Speicherung ebenfalls durch modernste technische Vorkehrungen wie Verschlüsselungsverfahren, beispielsweise die Ende-zu-Ende-Verschlüsselung der elektronischen Kommunikationsdaten, gewahrt werden. Werden elektronische Kommunikationsdaten verschlüsselt, so ist die Entschlüsselung ausschließlich dem Nutzer gestattet. Unbeschadet der Artikel 11a und 11b dieser Verordnung dürfen die Mitgliedstaaten den Betreibern elektronischer Kommunikationsdienste oder den Softwareherstellern keine Verpflichtungen auferlegen, die der Vertraulichkeit der Daten und der Integrität der Netze und Dienste oder der Endeinrichtungen dieser Unternehmen einschließlich der verwendeten Verschlüsselungsverfahren abträglich wären.</i></p>	
<p><b>nicht vorhanden</b></p>	<p><b>(1b) Betreiber elektronischer Kommunikationsdienste, Anbieter von Diensten der Informationsgesellschaft und Softwarehersteller, die das Abrufen und Darstellen von Informationen im Internet ermöglichen, dürfen weder mittels ihrer Geschäftsbedingungen noch auf vertraglicher Grundlage technische oder betriebliche Mittel einsetzen, durch die die Nutzer und Teilnehmer daran gehindert werden könnten, die besten verfügbaren Technologien gegen das Eindringen und Abfangen von Nachrichten einzusetzen und ihre Netze, ihre Endeinrichtungen und ihre elektronische Kommunikation zu sichern. Unbeschadet der Artikel 11a und 11b dieser Verordnung ist die Abschaltung, Entschlüsselung, Beschränkung oder Umgehung solcher Vorkehrungen der Nutzer oder Teilnehmer untersagt.</b></p>	

EU-Kommission	EU-Parlament	EU-Rat
<i>nicht vorhanden</i>	<b>(1c) Besteht ein besonderes Risiko, dass die Sicherheit von Netzen, elektronischen Kommunikationsdiensten, Diensten der Informationsgesellschaft oder Software beeinträchtigt werden könnte, so informiert der jeweilige Betreiber oder Hersteller alle Teilnehmer über dieses Risiko und – sofern das Risiko außerhalb des Wirkungsbereichs der vom Diensteanbieter zu treffenden Maßnahmen liegt – über mögliche Abhilfemaßnahmen. Er setzt auch die jeweiligen Hersteller und Diensteanbieter davon in Kenntnis.</b>	

**Kapitel IV  
UNABHÄNGIGE AUFSICHTSBEHÖRDEN UND DURCHSETZUNG**

<p><i>Artikel 18</i></p> <p><i>Unabhängige Aufsichtsbehörden</i></p> <p>(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 <b>werden</b> in Bezug auf die <b>Endnutzer</b> wahrgenommen.</p>	<p><i>Artikel 18</i></p> <p><i>Unabhängige Aufsichtsbehörden</i></p> <p>(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. <b>Bezieht sich die Verordnung (EU) 2016/679 auf betroffene Personen, so werden</b> die Aufgaben und Befugnisse der Aufsichtsbehörden in Bezug auf die <b>Nutzer gemäß dieser Verordnung</b> wahrgenommen. <b>Bezieht sich die Verordnung (EU) 2016/679 auf den Verantwortlichen, so werden die Aufgaben und Befugnisse der Aufsichtsbehörden in Bezug auf die Betreiber von elektronischen Kommunikationsdiensten, Dienste der Informationsgesellschaft und Softwarehersteller gemäß dieser Verordnung wahrgenommen.</b></p>	
--	--	--

EU-Kommission	EU-Parlament	EU-Rat
<p>(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.</p>	<p>(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.</p>	
<p><i>Artikel 19</i></p> <p><i>Europäischer Datenschutzausschuss</i></p> <p>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:</p>	<p><i>Artikel 19</i></p> <p><i>Europäischer Datenschutzausschuss</i></p> <p>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:</p>	
<p>a) Beratung der Kommission bezüglich etwaiger Vorschläge zur Änderung dieser Verordnung;</p>	<p>a) Beratung der Kommission bezüglich etwaiger Vorschläge zur Änderung dieser Verordnung;</p>	
<p><b>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.</b></p>	<p><b>ba) Erstellung von Leitlinien für die Aufsichtsbehörden in Bezug auf die Anwendung von Artikel 9 Absatz 1 und die Besonderheiten bei der Erklärung der Einwilligung durch juristische Personen;</b></p> <p><b>bb) Bereitstellung von Leitlinien, anhand deren bestimmt werden kann, durch welche technischen Spezifikationen und Hinweisverfahren die Bedingungen und Ziele gemäß Artikel 10 Absatz 1a erfüllt werden;</b></p> <p><b>bc) Bereitstellung von Leitlinien, Empfehlungen und bewährten Verfahren im Einklang mit Buchstabe b zur weiteren Erläuterung der Kriterien und Anforderungen für Arten von Diensten, die für rein persönliche o-</b></p>	

EU-Kommission	EU-Parlament	EU-Rat
	<p><b>der rein arbeitsbezogene Nutzungszwecke gemäß Artikel 6 Absatz 3a angefordert werden können;</b></p> <p><b>bd) Bereitstellung von Leitlinien, Empfehlungen und bewährten Verfahren im Einklang mit Buchstabe b zur weiteren Erläuterung der Kriterien und Anforderungen für</b></p> <p><b>i) die Messung der Reichweite eines Dienstes der Informationsgesellschaft gemäß Artikel 8 Absatz 1 Buchstabe d,</b></p> <p><b>ii) Sicherheitsaktualisierungen gemäß Artikel 8 Absatz 1 Buchstabe da,</b></p> <p><b>iii) Eingriffe im Rahmen von Arbeitsverhältnissen gemäß Artikel 8 Absatz 1 Buchstabe db,</b></p> <p><b>iv) die Verarbeitung von Informationen, die von der Endeinrichtung gemäß Artikel 8 Absatz 2 ausgesendet werden,</b></p> <p><b>v) technische Spezifikationen und Hinweisverfahren, die die Voraussetzungen für die Einwilligung und den Widerspruch gemäß Artikel 8 Absatz 2a erfüllen,</b></p> <p><b>vi) die Softwareeinstellungen gemäß Artikel 10 Absätze 1a und 1b und</b></p> <p><b>vii) technische Maßnahmen zur Wahrung der Vertraulichkeit und Integrität der Kommunikation gemäß Artikel 17 Absätze 1a, 1b und 1c.</b></p>	
<p>Artikel 20</p> <p>Zusammenarbeit und Kohärenzverfahren</p> <p>Jede Aufsichtsbehörde leistet einen Beitrag zur einheitlichen Anwendung dieser Verordnung in der gesamten Union. Zu diesem Zweck arbeiten die</p>	<p>Artikel 20</p> <p>Zusammenarbeit und Kohärenzverfahren</p> <p>Jede Aufsichtsbehörde leistet einen Beitrag zur einheitlichen Anwendung dieser Verordnung in der gesamten Union. Zu diesem Zweck arbeiten die</p>	

EU-Kommission	EU-Parlament	EU-Rat
<p>Aufsichtsbehörden untereinander sowie mit der Kommission nach Kapitel VII der Verordnung (EU) 2016/679 in den unter diese Verordnung fallenden Angelegenheiten zusammen.</p>	<p>Aufsichtsbehörden untereinander sowie mit der Kommission nach Kapitel VII der Verordnung (EU) 2016/679 in den unter diese Verordnung fallenden Angelegenheiten zusammen.</p>	
<h2 style="margin: 0;">Kapitel V</h2> <h3 style="margin: 0;">RECHTSBEHELFE, HAFTUNG UND SANKTIONEN</h3>		
<p><i>Artikel 21</i></p> <p><i>Rechtsbehelfe</i></p> <p>(1) Jeder Endnutzer elektronischer Kommunikationsdienste hat unbeschadet <b>anderweitiger verwaltungsrechtlicher oder gerichtlicher Rechtsbehelfe</b> dieselben Rechte, die in den Artikeln 77, 78 <b>und</b> 79 der Verordnung (EU) 2016/679 vorgesehen sind.</p>	<p><i>Artikel 21</i></p> <p><i>Rechtsbehelfe</i></p> <p>(1) Jeder Endnutzer elektronischer Kommunikationsdienste <b>und, falls zutreffend, jede Einrichtung, jede Organisation oder jeder Verband</b> hat unbeschadet <b>eines anderweitigen verwaltungsrechtlichen oder gerichtlichen Rechtsbehelfs</b> dieselben Rechte, die in den Artikeln 77, 78, 79 <b>und 80</b> der Verordnung (EU) 2016/679 vorgesehen sind.</p>	
<p><b>nicht vorhanden</b></p>	<p><b>(1a) Jeder Endnutzer elektronischer Kommunikationsdienste hat unbeschadet eines anderweitigen verwaltungsrechtlichen oder außergerichtlichen Rechtsbehelfs das Recht auf einen wirksamen gerichtlichen Rechtsbehelf gegen einen ihn betreffenden rechtsverbindlichen Beschluss einer Aufsichtsbehörde. Endnutzer haben ein solches Recht auch, wenn eine Aufsichtsbehörde eine Beschwerde nicht bearbeitet oder den Endnutzer nicht binnen drei Monaten über den Bearbeitungsfortschritt oder das Ergebnis der eingereichten Beschwerde informiert. Für Verfahren gegen eine Aufsichtsbehörde ist das Gericht des Mitgliedstaats zuständig, in dem die Aufsichtsbehörde ihren Sitz hat.</b></p>	
<p><b>nicht vorhanden</b></p>	<p><b>(1b) Jeder Endnutzer elektronischer Kommunikationsdienste hat das Recht auf einen wirksamen gerichtlichen Rechtsbehelf, wenn er</b></p>	

EU-Kommission	EU-Parlament	EU-Rat
	<p><b>der Ansicht ist, dass seine Rechte nach dieser Verordnung verletzt wurden. Für diese Verfahren gegen einen Betreiber eines elektronischen Kommunikationsdienstes, einen Betreiber eines öffentlich zugänglichen Verzeichnisses, einen Anbieter von Software, mit der elektronische Kommunikation ermöglicht wird, oder Personen, die gewerbliche Direktwerbung betreiben oder Informationen sammeln, die sich auf Endeinrichtungen der Endnutzer beziehen oder dort gespeichert sind, sind die Gerichte des Mitgliedstaats zuständig, in dem diese Betreiber oder Anbieter ihren Sitz bzw. diese Personen ihren Wohnsitz haben. Alternativ ist für diese Verfahren das Gericht des Mitgliedstaats zuständig, in dem der Endnutzer seinen gewöhnlichen Wohnsitz hat.</b></p>	
<p>(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.</p>	<p>(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.</p>	
<p><i>Artikel 22</i></p> <p><i>Haftung und Recht auf Schadenersatz</i></p> <p>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</p>	<p><i>Artikel 22</i></p> <p><i>Haftung und Recht auf Schadenersatz</i></p> <p>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</p>	

EU-Kommission	EU-Parlament	EU-Rat
Umstand, durch den der Schaden eingetreten ist, verantwortlich ist.	Umstand, durch den der Schaden eingetreten ist, verantwortlich ist.	
<p><i>Artikel 23</i></p> <p><i>Allgemeine Voraussetzungen für die Verhängung von Geldbußen</i></p> <p>(1) Für die Zwecke dieses Artikels findet Kapitel VII der Verordnung (EU) 2016/679 auf Verstöße gegen die vorliegende Verordnung Anwendung.</p>	<p><i>Artikel 23</i></p> <p><i>Allgemeine Voraussetzungen für die Verhängung von Geldbußen</i></p> <p>(1) Für die Zwecke dieses Artikels findet Kapitel VII der Verordnung (EU) 2016/679 auf Verstöße gegen die vorliegende Verordnung <b>sinngemäß</b> Anwendung.</p>	
<p>(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:</p>	<p>(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:</p>	
<p><b>a) die Verpflichtungen einer juristischen oder natürlichen Person, die elektronische Kommunikationsdaten nach Artikel 8 verarbeitet;</b></p>	<p><b>entfällt</b></p>	
<p><b>nicht vorhanden</b></p>	<p><b>aa) die Verpflichtungen des Betreibers eines elektronischen Kommunikationsdienstes nach Artikel 11c.</b></p>	
<p><b>b) die Verpflichtungen des Anbieters der Software, die eine elektronische Kommunikation nach Artikel 10 ermöglicht;</b></p>	<p><b>entfällt</b></p>	
<p><b>nicht vorhanden</b></p>	<p><b>ba) die Verpflichtungen der Betreiber öffentlich zugänglicher nummerngebundener interpersoneller Kommunikationsdienste nach den Artikeln 12, 13 und 14.</b></p>	



EU-Kommission	EU-Parlament	EU-Rat
c) die Verpflichtungen des Betreibers öffentlich zugänglicher Verzeichnisse nach Artikel 15;	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.	d) die Verpflichtungen einer juristischen oder natürlichen Person, die elektronische Kommunikationsdienste nach Artikel 16 nutzt.	
(3) Bei Verstößen gegen <b>den Grundsatz der Vertraulichkeit der Kommunikation, die erlaubte Verarbeitung elektronischer Kommunikationsdaten und Lösungsfristen nach den Artikeln 5, 6 und 7</b> werden im Einklang mit Absatz 1 <b>des vorliegenden Artikels</b> 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.	(3) Bei Verstößen gegen <b>die folgenden Bestimmungen dieser Verordnung</b> werden im Einklang mit Absatz 1 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:	
<b>nicht vorhanden</b>	<b>a) den Grundsatz der Vertraulichkeit der Kommunikation nach Artikel 5,</b>	
<b>nicht vorhanden</b>	<b>b) die rechtmäßige Verarbeitung elektronischer Kommunikationsdaten nach Artikel 6,</b>	
<b>nicht vorhanden</b>	<b>c) die Lösungsfristen und die Vertraulichkeitspflichten nach Artikel 7,</b>	
<b>nicht vorhanden</b>	<b>d) die Verpflichtungen einer juristischen oder natürlichen Person, die elektronische Kommunikationsdaten nach Artikel 8 verarbeitet.</b>	
<b>nicht vorhanden</b>	<b>e) die Anforderungen an die Einwilligung nach Artikel 9,</b>	

EU-Kommission	EU-Parlament	EU-Rat
<i>nicht vorhanden</i>	<b>f) die Verpflichtungen des Anbieters von Software, die elektronische Kommunikation nach Artikel 10 ermöglicht,</b>	
<i>nicht vorhanden</i>	<b>g) die Verpflichtungen der Betreiber elektronischer Kommunikationsdienste, der Anbieter von Diensten der Informationsgesellschaft oder der Softwarehersteller, die das Abrufen und Darstellen von Informationen im Internet ermöglichen, gemäß Artikel 17.</b>	
(4) <b>Die Mitgliedstaaten legen Vorschriften über Sanktionen für die in den Artikeln 12, 13, 14 und 17 genannten Verstöße fest.</b>	(4) <b>Bewirkt dieselbe Handlung oder Unterlassung durch dieselbe Person einen Verstoß gegen die Verordnung (EU) 2016/679 und die vorliegende Verordnung, so beläuft sich die Geldbuße höchstens auf den Höchstbetrag der für den jeweiligen Verstoß gemäß der vorliegenden Verordnung zu verhängenden Geldbuße.</b>	
(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.	(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.	(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	(7) Die Ausübung der eigenen Befugnisse durch eine Aufsichtsbehörde nach diesem Artikel muss angemessenen Verfahrensgarantien gemäß dem	

EU-Kommission	EU-Parlament	EU-Rat
<p>Unionsrecht und dem Recht der Mitgliedstaaten, einschließlich wirksamer gerichtlicher Rechtsbehelfe und ordnungsgemäßer Verfahren, unterliegen.</p>	<p>Unionsrecht und dem Recht der Mitgliedstaaten, einschließlich wirksamer gerichtlicher Rechtsbehelfe und ordnungsgemäßer Verfahren, unterliegen.</p>	
<p>(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.</p>	<p>(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.</p>	
<p><i>Artikel 24</i></p> <p><i>Sanktionen</i></p> <p>(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.</p>	<p><i>Artikel 24</i></p> <p><i>Sanktionen</i></p> <p>(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.</p>	
<p>(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.</p>	<p>(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.</p>	

EU-Kommission	EU-Parlament	EU-Rat
<p><b>Kapitel VI</b>  <b>DELEGIERTE RECHTSAKTE UND DURCHFÜHRUNGSRECHTSAKTE</b></p>		
<p><i>Artikel 25</i></p> <p><i>Ausübung der Befugnisübertragung</i></p> <p>(1) Die Befugnis zum Erlass delegierter Rechtsakte wird der Kommission unter den in diesem Artikel festgelegten Bedingungen übertragen.</p>	<p><i>Artikel 25</i></p> <p><i>Ausübung der Befugnisübertragung</i></p> <p>(1) Die Befugnis zum Erlass delegierter Rechtsakte wird der Kommission unter den in diesem Artikel festgelegten Bedingungen übertragen.</p>	
<p>(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.</p>	<p>(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.</p>	
<p>(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.</p>	<p>(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.</p>	
<p>(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.</p>	<p>(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.</p>	
<p>(5) Sobald die Kommission einen delegierten Rechtsakt erlässt, übermittelt sie ihn gleichzeitig dem Europäischen</p>	<p>(5) Sobald die Kommission einen delegierten Rechtsakt erlässt, übermittelt sie ihn gleichzeitig dem Europäischen</p>	

EU-Kommission	EU-Parlament	EU-Rat
Parlament und dem Rat.	Parlament und dem Rat.	
<p>(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.</p>	<p>(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.</p>	
<p><i>Artikel 26</i></p> <p><i>Ausschuss</i></p> <p>(1) Die Kommission <b>wird</b> 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<sup>29</sup>.</p>	<p><i>Artikel 26</i></p> <p><i>Ausschuss</i></p> <p>(1) <b>Für die Zwecke von Artikel 13 Absatz 2 und Artikel 16 Absatz 7 wird</b> die Kommission 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<sup>29</sup>.</p>	
<p>_____</p> <p><sup>29</sup> 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).</p>	<p>_____</p> <p><sup>29</sup> 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).</p>	
<p>(2) Wird auf diesen Absatz Bezug genommen, so gilt Artikel 5 der Verordnung (EU) Nr. 182/2011.</p>	<p>(2) Wird auf diesen Absatz Bezug genommen, so gilt Artikel 5 der Verordnung (EU) Nr. 182/2011.</p>	

EU-Kommission	EU-Parlament	EU-Rat
<h2 style="margin: 0;">Kapitel VII</h2> <h3 style="margin: 0;">SCHLUSSBESTIMMUNGEN</h3>		
<p><i>Artikel 27</i></p> <p><i>Aufhebung</i></p> <p>(1) Die Richtlinie 2002/58/EG <b>wird</b> mit Wirkung vom <b>25. Mai 2018</b> aufgehoben.</p>	<p><i>Artikel 27</i></p> <p><i>Aufhebung</i></p> <p>(1) Die Richtlinie 2002/58/EG <b>und die Verordnung (EU) Nr. 611/2013 der Kommission werden</b> mit Wirkung vom <b>[XXX]</b> aufgehoben.</p>	
<p>(2) Bezugnahmen auf die aufgehobene Richtlinie gelten als Bezugnahmen auf die vorliegende Verordnung.</p>	<p>(2) Bezugnahmen auf die aufgehobene Richtlinie gelten als Bezugnahmen auf die vorliegende Verordnung.</p>	
<p><i>Artikel 28</i></p> <p><i>Überwachung und Bewertung</i></p> <p>Die Kommission stellt spätestens zum <b>1. Januar 2018</b> ein detailliertes Programm für die Überwachung der Wirksamkeit dieser Verordnung auf.</p> <p>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.</p>	<p><i>Artikel 28</i></p> <p><i>Überwachung und Bewertung</i></p> <p>Die Kommission stellt spätestens zum <b>[Datum des Inkrafttretens dieser Verordnung]</b> ein detailliertes Programm für die Überwachung der Wirksamkeit dieser Verordnung auf.</p> <p>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.</p>	

EU-Kommission	EU-Parlament	EU-Rat		
<p><i>Artikel 29</i></p> <p><i>Inkrafttreten und Anwendung</i></p> <p>(1) Diese Verordnung tritt am zwanzigsten Tag nach ihrer Veröffentlichung im Amtsblatt der Europäischen Union in Kraft.</p>	<p><i>Artikel 29</i></p> <p><i>Inkrafttreten und Anwendung</i></p> <p>(1) Diese Verordnung tritt am zwanzigsten Tag nach ihrer Veröffentlichung im Amtsblatt der Europäischen Union in Kraft.</p>			
<p>(2) <b>Sie gilt ab dem 25. Mai 2018.</b></p>	<p>(2) Sie gilt ab dem <b>[ein Jahr nach dem Datum des Inkrafttretens dieser Verordnung].</b></p>			
<p>Diese Verordnung ist in allen ihren Teilen verbindlich und gilt unmittelbar in jedem Mitgliedstaat.</p>	<p>Diese Verordnung ist in allen ihren Teilen verbindlich und gilt unmittelbar in jedem Mitgliedstaat.</p>			
<p>Geschehen zu Brüssel am</p> <table style="width: 100%; border: none;"> <tr> <td style="width: 50%; text-align: center; border: none;"> <p>Im Namen des Europäischen Parlaments</p> <p>Der Präsident</p> </td> <td style="width: 50%; text-align: center; border: none;"> <p>Im Namen des Rates</p> <p>Der Präsident</p> </td> </tr> </table>			<p>Im Namen des Europäischen Parlaments</p> <p>Der Präsident</p>	<p>Im Namen des Rates</p> <p>Der Präsident</p>
<p>Im Namen des Europäischen Parlaments</p> <p>Der Präsident</p>	<p>Im Namen des Rates</p> <p>Der Präsident</p>			