RAT DER EUROPÄISCHEN UNION

Brüssel, den 20. November 2008 (21.11)
(OR. fr)

15899/08

Interinstitutionelles Dossier: 2007/0248 (COD)

TELECOM 203
MI 460
COMPET 490
DATAPROTECT 94
CONSOM 182
CODEC 1582

BERICHT

des	AStV
an den	RAT
Nr. Vordokument:	15106/08 TELECOM 177 MI 415 COMPET 439 DATAPROTECT 81 CONSOM165 CODEC 1471
Nr. Kommissionsvorschlag:	15387/07 TELECOM 151 MI 298 COMPET 392 DATAPROTECT 50 CONSOM 133 CODEC 1297 15422/08 TELECOM 186 MI 427 COMPET 456 DATAPROTECT 88 CONSOM 170 CODEC 1507
Betr.:	Überprüfung des Rechtsrahmens der EU für elektronische Kommunikationsnetze und -dienste: Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates zur Änderung der Richtlinie 2002/22/EG über den Universaldienst und Nutzerrechte bei elektronischen Kommunikationsnetzen und -diensten, der Richtlinie 2002/58/EG über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation und der Verordnung (EG) Nr. 2006/2004 über die Zusammenarbeit im Verbraucherschutz – Politische Einigung

I. EINLEITUNG

1. Die Kommission hat am 13. November 2007 ihre Legislativvorschläge für die Überprüfung des Rechtsrahmens der EU für elektronische Kommunikationsnetze und -dienste verabschiedet, die aus zwei Änderungsrichtlinien und einer Verordnung bestehen. Dieser Bericht befasst sich mit der als "Richtlinie 'Rechte der Bürger'" bekannten Richtlinie und ihrem Teil zur Änderung der geltenden Richtlinie 2002/58/EG über den Schutz der Privatsphäre in der elektronischen Kommunikation. Der Teil zur Änderung der Richtlinie 2002/22/EG über den Universaldienst wird im Rahmen eines gesonderten Berichts erörtert (Dok. 15896/08).

2. Eines der Hauptziele des Rechtsrahmens ist es, die Verbraucherinteressen in der EU zu wahren; dazu ist unter anderem ein umfassender Schutz der personenbezogenen Daten und der Privatsphäre sicherzustellen und die Integrität und Sicherheit der öffentlichen Kommunikationsnetze zu gewährleisten. Angesichts der wachsenden Zahl elektronischer Bedrohungen in den letzten Jahren, etwa durch Viren, unerbetene Werbung ("Spam"), Spähsoftware ("Spyware") und das Ausspionieren persönlicher Zugangsdaten ("Phishing"), sind diese Ziele heute wichtiger denn je.

   Der Kommissionsvorschlag hinsichtlich der Richtlinie über den Schutz der Privatsphäre in der elektronischen Kommunikation stellt auf Fragen ab wie etwa die Gewährleistung, dass die Verbraucher informiert werden, wenn personenbezogene Daten infolge von Verstößen gegen die Netzsicherheit beeinträchtigt werden, die stärkere Verantwortlichkeit der Betreiber und der NRB für die Sicherheit und Integrität aller elektronischen Kommunikationsnetze und -dienste, größere Umsetzungs- und Durchsetzungsbefugnisse der zuständigen Behörden, insbesondere im Kampf gegen "Spam" sowie die Klärung der Anwendbarkeit von EU-Rechtsvorschriften auf Datenerfassungs- und Identifizierungsgeräte, die öffentliche elektronische Kommunikationsnetze nutzen.

3. Ergebnis der Erörterungen unter slowenischem Vorsitz war ein Sachstandsbericht, über den am 12. Juni 2008 ein Gedankenaustausch geführt wurde. Unter französischem Vorsitz ist der Vorschlag eingehender geprüft worden, auch in Bezug auf die vom Europäischen Parlament in erster Lesung am 24. September 2008 angenommene Stellungnahme.

4. Die Kommission hat ihren im Anschluss an die erste Lesung des Europäischen Parlaments geänderten Vorschlag (Dok. 15422/08) am 6. November 2008 angenommen.

5. Der Europäische Wirtschafts- und Sozialausschuss (EWSA) hat am 29. Mai 2008 und der Ausschuss der Regionen (AdR) hat am 19. Juni 2008 Stellung genommen.

II. ERGEBNIS DER BERATUNGEN DES ASTV

1. Der Kompromissvorschlag des Vorsitzes zur Richtlinie über den Schutz der Privatsphäre in der elektronischen Kommunikation ist in der Anlage enthalten. Dieser Text bietet eine konsolidierte Fassung des Vorschlags für eine Änderungsrichtlinie auf der Grundlage des Ergebnisses der Beratungen des AStV vom 14. November 2008. Der Ausschuss ist zu einem weitgehenden Einvernehmen über den Text gelangt.

2. Nur eine Delegation erhält ihren Vorbehalt zu Artikel 6 Absatz 6a über die Verarbeitung von Verkehrsdaten aufrecht (S. 14).

3. Alle Delegationen erhalten sprachliche Vorbehalte zu dem Text aufrecht, und die Kommission hat sich ihren Standpunkt zum Kompromissvorschlag des Vorsitzes insgesamt vorbehalten.

III. AUFGABE DES RATES

Der Rat wird ersucht, die noch offenen Fragen im Hinblick auf eine politische Einigung zu prüfen. Der Text muss danach im Hinblick auf die Festlegung eines gemeinsamen Standpunkts des Rates den Rechts- und Sprachsachverständigen zur abschließenden Überarbeitung übermittelt werden.

KOMPROMISSVORSCHLAG DES VORSITZES FÜR DIE

KONSOLIDIERTE FASSUNG DES VORSCHLAGS ZUR ÄNDERUNG DER RICHTLINIE 2002/58/EG

(Datenschutzrichtlinie für elektronische Kommunikation)

DAS EUROPÄISCHE PARLAMENT UND DER RAT DER EUROPÄISCHEN UNION –

gestützt auf den Vertrag zur Gründung der Europäischen Gemeinschaft, insbesondere auf Artikel 95,

auf Vorschlag der Kommission,

nach Stellungnahme des Wirtschafts- und Sozialausschusses,

nach Anhörung des Ausschusses der Regionen,

gemäß dem Verfahren des Artikels 251 des Vertrags,

in Erwägung nachstehender Gründe:

[Hinsichtlich der Erwägungsgründe, die dieser Richtlinie und der Universaldienstrichtlinie gemein sind, sei auf die Universaldienstrichtlinie verwiesen.]

(27) Die Marktliberalisierung im Bereich der elektronischen Kommunikationsnetze und -dienste sowie die rasante technische Entwicklung treiben gemeinsam den Wettbewerb und das Wirtschaftswachstum voran, die ihrerseits eine große Vielfalt von Diensten für die Endnutzer hervorbringen, die über öffentliche elektronische Kommunikationsnetze zugänglich sind. Es ist dafür zu sorgen, dass den Verbrauchern und Nutzern unabhängig von der zur Erbringung eines bestimmten Dienstes verwendeten Technik der gleiche Schutz ihrer Privatsphäre und personenbezogenen Daten gewährt wird.

(30b) Bei der Durchführung von Maßnahmen zur Umsetzung der Richtlinie 2002/58/EG sollten die Behörden und Gerichte der Mitgliedstaaten nicht nur ihr nationales Recht im Einklang mit der genannten Richtlinie auslegen, sondern auch darauf achten, dass sie sich nicht auf eine Auslegung der Richtlinie stützen, die im Widerspruch zu anderen Grundrechten oder allgemeinen Grundsätzen des Gemeinschaftsrechts wie dem Grundsatz der Verhältnismäßigkeit stehen würde.

[Hinsichtlich der anderen Erwägungsgründe sei auf die einschlägigen Artikel verwiesen.] –

HABEN FOLGENDE RICHTLINIE ERLASSEN:

Artikel 1

Geltungsbereich und Zielsetzung

(1) Diese Richtlinie […] **sieht die Harmonisierung** der Vorschriften der Mitgliedstaaten **vor**, die erforderlich sind, um einen gleichwertigen Schutz der Grundrechte und Grundfreiheiten, insbesondere des Rechts auf Privatsphäre, in Bezug auf die Verarbeitung personenbezogener Daten im Bereich der elektronischen Kommunikation sowie den freien Verkehr dieser Daten und von elektronischen Kommunikationsgeräten und -diensten in der Gemeinschaft zu gewährleisten.

(2) Die Bestimmungen dieser Richtlinie stellen eine Detaillierung und Ergänzung der Richtlinie 95/46/EG im Hinblick auf die in Absatz1 genannten Zwecke dar. Darüber hinaus regeln sie den Schutz der berechtigten Interessen von Teilnehmern, bei denen es sich um juristische Personen handelt.

(3) Diese Richtlinie gilt nicht für Tätigkeiten, die nicht in den Anwendungsbereich des Vertrags zur Gründung der Europäischen Gemeinschaft fallen, beispielsweise Tätigkeiten gemäß den Titeln V und VI des Vertrags über die Europäische Union, und auf keinen Fall für Tätigkeiten betreffend die öffentliche Sicherheit, die Landesverteidigung, die Sicherheit des Staates (einschließlich seines wirtschaftlichen Wohls, wenn die Tätigkeit die Sicherheit des Staates berührt) und die Tätigkeiten des Staates im strafrechtlichen Bereich.

Artikel 2

Begriffsbestimmungen

Sofern nicht anders angegeben, gelten die Begriffsbestimmungen der Richtlinie 95/46/EG und der Richtlinie 2002/21/EG […] über einen gemeinsamen Rechtsrahmen für elektronische Kommunikationsnetze und -dienste ("Rahmenrichtlinie") auch für diese Richtlinie.

Weiterhin bezeichnet im Sinne dieser Richtlinie der Ausdruck

a) "Nutzer" eine natürliche Person, die einen öffentlich zugänglichen elektronischen Kommunikationsdienst für private oder geschäftliche Zwecke nutzt, ohne diesen Dienst notwendigerweise abonniert zu haben;

b) "Verkehrsdaten" Daten, die zum Zwecke der Weiterleitung einer Nachricht an ein elektronisches Kommunikationsnetz oder zum Zwecke der Fakturierung dieses Vorgangs verarbeitet werden;

c) "Standortdaten" Daten, die in einem elektronischen Kommunikationsnetz **oder von einem elektronischen Kommunikationsdienst** verarbeitet werden und die den geografischen Standort des Endgeräts eines Nutzers eines öffentlich zugänglichen elektronischen Kommunikationsdienstes angeben;

d) "Nachricht" jede Information, die zwischen einer endlichen Zahl von Beteiligten über einen öffentlich zugänglichen elektronischen Kommunikationsdienst ausgetauscht oder weitergeleitet wird. Dies schließt nicht Informationen ein, die als Teil eines Rundfunkdienstes über ein elektronisches Kommunikationsnetz an die Öffentlichkeit weitergeleitet werden, soweit die Informationen nicht mit dem identifizierbaren Teilnehmer oder Nutzer, der sie erhält, in Verbindung gebracht werden können;

e) in die Rahmenrichtlinie übernommen

f) Einwilligung" eines Nutzers oder Teilnehmers die Einwilligung der betroffenen Person im Sinne von Richtlinie 95/46/EG;

g) "Dienst mit Zusatznutzen" jeden Dienst, der die Bearbeitung von Verkehrsdaten oder anderen Standortdaten als Verkehrsdaten in einem Maße erfordert, das über das für die Übermittlung einer Nachricht oder die Fakturierung dieses Vorgangs erforderliche Maß hinausgeht;

h) "elektronische Post" jede über ein öffentliches Kommunikationsnetz verschickte Text-, Sprach-, Ton- oder Bildnachricht, die im Netz oder im Endgerät des Empfängers gespeichert werden kann, bis sie von diesem abgerufen wird;

i) "Verletzung des Schutzes personenbezogener Daten" eine Verletzung der Sicherheit, die auf unbeabsichtigte oder unrechtmäßige Weise zur Vernichtung, zum Verlust, zur Veränderung und zur unbefugten Weitergabe von bzw. zum unbefugten Zugang zu personenbezogenen Daten führt, die übertragen, gespeichert oder auf andere Weise im Zusammenhang mit der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste in der Gemeinschaft verarbeitet werden.

Artikel 3

Betroffene Dienste

Diese Richtlinie gilt für die Verarbeitung personenbezogener Daten in Verbindung mit der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste in öffentlichen Kommunikationsnetzen in der Gemeinschaft, **einschließlich öffentlicher Kommunikationsnetze, die Datenerfassungs- und Identifizierungsgeräte unterstützen**.

(2) Gestrichen.

(3) Gestrichen.

(27a neu) Im Einklang mit den Zielen des EU-Rechtsrahmens für elektronische Kommunikationsdienste sowie den Grundsätzen der Verhältnismäßigkeit und Subsidiarität und im Bemühen um Rechtssicherheit und Effizienz für die europäischen Unternehmen wie auch für die nationalen Regulierungsbehörden stellt diese Richtlinie auf öffentliche elektronische Kommunikationsnetze oder -dienste ab und findet keine Anwendung auf geschlossene Benutzergruppen oder Unternehmensnetze.

*(28) Der technische Fortschritt erlaubt die Entwicklung neuer Anwendungen auf der Grundlage von Datenerfassungs- und Identifizierungsgeräten, bei denen es sich auch um kontaktlos mit Funkfrequenzen arbeitende Geräte handeln kann. So werden beispielsweise in RFID-Funkfrequenzerkennungsgeräten (Radio Frequency Identification Devices) Funkfrequenzen genutzt, um von eindeutig gekennzeichneten Etiketten Daten auszulesen, die dann über bestehende Kommunikationsnetze weitergeleitet werden können. Die breite Nutzung solcher Technologien kann erhebliche wirtschaftliche und soziale Vorteile bringen und damit einen großen Beitrag zum Binnenmarkt leisten, wenn ihr Einsatz von den Bürgern akzeptiert wird. Dazu muss gewährleistet werden, dass **alle** Grundrechte des Einzelnen, **[…] einschließlich** des Rechts auf Privatsphäre und Datenschutz, gewahrt bleiben. Werden solche Geräte an öffentlich zugängliche elektronische Kommunikationsnetze angeschlossen oder werden elektronische Kommunikationsdienste als Grundinfrastruktur genutzt, so sollten die einschlägigen Bestimmungen der Richtlinie 2002/58/EG, insbesondere deren Vorschriften über Sicherheit, Datenverkehr, Standortdaten und Vertraulichkeit, zur Anwendung kommen.*

Artikel 4

Sicherheit der Verarbeitung

(1) Der Betreiber eines öffentlich zugänglichen elektronischen Kommunikationsdienstes muss geeignete technische und organisatorische Maßnahmen ergreifen, um die Sicherheit seiner Dienste zu gewährleisten; die Netzsicherheit ist hierbei erforderlichenfalls zusammen mit dem Betreiber des öffentlichen Kommunikationsnetzes zu gewährleisten. Diese Maßnahmen müssen unter Berücksichtigung des Standes der Technik und der Kosten ihrer Durchführung ein Sicherheitsniveau gewährleisten, das angesichts des bestehenden Risikos angemessen ist.

(2) Besteht ein besonderes Risiko der Verletzung der Netzsicherheit, muss der Betreiber eines öffentlich zugänglichen elektronischen Kommunikationsdienstes die Teilnehmer über dieses Risiko und – wenn das Risiko außerhalb des Anwendungsbereichs der vom Diensteanbieter zu treffenden Maßnahmen liegt – über mögliche Abhilfen, einschließlich der voraussichtlich entstehenden Kosten, unterrichten.

(3) Im Fall einer Verletzung des Schutzes personenbezogener Daten […] muss der Betreiber der betroffenen öffentlich zugänglichen elektronischen Kommunikationsdienste […] das Ausmaß der Verletzung des Schutzes personenbezogener Daten bewerten, die Schwere der Verletzung einschätzen und erwägen, ob die zuständige nationale Behörde und der betroffene Teilnehmer über die Verletzung unter Berücksichtigung der von der zuständigen nationalen Behörde gemäß Absatz 3a festgelegten Vorschriften benachrichtigt werden müssen.

Stellt die Verletzung personenbezogener Daten eine ernsthafte Bedrohung der Privatsphäre des Teilnehmers dar, so benachrichtigt der Betreiber der betroffenen öffentlich zugänglichen elektronischen Kommunikationsdienste die zuständige nationale Behörde und den betroffenen Teilnehmer ohne unnötige Verzögerung über die Verletzung.

In der Benachrichtigung des Teilnehmers sind mindestens die Art der Verletzung des Schutzes personenbezogener Daten und die Kontaktstellen, bei denen weitere Informationen erhältlich sind, genannt und werden Maßnahmen zur Abschwächung […] möglicher negativer Auswirkungen der Verletzung des Schutzes personenbezogener Daten vorgeschlagen. In der Benachrichtigung der zuständigen nationalen […] Behörde werden zusätzlich die Folgen der Verletzung des Schutzes personenbezogener Daten und die vom Betreiber nach der Verletzung vorgeschlagenen oder ergriffenen Maßnahmen dargelegt.

(28b) Der Betreiber eines öffentlich zugänglichen elektronischen Kommunikationsdienstes sollte geeignete technische und organisatorische Maßnahmen ergreifen, um die Sicherheit seiner Dienste zu gewährleisten. Unbeschadet der Richtlinie 95/46/EG sollten derartige Maßnahmen sicherstellen, dass nur ermächtigte Personen für rechtlich zulässige Zwecke Zugang zu personenbezogenen Daten erhalten und dass die gespeicherten oder übermittelten personenbezogenen Daten sowie Netz und Dienste geschützt sind. Außerdem sollte ein Sicherheitskonzept für die Verarbeitung personenbezogener Daten eingeführt werden, um Systemschwachstellen zu ermitteln, es sollte eine regelmäßige Überwachung erfolgen und es sollten vorbeugende, korrektive und schadensbegrenzende Maßnahmen getroffen werden.

(28c) Die zuständigen nationalen Behörden sollten die getroffenen Maßnahmen überwachen und optimale Verfahren unter den Betreibern öffentlich zugänglicher elektronischer Kommunikationsdienste verbreiten.

(29) Eine Sicherheitsverletzung, die zum Verlust oder zur Preisgabe personenbezogener Daten eines einzelnen Teilnehmers führt, kann erhebliche wirtschaftliche Schäden und soziale Nachteile einschließlich des Identitätsbetrugs nach sich ziehen, wenn nicht rechtzeitig und angemessen darauf reagiert wird. Deshalb ***sollte der Betreiber eines öffentlich zugänglichen elektronischen Kommunikationsdienstes unmittelbar nach Bekanntwerden einer solchen Verletzung die damit verbundenen Risiken evaluieren, indem er beispielsweise die Art der von der Verletzung betroffenen Daten (einschließlich Sensibilität der Daten, jeweilige Zusammenhänge und bestehende Sicherheitsmaßnahmen), die Ursache und das Ausmaß der Sicherheitsverletzung, die Zahl der betroffenen Teilnehmer und die mögliche Schädigung der Teilnehmer infolge der Verletzung (z.B. Identitätsdiebstahl, finanzieller Verlust, entgangene Geschäfts- oder Beschäftigungsmöglichkeiten, physische Schädigung) ermittelt.*** *Teilnehmer, die von […] Sicherheitsverletzungen betroffen sind,* ***die zu einer ernsthaften Bedrohung ihrer Privatsphäre führen könnten (z.B. Identitätsdiebstahl oder -betrug, physische Schädigung, erhebliche Demütigung oder Rufschaden)*** *sollten unverzüglich benachrichtigt […] werden, damit sie die erforderlichen Schutzvorkehrungen treffen können. Die Benachrichtigung sollte Informationen über die vom Betreiber nach der Verletzung ergriffenen Maßnahmen sowie Empfehlungen für den betroffenen Nutzer enthalten.* ***Der Anbieter sollte nicht verpflichtet sein, den Teilnehmer von einer Sicherheitsverletzung zu benachrichtigen, wenn er der zuständigen Behörde glaubhaft machen konnte, dass er geeignete technische Schutzmaßnahmen für die betroffenen Daten ergriffen hat. Diese technischen Schutzmaßnahmen verschlüsseln die Daten für alle unbefugten Personen.***

(30) Die nationalen Regulierungsbehörden sollten die Interessen der Bürger der Europäischen Union vertreten, indem sie u.a. einen Beitrag zur Gewährleistung eines hohen Schutzes der Privatsphäre und der personenbezogenen Daten leisten. Sie müssen daher über die zur Erfüllung ihrer Aufgaben erforderlichen Mittel verfügen, z.B. vollständige und verlässliche Daten über Sicherheitsverletzungen, in deren Folge die personenbezogenen Daten natürlicher Personen preisgegeben wurden.

(3a) Die Mitgliedstaaten stellen sicher, dass die zuständige nationale Behörde in der Lage ist, ausführliche Vorschriften festzulegen und gegebenenfalls Anweisungen zu erteilen bezüglich der Umstände, unter denen die Benachrichtigung über eine Verletzung des Schutzes personenbezogener Daten durch den Betreiber eines öffentlich zugänglichen elektronischen Kommunikationsdienstes erforderlich ist, sowie bezüglich des Formates und der Verfahrensweise für die Benachrichtigung.

(4) Zur Gewährleistung einer einheitlichen Anwendung der in den Absätzen 1, 2, 3 und 3a vorgesehenen Maßnahmen kann die Kommission nach Anhörung der Europäischen Agentur für Netz- und Informationssicherheit, der Datenschutzgruppe und des Europäischen Datenschutzbeauftragten […] Empfehlungen unter anderem in Bezug auf Umstände, Form und Verfahren der in diesem Artikel vorgeschriebenen Informationen und Benachrichtigungen erlassen.

[...]

(31) […] Es sollte [...] vorgesehen werden, dass ***die Kommission Empfehlungen erlässt, in denen dargelegt wird, wie*** *der Schutz der Privatsphäre und die Sicherheit der übermittelten und verarbeiteten personenbezogenen Daten im Zusammenhang mit der Nutzung elektronischer Kommunikationsnetze innerhalb des Binnenmarktes hinreichend gewährleistet werden kann.*

(32) Bei der detaillierten Regelung des Formats und der Verfahren für die Meldung von […] Verletzungen des Schutzes ***personenbezogener Daten*** *sollten die Umstände der Verletzung hinreichend berücksichtigt werden, z.B. ob die personenbezogenen Daten durch Verschlüsselung oder andere Mittel geschützt waren, die die Wahrscheinlichkeit des Identitätsbetrugs oder anderer Formen des Missbrauchs effektiv verringern. Überdies sollten solche Regeln und Verfahren den berechtigten Interessen der Strafverfolgungsbehörden in Fällen Rechnung tragen, in denen die Untersuchung der Umstände der Verletzung durch ein frühzeitiges Bekanntwerden in unnötiger Weise behindert würde.*

Erwägungsgrund 33 wird gestrichen.

Artikel 5

Vertraulichkeit der Kommunikation

(1) Die Mitgliedstaaten stellen die Vertraulichkeit der mit öffentlichen Kommunikationsnetzen und öffentlich zugänglichen Kommunikationsdiensten übertragenen Nachrichten und der damit verbundenen Verkehrsdaten durch innerstaatliche Vorschriften sicher. Insbesondere untersagen sie das Mithören, Abhören und Speichern sowie andere Arten des Abfangens oder Überwachens von Nachrichten und der damit verbundenen Verkehrsdaten durch andere Personen als die Nutzer, wenn keine Einwilligung der betroffenen Nutzer vorliegt, es sei denn, dass diese Personen gemäß Artikel 15 Absatz 1 gesetzlich dazu ermächtigt sind. Diese Bestimmung steht – unbeschadet des Grundsatzes der Vertraulichkeit – der für die Weiterleitung einer Nachricht erforderlichen technischen Speicherung nicht entgegen.

(2) Absatz 1 betrifft nicht das rechtlich zulässige Aufzeichnen von Nachrichten und der damit verbundenen Verkehrsdaten, wenn dies im Rahmen einer rechtmäßigen Geschäftspraxis zum Nachweis einer kommerziellen Transaktion oder einer sonstigen geschäftlichen Nachricht geschieht.

(3) Die Mitgliedstaaten stellen sicher, dass die **[…] Speicherung von** Informationen oder […] der Zugriff auf Informationen, die **bereits** im Endgerät eines Teilnehmers oder Nutzers gespeichert sind, nur unter der Bedingung gestattet ist, dass der betreffende Teilnehmer oder Nutzer gemäß der Richtlinie 95/46/EG klare und umfassende Informationen insbesondere über die Zwecke der Verarbeitung erhält und durch den für diese Verarbeitung Verantwortlichen auf das Recht hingewiesen wird, diese Verarbeitung zu verweigern. Dies steht einer technischen Speicherung oder dem Zugang nicht entgegen, wenn der alleinige Zweck die Durchführung oder Erleichterung der Übertragung einer Nachricht über ein elektronisches Kommunikationsnetz ist oder, soweit dies unbedingt erforderlich ist, um einen vom Teilnehmer oder Nutzer ausdrücklich gewünschten Dienst der Informationsgesellschaft zur Verfügung zu stellen.

(34) Computerprogramme, die heimlich zugunsten Dritter das Verhalten des Nutzers überwachen oder die Funktionsweise seines Endgerätes beeinträchtigen (so genannte "Spähsoftware") sind eine ernste Bedrohung für die Privatsphäre des Nutzers. Ein hoher und einheitlicher Schutz der Privatsphäre der Nutzer muss unabhängig davon gewährleistet werden, ob unerwünschte Spähprogramme versehentlich über elektronische Kommunikationsnetze heruntergeladen werden oder aber versteckt in anderer Software, die auf externen Speichermedien wie CD, CD-ROM oder USB-Speicherstift verbreitet wird, ausgeliefert und installiert werden. ***Die Mitgliedstaaten sollten die Endnutzer ermutigen, die notwendigen Maßnahmen zu ergreifen, um ihre Endgeräte vor Viren und Spähsoftware zu schützen.***

Artikel 6

Verkehrsdaten

(1) Verkehrsdaten, die sich auf Teilnehmer und Nutzer beziehen und vom Betreiber eines öffentlichen Kommunikationsnetzes oder eines öffentlich zugänglichen Kommunikationsdienstes verarbeitet und gespeichert werden, sind unbeschadet der Absätze 2, 3, **[…]**, 5 **und 6a** des vorliegenden Artikels und des Artikels 15 Absatz 1 zu löschen oder zu anonymisieren, sobald sie für die Übertragung einer Nachricht nicht mehr benötigt werden.

(2) Verkehrsdaten, die zum Zwecke der Gebührenabrechnung und der Bezahlung von Zusammenschaltungen erforderlich sind, dürfen verarbeitet werden. Diese Verarbeitung ist nur bis zum Ablauf der Frist zulässig, innerhalb deren die Rechnung rechtlich angefochten oder der Anspruch auf Zahlung geltend gemacht werden kann.

(3) Der Betreiber eines öffentlich zugänglichen elektronischen Kommunikationsdienstes kann die in Absatz 1 genannten Daten zum Zwecke der Vermarktung elektronischer Kommunikationsdienste oder zur Bereitstellung von Diensten mit Zusatznutzen im dazu erforderlichen Maß und innerhalb des dazu oder zur Vermarktung erforderlichen Zeitraums verarbeiten, sofern der Teilnehmer oder der Nutzer, auf den sich die Daten beziehen, zuvor seine Einwilligung gegeben hat. Der Nutzer oder der Teilnehmer hat die Möglichkeit, seine Einwilligung zur Verarbeitung der Verkehrsdaten jederzeit zurückzuziehen.

(4) Der Diensteanbieter muss dem Teilnehmer oder Nutzer mitteilen, welche Arten von Verkehrsdaten für die in Absatz 2 genannten Zwecke verarbeitet werden und wie lange das geschieht; bei einer Verarbeitung für die in Absatz 3 genannten Zwecke muss diese Mitteilung erfolgen, bevor um Einwilligung ersucht wird.

(5) Die Verarbeitung von Verkehrsdaten gemäß den Absätzen 1, 2, 3 und 4 darf nur durch Personen erfolgen, die auf Weisung der Betreiber öffentlicher Kommunikationsnetze und öffentlich zugänglicher Kommunikationsdienste handeln und die für Gebührenabrechnungen oder Verkehrsabwicklung, Kundenanfragen, Betrugsermittlung, die Vermarktung der elektronischen Kommunikationsdienste oder für die Bereitstellung eines Dienstes mit Zusatznutzen zuständig sind; ferner ist sie auf das für diese Tätigkeiten erforderliche Maß zu beschränken.

(6) Die Absätze 1, 2, 3 und 5 gelten unbeschadet der Möglichkeit der zuständigen Gremien, in Einklang mit den geltenden Rechtsvorschriften für die Beilegung von Streitigkeiten, insbesondere Zusammenschaltungs- oder Abrechnungsstreitigkeiten, von Verkehrsdaten Kenntnis zu erhalten.

(6a) […] Verkehrsdaten können im […] strikt notwendigen Ausmaß verarbeitet werden, um […] die Netz- und Informationssicherheit gemäß der Definition in Artikel 4 Buchstabe c der Verordnung (EG) Nr. 460/2004 des Europäischen Parlaments und des Rates vom 10. März 2004 zur Errichtung der Europäischen Agentur für Netz- und Informationssicherheit zu gewährleisten […].[1]

(26a) Die Verarbeitung von Verkehrsdaten in dem für die Aufdeckung, Lokalisierung und Beseitigung von Störungen und Fehlfunktionen des Netzes und für die Zwecke der Informationssicherheit strikt notwendigen Ausmaß, durch die die Verfügbarkeit, Authentizität, Integrität und Vertraulichkeit gespeicherter oder übermittelter Daten sichergestellt wird, […] trägt dazu bei, unberechtigten Zugang und die Verbreitung störender Programmcodes sowie Angriffe, die Dienstleistungsverhinderungen bewirken, […] und Schädigungen von Computersystemen und Systemen der elektronischen Kommunikation zu unterbinden. [...]

[1] DE hat Vorbehalt zu Absatz 6a.

Artikel 7

Einzelgebührennachweis

(1) Die Teilnehmer haben das Recht, Rechnungen ohne Einzelgebührennachweis zu erhalten.

(2) Die Mitgliedstaaten wenden innerstaatliche Vorschriften an, um das Recht der Teilnehmer, Einzelgebührennachweise zu erhalten, und das Recht anrufender Nutzer und angerufener Teilnehmer auf Vertraulichkeit miteinander in Einklang zu bringen, indem sie beispielsweise sicherstellen, dass diesen Nutzern und Teilnehmern genügend andere, den Schutz der Privatsphäre fördernde Methoden für die Kommunikation oder Zahlungen zur Verfügung stehen.

Artikel 8

Anzeige der Rufnummer des Anrufers und des Angerufenen und deren Unterdrückung

(1) Wird die Anzeige der Rufnummer des Anrufers angeboten, so muss der Diensteanbieter dem anrufenden Nutzer die Möglichkeit geben, die Rufnummernanzeige für jeden Anruf einzeln auf einfache Weise und gebührenfrei zu verhindern. Dem anrufenden Teilnehmer muss diese Möglichkeit anschlussbezogen zur Verfügung stehen.

(2) Wird die Anzeige der Rufnummer des Anrufers angeboten, so muss der Diensteanbieter dem angerufenen Teilnehmer die Möglichkeit geben, die Anzeige der Rufnummer eingehender Anrufe auf einfache Weise und für jede vertretbare Nutzung dieser Funktion gebührenfrei zu verhindern.

(3) Wird die Anzeige der Rufnummer des Anrufers angeboten und wird die Rufnummer vor der Herstellung der Verbindung angezeigt, so muss der Diensteanbieter dem angerufenen Teilnehmer die Möglichkeit geben, eingehende Anrufe, bei denen die Rufnummernanzeige durch den anrufenden Nutzer oder Teilnehmer verhindert wurde, auf einfache Weise und gebührenfrei abzuweisen.

(4) Wird die Anzeige der Rufnummer des Angerufenen angeboten, so muss der Diensteanbieter dem angerufenen Teilnehmer die Möglichkeit geben, die Anzeige seiner Rufnummer beim anrufenden Nutzer auf einfache Weise und gebührenfrei zu verhindern.

(5) Absatz 1 gilt auch für aus der Gemeinschaft kommende Anrufe in Drittländern. Die Absätze 2, 3 und 4 gelten auch für aus Drittländern kommende Anrufe.

(6) Wird die Anzeige der Rufnummer des Anrufers und/oder des Angerufenen angeboten, so stellen die Mitgliedstaaten sicher, dass die Betreiber öffentlich zugänglicher elektronischer Kommunikationsdienste die Öffentlichkeit hierüber und über die in den Absätzen 1, 2, 3 und 4 beschriebenen Möglichkeiten unterrichten.

Artikel 9

Andere Standortdaten als Verkehrsdaten

(1) Können andere Standortdaten als Verkehrsdaten in Bezug auf die Nutzer oder Teilnehmer von öffentlichen Kommunikationsnetzen oder öffentlich zugänglichen Kommunikationsdiensten verarbeitet werden, so dürfen diese Daten nur im zur Bereitstellung von Diensten mit Zusatznutzen erforderlichen Maß und innerhalb des dafür erforderlichen Zeitraums verarbeitet werden, wenn sie anonymisiert wurden oder wenn die Nutzer oder Teilnehmer ihre Einwilligung gegeben haben. Der Diensteanbieter muss den Nutzern oder Teilnehmern vor Einholung ihrer Einwilligung mitteilen, welche Arten anderer Standortdaten als Verkehrsdaten verarbeitet werden, für welche Zwecke und wie lange das geschieht und ob die Daten zum Zwecke der Bereitstellung des Dienstes mit Zusatznutzen an einen Dritten weitergegeben werden. Die Nutzer oder Teilnehmer können ihre Einwilligung zur Verarbeitung anderer Standortdaten als Verkehrsdaten jederzeit zurückziehen.

(2) Haben die Nutzer oder Teilnehmer ihre Einwilligung zur Verarbeitung von anderen Standortdaten als Verkehrsdaten gegeben, so müssen sie auch weiterhin die Möglichkeit haben, die Verarbeitung solcher Daten für jede Verbindung zum Netz oder für jede Übertragung einer Nachricht auf einfache Weise und gebührenfrei zeitweise zu untersagen.

(3) Die Verarbeitung anderer Standortdaten als Verkehrsdaten gemäß den Absätzen 1 und 2 muss auf das für die Bereitstellung des Dienstes mit Zusatznutzen erforderliche Maß sowie auf Personen beschränkt werden, die im Auftrag des Betreibers des öffentlichen Kommunikationsnetzes oder öffentlich zugänglichen Kommunikationsdienstes oder des Dritten, der den Dienst mit Zusatznutzen anbietet, handeln.

Artikel 10

Ausnahmen

Die Mitgliedstaaten stellen sicher, dass es transparente Verfahren gibt, nach denen der Betreiber eines öffentlichen Kommunikationsnetzes und/oder eines öffentlich zugänglichen elektronischen Kommunikationsdienstes

a) die Unterdrückung der Anzeige der Rufnummer des Anrufers vorübergehend aufheben kann, wenn ein Teilnehmer beantragt hat, dass böswillige oder belästigende Anrufe zurückverfolgt werden; in diesem Fall werden nach innerstaatlichem Recht die Daten mit der Rufnummer des anrufenden Teilnehmers vom Betreiber des öffentlichen Kommunikationsnetzes und/oder des öffentlich zugänglichen elektronischen Kommunikationsdienstes gespeichert und zur Verfügung gestellt;

b) die Unterdrückung der Anzeige der Rufnummer des Anrufers aufheben und Standortdaten trotz der vorübergehenden Untersagung oder fehlenden Einwilligung durch den Teilnehmer oder Nutzer verarbeiten kann, und zwar anschlussbezogen für Einrichtungen, die Notrufe bearbeiten und dafür von einem Mitgliedstaat anerkannt sind, einschließlich Strafverfolgungsbehörden, Ambulanzdiensten und Feuerwehren, zum Zwecke der Beantwortung dieser Anrufe.

Artikel 11

Automatische Anrufweiterschaltung

Die Mitgliedstaaten stellen sicher, dass jeder Teilnehmer die Möglichkeit hat, auf einfache Weise und gebührenfrei die von einer dritten Partei veranlasste automatische Anrufweiterschaltung zum Endgerät des Teilnehmers abzustellen.

Artikel 12

Teilnehmerverzeichnisse

(1) Die Mitgliedstaaten stellen sicher, dass die Teilnehmer gebührenfrei und vor Aufnahme in das Teilnehmerverzeichnis über den Zweck bzw. die Zwecke von gedruckten oder elektronischen, der Öffentlichkeit unmittelbar oder über Auskunftsdienste zugänglichen Teilnehmerverzeichnissen, in die ihre personenbezogenen Daten aufgenommen werden können, sowie über weitere Nutzungsmöglichkeiten aufgrund der in elektronischen Fassungen der Verzeichnisse eingebetteten Suchfunktionen informiert werden.

(2) Die Mitgliedstaaten stellen sicher, dass die Teilnehmer Gelegenheit erhalten, festzulegen, ob ihre personenbezogenen Daten – und gegebenenfalls welche – in ein öffentliches Verzeichnis aufgenommen werden, sofern diese Daten für den vom Anbieter des Verzeichnisses angegebenen Zweck relevant sind, und diese Daten prüfen, korrigieren oder löschen dürfen. Für die Nicht-Aufnahme in ein der Öffentlichkeit zugängliches Teilnehmerverzeichnis oder die Prüfung, Berichtigung oder Streichung personenbezogener Daten aus einem solchen Verzeichnis werden keine Gebühren erhoben.

(3) Die Mitgliedstaaten können verlangen, dass eine zusätzliche Einwilligung der Teilnehmer eingeholt wird, wenn ein öffentliches Verzeichnis anderen Zwecken als der Suche nach Einzelheiten betreffend die Kommunikation mit Personen anhand ihres Namens und gegebenenfalls eines Mindestbestands an anderen Kennzeichen dient.

(4) Die Absätze 1 und 2 gelten für Teilnehmer, die natürliche Personen sind. Die Mitgliedstaaten tragen im Rahmen des Gemeinschaftsrechts und der geltenden einzelstaatlichen Rechtsvorschriften außerdem dafür Sorge, dass die berechtigten Interessen anderer Teilnehmer als natürlicher Personen in Bezug auf ihre Aufnahme in öffentliche Verzeichnisse ausreichend geschützt werden.

Artikel 13

Unerbetene Nachrichten

(1) Die Verwendung von automatischen Anrufsystemen ohne menschlichen Eingriff (automatische Anrufmaschinen), Faxgeräten oder elektronischer Post **(einschließlich Kurznachrichtendiensten (SMS) und Multimediadiensten (MMS))** für die Zwecke der Direktwerbung darf **nur** bei vorheriger Einwilligung der Teilnehmer **oder Nutzer** gestattet werden.

(2) Ungeachtet des Absatzes 1 kann eine natürliche oder juristische Person, wenn sie von ihren Kunden im Zusammenhang mit dem Verkauf eines Produkts oder einer Dienstleistung gemäß der Richtlinie 95/46/EG deren elektronische Kontaktinformationen für elektronische Post erhalten hat, diese zur Direktwerbung für eigene ähnliche Produkte oder Dienstleistungen verwenden, sofern die Kunden klar und deutlich die Möglichkeit erhalten, eine solche Nutzung ihrer elektronischen Kontaktinformationen **[…] zum Zeitpunkt der Erhebung der Kontaktinformationen** und bei jeder Übertragung gebührenfrei und problemlos abzulehnen, wenn der Kunde diese Nutzung nicht von vornherein abgelehnt hat.

(3) Die Mitgliedstaaten ergreifen geeignete Maßnahmen, um […] sicherzustellen, dass außer in den in den Absätzen 1 und 2 genannten Fällen unerbetene Nachrichten zum Zwecke der Direktwerbung, die entweder ohne die Einwilligung der betreffenden Teilnehmer **oder Nutzer** erfolgen oder an Teilnehmer **oder Nutzer** gerichtet sind, die keine solchen Nachrichten erhalten möchten, nicht gestattet sind; welche dieser Optionen gewählt wird, ist im innerstaatlichen Recht zu regeln, **wobei zu berücksichtigen ist, dass beide Optionen für den Teilnehmer gebührenfrei sein müssen**.

(4) Auf jeden Fall verboten ist die Praxis des Versendens elektronischer Nachrichten zu Zwecken der Direktwerbung, bei der die Identität des Absenders, in dessen Auftrag die Nachricht übermittelt wird, verschleiert oder verheimlicht wird, **bei der gegen Artikel 6 der Richtlinie 2000/31/EG verstoßen wird** oder bei der keine gültige Adresse vorhanden ist, an die der Empfänger eine Aufforderung zur Einstellung solcher Nachrichten richten kann.

(5) Die Absätze 1 und 3 gelten für Teilnehmer, die natürliche Personen sind. Die Mitgliedstaaten tragen im Rahmen des Gemeinschaftsrechts und der geltenden einzelstaatlichen Rechtsvorschriften außerdem dafür Sorge, dass die berechtigten Interessen anderer Teilnehmer als natürlicher Personen in Bezug auf unerbetene Nachrichten ausreichend geschützt werden.

(6) Unbeschadet etwaiger Verwaltungsvorschriften, die unter anderem gemäß Artikel 15a Absatz 2 erlassen werden können, stellen die Mitgliedstaaten sicher, dass natürliche und juristische Personen, die […] durch Verstöße gegen die aufgrund dieses Artikels erlassenen nationalen Vorschriften beeinträchtigt werden und daher ein berechtigtes Interesse an der Einstellung oder dem Verbot solcher Verstöße haben, einschließlich der Anbieter elektronischer Kommunikationsdienste, die ihre berechtigten Geschäftsinteressen […] schützen wollen, gegen solche Verstöße gerichtlich vorgehen können. Die Mitgliedstaaten können auch spezifische Vorschriften über Sanktionen festlegen, die gegen Betreiber elektronischer Kommunikationsdienste zu verhängen sind, die durch […] Fahrlässigkeit zu Verstößen gegen die aufgrund dieses Artikels erlassenen nationalen Vorschriften beitragen.

(35) Die Anbieter elektronischer Kommunikationsdienste müssen zur Bekämpfung unerbetener Werbung ("Spam") erhebliche Investitionen tätigen. Außerdem sind sie aufgrund der erforderlichen Sachkenntnis und Ressourcen besser als die Endnutzer in der Lage, Spam-Versender festzustellen und zu identifizieren. Die Betreiber von E-Mail-Diensten und andere Diensteanbieter sollten daher die Möglichkeit haben, rechtlich gegen Spam-Versender ***wegen derartiger Verstöße*** *vorzugehen, um auf diese Weise die Interessen ihrer Kunden* ***[…] als Teil*** *ihrer eigenen rechtmäßigen Geschäftsinteressen zu schützen.*

Artikel 14

Technische Merkmale und Normung

(1) Bei der Durchführung der Bestimmungen dieser Richtlinie stellen die Mitgliedstaaten vorbehaltlich der Absätze 2 und 3 sicher, dass keine zwingenden Anforderungen in Bezug auf spezifische technische Merkmale für Endgeräte oder sonstige elektronische Kommunikationsgeräte gestellt werden, die deren Inverkehrbringen und freien Vertrieb in und zwischen den Mitgliedstaaten behindern können.

(2) Soweit die Bestimmungen dieser Richtlinie nur mit Hilfe spezifischer technischer Merkmale elektronischer Kommunikationsnetze durchgeführt werden können, unterrichten die Mitgliedstaaten die Kommission darüber gemäß der Richtlinie 98/34/EG des Europäischen Parlaments und des Rates vom 22. Juni 1998 über ein Informationsverfahren auf dem Gebiet der Normen und technischen Vorschriften und der Vorschriften für die Dienste der Informationsgesellschaft.

(3) Erforderlichenfalls können gemäß der Richtlinie 1999/5/EG und dem Beschluss 87/95/EWG des Rates vom 22. Dezember 1986 über die Normung auf dem Gebiet der Informationstechnik und der Telekommunikation Maßnahmen getroffen werden, um sicherzustellen, dass Endgeräte in einer Weise gebaut sind, die mit dem Recht der Nutzer auf Schutz und Kontrolle der Verwendung ihrer personenbezogenen Daten vereinbar ist.

Artikel 14a

Ausschuss

Gestrichen.

Artikel 15

Anwendung einzelner Bestimmungen der Richtlinie 95/46/EG

(1) Die Mitgliedstaaten können Rechtsvorschriften erlassen, die die Rechte und Pflichten gemäß Artikel 5, Artikel 6, Artikel 8 Absätze 1, 2, 3 und 4 sowie Artikel 9 dieser Richtlinie beschränken, sofern eine solche Beschränkung gemäß Artikel 13 Absatz 1 der Richtlinie 95/46/EG für die nationale Sicherheit (d.h. die Sicherheit des Staates), die Landesverteidigung, die öffentliche Sicherheit sowie die Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten oder des unzulässigen Gebrauchs von elektronischen Kommunikationssystemen in einer demokratischen Gesellschaft notwendig, angemessen und verhältnismäßig ist. Zu diesem Zwecke können die Mitgliedstaaten unter anderem durch Rechtsvorschriften vorsehen, dass Daten aus den in diesem Absatz aufgeführten Gründen während einer begrenzten Zeit aufbewahrt werden. Alle in diesem Absatz genannten Maßnahmen müssen den allgemeinen Grundsätzen des Gemeinschaftsrechts einschließlich den in Artikel 6 Absätze 1 und 2 des Vertrags über die Europäische Union niedergelegten Grundsätzen entsprechen.

(1a) Absatz1 gilt nicht für Daten, für die in der Richtlinie 2006/24/EG des Europäischen Parlaments und des Rates vom 15. März 2006 über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste oder öffentlicher Kommunikationsnetze erzeugt oder verarbeitet werden, eine Vorratsspeicherung zu den in Artikel 1 Absatz 1 der genannten Richtlinie aufgeführten Zwecken ausdrücklich vorgeschrieben ist.

(2) Die Bestimmungen des Kapitels III der Richtlinie 95/46/EG über Rechtsbehelfe, Haftung und Sanktionen gelten im Hinblick auf innerstaatliche Vorschriften, die nach der vorliegenden Richtlinie erlassen werden, und im Hinblick auf die aus dieser Richtlinie resultierenden individuellen Rechte.

(3) Die gemäß Artikel 29 der Richtlinie 95/46/EG eingesetzte Datenschutzgruppe nimmt auch die in Artikel 30 jener Richtlinie festgelegten Aufgaben im Hinblick auf die von der vorliegenden Richtlinie abgedeckten Aspekte, nämlich den Schutz der Grundrechte und der Grundfreiheiten und der berechtigten Interessen im Bereich der elektronischen Kommunikation wahr.

Artikel 15a

Umsetzung und Durchsetzung

(1) Die Mitgliedstaaten legen fest, welche Sanktionen bei einem Verstoß gegen die innerstaatlichen Vorschriften zur Umsetzung dieser Richtlinie zu verhängen sind, und treffen die zu deren Durchsetzung erforderlichen Maßnahmen. Die vorgesehenen Sanktionen müssen wirksam, verhältnismäßig und abschreckend sein; sie können für den gesamten Zeitraum einer Verletzung angewendet werden, auch wenn die Verletzung in der Folge abgestellt wurde. Die Mitgliedstaaten teilen der Kommission diese Vorschriften bis spätestens [Termin für die Umsetzung des Änderungsrechtsaktes] mit und melden ihr unverzüglich etwaige spätere Änderungen, die diese Vorschriften berühren.

(2) […] Die Mitgliedstaaten stellen sicher, dass die […] zuständige nationale Behörde und gegebenenfalls andere nationale Behörden befugt sind, die Einstellung der in Absatz 1 genannten Verstöße anzuordnen.

(3) Die Mitgliedstaaten stellen sicher, dass die […] zuständigen nationalen Regulierungsbehörden und gegebenenfalls andere nationale Behörden über alle erforderlichen Untersuchungsbefugnisse und Mittel verfügen, einschließlich der Möglichkeit, sämtliche zweckdienliche Informationen zu erlangen, die sie benötigen, um die Einhaltung der gemäß dieser Richtlinie erlassenen innerstaatlichen Rechtsvorschriften zu überwachen und durchzusetzen.

(4) Zur Gewährleistung einer wirksamen grenzübergreifenden Koordinierung der Durchsetzung der gemäß dieser Richtlinie erlassenen innerstaatlichen Rechtsvorschriften und zur Schaffung harmonisierter Bedingungen für die Erbringung von Diensten, mit denen ein grenzüberschreitender Datenfluss verbunden ist, kann die Kommission nach Anhörung […] der ENISA, der Datenschutzgruppe und der betroffenen Regulierungsbehörden […] Empfehlungen erlassen.

[...]

(36) Angesichts der Notwendigkeit, in der Gemeinschaft einen angemessenen Schutz der Privatsphäre und personenbezogener Daten bei deren Übermittlung und Verarbeitung im Zusammenhang mit der Nutzung elektronischer Kommunikationsnetze zu gewährleisten, müssen als hinreichender Anreiz für die Einhaltung der Schutzbestimmungen wirksame Um- und Durchsetzungsbefugnisse geschaffen werden. Die ***zuständigen*** *nationalen […] Behörden* ***und gegebenenfalls andere relevante nationale Behörden*** *sollten mit ausreichenden Befugnissen und Ressourcen ausgestattet werden, um Verstöße effektiv untersuchen zu können, und alle benötigten Informationen einholen können, damit sie Beschwerden nachgehen und bei Verstößen Sanktionen verhängen können.*

(36a) Die Um- und Durchsetzung dieser Richtlinie erfordert häufig eine Zusammenarbeit zwischen den nationalen Regulierungsbehörden zweier oder mehrerer Mitgliedstaaten, wie etwa bei der Bekämpfung von grenzübergreifender unerbetener Werbung ("Spam") und Spähsoftware ("Spyware"). Damit in diesen Fällen eine reibungslose und schnelle Zusammenarbeit gewährleistet ist, sollten im Rahmen von Empfehlungen Verfahren festgelegt werden, in denen beispielsweise auf die Menge und das Format der zwischen Behörden ausgetauschten Informationen oder auf die einzuhaltenden Fristen Bezug genommen wird. Diese Verfahren werden auch die Harmonisierung der daraus resultierenden Pflichten der Marktteilnehmer ermöglichen und damit zur Schaffung gleicher Wettbewerbsbedingungen in der Gemeinschaft beitragen.

Artikel 16

Übergangsbestimmungen

(1) Artikel 12 gilt nicht für Ausgaben von Teilnehmerverzeichnissen, die vor dem Inkrafttreten der nach dieser Richtlinie erlassenen innerstaatlichen Vorschriften bereits in gedruckter oder in netzunabhängiger elektronischer Form produziert oder in Verkehr gebracht wurden.

(2) Sind die personenbezogenen Daten von Teilnehmern von Festnetz- oder Mobil-Sprachtelefondiensten in ein öffentliches Teilnehmerverzeichnis gemäß der Richtlinie 95/46/EG und gemäß Artikel 11 der Richtlinie 97/66/EG aufgenommen worden, bevor die nach der vorliegenden Richtlinie erlassenen innerstaatlichen Rechtsvorschriften in Kraft treten, so können die personenbezogenen Daten dieser Teilnehmer in der gedruckten oder elektronischen Fassung, einschließlich Fassungen mit Umkehrsuchfunktionen, in diesem öffentlichen Verzeichnis verbleiben, sofern die Teilnehmer nach Erhalt vollständiger Informationen über die Zwecke und Möglichkeiten gemäß Artikel 12 nicht etwas anderes wünschen.

[Artikel 4

Umsetzung

Artikel 5

Inkrafttreten

Artikel 6

Adressaten]

_____