



**RAT DER
EUROPÄISCHEN UNION**

**Brüssel, den 24. Mai 2005 (30/05)
(OR. en)**

**DOKUMENT TEILWEISE
ZUGÄNLICH**

**8864/1/05
REV 1**

LIMITE

**COPEN 91
TELECOM 33**

VERMERK

des Vorsitzes
für den Rat

Nr. Vordokument: 8864/05 COPEN 91 TELECOM 33

Betr.: Entwurf eines Rahmenbeschlusses über die Vorratsspeicherung von Daten, die in Verbindung mit der Bereitstellung öffentlicher elektronischer Kommunikationsdienste verarbeitet und aufbewahrt werden, oder von Daten, die in öffentlichen Kommunikationsnetzen vorhanden sind, für die Zwecke der (...) Untersuchung, Feststellung und Verfolgung von Straftaten, einschließlich Terrorismus

I. EINLEITUNG

Der AStV hat den oben genannten Entwurf eines Rahmenbeschlusses am 19. Mai 2005 auf der Grundlage von Dok. 8864/05 COPEN 91 TELECOM 33 geprüft. Artikel 2 Absatz 2 und Artikel 6 wurden am 20. Mai 2005 gemäß den Weisungen des AStV von den JI-Referenten geprüft.

Der aus diesen Prüfungen hervorgegangene Text ist in der Anlage wiedergegeben.

Das Europäische Parlament ist gebeten worden, eine Stellungnahme zu dem Entwurf abzugeben.

Mehrere Delegationen haben allgemeine Prüfungsvorbehalte und allgemeine Parlamentsvorbehalte zu dem Entwurf eingelegt. Die Kommission hat einen allgemeinen Prüfungsvorbehalt eingelegt.

Der Rat wird ersucht, die in Abschnitt II aufgeführten Fragen zu prüfen. Bestimmte weitere Fragen sind in den Fußnoten zum Rahmenbeschluss dargelegt.

II. FRAGEN FÜR DEN RAT

- a. **Artikel 2 - Liste der auf Vorrat zu speichernden Kommunikationsdaten**
Artikel 4 - Fristen für die Vorratsspeicherung von Kommunikationsdaten

Der Vorschlag des Vorsitzes für Artikel 2 (siehe Anlage) geht auf den Vorschlag zurück, eine von der **GESTRICHEN** Delegation vorgelegte Liste (siehe Dok. 7833/05 COPEN 69 TELECOM 22) inhaltlich in Artikel 2 einzuarbeiten.

Die Delegationen konnten diesem Ansatz im Wesentlichen - und unbeschadet einer Prüfung bestimmter technischer Einzelheiten der Liste durch Experten - zustimmen.

Zwei Delegationen (**GESTRICHEN**) waren allerdings der Ansicht, die Liste solle, was die Telefonie anbelangt, auf erfolgreich abgehende Anrufe beschränkt werden. Die große Mehrzahl der anderen Delegationen war nicht für eine solche Beschränkung.

Vorbehaltlich der Prüfungsvorbehalte einiger Delegationen konnten die meisten Delegationen die Fristen in Artikel 4 akzeptieren.

In Artikel 4 Absatz 1 ist als allgemeine Regelung vorgesehen, dass Kommunikationsdaten 12 Monate lang auf Vorrat gespeichert werden. Nach Artikel 4 Absatz 3 wäre es den Mitgliedstaaten möglich, in Ausnahmefällen eine kürzere Frist vorzusehen. Diese muss jedoch mindestens 6 Monate betragen. **GESTRICHEN** vertraten die Ansicht, dass eine Frist von mindestens 6 Monaten für bestimmte Arten von Daten zu lang sein könnte. **GESTRICHEN** legte einen Prüfungsvorbehalt ein und würde es vorziehen, wenn die Telefonie aus dem Geltungsbereich von Artikel 4 Absatz 3 ausgenommen würde.

Der Rat wird ersucht,

- *das Einvernehmen über den Ansatz des Vorsitzes für Artikel 2 zu bestätigen. Hierzu gehört eine Mindestliste der auf Vorrat zu speichernden Kommunikationsdaten. Diese Liste sollte vor allem praktisch ausgerichtet sein (sie sollte sich auf das konzentrieren, was den Daten zu entnehmen sein sollte), aber auch einige technische Einzelheiten zu bestimmten Arten des Fernmeldeverkehrs umfassen. Diese technischen Einzelheiten sollten auf ein Minimum begrenzt sein, so dass die Liste nicht ständig aktualisiert werden muss;*
- *zu prüfen, ob die Liste in Artikel 2 Absatz 2, was die Telefonie anbelangt, auf erfolgreich abgehende Anrufe beschränkt werden sollte oder ob eine kürzere Liste für nicht erfolgreich abgehende Anrufe in Betracht gezogen werden sollte;*
- *zuzustimmen, dass die Gruppe ein spezielles und flexibles Verfahren festlegt, um sicherzustellen, dass die Liste in Artikel 2 Absatz 2 nicht aufgrund technischer Entwicklungen obsolet wird;*
- *Artikel 4 zu billigen. Falls keine Einigung zu Artikel 4 Absatz 3 erzielt wird, wird der Rat ersucht, die Gruppe mit der Prüfung der Frage zu beauftragen, für welche Daten eine kürzere Mindestfrist als 6 Monate erforderlich sein könnte, wobei zu bedenken ist, dass Absatz 3 nur als Ausnahmeregelung für bestimmte Daten Anwendung finden sollte.*

b. Artikel 6 - Zugang zu auf Vorrat gespeicherten Daten
Artikel 7 - Justizielle Zusammenarbeit

Artikel 6 wurde in der Sitzung der JI-Referenten leicht umformuliert, um Bedenken von **GESTRICHEN** Rechnung zu tragen. Die ersten Reaktionen auf die neue Formulierung waren positiv, wobei einige Delegationen noch einen Prüfungsvorbehalt hatten. Die Kommission legte einen Vorbehalt ein; ihres Erachtens sollte Artikel 6 gestrichen werden.

In Bezug auf Rechtshilfeersuchen zu Daten, die nach Maßgabe des Rahmenbeschlusses auf Vorrat gespeichert worden sind, ist im zweiten Satz von Artikel 7 vorgesehen, dass der ersuchte Mitgliedstaat seine Zustimmung zu einem solchen Ersuchen mit den Auflagen versehen kann, die in einem vergleichbaren innerstaatlichen Fall gelten würden. Mehrere Delegationen und die Kommission baten um die Streichung dieses Satzes, der ihrer Ansicht nach dazu führen könnte, dass Rechtshilfeersuchen in einem größeren Umfang abgelehnt werden könnten, als es im Rahmen der derzeitigen Rechtsinstrumente möglich ist. Andere Delegationen (**GESTRICHEN**) waren hingegen der Meinung, dass dieser Satz nicht gestrichen werden sollte.

Offenbar könnten die Delegationen, die sich für den zweiten Satz ausgesprochen hatten, akzeptieren, dass auf Kommunikationsdaten die gegenwärtigen Rechtshilfevereinbarungen angewandt würden. Diese Art von Daten gibt es bereits, und sie können auch jetzt schon Gegenstand eines Rechtshilfeersuchens sein. Es wäre allerdings eine neue Situation gegeben, wenn diese Daten unter die Europäische Beweisverordnung fallen würden. Der derzeitige Entwurf des Rahmenbeschlusses über die Europäische Beweisverordnung bezieht offenbar die Kommunikationsdaten ein. Die Anwendung der Europäischen Beweisverordnung auf diese Daten könnte für einige Mitgliedstaaten bedeuten, dass ihr Spielraum zur Ablehnung der Übermittlung von Kommunikationsdaten im Vergleich zur gegenwärtigen Situation eingeschränkt würde.

Vor dem Hintergrund der Beratungen verwies der Vorsitz darauf, dass ein Ausweg darin bestehen könnte, diese Frage nicht im Rahmenbeschluss über die Vorratsspeicherung von Kommunikationsdaten, sondern im Zusammenhang mit der Europäischen Beweisverordnung zu regeln. Um nicht die Annahme des ersten Rechtsinstrumentes zur Europäischen Beweisverordnung zu verzögern, könnte in Betracht gezogen werden, diejenigen Kommunikationsdaten, die der Vollstreckungsbehörde bei Erlass der Anordnung noch nicht vorliegen, auszunehmen und diese Daten in einer zweiten Phase zu behandeln¹. Viele Delegationen könnten diesem Ansatz zustimmen. **GESTRICHEN** und KOM haben einen Vorbehalt eingelegt.

Der Vorsitz ersucht den AStV/Rat,

- *den in der Anlage wiedergegebenen Artikel 6 zu billigen und*
- *folgender Lösung für Artikel 7 zuzustimmen:*
 - *der zweite Satz von Artikel 7 wird gestrichen und*
 - *Kommunikationsdaten, die der Vollstreckungsbehörde bei Erlass einer sich auf die Kommunikationsdaten erstreckenden Europäischen Beweisverordnung noch nicht vorliegen, werden aus dem ersten Rechtsinstrument zur Europäischen Beweisverordnung ausgenommen; sie sollen unter noch genauer zu klärenden Bedingungen in ein späteres Rechtsinstrument aufgenommen werden.*

¹ Dies würde bedeuten, dass in Artikel 3 Absatz 2 des Entwurfs eines Rahmenbeschlusses über die Europäische Beweisverordnung eine Bezugnahme auf Kommunikationsdaten aufgenommen würde. Artikel 3 Absatz 2 des genannten Entwurfs würde Anwendung finden. Die Angaben beziehen sich auf Dok. 8416/05 COPEN 79.

c. Rechtsgrundlage

Nach dem Vorschlag für einen Rahmenbeschluss sind die Mitgliedstaaten verpflichtet sicherzustellen, dass bestimmte Kommunikationsdaten für einen festgelegten Zeitraum auf Vorrat gespeichert werden. Darunter können auch Daten fallen, die ansonsten nach der Richtlinie 2002/58/EG über den Schutz der Privatsphäre und die elektronische Kommunikation gelöscht werden müssten.

Der Vorschlag für einen Rahmenbeschluss ist auf Artikel 31 Absatz 1 Buchstabe c und Artikel 34 Absatz 2 Buchstabe b EUV gestützt. Die Kommission hat in einer frühen Phase der Verhandlungen einen Prüfungsvorbehalt zur Rechtsgrundlage eingelegt und ist auf der Tagung des Rates (Justiz und Inneres) vom 2. Dezember 2004 bei dieser Haltung geblieben. Nachdem sie diese Frage geprüft hat, hat die Kommission einen Vorbehalt zur Rechtsgrundlage eingelegt. Die Dienststellen der Kommission haben die Gründe für diesen Vorbehalt in Dok. 7735/05 COPEN 64 JUR 138 dargelegt. Nach Ansicht der Kommission fallen die Teile des Vorschlags, in denen eine Harmonisierung der auf Vorrat zu speichernden Datentypen vorgesehen ist, und die Fristen für die Vorratsspeicherung dieser Daten in die Zuständigkeit der EG und müssen auf der Grundlage von Artikel 95 EGV angenommen werden.

Der Juristische Dienst des Rates hat in Dok. 7688/05 JUR 137 COPEN 62 TELECOM 21 zu dieser Frage Stellung genommen. **GESTRICHEN**

Die Kommission erarbeitet derzeit einen Vorschlag für eine Richtlinie über die Vorratsspeicherung von Daten.

Die Delegationen der vier Mitgliedstaaten, die den Vorschlag für einen Rahmenbeschluss unterbreitet hatten (**GESTRICHEN**), wurden von einigen anderen Delegationen unterstützt, die die Auffassung vertraten, dass Titel VI EUV die richtige Rechtsgrundlage für den Vorschlag sei. Mehrere Delegationen legten einen Prüfungsvorbehalt zu dieser Frage ein, die auf höherer Ebene geprüft werden muss.

Der AStV/Rat wird ersucht, die Frage der Rechtsgrundlage und ihre möglichen Auswirkungen auf die Beratungen zu prüfen, wobei zu bedenken ist, dass der Europäische Rat in seiner Erklärung vom 25. März 2004 zum Kampf gegen den Terrorismus dazu aufgerufen hat, bis Juni 2005 ein Rechtsinstrument über die Aufbewahrung von Daten anzunehmen.

III. FAZIT

Der AStV/Rat wird ersucht, die in Abschnitt II dargelegten Fragen zu prüfen, damit so schnell wie möglich eine endgültige Einigung über den Entwurf erzielt werden kann, wobei zu bedenken ist, dass der Europäische Rat in seiner Erklärung vom 25. März 2004 zum Kampf gegen den Terrorismus dazu aufgerufen hat, bis Juni 2005 ein Rechtsinstrument über die Aufbewahrung von Daten anzunehmen.

Entwurf**Rahmenbeschluss**

über die Vorratsspeicherung von Daten, die in Verbindung mit der Bereitstellung öffentlicher elektronischer Kommunikationsdienste verarbeitet und aufbewahrt werden, oder von Daten, die in öffentlichen Kommunikationsnetzen vorhanden sind, für die Zwecke der (...), Untersuchung, Feststellung und Verfolgung von Straftaten, einschließlich Terrorismus^{1 2}

DER RAT DER EUROPÄISCHEN UNION –

gestützt auf den Vertrag über die Europäische Union, insbesondere auf Artikel 31 Absatz 1 Buchstabe c und Artikel 34 Absatz 2 Buchstabe b,

auf Initiative der Französischen Republik, Irlands, des Königreichs Schweden und des Vereinigten Königreichs,

nach Stellungnahme des Europäischen Parlaments,

in Erwägung nachstehender Gründe:

- (1) Ein hohes Maß an Schutz in einem Raum der Freiheit, der Sicherheit und des Rechts erfordert eine angemessene (...), Untersuchung, Feststellung und Verfolgung von Straftaten.
- (2) Die Forderung nach Maßnahmen gegen die Hightech-Kriminalität wurde im Aktionsplan des Rates und der Kommission zur bestmöglichen Umsetzung der Bestimmungen des Amsterdamer Vertrags über den Aufbau eines Raumes der Freiheit, der Sicherheit und des Rechts, in den Schlussfolgerungen des Europäischen Rates (Tampere, 15./16. Oktober 1999 und Santa Maria da Feira, 19./20. Juni 2000), von der Kommission im "Fortschrittsanzeiger" sowie vom Europäischen Parlament in seiner Entschließung vom 19. Mai 2000 zum Ausdruck gebracht.

¹ Die Präambel wird später geprüft.

² Angesichts der Ausführungen **GESTRICHEN** auf der Tagung des AStV vom 19. Mai 2005 hat der Vorsitz, vorbehaltlich einer weiteren Prüfung, den Ausdruck "Vorbeugung" aus dem Titel des Entwurfs und aus bestimmten Erwägungsgründen gestrichen.

- (3) Der Rat weist in seinen Schlussfolgerungen vom 20. September 2001 darauf hin, dass dafür zu sorgen ist, dass die Strafverfolgungsbehörden die Möglichkeit erhalten, Ermittlungen zu kriminellen Handlungen durchzuführen, die unter Nutzung elektronischer Kommunikationssysteme begangen wurden, und Maßnahmen gegen die Urheber zu ergreifen, wobei darauf zu achten ist, dass ein Gleichgewicht zwischen dem Schutz personenbezogener Daten und der Notwendigkeit des Zugangs der Strafverfolgungsbehörden zu Daten für strafrechtliche Ermittlungszwecke gewährleistet wird. Der Rat stellt in seinen Schlussfolgerungen vom 19. Dezember 2002 fest, dass die beträchtliche Zunahme der Möglichkeiten elektronischer Kommunikation dazu geführt hat, dass Daten über die Nutzung elektronischer Kommunikationsmittel heutzutage ein besonders wichtiges und hilfreiches Mittel bei der (...), Untersuchung, Feststellung und Verfolgung von Straftaten, insbesondere von organisierter Kriminalität und Terrorismus, darstellen.
- (4) In der vom Europäischen Rat am 25. März 2004 angenommenen Erklärung zum Kampf gegen den Terrorismus wurde der Rat beauftragt, im Hinblick auf ihre Annahme bis Juni 2005 Maßnahmen für die Erarbeitung von Rechtsvorschriften über die Aufbewahrung von Verkehrsdaten durch Diensteanbieter zu prüfen.
- (5) Es ist von wesentlicher Bedeutung, dass in öffentlichen Kommunikationsnetzen vorhandene Daten, die aufgrund eines Kommunikationsvorgangs erzeugt worden sind, nachstehend "Daten" genannt, für die (...) Untersuchung, Feststellung und Verfolgung von Straftaten, die unter Nutzung elektronischer Kommunikationssysteme begangen wurden, auf Vorrat gespeichert werden. Dieser Vorschlag bezieht sich nur auf Daten, die aufgrund eines Kommunikationsvorgangs erzeugt worden sind, und nicht auf Daten, die den Kommunikationsinhalt darstellen. Es ist insbesondere erforderlich, Daten auf Vorrat zu speichern, um die Quelle eines illegalen Inhalts, z.B. Kinderpornografie und rassistisches und fremdenfeindliches Material, sowie die Urheber von Angriffen auf Informationssysteme ermitteln und diejenigen identifizieren zu können, die an der Nutzung elektronischer Kommunikationsnetze für die Zwecke der organisierten Kriminalität und des Terrorismus beteiligt sind.

- (6) Die Sicherungsspeicherung bestimmter Daten zu bestimmten Personen in besonderen Fällen allein reicht nicht aus, um diesen Anforderungen zu entsprechen. Bei den Ermittlungen kann es vorkommen, dass die benötigten Daten oder die beteiligte Person erst Monate oder Jahre nach dem ursprünglichen Kommunikationsvorgang identifiziert werden können. Daher ist es erforderlich, bestimmte Datentypen, die bereits zu Fakturierungszwecken, zu kommerziellen Zwecken oder zu anderen rechtmäßigen Zwecken verarbeitet und gespeichert werden, während eines bestimmten zusätzlichen Zeitraums aus der Überlegung heraus auf Vorrat zu speichern, dass sie für künftige Ermittlungen oder Gerichtsverfahren erforderlich sein könnten. Dieser Rahmenbeschluss betrifft daher die Vorratsspeicherung von Daten und nicht die Sicherungsspeicherung von Daten.
- (7) In Anerkennung der Notwendigkeit, Daten auf Vorrat zu speichern, wurde in Artikel 15 der Richtlinie 2002/58/EG die Möglichkeit vorgesehen, Rechtsvorschriften zu erlassen, die unter bestimmten Voraussetzungen die Vorratsspeicherung von Daten für die Zwecke der Vorbeugung, Untersuchung, Feststellung und Verfolgung von Straftaten ermöglichen. Der vorliegende Rahmenbeschluss betrifft nicht die anderen Zielsetzungen nach Artikel 15 der genannten Richtlinie und enthält daher keine Vorschriften über die Vorratsspeicherung von Daten für den Schutz der nationalen Sicherheit (d.h. die Sicherheit des Staates), die Landesverteidigung und die öffentliche Sicherheit. Er betrifft auch nicht die unrechtmäßige Nutzung des elektronischen Kommunikationssystems, wenn diese Nutzung keine strafbare Handlung darstellt.
- (8) Viele Mitgliedstaaten haben Rechtsvorschriften über eine Vorratsspeicherung von Daten zum Zwecke der Vorbeugung, Untersuchung, Feststellung und Verfolgung von Straftaten erlassen. In anderen Mitgliedstaaten sind entsprechende Arbeiten im Gang. Der Inhalt dieser Rechtsvorschriften ist in den einzelnen Mitgliedstaaten sehr unterschiedlich.

- (9) Die Unterschiede zwischen den Rechtsvorschriften der Mitgliedstaaten beeinträchtigt die Zusammenarbeit der für die (...) Untersuchung, Feststellung und Verfolgung von Straftaten zuständigen Behörden. Für eine wirksame polizeiliche und justizielle Zusammenarbeit in Strafsachen muss daher sichergestellt werden, dass alle Mitgliedstaaten die erforderlichen Schritte unternehmen, um bestimmte Datentypen eine gewisse Zeit gemäß festgelegten Vorgaben für die Zwecke der (...) Untersuchung, Feststellung und Verfolgung von Straftaten, einschließlich Terrorismus, auf Vorrat zu speichern. Diese Daten sollten den anderen Mitgliedstaaten gemäß den nach Titel VI des Vertrags über die Europäische Union angenommenen Rechtsakten über die justizielle Zusammenarbeit in Strafsachen zur Verfügung stehen. Dies sollte auch für Regelungen gelten, die nicht gemäß diesem Titel angenommen wurden, denen aber die Mitgliedstaaten beigetreten sind und auf die in den Rechtsakten über die justizielle Zusammenarbeit in Strafsachen Bezug genommen wird, die nach Titel VI des Vertrags über die Europäische Union angenommen wurden.
- (10) Diese Vorratsspeicherung von Daten und der Zugriff auf diese Daten können einen Eingriff in das Privatleben des Einzelnen darstellen. Diese Eingriffe stellen jedoch keine Verletzung der internationalen Vorschriften über den Schutz der Privatsphäre und die Verarbeitung personenbezogener Daten dar, die insbesondere in der Europäischen Konvention zum Schutze der Menschenrechte und Grundfreiheiten vom 4. November 1950, im Übereinkommen Nr. 108 des Europarates zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten sowie in den Richtlinien 95/46/EG, 97/66/EG und 2002/58/EG enthalten sind, in denen solche Eingriffe gesetzlich vorgesehen sind, sofern sie zweckdienlich sind, in einem strikt angemessenen Verhältnis zum intendierten Zweck stehen und innerhalb einer demokratischen Gesellschaft notwendig sind und sofern sie mit angemessenen Garantien im Hinblick auf die (...) Untersuchung, Feststellung und Verfolgung von Straftaten, einschließlich Terrorismus, verbunden sind.
- (11) Angesichts der Notwendigkeit einer wirksamen und harmonisierten Vorratsspeicherung der Daten und des Erfordernisses, den Mitgliedstaaten wegen der Unterschiede zwischen den einzelstaatlichen strafrechtlichen Systemen genügend Handlungsspielraum für ihre eigene individuelle Bewertung einzuräumen, sollten Parameter für die Vorratsspeicherung von Daten festgelegt werden.

- (12) Daten dürfen je nach Datentyp für unterschiedliche Fristen auf Vorrat gespeichert werden. Die Fristen für die Vorratsspeicherung der einzelnen Datentypen richten sich nach dem Nutzen der Daten für die (...) Untersuchung, Feststellung und Verfolgung von Straftaten und nach den Kosten der Vorratsspeicherung der Daten. Die Fristen der Vorratsspeicherung müssen in einem angemessenen Verhältnis zur Notwendigkeit solcher Daten für die Zwecke der (...) Untersuchung, Feststellung und Verfolgung von Straftaten sowie zum Eingriff in die Privatsphäre stehen, zu der eine solche Vorratsspeicherung im Falle einer Freigabe solcher Daten führen wird.
- (13) Bei der Erstellung von Listen der auf Vorrat zu speichernden Datentypen ist auf eine ausgewogene Berücksichtigung des Nutzens der Aufbewahrung der einzelnen Datentypen für die (...) Untersuchung, Feststellung und Verfolgung von Straftaten und des damit verbundenen Umfangs des Eingriffs in die Privatsphäre zu achten.
- (14) Dieser Rahmenbeschluss gilt nicht für den Zugriff auf Daten während der Übertragung, d.h. für das Abhören, die Überwachung oder die Aufzeichnung von Telekommunikationsvorgängen.
- (15) Die Mitgliedstaaten müssen sicherstellen, dass der Zugriff auf die auf Vorrat gespeicherten Daten unter Beachtung der Datenschutzbestimmungen erfolgt, die in den völkerrechtlichen Vorschriften über den Schutz personenbezogener Daten festgelegt sind.
- (16) Die Mitgliedstaaten stellen sicher, dass die Durchführung des Rahmenbeschlusses nach entsprechender Konsultation der Industrie erfolgt –

HAT FOLGENDEN RAHMENBESCHLUSS ANGENOMMEN:

Artikel 1¹

Geltungsbereich und Ziel

(1) Mit diesem Rahmenbeschluss soll die justizielle Zusammenarbeit in Strafsachen erleichtert werden, indem die Rechtsvorschriften der Mitgliedstaaten über die Vorratsspeicherung von Kommunikationsdaten², die von Anbietern eines öffentlich zugänglichen elektronischen Kommunikationsdienstes oder von Betreibern eines öffentlichen Kommunikationsnetzes erzeugt oder verarbeitet³ werden, für die Zwecke der Untersuchung, Feststellung und Verfolgung von Straftaten angeglichen werden.⁴

¹ **GESTRICHEN** haben einen Prüfungsvorbehalt zu Artikel 1.

² **GESTRICHEN** legte einen Prüfungsvorbehalt zur Verwendung des Begriffs "*communication*" ein, der in der Richtlinie 2002/58/EG definiert ist. Der Vorsitzende bemerkte dazu, dass im vorliegenden Entwurf der Begriff "*communication data*" ("Kommunikationsdaten") und nicht nur "*communication*" benutzt werde und der Text somit nicht in Konflikt mit der Definition von "*communication*" ("Nachricht") in der genannten Richtlinie stehe.

³ **GESTRICHEN** schlug den folgenden Erwägungsgrund vor: "Der Begriff "verarbeitet" sollte sich nur auf solche Daten beziehen, die erforderlich sind, um Verbindungen für diesen Dienst herzustellen, aufrecht zu erhalten und zu verwalten (Verkehrsdaten zu Teilnehmern und Nutzern, die vom Betreiber eines öffentlichen Kommunikationsnetzes oder vom Anbieter eines öffentlich zugänglichen elektronischen Kommunikationsdienstes verarbeitet werden); Daten, die hierzu nicht erforderlich sind, sollten nicht eingeschlossen sein (z.B. die Betreffzeile in einer E-Mail)."

Einige Delegationen haben einen Prüfungsvorbehalt zu diesem Vorschlag.

⁴ **GESTRICHEN** schlägt folgenden neuen Erwägungsgrund vor:
"(10) Schon die Speicherung von Verkehrs- und Standortdaten stellt einen erheblichen Eingriff in die persönlichen Freiheitsrechte der Nutzer von Telekommunikationsdiensten dar, insbesondere in diejenigen persönlichen Freiheitsrechte, die in den Richtlinien 95/46/EG und 2002/58/EG sowie in Artikel 7 und 8 der Charta der Grundrechte der Europäischen Union verankert sind. Somit ist die Einführung einer rechtlichen Verpflichtung für Netzbetreiber und Diensteanbieter, solche Daten über einen bestimmten Zeitraum zu speichern, in einem Raum der Freiheit, der Sicherheit und des Rechts nur dann zu rechtfertigen, wenn dies notwendig ist, um in einer demokratischen Gesellschaft wichtige Interessen zu wahren. Unbeschadet zusätzlicher gesetzlicher Regelungen in Bezug auf den Zugang zu gespeicherten Daten in den Mitgliedstaaten, ergibt sich diese Notwendigkeit aus der großen Bedeutung, die der späteren Auswertung von Verkehrs- und Standortdaten insbesondere für die Aufklärung von terroristischen Straftaten oder anderen schweren Straftaten zukommt. Dies ist darauf zurückzuführen, dass historische Verkehrs- und Standortdaten oftmals den einzigen Erfolg versprechenden Ermittlungsansatz für eine tatsächliche Aufklärung solcher Straftaten darstellen und ihre Verfügbarkeit für einen bestimmten Zeitraum nur mit Hilfe einer gesetzlichen Verpflichtung auf zuverlässige Weise gewährleistet werden kann."

(2) Dieser Rahmenbeschluss gilt für alle Formen der elektronischen Kommunikation ¹, darunter insbesondere

- a)² Telefonie, ausgenommen SMS-Dienste (Short Message Services), EMS-Dienste (Enhanced Messaging Services) und MMS-Dienste (Multi Media Messaging Services);
- b) SMS-Dienste, EMS-Dienste und MMS-Dienste, die als Teil eines Telefondienstes angeboten werden;
- c) Internetzugangsdienste und Internetdienste.

(3) Dieser Rahmenbeschluss gilt nicht für den Inhalt des Kommunikationsaustauschs, auch nicht für den Abruf von Informationen unter Verwendung eines elektronischen Kommunikationsnetzes.

(4) Unberührt von diesem Rahmenbeschluss bleiben

- nationale Rechtsvorschriften über die Vorratsspeicherung von Kommunikationsdaten, die von Anbietern eines öffentlich zugänglichen elektronischen Kommunikationsdienstes oder von Betreibern eines öffentlichen Kommunikationsnetzes für die Zwecke der Verhütung von Straftaten verarbeitet oder erzeugt werden;
- die für die justizielle Zusammenarbeit in Strafsachen geltenden Vorschriften über die Überwachung und Aufzeichnung von Telekommunikationsvorgängen;
- die im Rahmen der polizeilichen Zusammenarbeit geltenden Vorschriften über den Informationsaustausch; ³
- Maßnahmen im Bereich der öffentlichen Sicherheit, der Landesverteidigung und der nationalen Sicherheit (d.h. der Sicherheit des Staates);

¹ **GESTRICHEN** schlug folgende Formulierung vor: "...für alle Formen der öffentlich zugänglichen Telekommunikation in öffentlichen Netzen". Einige Delegationen äußerten sich hierzu positiv. Andere Delegationen fanden, dies könne Verwirrung stiften; dieser Aspekt sei durch Artikel 1 Absatz 1 abgedeckt. Prüfungsvorbehalt von **GESTRICHEN**.

² Die Buchstaben a und b können je nach Ergebnis der Beratungen über Artikel 4 Absatz 3 eventuell zusammengelegt werden.

³ Prüfungsvorbehalt von **GESTRICHEN**.

Artikel 2

Begriffsbestimmungen

- (1) Im Sinne dieses Rahmenbeschlusses bezeichnet der Ausdruck "Kommunikationsdaten"
- a) Verkehrsdaten und Standortdaten nach Artikel 2 der Richtlinie 2002/58/EG;
 - b) Nutzerdaten, d.h. Daten zu einem Nutzer¹, der einen öffentlich zugänglichen elektronischen Kommunikationsdienst für private oder geschäftliche Zwecke nutzt, ohne dass er diesen Dienst notwendigerweise abonniert haben muss;
 - c) Teilnehmerdaten, d.h. Daten zu einer juristischen oder natürlichen Person, die einen öffentlich zugänglichen elektronischen Kommunikationsdienst für private oder geschäftliche Zwecke abonniert hat, ohne diesen Dienst notwendigerweise in Anspruch genommen zu haben.

¹ Prüfungsvorbehalt von **GESTRICHEN**.

(2)¹²³ Kommunikationsdaten, die für die in Artikel 1 genannten Zwecke auf Vorrat zu speichern sind, umfassen⁴

- a) Daten, die zur Rückverfolgung und Identifizierung der Quelle einer Nachricht erforderlich sind, einschließlich von Einzelheiten zur Person, Kontaktinformationen und Informationen zur Identifizierung der abonnierten Dienste⁵; dazu gehören mindestens folgende Daten:
 1. Telefonfestnetz
 - a) Rufnummer des anrufenden und angerufenen Anschlusses,
 - b) Namen und Anschriften der Teilnehmer, auf die die Telefonnummern zum Zeitpunkt der Verbindung angemeldet waren,
 - c) in Anspruch genommener Telefondienst;
 2. Mobilfunk
 - a) Rufnummer des anrufenden und angerufenen Anschlusses und soweit vorhanden Kennung der Endeinrichtung (IMEI),
 - b) in Anspruch genommener Telefondienst,
 - c) Namen und Anschriften der Teilnehmer, auf die die Telefonnummern zum Zeitpunkt der Verbindung angemeldet waren;
 3. Internet
 - a) vom Internetzugangsanbieter einer Verbindung zugewiesene dynamische oder statische IP-Adressen,
 - b) Name und Anschrift des Nutzers, dem die Anschluss- oder Benutzerkennung zum Zeitpunkt der Verbindung zugewiesen war,
 - c) Anschluss- oder Benutzerkennung, über die die Verbindung zum Internetzugangsanbieter hergestellt wurde;

¹ Siehe Abschnitt II.a der Einleitung. Artikel 2 Absatz 2 Buchstaben b, c, d, e und f könnten geändert/gestrichen werden, je nachdem, welche endgültige Fassung Artikel 2 Absatz 2 Buchstabe a erhält. **GESTRICHEN** hat mehrere Vorschläge unterbreitet, die von den Experten weiter geprüft werden.

² Einige Delegationen haben Vorbehalte zu Buchstabe b ("Leitweg") und Buchstabe f ("während").

³ **GESTRICHEN** waren der Auffassung, dass im Zusammenhang mit der Telefonie nur erfolgreich abgehende Anrufe abgedeckt sein sollten.

⁴ **GESTRICHEN** schlägt folgende Formulierung vor:

"Für die Zwecke dieses Rahmenbeschlusses sollte eine Vorratsspeicherung von Daten in jedem Fall auf solche Verkehrsdaten beschränkt werden, die vom Betreiber beim Zugang eines Teilnehmers zum Netz erzeugt werden und die erforderlich sind, um eine (zu einem bestimmten Zeitpunkt) genutzte Netzadresse einem bestimmten Teilnehmer zuzuordnen ("Zugangsdaten").

Zu diesen Daten gehören die im Anhang dieses Rahmenbeschlusses aufgelisteten Daten."

⁵ **GESTRICHEN** schlug folgende Formulierung vor: "Daten, die zur Rückverfolgung und Identifizierung der Quelle einer Nachricht erforderlich sind, und die mit dieser Quelle verbundenen Nutzer- oder Teilnehmerdaten." **GESTRICHEN** schlug folgende Formulierung vor: "Daten, die zur Rückverfolgung und Identifizierung der Quelle einer Nachricht erforderlich sind, und die mit dieser Quelle verbundenen Nutzerdaten und Einzelheiten zum Teilnehmer."

- b) Daten, die zur Ermittlung des Leitwegs und des Bestimmungsziels einer Nachricht notwendig sind;¹
- c) Daten, die zur Ermittlung des Zeitpunkts und des Datums sowie der Dauer eines Kommunikationsvorgangs notwendig sind; dazu gehören mindestens folgende Daten:
für Telefonfestnetz, Mobilfunk und Internet
- a) Beginn,
- b) Dauer oder Ende der Verbindung
mit Angabe von Datum und Uhrzeit auf der Grundlage einer bestimmten Zeitzone;
- d) Daten, die zur Identifizierung des Telekommunikationsvorgangs notwendig sind;
- e) Daten, die zur Ermittlung der Endeinrichtung oder der vorgeblichen Endeinrichtung erforderlich sind;
- f) Daten, die zur Ermittlung des Standorts zu Beginn und während der gesamten Dauer des Kommunikationsvorgangs notwendig sind²; dazu gehören mindestens folgende Daten:
für den Mobilfunk: die Standortkennung (Cell-ID) zu Beginn der Verbindung.

¹ **GESTRICHEN** schlug folgende Formulierung vor: "Daten, die zur Ermittlung des Zwischen- und Endbestimmungsziels einer Nachricht notwendig sind;".

² **GESTRICHEN** schlug folgende Formulierung vor: "Daten, die zur Ermittlung des Standorts zu Beginn, am Ende und gegebenenfalls während der gesamten Dauer des Kommunikationsvorgangs notwendig sind".

*Artikel 3*¹

Vorratsspeicherung von Kommunikationsdaten

(1) Jeder Mitgliedstaat trifft die erforderlichen Maßnahmen, um sicherzustellen, dass für die Zwecke der justiziellen Zusammenarbeit in Strafsachen Kommunikationsdaten nach Artikel 2 Absatz 2, die von Anbietern eines öffentlich zugänglichen elektronischen Kommunikationsdienstes oder von Betreibern eines öffentlichen Kommunikationsnetzes erzeugt oder verarbeitet werden, gemäß den Bestimmungen dieses Rahmenbeschlusses auf Vorrat gespeichert werden.

(2)² Die Mitgliedstaaten ergreifen die geeigneten Maßnahmen für die technische Umsetzung von Absatz 1.

¹ Es wurde vorgeschlagen, Artikel 3 und 4 zu verschmelzen.

² Ob Artikel 3 Absatz 2 aufgenommen wird, oder wie weiter mit ihm verfahren wird, hängt von den weiteren Beratungen über Artikel 2 ab.

Artikel 4^{1 2}

Fristen für die Vorratsspeicherung von Kommunikationsdaten

- (1) Jeder Mitgliedstaat trifft die erforderlichen Maßnahmen, um sicherzustellen, dass die in Artikel 3 genannten Kommunikationsdaten nach ihrer Erzeugung 12 Monate lang auf Vorrat gespeichert werden. Für Teilnehmerdaten läuft diese Frist ab dem Ende des Abonnements.
- (2) Abweichend von Absatz 1 kann ein Mitgliedstaat für die Vorratsspeicherung der in Artikel 3 genannten Kommunikationsdaten gemäß den nationalen Kriterien längere Fristen von bis zu 48 Monaten vorsehen, wenn dies eine notwendige, angemessene und verhältnismäßige Maßnahme innerhalb einer demokratischen Gesellschaft darstellt.
- (3) Abweichend von Absatz 1 kann ein Mitgliedstaat für die Vorratsspeicherung der in Artikel 3 genannten Kommunikationsdaten in Bezug auf die Kommunikationsform nach Artikel 1 Absatz 2³ kürzere Fristen von mindestens 6 Monaten⁴ vorsehen, wenn er die Fristen für die Vorratsspeicherung nach Absatz 1 gemäß nationalen Verfahrens- oder Konsultationsprozessen nicht für annehmbar hält.
- (4) Ein Mitgliedstaat, der beschließt, Absatz 2 oder 3 anzuwenden, setzt den Rat und die Kommission von den für die Vorratsspeicherung vorgesehenen Fristen unter Angabe der betreffenden Kommunikationsdaten in Kenntnis. Diese Ausnahmen werden mindestens alle fünf Jahre überprüft.

¹ Siehe Abschnitt II.a der Einleitung.

² **GESTRICHEN** haben einen Prüfungsvorbehalt zu Artikel 4.

³ Vorbehalt von **GESTRICHEN**, die keine Mindestfrist wünschte und der Auffassung war, dass drei Monate in jedem Fall ausreichend seien. Prüfungsvorbehalt von **GESTRICHEN**.

⁴ Prüfungsvorbehalt von **GESTRICHEN**, die der Ansicht war, dass die Bezugnahme auf Artikel 1 Absatz 2 durch eine Bezugnahme auf Artikel 1 Absatz 2 Buchstaben b und c (den früheren Text) ersetzt werden sollte.

Artikel 5¹
Datensicherheit

Jeder Mitgliedstaat trägt dafür Sorge, dass in Bezug auf die nach diesem Rahmenbeschluss auf Vorrat gespeicherten Kommunikationsdaten mindestens die nachstehenden Datensicherheitsgrundsätze eingehalten werden:

- a) Die auf Vorrat gespeicherten Daten sind von derselben Qualität wie die im Netz vorhandenen Daten;
- b) in Bezug auf die Daten werden geeignete technische und organisatorische Maßnahmen getroffen, um die Daten gegen zufällige oder unrechtmäßige Zerstörung, zufälligen Verlust, unberechtigte Änderung, unberechtigte Weitergabe oder unberechtigten Zugang und gegen jede andere Form der unrechtmäßigen Verarbeitung zu schützen;
- c) alle Daten werden am Ende der Vorratsspeicherungsfrist vernichtet, mit Ausnahme jener Daten, die abgerufen und gesichert worden sind;

¹ **GESTRICHEN** verwies auf ihren Vorschlag in Dok. 6909/05 COPEN 45 TELECOM 14.

GESTRICHEN schlug mit Unterstützung mehrerer Delegationen (**GESTRICHEN**) folgenden Wortlaut vor:

"Jeder Mitgliedstaat trägt dafür Sorge, dass die nach diesem Rahmenbeschluss auf Vorrat gespeicherten Daten mindestens den folgenden Datensicherheitsgrundsätzen unterliegen und dass die Bestimmungen von Artikel 4 der Richtlinie 2002/58/EG eingehalten werden:

- a) (unverändert)
- b) (unverändert)
- c) die Daten werden nicht an Personen weitergegeben, die nicht rechtmäßig für die Ermittlungen oder die Kontrolle der Rechtmäßigkeit der Ermittlungen zuständig sind;
- d) jeder Mitgliedstaat garantiert auf wirksame Weise durch technische und organisatorische Maßnahmen, dass der Zugang zu den auf Vorrat gespeicherten Daten nur berechtigten Personen und nur für einen im Einzelfall vorher festgelegten und begrenzten Zeitraum gewährt wird, nachdem die zuständige Justizbehörde die Rechtmäßigkeit des Zugangs geprüft hat;
- e) (ehemaliger Buchstabe c unverändert).

GESTRICHEN schlug mit Unterstützung von **GESTRICHEN** vor, Artikel 5 zu streichen und folgenden Erwägungsgrund aufzunehmen:

"(9a) Anbieter eines öffentlich zugänglichen elektronischen Telekommunikationsdienstes oder Betreiber eines öffentlichen Kommunikationsnetzes sind bei der Verarbeitung personenbezogener Daten an nationale, ein hohes Datenschutzniveau bietende Datenschutzbestimmungen gebunden, insbesondere an diejenigen Vorschriften, die nach der Richtlinie 95/46/EG zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr und der Richtlinie 2002/58/EG über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation erlassen worden sind. Diese Vorschriften sind einzuhalten, wenn personenbezogene Daten nach Maßgabe dieses Rahmenbeschlusses verarbeitet werden."

Mehrere Delegationen legten einen Prüfungsvorbehalt zu Artikel 5 ein. Einige Delegationen waren der Meinung, dass diese Bestimmung gestrichen werden sollte. Es gab eine gewisse Unterstützung für die ersten beiden Gedankenstriche des Vorschlags von **GESTRICHEN**.

Artikel 6¹

Zugang zu auf Vorrat gespeicherten Kommunikationsdaten

Jeder Mitgliedstaat stellt sicher, dass der Zugang zu den nach diesem Rahmenbeschluss auf Vorrat gespeicherten Kommunikationsdaten zu den in Artikel 1 genannten Zwecken² mindestens den nachstehenden Vorschriften unterliegt, und sieht Rechtsbehelfe gemäß den Bestimmungen des Kapitels III der Richtlinie 95/46/EG über "Rechtsbehelfe, Haftung und Sanktionen" vor:

- a) Die Daten werden von den zuständigen Behörden fallbezogen gemäß den nationalen Rechtsvorschriften nur für festgelegte, eindeutige und rechtmäßige Zwecke abgerufen und sie werden nur in einer Weise weiter verarbeitet, die mit diesen Zwecken vereinbar ist;
- aa) jeder Mitgliedstaat legt im innerstaatlichen Recht das Verfahren und die Bedingungen fest, die für den Abruf von auf Vorrat gespeicherten Daten und für die Sicherung abgerufener Daten einzuhalten sind³;
- b) die Daten entsprechen den Zwecken, für die sie abgerufen werden, sind für sie von Belang und stehen in angemessenem Verhältnis zu ihnen. Die Daten werden nach Recht und Billigkeit verarbeitet;
- c) von den zuständigen Behörden abgerufene Daten dürfen in einer Form, die die Identifizierung der betroffenen Personen ermöglicht, nicht länger gespeichert werden, als es für die Zwecke, für die sie erhoben und/oder weiter verarbeitet werden, erforderlich ist;
- d) die Vertraulichkeit und die Integrität der Daten ist zu gewährleisten;
- e) die Daten sind richtig und es werden alle erforderlichen Maßnahmen getroffen, damit personenbezogene Daten, die im Hinblick auf die Zwecke, für die sie erhoben und/oder weiter verarbeitet werden, unzutreffend sind, gelöscht oder berichtigt werden.

¹ Siehe Abschnitt II.b der Einleitung.

² Änderung, um den Bedenken von **GESTRICHEN** Rechnung zu tragen. Einige Delegationen haben einen Prüfungsvorbehalt dazu.

³ Prüfungsvorbehalt von **GESTRICHEN**.

Artikel 7

Ersuchen um Übermittlung von auf Vorrat gespeicherten Kommunikationsdaten im Rahmen der justiziellen Zusammenarbeit in Strafsachen

Jeder Mitgliedstaat kommt einem Ersuchen eines anderen Mitgliedstaats um Übermittlung von Kommunikationsdaten, die gemäß den Artikeln 3 und 4 auf Vorrat gespeichert wurden, gemäß den für die justizielle Zusammenarbeit in Strafsachen geltenden Rechtsakten nach. [Der ersuchte Mitgliedstaat kann seine Zustimmung zu einem solchen Ersuchen um Kommunikationsdaten mit den Auflagen versehen, die in einem vergleichbaren innerstaatlichen Fall gelten würden.]¹

Artikel 8

Umsetzung

Die Mitgliedstaaten treffen die erforderlichen Maßnahmen, um diesem Rahmenbeschluss (...) innerhalb von zwei Jahren nach seiner Annahme nachzukommen.

Innerhalb derselben Frist teilen die Mitgliedstaaten dem Generalsekretariat des Rates und der Kommission den Wortlaut der Bestimmungen mit, mit denen sie die sich aus diesem Rahmenbeschluss ergebenden Verpflichtungen in ihr innerstaatliches Recht umgesetzt haben. Das Generalsekretariat des Rates übermittelt den Mitgliedstaaten die gemäß diesem Artikel erhaltenen Informationen.

Die Kommission legt dem Rat bis [1. Januar 2008] einen Bericht vor, in dem untersucht wird, inwieweit die Mitgliedstaaten Maßnahmen getroffen haben, um diesem Rahmenbeschluss nachzukommen.

¹ Siehe Abschnitt II.b der Einleitung.

Artikel 9

Inkrafttreten

Dieser Rahmenbeschluss tritt am zwanzigsten Tag nach seiner Veröffentlichung im Amtsblatt der Europäischen Union in Kraft.
