

Brüssel, den 3 September 1998

10951/98

EINGEGANGEN am

LIMITE

15. Sep. 1998

ENFOPOL 98

**VERMERK**

---

des :       Vorsitzes

an :        die Gruppe "Polizeiliche Zusammenarbeit"

---

Nr. Vordok. : Abl. C 329, 4.11.1996, S. 1, 10102/98 ENFOPOL 87

---

betrifft : **Überwachung des Telekommunikationsverkehrs;  
Entwurf einer Ratsentschließung in bezug auf neue Technologien**

---

**Vorbemerkung:**

Die Delegationen erhalten für das Expertenmeeting der RAG "Polizeiliche Zusammenarbeit" am 3./4. September 1998 den Entwurf einer Ratsentschließung bezüglich der Überwachung des Telekommunikationsverkehrs betreffend erläuternder Memoranden, ergänzenden Anforderungen und Begriffsbestimmungen in bezug auf neue Technologien wie S-PCS, Internet, Bereitstellung von teilnehmer- und verbindungsrelevanten Daten, Kryptographie und Sicherheitsmaßnahmen bei Netzbetreibern/Diensteanbietern, wobei die verschiedenen Textstellen von den technischen Expertengruppen ILET, STC und IUR ausgearbeitet wurden.

# ENTWURF

## ENTSCHLIESSUNG DES RATES

vom ...

über die rechtmäßige Überwachung des Telekommunikationsverkehrs  
in bezug auf neue Technologien.

DER RAT DER EUROPÄISCHEN UNION -

( P R Ä A M B E L )

HAT FOLGENDE ENTSCHLIESSUNG ANGENOMMEN:

1. Der Rat nimmt zur Kenntnis, daß aufgrund der fortschreitenden technischen Entwicklung im Bereich der Telekommunikation sich auch die Anforderungen der gesetzlich ermächtigten Überwachungsbehörden an Netzbetreiber und Provider für die Zwecke der rechtmäßigen Überwachung des Telekommunikationsverkehrs, wie sie in der Entschließung des Rates vom 17.1.1995 (96/C 329/01) beschrieben sind, geändert haben.
2. Der Rat vertritt die Meinung, daß die Anforderungen der Entschließung des Rates vom 17.1.1995 auch auf neue bestehende Technologien insbesondere Satellitenkommunikation, Internet, Kryptographie, Prepaid Cards, udgl., sowie auf neue zukünftige Technologien zur sinngemäßen Anwendung geeignet sind.

3. Der Rat vertritt weiters die Meinung, daß aufgrund der fortgeschrittenen technischen Entwicklung im Bereich der Telekommunikation, ergänzende Anforderungen einschließlich jener über Sicherheitsmaßnahmen bei Netzbetreibern und Diensteanbietern sowie ergänzende Begriffsbestimmungen notwendig geworden sind.
4. Der Rat ist der Auffassung, daß die vorgenannten im Anhang aufgeführten erläuternden Memoranden und ergänzenden Anforderungen bei der Durchführung von Maßnahmen der rechtmäßigen Überwachung des Telekommunikationsverkehrs ebenfalls berücksichtigt werden sollten und ersucht die Mitgliedsstaaten, die für das Telekommunikationswesen verantwortlichen Minister aufzufordern, diese Auffassung zu unterstützen und mit den für Justiz und Inneres verantwortlichen Ministern mit dem Ziel einer Umsetzung der ergänzenden Anforderungen und Begriffsbestimmungen gegenüber den Netzbetreibern/Diensteanbietern zusammenzuarbeiten.

---

## ANHANG

### IN BEZUG AUF NEUE TECHNOLOGIEN

zu der im Amtsblatt der Europäischen Gemeinschaft veröffentlichten Entschließung des Rates vom 17.1.1995 über die rechtmäßige Überwachung des Telekommunikationsverkehrs (96/C329/01).

#### Teil 1: Erläuternde Memoranden

##### Einführungen zum Thema S-PCS:

Der Zweck dieses Explanatory Memorandums ist es, die Anwendbarkeit der Anforderungen der gesetzlich ermächtigten Behörden an mobile satellitengestützte Dienste (Mobile Satellite Services MSS) zu bewerten. Im wesentlichen werden für jede Anforderung die technischen und die Fragen der Zuständigkeit bewertet. Die technischen Fragen beziehen sich auf Funktionsvermögen und Kapazität einer Überwachungslösung in einem MSS-Netz. Die Fragen der Zuständigkeit beziehen sich auf die einzelstaatlichen Verfahrensweisen, die im Umgang mit einem multinationalen Diensteanbieter einen Einfluß auf die gesetzlich ermächtigten Behörden haben können.

Diese Dienste bestehen aus verschiedenen operationalen Architekturen und umfassen Sprache, Daten und Paging-Dienste. Betriebliche Szenarien umfassen die folgenden Verbindungen: mobil zu mobil (via Satellit), mobil zu mobil (terrestrisch), mobil (via Satellit oder terrestrisch) zum öffentlichen Telefonnetz (PSTN) und PSTN zu mobil (via Satellit oder terrestrisch). Die Überwachung von solchen satellitengestützten Diensten unterliegt den nationalen Gesetzen der ersuchenden gesetzlich ermächtigten Behörden sowie dem Gateway-Gastland.

## Einführungen zum Thema INTERNET:

Die Internationalen Anforderungen für Überwachung wurden von den gesetzlich ermächtigten Behörden entwickelt, um ihre gemeinsamen Anforderungen zur Orientierung der Telekommunikationsbranche zum Ausdruck zu bringen. Diese Anforderungen (Version 1.0) wurden durch die Entschließung des Rates vom 17. Jänner 1995 über rechtmäßige Überwachung von Telekommunikation angenommen und im Amtsblatt der Europäischen Gemeinschaften Nr. C329, 4. 11. 1996, p1, veröffentlicht. Die Regierungen der Vereinigten Staaten von Amerika, Kanadas und Australiens haben formell zugestimmt, die Anforderungen bei nationalen Verfahrensweisen zu berücksichtigen und zu empfehlen, daß sie als Basis für Diskussionen mit der Telekommunikationsbranche, Standardisierungsstellen und anderen verwendet werden.

Das Anforderungsdokument enthält alle Anforderungen der Behörden, doch hat die Erfahrung gezeigt, daß in manchen Fällen weitere Erklärungen benötigt werden und daß die Anwendung der Anforderungen auch auf neue und weiter um sich greifende Technologien abgeklärt werden muß.

Um sicherzustellen, daß die Internationalen Benutzeranforderungen für Überwachung weiterhin dem Zweck dienen, für den sie beabsichtigt waren, wird das grundlegende Dokument durch Explanatory Memoranda auf eine Weise erweitert und erklärt, die von den gesetzlich ermächtigten Behörden als Ausdruck ihrer gemeinsamen Anforderung vereinbart wurde.

## UMFANG

### *Allgemeines*

Dieses Explanatory Memorandum bezieht sich auf die Anforderungen der gesetzlich ermächtigten Behörden für die Überwachung von öffentlichen auf IP basierenden (Internet)-Diensten.

### *Anwendbare Dienste*

Beispiele für Internet-Dienste, für die dieses Memorandum gilt, umfassen folgendes, sind aber nicht darauf beschränkt:

- Einwahldienste
- Über HFC-Kabel angeschlossene Dienste

- Über Satellit gelieferte Dienste
- Direkt angeschlossene Dienste, z.B. LAN´s, die über einen Router angeschlossen sind

1. Die gesetzlich ermächtigten Behörden benötigen Zugriff auf den gesamten Fernmeldeverkehr, der von der Rufnummer oder sonstigen Kennung des überwachten Telekommunikationsdienstes, die die überwachte Person in Anspruch nimmt, übertragen wird (oder für die Übertragung generiert wird) bzw. dort ankommt. Die gesetzlich ermächtigten Behörden benötigen ferner Zugriff auf verbindungsrelevante Daten, die zur Verarbeitung des Anrufs generiert werden (Anforderungen Pkt. 1 - Abl. 96/C 329/01)

Erläuterungen in bezug auf S-PCS:

Die terrestrische Netzarchitektur eines MSS-Netzes ist der eines zellularen oder PCS-Netzes sehr ähnlich. Die MSS-Netze verwenden ähnliche Mobilitätskonzeptionen wie die terrestrischen drahtlosen Netze (IS-41 oder GSM). Die Datendienste können eine andere Architektur ohne derartige Komponenten haben.

Terrestrische Gateway-Stationen sind ein gemeinsamer und einfacher Standort für Überwachungslösungen für den Zugriff auf Telekommunikation und anrufbezogene Daten, doch können zwei Mobiltelefone miteinander auch ohne Miteinbeziehung der terrestrischen Gateway-Stationen kommunizieren, wodurch die Überwachungslösung zusätzliche Komplexität erfordert.

Die Nummer des vom Überwachten verwendeten Zieldiensts kann entweder Teil des vorhandenen Landescodes oder ein gesonderter Landecode für einen MSS-Provider sein.

In den meisten MSS-Netzen ist die Kapazität auf den Umfang an Frequenzbandbreite und/oder die innerhalb der Satellitenkonstellation verfügbare Satellitenleistung beschränkt. Die Überwachungsanforderung wird eine Auswirkung auf die MSS-Netzkapazität für Anrufe zwischen zwei Mobiltelefonen, die üblicherweise keinen Link zu einem terrestrischen Gateway benötigen würden, haben.

Die meisten MSS-Provider planen ihre Netzarchitektur auf Grundlage von technischen und finanziellen Fragen. Die derzeit vorgeschlagenen Architekturen decken einige dieser Fragen ab, indem sie mehrere Staaten von einem einzigen terrestrischen Gateway aus bedienen. Dies wirft zahlreiche Fragen bezüglich nationaler Verfahrensweisen und Souveränität für die betroffenen Staaten auf.

Der Zugriff auf Teilnehmerinformationen oder von Gateways aus, die mit anderen Staaten in Verbindung stehen, kann Souveränitätsfragen für jeden betroffenen Staat aufwerfen.

Es kann notwendig sein, Überwachungsanordnungen von einem Staat an einen anderen Staat weiterzugeben, damit der Diensteanbieter Überwachungen aktivieren kann.

#### Erläuterungen in Bezug auf INTERNET:

Der Begriff "Telekommunikationsverkehr" ist im Glossar der Internationalen Benutzeranforderungen definiert. Im Zusammenhang mit dem Internet versteht man unter Telekommunikationsverkehr zum und vom Zieldienst (siehe unten) alle zum und vom Ziel-Host gesendeten IP-Datagramme plus e-mail, die in einem e-mail-Server zur späteren Abholung durch das Überwachungssubjekt deponiert werden, sowie dieselbe e-mail, wenn sie vom Überwachungssubjekt abgeholt wird. Der Begriff umfaßt auch den Telekommunikationsverkehr zwischen dem Überwachungssubjekt und dem Internet Service Provider z.B. zur Passwortänderung.

Die Kennung eines Internet-Dienstes, der ein Zieldienst ist, ist gewöhnlich das Mittel, durch das der Dienst dem Service Provider bekannt ist und das zur Authentifizierung (und möglicherweise zur Vergebührung) einer Person verwendet wird, die versucht, den Zieldienst zu benutzen, und/oder das Mittel, durch das der Verkehr zum Dienst geleitet wird. Beispiele für Dienstkennungen sind:

- IP-Adresse (für Dienste mit einer fixen IP-Adresse)
- Kundenkontonummer
- Logon-ID/Passwort

- PIN
- e-mail-Adresse

Die verbindungsrelevanten Daten beziehen sich auf die Signalisierungsinformation, die in den IP-Datagrammen enthalten ist, sowie, wo es möglich ist, auf die Kennung der rufenden Leitung des vom Überwachungssubjekt für die Anschaltung an den Internet Service Provider verwendeten Telefondienstes.

**1.1. Die gesetzlich ermächtigten Behörden benötigen Zugriff in den Fällen, in denen die überwachte Person ein Telekommunikationssystem vorübergehend oder andauernd nutzt (Anforderungen Pkt. 1.1 - Abl. 96/C 329/01).**

Erläuterungen in bezug auf S-PCS:

Getrennte oder unterteilte Gateways können Teilnehmer-Profildaten und Kanalressourcen nach Diensteanbieter und Staat physisch oder logisch trennen, wodurch eine Barriere für den Zugriff der gesetzlich ermächtigten Behörden auf die Profildaten eines Teilnehmers oder Benutzers, die verbindungsrelevanten Daten und den Telekommunikationsverkehr geschaffen wird.

Die Definition des "Telekommunikationssystems" kann eine wesentliche Auswirkung auf einen MSS-Provider haben. Für einige MSS-Provider erstreckt sich das System auf die ganze Welt. Es kann sein, daß der Zugriff der Exekutive auf ein Telekommunikationssystem auf einen Staat beschränkt sein muß.

Wenn die mobilen satellitengestützten Dienste von einem internationalen Diensteanbieter bereitgestellt werden, kann internationales Recht gelten, um den Zugriff auf die Kommunikation eines Teilnehmers oder Benutzers zu ermöglichen.

Erläuterungen in bezug auf INTERNET:

Ein Überwachungssubjekt wird als ständig innerhalb eines Netzes operierend angesehen, wenn zwischen dem Host und dem Internet Service Provider eine ständige physische Verbindung besteht. Dies ist analog zu einem drahtgebundenen Telefondienst.

Zugriff wird auch gefordert, wenn ein Überwachungssubjekt persönliche oder Gerätemobilität hat, wie es bei Wählzugriff der Fall ist. Dies ist analog zu einem Mobiltelefondienst im Roaming-Betrieb. Zugriff wird gefordert, wann immer das Überwachungssubjekt an das Internet angeschlossen ist.

Es sollte festgehalten werden, daß die Bedingungen, unter denen eine Überwachungsanordnung gültig ist, durch einzelstaatliche Gesetze eingeschränkt werden können. In manchen Fällen kann es beispielsweise nicht rechtmäßig sein, einen Dienst zu überwachen, wenn sich das Überwachungssubjekt oder der Point-of-Presence außerhalb des Zuständigkeitsbereichs der Überwachungsanordnung befindet.

**1.2. Die gesetzlich ermächtigten Behörden benötigen Zugriff in den Fällen, in denen die überwachte Person Leistungsmerkmale zur Weiterleitung von anrufen zu anderen Telekommunikationsdiensten oder Endeinrichtungen nutzt; dies schließt anrufe ein, die zwischen verschiedenen Netzen vermittelt werden oder die vor Zustandekommen der Verbindung von verschiedenen Netzbetreibern/Diensterbringern verarbeitet werden (Anforderungen Pkt. 1.2. - Abl. 96/C 329/01)**

Erläuterungen in bezug auf S-PCS:

Alle Auswirkungen, die mit den innerhalb von zellularen, PCS- und drahtlosen Netzen verwendeten Zusatzdiensten, z.B. modernen Leistungsmerkmalen, Voice Mail etc., zusammenhängen, werden auch für MSS aufgrund von Ähnlichkeiten in der terrestrischen Infrastruktur relevant sein. Es gibt eine Unterscheidung zwischen netzübergreifendem und netzinternem Verkehr.

Erläuterungen in bezug auf INTERNET:

In der leitungsvermittelten Umgebung bezieht sich diese Anforderung auf Anrufe, die zum Zieldienst gerichtet sind. In der Internet-Umgebung bezieht sie sich auf Sitzungen, die nicht vom Zieldienst initiiert werden (üblicherweise e-mail zum Zieldienst). In diesen Fällen ist Zugriff auf den gesamten Telekommunikationsverkehr erforderlich, auch wenn er zu einem anderen Ziel umgeleitet wird, z.B. bei der Umleitung von e-mail.

- 1.3. Für die gesetzlich ermächtigten Behörden ist es erforderlich, daß ein Zugriff auf den vom Anschluß der überwachten Person abgehenden bzw. dort eingehenden Fernmeldeverkehr möglich ist; nicht übermittelt werden darf Fernmeldeverkehr, der nicht in der Überwachungsanordnung erfaßt ist (Anforderungen Pkt. 1.3. - Abl. 96/C 329/01)

Erläuterungen in bezug auf S-PCS:

Hier sollte es keine Auswirkungen oder Fragen geben, die spezifisch für einen MSS-Provider sind. Jeder MSS-Provider sollte in der Lage sein, diese Anforderung zu erfüllen.

Erläuterungen in bezug auf INTERNET:

Sowohl für leitungsvermittelte als auch für paketvermittelte Dienste bedeutet diese Anforderung, daß die gesetzlich ermächtigten Behörden vom Netzbetreiber/Diensteanbieter verlangen, das Überwachungsprodukt einem zusammengesetzten oder Multiplex-Datenstrom zu entnehmen, bevor es der gesetzlich ermächtigten Behörde zur Verfügung gestellt wird.

- 1.4. Die gesetzlich ermächtigten Behörden benötigen Zugriff auf die folgenden verbindungsrelevanten Daten (Anforderungen Pkt. 1.4. - Abl. 96/C 329/01):

1.4.1. Zeichengabe für Bereitzustand (Anforderungen Pkt. 1.4.1. - Abl. 96/C 329/01)

Erläuterungen in bezug auf S-PCS:

Physisch getrennte oder logisch unterteilte Gateways können Teilnehmer-Profildaten nach Diensteanbieter oder Staat trennen, die sich von jenem Diensteanbieter oder Staat unterscheiden können, die ein Überwachungsansuchen der gesetzlich ermächtigten Behörde erhalten. Diese Trennung kann ein Hindernis für den Zugriff der gesetzlich ermächtigten Behörden auf die Profildaten eines Teilnehmers oder Benutzers darstellen.

Die gesetzlich ermächtigten Behörden fordert diese Daten während der ersten und aller folgenden Anmeldungen des Mobiltelefons im Netz.

Erläuterungen in bezug auf INTERNET:

Anforderungen 1.4.1 beschreibt die von den gesetzlich ermächtigten Behörden geforderte Signalisierungsinformation bei leitungsvermittelten Diensten.

Im Zusammenhang mit dem Internet sind diese spezifischen Anforderungen irrelevant, da die Signalisierungsinformation im Header der IP-Datagramme enthalten ist.

**1.4.2. Nummer des gerufenen Teilnehmers bei abgehenden Verbindungen, selbst wenn es nicht zum Aufbau einer Verbindung kommt (Anforderungen Pkt. 1.4.2. - Abl. 96/C 329/01)**

Erläuterungen in bezug auf S-PCS:

Befindet sich ein Mobiltelefon vorübergehend in einem Staat, kann diese Information für erfolglose Verbindungen nicht zur Verfügung stehen.

Physisch getrennte oder logisch unterteilte Gateways können Teilnehmer-Profildaten nach Diensteanbieter oder Staat trennen, die sich von jenem Diensteanbieter oder Staat unterscheiden können, die ein Überwachungsansuchen der gesetzlich ermächtigten Behörde erhalten. Diese Trennung kann ein Hindernis für den Zugriff der gesetzlich ermächtigten Behörde auf die verbindungsrelevanten Daten eines Teilnehmers darstellen.

Es ist wesentlich, daß der gesetzlich ermächtigten Behörde diese Informationen zur Verfügung stehen.

Erläuterungen in bezug auf INTERNET:

Anforderungen 1.4.2. beschreibt die von den gesetzlich ermächtigten Behörden geforderte Signalisierungsinformation bei leitungsvermittelten Diensten.

Im Zusammenhang mit dem Internet sind diese spezifischen Anforderungen irrelevant, da die Signalisierungsinformation im Header der IP-Datagramme enthalten ist.

**1.4.3. Nummer des rufenden Teilnehmers bei ankommenden Verbindungen, wenn es nicht zum Aufbau einer Verbindung kommt (Anforderungen Pkt. 1.4.3. - Abl. 96/C 329/01)**

Erläuterungen in bezug auf SPC-S:

MSS mit Intersatelliten-Verbindungen können die Verbindungsgebühren minimieren, indem Anrufe über die Intersatelliten-Verbindungen zum nächstliegenden statt zum spezifischen für die Überwachung von Anrufen mobilen Ursprungs vorgesehenen MSS-Gateway geleitet werden (falls diese nicht identisch sind). Bei MSS mit Gateways, die große Gebiete abdecken, können durch automatische Wahl der kostengünstigsten Verbindung (Least Cost Routing) zu einem Gateway, der redundant zum Gateway des für die Überwachung vorgesehenen Gateways des Teilnehmers ist, die Überwachungen von Anrufen sowohl internationalen als auch nationalen Ursprungs umgangen werden.

Es ist wesentlich, daß der Exekutive diese Informationen zur Verfügung stehen, unabhängig davon, welcher Gateway vom Dienst des Teilnehmers oder Benutzers verwendet wird.

Erläuterungen in bezug auf INTERNET:

Anforderungen 1.4.3. beschreibt die von den gesetzlich ermächtigten Behörden geforderte Signalisierungsinformation bei leitungsvermittelten Diensten.

Im Zusammenhang mit dem Internet sind diese spezifischen Anforderungen irrelevant, da die Signalisierungsinformation im Header der IP-Datagramme enthalten ist.

**1.4.4. Alle von der überwachten Einrichtung erzeugten Signale, einschließlich der nach Aufbau der Verbindung erzeugten Signale, mit denen Funktionen wie beispielsweise Konferenzschaltung und Anrufumleitung aktiviert werden (Anforderungen Pkt. 1.4.4. - Abl. 96/C 329/01)**

Erläuterungen in bezug auf S-PCS:

Hier sollte es keine Auswirkungen oder Fragen spezifisch für einen MSS-Provider geben. Jeder MSS sollte in der Lage sein, diese Anforderung zu erfüllen.

Dazu gehören Signalisierung des Anrufsprungs und Signalisierung nach der Durchschaltung.

Erläuterungen in bezug auf INTERNET:

Anforderungen 1.4.4. beschreibt die von den gesetzlich ermächtigten Behörden geforderte Signalisierungsinformation bei leitungsvermittelten Diensten.

Im Zusammenhang mit dem Internet sind diese spezifischen Anforderungen irrelevant, da die Signalisierungsinformation im Header der IP-Datagramme enthalten ist.

**1.4.5. Beginn, Ende und Dauer der Verbindung (Anforderungen Pkt. 1.4.5. - Abl. 96/C 329/01)**

Erläuterungen in bezug auf S-PCS:

Hier sollte es keine Auswirkungen oder Fragen spezifisch für einen MSS-Provider geben. Jeder MSS sollte in der Lage sein, diese Anforderung zu erfüllen.

Erläuterungen in bezug auf INTERNET:

Anforderungen 1.4.5. beschreibt die von den gesetzlich ermächtigten Behörden geforderte Signalisierungsinformation bei leitungsvermittelten Diensten.

Im Zusammenhang mit dem Internet sind diese spezifischen Anforderungen irrelevant, da die Signalisierungsinformation im Header der IP-Datagramme enthalten ist.

**1.4.6. Tatsächliche Zielrufnummer und zwischengeschaltene Rufnummer, falls der Anruf weitergeschaltet wurde (Anforderungen Pkt. 1.4.6. - Abl. 96/C 329/01)**

Erläuterungen in bezug auf S-PCS:

Für Anrufe, die über einen Satellitenkanal weitergeleitet wurden, kann eingeschränkte satellitengestützte Signalisierung (aufgrund von knappen Satellitenressourcen) im Vergleich zu drahtgebundener Signalisierung eine Grenze für das Ausmaß der verbindungsrelevanten Daten darstellen, die der gesetzlich ermächtigten Behörde zur Verfügung stehen.

Bei der Protokollübersetzung zwischen einzelstaatlichen Netzen kann es zu einem Informationsverlust kommen.

Erläuterungen in bezug auf INTERNET:

Anforderung 1.4.6. beschreibt die von den gesetzlich ermächtigten Behörden geforderte Signalisierungsinformation bei leitungsvermittelten Diensten.

Im Zusammenhang mit dem Internet sind diese spezifischen Anforderungen irrelevant, da die Signalisierungsinformation im Header der IP-Datagramme enthalten ist.

**1.5. Für Teilnehmer mobiler Dienste benötigen die gesetzlich ermächtigten Behörden Informationen über den möglichst genauen geographischen Standort innerhalb des Netzes (Anforderungen Pkt. 1.5. - Abl. 96/C 329/01)**

Erläuterungen in bezug auf S-PCS:

Die Entfernung der Satelliten von der Erde führt zu einem hohen Grad an Granularität für den Teilnehmerstandort verglichen mit terrestrischen drahtlosen Systemen, die von einigen hundert Metern bis zu vielen Kilometern reichen.

Da der Standort nicht genau angegeben werden kann, kann es sein, daß ein MSS nicht in der Lage ist, ein Überwachungsobjekt, das einige Kilometer von verschiedenen Landesgrenzen entfernt ist, dem richtigen Land zuzuordnen.

Erläuterungen in bezug auf INTERNET:

Bei Einwahldiensten fordern die gesetzlich ermächtigten Behörden die Kennung der rufenden Leitung, wo diese dem Service Provider zur Verfügung steht.

- 1.6. Die gesetzlich ermächtigten Behörden benötigen Daten über die spezifischen Dienste, die die überwachte Person in Anspruch nimmt, und über die technischen Parameter dieser Kommunikationsarten (Anforderungen Pkt. 1.6. - Abl. 96/C 329/01)**

Erläuterungen in bezug auf S-PCS:

Für einen Überwachten, der sich von einem Staat in einen anderen bewegt (Roaming) wird nur ein Teil des Teilnehmerprofils am Roaming-Gateway zur Verfügung stehen. Die gesetzlich ermächtigten Behörden würde ein Mittel benötigen, um die restliche Information vom Heimat-Gateway, der sich in einem anderen Land befindet, zu erhalten.

Erläuterungen in bezug auf INTERNET:

Bei einem Internet-Dienst umfaßt dies die Art der Verbindung (Einwählen, LAN, Satellit, Kabel, etc.), die Übertragungsgeschwindigkeit in beide Richtungen und Informationen, die sich auf die vom Überwachungssubjekt verwendeten e-mail-Server beziehen.

- 2. Die gesetzlich ermächtigten Behörden benötigen eine permanente Überwachung des Fernmeldeverkehrs in Echtzeit. Verbindungsrelevante Daten sollen auch in Echtzeit bereitgestellt werden. Falls diese verbindungsrelevanten Daten nicht in Echtzeit zur Verfügung gestellt werden können, benötigen die gesetzlich ermächtigten Behörden die Daten so bald wie möglich nach Anrufende (Anforderungen Pkt. 2. - Abl. 96/C 329/01).**

Erläuterungen in bezug auf S-PCS:

Durch die globale Topologie des MSS kann sich die Übergabe der verbindungsrelevanten Daten mehr verzögern als bei terrestrischen zellularen drahtlosen Diensten.

Der Anruferinhalt sollte den Strafverfolgungsbehörden in Echtzeit geliefert werden. Die verbindungsrelevanten Daten sollten innerhalb von Millisekunden nach dem Anrufereignis ("call event") statt nach dem Anrufende ("call completion") verfügbar sein. 100 Millisekunden bis 500 Millisekunden werden gewünscht. Es ist unumgänglich, daß die verbindungsrelevanten Daten innerhalb dieses kurzen Zeitrahmens zur Verfügung stehen, um die Korrelation von Anrufereignis mit Anruferdetails zu erlauben.

Erläuterungen in bezug auf INTERNET:

Im Zusammenhang mit dem Internet ist ein Hinweis auf verbindungsrelevante Daten nicht anwendbar.

3. Für die gesetzlich ermächtigten Behörden ist es erforderlich, daß Netzbetreiber/Diensterbringer eine oder mehrere Schnittstellen bereitstellen, von denen aus der überwachte Fernmeldeverkehr zur Überwachungseinrichtung der gesetzlich ermächtigten Behörde übertragen werden kann. Diese Schnittstellen müssen von den Behörden und den Netzbetreibern/ Diensteanbietern einvernehmlich festgelegt werden. Weitere Fragen im Zusammenhang mit diesen Schnittstellen werden entsprechend den in den einzelnen Staaten praktizierten Verfahren geregelt (Anforderungen Pkt. 3. - Abl. 96/C 329/01)

Erläuterungen in bezug auf S-PCS:

Die Überwachung kann an einem MSS-Gateway vorgesehen sein, der eine Reihe von Ländern bedient; verschiedene Typen von Übertragungseinrichtungen oder Signalisierungsprotokollen könnten für den Transfer des überwachten Telekommunikationsverkehrs und der verbindungsrelevanten Daten an die Exekutive verwendet werden.

Während einer solchen Übertragung können die abgefangenen Daten auf keinerlei Weise geändert oder manipuliert werden.

Zwischen Netzbetreiber(n) und Diensteanbieter(n) sowie zwischen Netzbetreiber(n) und Diensteanbieter(n) und der Exekutive müssen Koordinierungsmaßnahmen erfolgen.

Erläuterungen in bezug auf INTERNET:

Diese Anforderung gilt unverändert auch für Internet-Dienste.

Erläuterungen in bezug auf die BEREITSTELLUNG VON TEILNEHMER- UND VERBINDUNGS-RELEVANTEN DATEN:

Diese Anforderung umfaßt die Bereitstellung allgemein vereinbarter Schnittstellen, die die Übertragung von Teilnehmerdetails erlauben.

- 3.1. Für die gesetzlich ermächtigten Behörden ist es erforderlich, daß Netzbetreiber/Diensteanbieter verbindungsrelevante Daten des überwachten Telekommunikationsdienstes und Anrufinhalte so bereitstellen, daß zwischen den verbindungsrelevanten Daten und Anrufinhalte eine einwandfreie Korrelation hergestellt werden kann (Anforderungen Pkt. 3.1. - Abl. 96/C 329/01).**

Erläuterungen in bezug auf S-PCS:

Die gesetzlich ermächtigte Behörde muß wissen, wo diese Informationen ihren Ursprung haben.

Erläuterungen in bezug auf INTERNET:

Diese Anforderung ist nicht anwendbar.

- 3.2. Für die gesetzlich ermächtigten Behörden ist es erforderlich, daß für die Übertragung des überwachten Fernmeldeverkehrs an die Überwachungseinrichtung ein allgemein verfügbares Format verwendet wird. Dieses Format wird auf Ebene der jeweiligen Staaten festgelegt (Anforderungen Pkt. 3.2. - Abl. 96/C 329/01)**

Erläuterungen in bezug auf S-PCS:

Das verwendete Format darf kein "gesetzlich geschütztes" Format sein, sondern sollte ein leicht verfügbares und "angemessenes" Format sein.

Erläuterungen in bezug auf INTERNET:

Diese Anforderung gilt unverändert auch für Internet-Dienste.

- 3.3. Falls Netzbetreiber/Diensteanbieter Kodierungs-, Kompressions- oder Verschlüsselungsverfahren zur Anwendung bringen, ist es für die gesetzlich ermächtigten Behörden ist es erforderlich, daß die Netzbetreiber/Diensteanbieter den überwachten Fernmeldeverkehr in Klarform bereitstellen (Anforderungen Pkt. 3.3. - Abl. 96/C 329/01).**

Erläuterungen in bezug auf S-PCS:

Diese Anforderung umfaßt Informationen über Anrufrdetails sowie Daten über den Gesprächsinhalt.

Erläuterungen in bezug auf INTERNET:

Diese Anforderung gilt unverändert auch für Internet-Dienste. Es ist festzuhalten, daß es die Aufgabe der überwachenden Behörde ist, die Nachricht aus dem erhaltenen Produkt zu extrahieren, wenn ein Ziel den Verkehr durch Verschlüsselung oder durch Anwendung anderer Verfahren modifiziert.

- 3.4. Für die gesetzlich ermächtigten Behörden ist es erforderlich, daß Netzbetreiber/Diensteanbieter in der Lage sind, den überwachten Fernmeldeverkehr über Fest- und Wählverbindungen an die Überwachungseinrichtung der gesetzlich ermächtigten Behörde zu übertragen (Anforderungen Pkt. 3.4. - Abl. 96/C 329/01)**

Erläuterungen in bezug auf S-PCS:

Hier sollte es keine Auswirkungen oder Fragen geben, die spezifisch für einen MSS-Provider sind. Jeder MSS-Provider sollte in der Lage sein, diese Anforderung zu erfüllen.

Erläuterungen in bezug auf INTERNET:

Diese Anforderung gilt unverändert auch für Internet-Dienste.

- 3.5. Für die gesetzlich ermächtigten Behörden ist es erforderlich, daß die Übertragung des überwachten Fernmeldeverkehrs an die Überwachungseinrichtung den geltenden Sicherheitsanforderungen genügt (Anforderungen Pkt. 3.5. - Abl. 96/C 329/01)**

Erläuterungen in bezug auf S-PCS:

Hier sollte es keine Auswirkungen oder Fragen geben, die spezifisch für einen MSS-Provider sind. Jeder MSS-Provider sollte in der Lage sein, diese Anforderung zu erfüllen. Für weitere Einzelheiten wird auf die Internationalen Benutzeranforderungen (IUR) - Sicherheitsdokument Bezug genommen.

Die Definition der "geltenden Sicherheitsanforderungen" kann einen wichtigen Einfluß auf multinationale MSS-Provider haben.

Sicherheitsthemen für den internationalen Informationsaustausch können Souveränitätsfragen auslösen.

Erläuterungen in bezug auf INTERNET:

Diese Anforderung gilt unverändert auch für Internet-Dienste.

- 4. Für die gesetzlich ermächtigten Behörden ist es erforderlich, daß Überwachungsmaßnahmen so durchgeführt werden, daß weder die überwachte Person noch eine andere unbefugte Person über Änderungen, die zur Durchführung der Überwachungsanordnung vorgenommen werden, Kenntnis erhält. Insbesondere muß sich der Betrieb des überwachten Telekommunikationsdienstes der überwachten Person als unverändert darstellen (Anforderungen Pkt. 4. - Abl. 96/C 329/01)**

Erläuterungen in bezug auf S-PCS:

Es darf keine Verschlechterung der Sprachqualität des Zieldienstes aufgrund der Überwachung geben. Dies umfaßt, ist aber nicht darauf beschränkt: verzögerter Anrufaufbau, verzögerte Sprachübertragung, verzögerte Fähigkeit, Leistungsmerkmale zu initiieren, Verweigerung von Rechenleistung, schlechte Sprachqualität und "abnormale" Anzeigen am Display des Mobiltelefons des Ziels.

Durch die Notwendigkeit für internationale Kooperation der Exekutive kann die Anzahl der "befugten" Mitarbeiter, die Zugang zu einer Überwachungsanordnung haben, deutlich steigen.

Die Definition der "unbefugten Person" kann eine ernsthafte Auswirkung auf die Abwicklung der Überwachung durch den MSS-Provider haben. Bei einem Gateway, der mehrere Staaten bedient, können Ausländer Zugang zu Überwachungsanordnungen haben.

Erläuterungen in bezug auf INTERNET:

Diese Anforderung gilt unverändert auch für Internet-Dienste.

5. Für die gesetzlich ermächtigten Behörden ist es erforderlich, daß die Überwachung so geplant und durchgeführt wird, daß eine unbefugte oder unsachgemäße Verwendung ausgeschlossen ist und Informationen mit Bezug auf die Überwachung geschützt sind (Anforderungen Pkt. 5. - Abl. 96/C 329/01).

Erläuterungen in bezug auf S-PCS:

Durch die Notwendigkeit für internationale Kooperation der Exekutive kann die Anzahl der "befugten" Mitarbeiter, die Zugang zu einer Überwachungsanordnung haben, deutlich steigen.

Die Definition der "unbefugten Person" kann eine ernsthafte Auswirkung auf die Abwicklung der Überwachung durch den MSS-Provider haben. Bei einem Gateway, der mehrere Staaten bedient, können Ausländer Zugang zu Überwachungsanordnungen haben.

Unbefugte Mitarbeiter dürfen keinen Zugang zum "Produkt" der Überwachung oder zu Audit-Informationen oder andere mit der Überwachung zusammenhängende Daten haben.

Erläuterungen in bezug auf INTERNET:

Diese Anforderung gilt unverändert auch für Internet-Dienste.

Erläuterungen in bezug auf die BEREITSTELLUNG VON TEILNEHMER- UND VERBINDUNGS-RELEVANTEN DATEN:

Diese Anforderung enthält eine Forderung, alle Informationen in Zusammenhang mit Ansuchen um Teilnehmerdetails zu schützen.

- 5.1. Für die gesetzlich ermächtigten Behörden ist es erforderlich, daß Netzbetreiber/Diensteanbieter die Informationen über Gegenstand und Anzahl laufender oder bereits durchgeführter Überwachungsmaßnahmen schützen und keine Informationen weitergeben, wie Überwachungsmaßnahmen durchgeführt werden (Anforderungen Pkt. 5.1 - Abl. 96/C 329/01).**

Erläuterungen in bezug auf S-PCS:

Hier sollte es keine Auswirkungen oder Fragen geben, die spezifisch für einen MSS-Provider sind. Jeder MSS-Provider sollte in der Lage sein, diese Anforderung zu erfüllen.

Die Anforderung umfaßt Identifikationsinformation über das Ziel.

Erläuterungen in bezug auf INTERNET:

Diese Anforderung gilt unverändert auch für Internet-Dienste.

- 5.2. Für die gesetzlich ermächtigten Behörden ist es erforderlich, daß Netzbetreiber/Diensteanbieter sicherstellen, daß der überwachte Fernmeldeverkehr nur an die in der Überwachungsanordnung angegebene Überwachungsbehörde übertragen wird (Anforderungen Pkt. 5.2. - Abl. 96/C 329/01)**

Erläuterungen in bezug auf S-PCS:

Hier sollte es keine Auswirkungen oder Fragen geben, die spezifisch für einen MSS-Provider sind. Jeder MSS-Provider sollte in der Lage sein, diese Anforderung zu erfüllen.

Erläuterungen in bezug auf INTERNET:

Diese Anforderung gilt unverändert auch für Internet-Dienste

- 5.3. Entsprechend der nationalen Bestimmungen können die Netzbetreiber/Diensteanbieter verpflichtet werden, gleichartig geschützte Aufzeichnungen über die Aktivierung der Überwachungsfunktionalitäten zu führen (Anforderungen Pkt. 5.3. - Abl. 96/C 329/01)**

Erläuterungen in bezug auf S-PCS:

Hier sollte es keine Auswirkungen oder Fragen geben, die spezifisch für einen MSS-Provider sind. Jeder MSS-Provider sollte in der Lage sein, diese Anforderung zu erfüllen.

Erläuterungen in bezug auf INTERNET:

Diese Anforderung gilt unverändert auch für Internet-Dienste.

- 6. Vor Durchführung der Überwachung fordern die gesetzlich ermächtigten Behörden beim Netzbetreiber/Diensteanbieter im Rahmen einer rechtmäßigen Anfrage folgende Informationen an: (1) Angaben zur Identität der überwachten Person, die Rufnummer oder eine andere Kennung; (2) Informationen über die Dienste und Leistungsmerkmale des Telekommunikationssystems, welche die überwachte Person in Anspruch nimmt und die von Netzbetreibern/Diensteanbietern bereitgestellt werden; (3) Informationen über die technischen Parameter für die Übertragung an die Überwachungseinrichtung der gesetzlich ermächtigten Behörden (Anforderungen Pkt. 6. - Abl. 96/C 329/01)**

Erläuterungen in bezug auf S-PCS:

Dazu gehören die terrestrischen Anbieter von Telekommunikationsdiensten, falls vorhanden, zu denen der Teilnehmer oder Benutzer Zugang hat.

Die von der gesetzlich ermächtigten Behörde für die Überwachung benötigte Information kann in Gateways resident sein, die im Besitz einer ausländischen Organisation oder eines ausländischen Unternehmens sind oder von diesen betrieben werden.

Diese Informationen können auch beim Anbieter des Zieldienstes resident sein.

Erläuterungen in bezug auf INTERNET:

Diese Anforderung gilt unverändert auch für Internet-Dienste.

7. Während der Überwachung können die gesetzlich ermächtigten Behörden von den Netzbetreibern/Diansteanbietern Informationen und/oder Unterstützung anfordern, um sicherzustellen, daß der an der Überwachungsschnittstelle übergebene Fernmeldeverkehr mit dem überwachten Telekommunikationsdienst im Zusammenhang steht. Die Art der angeforderten Information und/oder Unterstützung richtet sich nach den vereinbarten praktischen Regelungen der einzelnen Staaten (Anforderungen Pkt. 7. - Abl. 96/C 329/01)

Erläuterungen in bezug auf S-PCS:

Hier sollte es keine Auswirkungen oder Fragen geben, die spezifisch für einen MSS-Provider sind. Jeder MSS-Provider sollte in der Lage sein, diese Anforderung zu erfüllen. Wenn ein Land verlangt, daß ein Mitarbeiter eines Netzbetreibers/Diansteanbieters vor Gericht aussagt, kann dies eine Frage für multinationale MSS-Provider sein.

Erläuterungen in bezug auf INTERNET:

Diese Anforderung gilt unverändert auch für Internet-Dienste.

Erläuterungen in bezug auf die BEREITSTELLUNG VON TEILNEHMER- UND VERBINDUNGS-RELEVANTEN DATEN:

Mit der Einführung einer solchen Funktionalität im Telekommunikationsnetz wie Nummernportabilität wird diese Anforderung ausgeweitet und enthält auch die Forderung an den Netzbetreiber/Diansteanbieter, die überwachende Behörde zu informieren, wenn der Zieldienst zu einem anderen Netzbetreiber/Diansteanbieter "portiert" wird, während eine Überwachungsanordnung in Kraft ist.

8. Für die gesetzlich ermächtigten Behörden ist es erforderlich, daß Netzbetreiber/ Diensteanbieter Vorbereitungen für eine Reihe gleichzeitiger Überwachungsmaßnahmen treffen. Eine Mehrfachüberwachung in bezug auf einen speziellen überwachten Telekommunikationsdienst kann erforderlich sein, um mehreren gesetzlich ermächtigten Behörden eine Überwachung zu ermöglichen. In diesem Fall sollten die Netzbetreiber/Diensteanbieter Vorsichtsmaßnahmen treffen, um die Identität der Überwachungsbehörde zu schützen und die Vertraulichkeit der Ermittlungen sicherzustellen. Die Höchstzahl gleichzeitiger durchführbarer Überwachungsmaßnahmen bei einer bestimmten Teilnehmergruppe wird entsprechend den einzelstaatlichen Anforderungen festgelegt (Anforderungen Pkt. 8. - Abl. 96/C 329/01).

Erläuterungen in bezug auf S-PCS:

Da ein MSS-Gateway mehreren Nationen satellitengestützte Versorgung anbieten kann, sollte jedes betroffene Land die Kapazität für die Überwachungen angeben.

Die maximale Anzahl von gleichzeitigen Überwachungen eines bestimmten Teilnehmers kann durch die Kapazitätsanforderungen mehrerer Staaten bestimmt werden. Mehrere Länder können Überwachungen desselben mobilen Teilnehmers durchführen, der von einem Gateway bedient wird.

Einzelstaatliche Anforderungen werden als Anforderungen mehrerer Länder definiert.

"Markierte" Nummern müssen alle Kapazitätsbedürfnisse der einzelstaatlichen Strafverfolgungsbehörden erfüllen.

Erläuterungen in bezug auf INTERNET:

Diese Anforderung gilt unverändert auch für Internet-Dienste.

9. Für die gesetzlich ermächtigten Behörden ist es erforderlich, daß Netzbetreiber/ Diensteanbieter die Überwachungsmaßnahmen so rasch wie möglich durchführen (in dringenden Fällen innerhalb weniger Stunden oder Minuten). Die Anforderungen der gesetzlich ermächtigten Behörden hinsichtlich der Reaktionszeit sind von Land zu Land unterschiedlich und richten sich nach der Art des zu überwachenden Telekommunikationsdienstes (Anforderungen Pkt. 9. - Abl. 96/C 329/01)

Erläuterungen in bezug auf S-PCS:

Sprache, Zeitunterschiede, technische Schnittstellen können einen deutlichen Einfluß auf die Überwachung und somit auf die Zeit haben, die erforderlich ist, um Überwachungen in einem Gateway, der mehrere Länder bedient, durchzuführen.

Souveränitätsfragen können weitere Verzögerungen verursachen, wenn Kooperation von Strafverfolgungsbehörden in verschiedenen Ländern erforderlich ist.

Erläuterungen in bezug auf INTERNET:

Diese Anforderung gilt unverändert auch für Internet-Dienste.

Erläuterung in bezug auf die BEREITSTELLUNG VON TEILNEHMER- UND VERBINDUNGS-RELEVANTEN DATEN:

Diese Anforderung enthält die Bereitstellung von Zugriff auf die Teilnehmerdaten, die notwendig sind, um die richterliche Anordnung so rasch wie möglich zu erhalten und zu implementieren.

10. Für die gesetzlich ermächtigten Behörden ist es erforderlich, daß die Dienste, die sie bei einer Überwachung nutzen, für die Dauer der Überwachung mindestens die gleiche Zuverlässigkeit aufweisen wie die überwachten Telekommunikationsdienste, die für die überwachte Person bereitgestellt werden. Für die die gesetzlich ermächtigten Behörden ist es erforderlich, daß die Güte des Dienstes, der für die Übertragung des überwachten Fernmeldeverkehrs an die Überwachungseinrichtung genutzt wird, dem üblichen Leistungsniveau der Netzbetreiber/Diensteanbieter entspricht (Anforderungen Pkt. 10. - Abl. 96/C 329/01)

Erläuterungen in bezug auf S-PCS:

Leistungsstandards müssen auf annehmbaren Niveau sein und unterliegen den Standards des ursprünglichen Anrufs.

Erläuterungen in bezug auf INTERNET:

Diese Anforderung gilt unverändert auch für Internet-Dienste.

## Teil 2: Ergänzende Anforderungen

### A. ANFORDERUNGEN IN BEZUG AUF DIE BEREITSTELLUNG VON TEILNEHMER- UND VERBINDUNGSRELEVANTEN DATEN

#### **Allgemeines**

Die nachfolgend angeführten Anforderungen der gesetzlich ermächtigten Behörden beziehen sich auf Informationen über:

- die Identität von Teilnehmern;
- die von den Teilnehmern verwendeten Dienste, Geräte und Leistungsmerkmale; und
- die Verwendung von Telekommunikationsdiensten (Gebührenaufzeichnungen, Internet-Footprints etc.) durch Teilnehmer.

#### **Anwendbare Dienste**

Die gesetzlich ermächtigten Behörden fordern Zugriff auf Informationen über nachfolgend demonstrativ angeführte Telekommunikationsdienste:

- Leitungsvermittelte Telefoniedienste, z.B. PSTN, ISDN;
- Terrestrische mobile Dienste, z.B. GSM, AMPS, D-AMPS, CDMA, DCS1800;
- Satellitengestützte mobile Dienste, z.B. Iridium, Globalstar, ICO;
- Gebündelte mobile Dienste, z.B. TETRA;
- Internet-Dienste sowohl mit Wähl- als auch mit fixem Zugriff;
- Wertkartendienste, sowohl vorausbezahlt als auch kontogestützt;
- Rückrufdienste;
- Fernverkehrs- und internationale Dienste;
- Paging-Dienste;
- Datendienste, z.B. X.25, X.400, ATM, Frame Relay; und
- Voice Mail-Dienste.

Die gesetzlich ermächtigten Behörden benötigen auch die Mittel für den Zugriff auf Informationen über Teilnehmer in anderen Ländern in Situationen, in denen diese Teilnehmer vielleicht innerhalb der Zuständigkeit der Behörde operieren. Beispiele für diese Situationen umfassen, sind aber nicht auf folgendes beschränkt:

- Internationale mobile Roaming-Teilnehmer;
- Teilnehmer von S-PCS, beispielsweise Iridium; und
- Teilnehmer von internationalen Betreibern, wo sich die Teilnehmerdatenbank in einem anderen Land befindet.

### **Anforderungen**

Basierend auf der Ratsentschließung vom 17.1.1995, sind in Ergänzung zu den bestehenden Anforderungen im Pkt. 6, die folgenden Punkte 6.1. – 6.7. als Ergänzung anzuhängen.

- 6. Vor Durchführung der Überwachung fordern die gesetzlich ermächtigten Behörden beim Netzbetreiber/Diensteanbieter im Rahmen einer rechtmäßigen Anfrage folgende Informationen an: (1)Angaben zur Identität der überwachten Person, die Rufnummer oder eine andere Kennung;(2)Informationen über die Dienste und Leistungsmerkmale des Telekommunikationssystems, welche die überwachte Person in Anspruch nimmt und die von Netzbetreibern/Diensteanbietern bereitgestellt werden;(3) Informationen über die technischen Parameter für die Übertragung an die Überwachungseinrichtung der gesetzlich ermächtigten Behörden (Anforderungen Pkt. 6. - Abl. 96/C 329/01)**

## ERGÄNZENDE ANFORDERUNGEN zu Pkt. 6.

6.1. Die gesetzlich ermächtigten Behörden fordern den Zugriff auf Informationen über die Identität des Subjektes im Besitz von Betreibern/Anbietern von Telekommunikationsnetzen, Telekommunikationsdiensten und Internet-Diensten. Beispiele für diese Informationen umfassen, sind aber nicht auf folgendes beschränkt:

- \* den vollständigen Namen und die vollständige Adresse des Überwachten, einschließlich Postleitzahl;
- \* den vollständigen Namen und die vollständige Adresse (einschließlich Postleitzahl) der Person, die die Rechnung für die dem Überwachten bereitgestellten Dienste bezahlt;
- \* ausreichende Kreditkartendetails, um das Kundenkonto zu identifizieren, wenn der Überwachte mit Kreditkarte bezahlt; und
- \* den Namen und die Adresse, wie sie im Verzeichnis angegeben sind.

6.2. Die gesetzlich ermächtigten Behörden fordern das Mittel für den Zugriff auf Informationen über Numerierungspläne oder Identifizierungsnummern für Telekommunikationsdienste, um bei der Identifizierung des Betreibers eines Überwachungssubjekts zu helfen. Zu den typischen Diensten, die vielleicht identifiziert werden müssen, zählen folgende, sind aber nicht darauf beschränkt:

- \* ISDN-Dienste;
- \* Paketvermittelte und leitungsvermittelte Dienste;
- \* Telex-Dienste;
- \* Internet-Domain-Namen.

6.3. Die gesetzlich ermächtigten Behörden fordern Zugriff auf Informationen im Besitz von Betreibern/Anbietern von Telekommunikationsnetzen, Telekommunikationsdiensten und Internet-Diensten über die Dienstnummer oder eine andere eindeutige Kennung des Überwachten. Beispiele für diese Informationen umfassen, sind aber nicht auf folgendes beschränkt:

- \* Vom Überwachten verwendete Dienst- und Leistungsmerkmaltypen;
- \* Drahtgebundene Rufnummern;
- \* Technische Kennungen und Codes von Telekommunikationsgeräten, z.B. MSISDN, IMSI und IMEI bei GSM, die der Überwachte vom Betreiber erhält;
- \* Das Mittel, mit dem ein Betreiber einen Internet-Teilnehmer auf einer Kabel-TV-Leitung identifiziert;
- \* Benutzerkennung oder -code, die vom Anrufer angegeben und von einem Internet-Anbieter verwendet werden, um den Benutzer zu authentifizieren und zu vergebühren;
- \* Kabel- oder Kanalkennungen für Festpunktdienste;
- \* IP-Adresse für Benutzer von fixen Internet-Diensten;
- \* Zugehörige Rufnummer für einen Voice Mail-Dienst;
- \* e-mail-Adresse;
- \* PIN oder Code, die vom Anrufer angegeben und von einem Anbieter verwendet werden, um den Benutzer von Wertkartendiensten zu authentifizieren und zu vergebühren; und
- \* Das Mittel, mit dem ein internationaler oder Fernverkehrsbetreiber einen Anrufer authentifiziert.

6.4. Die gesetzlich ermächtigten Behörden fordern Zugriff auf Informationen im Besitz von Betreibern/Anbietern von Telekommunikationsnetzen, Telekommunikations- und Internet-Diensten über die optionalen Dienste und Merkmale des Überwachten. Beispiele für diese Informationen umfassen, sind aber nicht auf folgendes beschränkt:

- \* In drahtgebundenen öffentlichen Telefonnetzen gehören zu diesen Leistungsmerkmalen Anrufumleitung, Anklopfen, Anrufübergabe, Vorauswahl eines Fernverkehrsbetreibers, Voice Mail und Kurzwahl;
- \* In GSM-Netzen umfassen diese Leistungsmerkmale zusätzlich MSISDN für Fax und Daten, Voice Mail, SMS, spezielle Roaming-Genehmigung und Hochgeschwindigkeitsdaten; und
- \* Bei Internet-Diensten können sie sowohl e-mail als auch e-mail-Umleitung umfassen.

Diese Anforderung gilt auch für jene Dienste, die die Verwendung von vorausbezahlten Wertkarten beinhalten.

- 6.5. Die gesetzlich ermächtigten Behörden fordern Zugriff auf Verkehrs- und Vergebührungsaufzeichnungen eines Überwachten.
- 6.6. Die gesetzlich ermächtigten Behörden fordern von den Betreibern/Anbietern von Telekommunikationsnetzen, Telekommunikationsdiensten und Internet-Diensten das Führen eines aktuellen Verzeichnisses der IMEI-Codes der mobilen Kommunikationsgeräte, die von diesen Betreibern an ihre Kunden verkauft werden.
- 6.7. Die gesetzlich ermächtigten Behörden fordern, daß die gesamte Teilnehmerinformation in einer Suche erhalten wird, die mit folgendem beginnt:
- \* der Dienstnummer oder einer anderen eindeutigen Kennung oder
  - \* einem der Elemente der vorstehend angegebenen Teilnehmeridentität, d.h. Name oder Adresse oder Kreditkartendienst.

## **A. ANFORDERUNGEN FÜR SICHERHEITSMASSNAHMEN BEI NETZBETREIBERN/ DIENSTANBIETERN**

### **Einführung**

Es werden die Anforderungen für Sicherheitsmaßnahmen spezifiziert, die Netzbetreiber/-Dienstanbieter erfüllen müssen. Diese Anforderungen werden zur Wahrung der Interessen der zur Durchführung von Telekommunikationsüberwachungen ermächtigten gesetzlich ermächtigten Behörden festgelegt.

Diese Anforderungen sind Erweiterungen der Anforderungen der Ratsentschließung vom 17.1.1995 (Punkte 3.5, 5., 5.1, 5.2, 5.3), (Abl. 96/C 329/01).

Die Einhaltung dieser Anforderungen soll folgendes sicherstellen:

- Schutz der Interessen der von einer Überwachung betroffenen Personen vor Offenbarung ihres Telekommunikationsverkehrs an andere Parteien als die überwachende Behörde;
- Verhinderung, daß der Zugriff der überwachenden Behörden auf die Telekommunikation blockiert wird; und
- Verhinderung sowie Rückverfolgung des Mißbrauchs der technischen Einrichtungen zur Überwachung von Telekommunikation, die von den Netzbetreibern/Dienstanbietern verwendet werden.

### **ERGÄNZENDE ANFORDERUNGEN:**

**11. Die gesetzlich ermächtigten Behörden fordern, daß der Netzbetreiber/ Dienstanbieter an seinem Standort Sicherheitsverfahren implementiert.**

**Diese Verfahren sind mit den gesetzlich ermächtigten Behörden zu vereinbaren.**

**11.1. Der Netzbetreiber/Dienstanbieter soll regelmäßigen Sicherheitskontrollen durch die gesetzlich ermächtigten Behörden zustimmen.**

- 11.2. Überwachungsanordnungen und Überwachungsdaten sollen im Einklang mit der entsprechenden einzelstaatlichen Sicherheitsebene geheim sein. Die gesetzlich ermächtigten Behörden fordern, daß der Netzbetreiber/ Diensteanbieter die Vertraulichkeit aller Überwachungsanordnungen und Überwachungsdaten sicherstellt.
- 11.3. Je nach einzelstaatlicher Gesetzgebung und deren Verfahren müssen Überwachungsanordnungen vom Netzbetreiber/Diensteanbieter innerhalb eines gewissen Zeitraums vernichtet werden.
- 11.4. Die gesetzlich ermächtigten Behörden fordern, daß im Falle der Verletzung der Integrität und/oder der Vertraulichkeit der Überwachungsanordnung oder der Überwachungsdaten der Netzbetreiber/Diensteanbieter alle erforderlichen Maßnahmen ergreifen soll, um die Verbreitung der Informationen zu verhindern. Es wird die verantwortliche Behörde des Gastlandes so rasch wie möglich von der Verletzung informieren. Weiters fordern die gesetzlich ermächtigten Behörden vom Netzbetreiber/Diensteanbieter, alle gebührenden Maßnahmen zur Verhinderung eines derartigen Vorfalls in Zukunft zu treffen.
12. Die gesetzlich ermächtigten Behörden fordern, daß sich alle Personen, die Überwachungsanordnungen abwickeln oder überwachen, oder die mit dem Überwachungsprozeß zu tun haben, einer Sicherheitskontrolle unterziehen, wie es von den einzelstaatlichen Behörden gefordert wird.
- 12.1. Eine Liste mit Namen und Jobbeschreibungen dieser Personen ist den gesetzlich ermächtigten Behörden zu übergeben.
13. Die gesetzlich ermächtigten Behörden fordern vom Netzbetreiber/Diensteanbieter, alle erforderlichen organisatorischen und technischen Maßnahmen zu treffen, um alle für das Routing von überwachtem Telekommunikationsverkehr verwendeten technischen Schnittstellen und alle administrativen Komponenten, die der Durchführung oder Änderung von Überwachungen dienen, vor Mißbrauch zu schützen.

- 13.1. Der Netzbetreiber/Diensteanbieter muß sicherstellen, daß die Integrität und die Vertraulichkeit der Überwachungsdaten während der Übertragung in dem von den gesetzlich ermächtigten Behörden geforderten Ausmaß geschützt wird. Daher sind alle für Überwachungszwecke verwendeten Kommunikationsleitungen zu schützen.
- 13.2. Die gesetzlich ermächtigten Behörden fordern, daß Informationen über die einem bestimmten Telekommunikationssystem durchgeführten tatsächlichen Überwachungen unbefugten Personen nicht zur Verfügung gestellt werden.
14. Die gesetzlich ermächtigten Behörden fordern, daß die Standorte, an denen sich Überwachungsanordnungen und -daten befinden, Sperrbereiche mit kontrolliertem Zugang sind. Der Netzbetreiber/Diensteanbieter hat die gesetzlich ermächtigten Behörden über den genauen Standort und die durchgeführten Sicherheitsmaßnahmen zu informieren und eine Liste mit den Mitarbeitern zu übergeben, die befugt sind, diese Standorte zu betreten.
- 14.1. Die gesetzlich ermächtigten Behörden fordern vom Netzbetreiber/Diensteanbieter, die Überwachungsanordnung im Einklang mit den einzelstaatlichen Sicherheitsstandards zu speichern. Es ist dem Netzbetreiber/Diensteanbieter nicht erlaubt, den Gesprächsinhalt zu speichern.

C. ANFORDERUNGEN AN DIENSTEANBIETER IN BEZUG AUF KRYPTOGRAPHIE

15. Basierend auf einer rechtmäßigen Anfrage und nach Erhalt einer Zielkennung oder anderer Informationen über das Ziel oder verschlüsselte Daten mit zugehörigen Informationen fordern die gesetzlich ermächtigten Behörden
- Vollständige Details über das Ziel einschließlich der Dienstnummer;
- \* Informationen, die die vom Ziel verwendeten kryptographischen Dienste vollständig identifizieren; und die technischen Parameter der zur Implementierung des kryptographischen Dienstes verwendeten Methode.

16. Die gesetzlich ermächtigten Behörden benötigen Zugriff auf die entschlüsselte Nachricht so schnell wie möglich (in dringenden Fällen innerhalb einiger Stunden oder Minuten). Die gesetzlich ermächtigten Behörde wird spezifizieren, wie sie zu diesem Ergebnis kommen möchte: entweder durch die Bereitstellung von kryptographischem Schlüsselmaterial und der gesamten Information, die erforderlich ist, um die Daten zu entschlüsseln oder durch Bereitstellung der Daten im Klartext. Zugriff auf die entschlüsselte Nachricht muß für jene Verschlüsselungssysteme verfügbar sein, die sowohl nationalen als auch internationalen Betrieb erlauben.
- 16.1. Die Übergabe von kryptographischem Schlüsselmaterial sollte sofort erfolgen. Der Rechen- und Operationsprozeß, den eine gesetzlich ermächtigte Behörde übernehmen muß, um die Daten zu entschlüsseln, einschließlich der Rekonstruktion von Schlüsseln, sollte minimale Zeit und Ressourcen erfordern, damit eine effiziente, wirtschaftliche und aktuelle Operation sichergestellt wird.
- 16.2. Die Bereitstellung der Daten im Klartext sollte so bald wie möglich erfolgen, in dringenden Fällen innerhalb einiger Stunden oder Minuten.
17. Die gesetzlich ermächtigten Behörden fordern, daß der Entschlüsselungsprozeß so gestaltet und implementiert wird, um unbefugte oder unzulässige Verwendung auszuschließen und die mit der Operation zusammenhängende Information zu schützen.
- 17.1. Wenn kryptographisches Schlüsselmaterial bereitgestellt wird, muß es entweder in elektronischem Format oder einem anderen vereinbarten Format unter Verwendung eines sicheren Übertragungsmittels geliefert werden. Dieses muß geschützt sein, um die Echtheit, Integrität und Vertraulichkeit von derartigem Material sicherzustellen, und es muß auf nicht zurückweisbare (non-repudiational) Art und Weise bereitgestellt werden.
- 17.2. Das kryptographische Schlüsselmaterial oder die Klartextdaten dürfen nur an die in der Ermächtigung spezifizierte Behörde übertragen werden.

- 17.3. Die gesetzlich ermächtigten Behörden fordern von Anbietern kryptographischer Dienste, dem Ziel oder einem Dritten nicht zu offenbaren, daß es eine Ermächtigung gibt;
- \* das Ziel der Ermächtigung,
  - \* daß kryptographisches Schlüsselmaterial oder Klartextdaten geliefert werden; und Informationen, wie die Operation ausgeführt wird.
18. Nach Maßgabe nationaler Vorschriften können die Anbieter verpflichtet werden, entsprechend geschützte Aufzeichnungen über die Bereitstellung von Schlüsselmaterial und -daten zu führen, die jedoch nur befugten Mitarbeitern zugänglich gemacht werden dürfen.

**Teil 3: Ergänzende Begriffsbestimmungen zum Glossar**  
**der Anforderungen der Ratsentschließung vom 17.1.1995**

**ANRUF, VERBINDUNG (Glossar Abl. 96/C 329/01)**

Jede (feste oder vorübergehend) Verbindung, über die Informationen zwischen zwei oder mehr Teilnehmern eines Telekommunikationssystems übertragen werden können.

**DATEN (Neu)**

Die Darstellung von Information auf eine für Kommunikation, Interpretation, Speicherung oder Verarbeitung geeignete Weise.

**DIENSTGÜTE (Glossar Abl. 96/C 329/01)**

Die Qualitätsspezifikation für einen Kommunikationskanal, ein Kommunikationssystem, einen virtuellen Kanal, eine computergesteuerte Kommunikation usw. Die Dienstgüte läßt sich beispielsweise als Rauschabstand, Bitfehlrate, Durchsatzrate oder Blockierungswahrscheinlichkeit messen.

**ECHTHEIT (Neu)**

Stellt die Richtigkeit einer angegebenen Identität eines Benutzers, einer Vorrichtung oder eines anderen Rechtssubjekts in einem Informations- oder Kommunikationssystem fest.

**ENTSCHLÜSSELUNG (NEU)**

Die entgegengesetzte Funktion von Verschlüsselung.

**GESETZLICH ERMÄCHTIGTE BEHÖRDE (Glossar Abl. 96/C 329/01)**

Eine Behörde, die gesetzlich befugt ist, den Telekommunikationsverkehr zu überwachen

**GESETZLICH ERMÄCHTIGTE BEHÖRDE IN BEZUG AUF KRYPTOGRAPHIE (Neu)**

Eine Behörde, die gesetzlich befugt ist, kryptographisches Schlüsselmaterial und alle Informationen zu empfangen, die für die Entschlüsselung der Daten oder der Klartextdaten erforderlich sind.

**HOST (Neu)**

Jedes (Endbenutzer)- Computersystem, daß eine Verbindung zum Netz hat.

**INTEGRITÄT (Neu)**

Das Merkmal, daß Daten oder Informationen nicht auf unbefugte Weise geändert wurden.

**INTERNET (Neu)**

Die Gesamtheit von Netzen und Gateways, wo das TCP/IP-Protokoll verwendet wird und wie ein einziges kooperatives Netz funktionieren.

**INTERNET PROTOKOLL / IP (Neu)**

Internet Protocol. Das TCP/IP-Standardprotokoll, das das IP-Datagramm als jene Informationseinheit definiert, die durch ein Internet geleitet wird und die Grundlage für verbindungslosen, "best-effort" Paket-Übergabedienst darstellt. Das IP enthält als integrierenden Bestandteil ICMP (Internet Control and error Message Protocol). Die gesamte Protokollfolge wird oft als TCP/IP bezeichnet, da TCP und IP die grundlegendsten Protokolle sind.

**IP-ADRESSE (Internet Adresse) (Neu)**

Die 32-bit Adresse, welche an Hosts vergeben wird, die an einem TCP/IP-Internet teilnehmen.

**IP-DATAGRANM (Neu)**

Die grundlegende Informationseinheit, die durch ein TCP/IP-Internet geleitet wird. Sie enthält eine Ursprungs- und eine Zieladresse sowie Daten.

**IUR (Neu)**

International User Requirements for Interception - Internationale Benutzeranforderungen für Überwachung

**KLARTEXT (Neu)**

Verständliche Daten.

**KRYPTOGRAPHIE (Neu)**

Das Fachgebiet, das Prinzipien, Mittel und Methoden zur Umwandlung von Daten umfaßt, um ihren Informationsgehalt zu verbergen, ihre Echtheit festzustellen, ihre unerkannte Modifizierung zu verhindern, ihre Nichtanerkennung zu verhindern und/oder ihre unbefugte Verwendung zu verhindern.

**KRYPTOGRAPHISCHER DIENST (Neu)**

Einrichtung zur Bereitstellung von Kryptographie.

**KRYPTOGRAPHISCHER SCHLÜSSEL (Neu)**

Parameter, der mit einem kryptographischen Algorithmus verwendet wird, um Daten umzuwandeln, für gültig zu erklären, zu authentifizieren, zu verschlüsseln oder zu entschlüsseln.

**NETZBETREIBER/DIENSTEANBIETER (Glossar Abl. 96/C 329/01)**

Netzbetreiber ist der Betreiber einer öffentlich zugänglichen Telekommunikationsstruktur, die die Übertragung von Signalen zwischen definierten Netzabschlußpunkten über Draht, Funk, optische Medien oder andere elektromagnetische Mittel erlaubt.

Diansteanbieter ist eine natürliche oder juristische Person, die einen öffentlichen Telekommunikationsdienst anbietet, dessen Bereitstellung ganz oder teilweise in der Übertragung und Weiterleitung von Signalen über Telekommunikationsnetze besteht.

**RECHTMÄSSIGE GENEHMIGUNG (Glossar Abl. 96/C 329/01)**

Die unter bestimmten Bedingungen einer gesetzlich ermächtigten Behörde erteilte Genehmigung zur Überwachung bestimmter Fernmeldeverkehre. in der Regel bezeichnet der Ausdruck eine gerichtliche Anordnung oder Verfügung.

**ROAMING (Glossar Abl. 96/C 329/01)**

Die für Teilnehmer mobiler Telekommunikationsdienste bestehende Möglichkeit, Anrufe auch außerhalb ihres festgelegten Heimatbereiches herzustellen, aufrechtzuerhalten und zu empfangen.

**SESSION (Neu)**

Eine zusammenhängende Serie von Datentransfers zwischen denselben zwei Teilnehmern.

**TCP (Neu)**

Transmission Control Protocol. Der TCP/IP-Standard transportiert ein Stufenprotokoll, das den zuverlässigen Datenstrom im Vollduplexmodus vorsieht, von dem viele Anwendungsprotokolle abhängen.

**TELEKOMMUNIKATION, FERNMELDEVERKEHR (Glossar Abl. 96/C 329/01)**

die vollständige oder teilweise Übertragung von Zeichen, Signalen, schriftlichen Aufzeichnungen, Bildern, Tönen, Daten oder Information jeglicher Art über ein leitungsgebundenes, funkunterstütztes, elektromagnetisches, photoelektronisches oder photooptisches System.

**ÜBERWACHUNG (Glossar Abl. 96/C 329/01)**

Im hier verwendeten Sinne die gesetzlich begründete Maßnahme des Zugriffs und der Weiterleitung des Fernmeldeverkehrs einer Person sowie der verbindungsrelevanten Daten an die gesetzlich ermächtigte Behörde.

**ÜBERWACHUNGSANORDNUNG (Glossar Abl. 96/C 329/01)**

Eine einem Netzbetreiber/Diensteanbieter gegenüber ausgesprochene Anordnung, eine gesetzlich ermächtigte Behörde bei einer rechtmäßig genehmigten Überwachung des Fernmeldeverkehrs zu unterstützen.

**ÜBERWACHUNGSDATEN (Neu)**

Darunter versteht man Gesprächsinhalte; verbindungsrelevante Daten und teilnehmerbezogene Daten.

**ÜBERWACHUNGSSEINRICHTUNG DER GESETZLICH ERMÄCHTIGTEN BEHÖRDE (Glossar Abl. 96/C 329/01)**

Eine Einrichtung der gesetzlich ermächtigten Behörde, die als Empfänger des überwachten Fernmeldeverkehrs und der verbindungsrelevanten Daten einer bestimmten überwachten Person bestimmt ist. Der Ort, an dem sich Überwachungs-/Aufzeichnungsgeräte befinden.

**ÜBERWACHUNGSSCHNITTSTELLE (Glossar Abl. 96/C 329/01)**

Der physische Ort innerhalb der Telekommunikationseinrichtungen des Netzbetreibers/Diensterbringers, an dem der überwachte Fernmeldeverkehr und verbindungsrelevante Daten den gesetzlich ermächtigten Behörden bereitgestellt werden. Bei der Überwachungsschnittstelle handelt es sich nicht notwendigerweise um einen einzelnen festen Punkt.

**ÜBERWACHTE PERSON (Glossar Abl. 96/C 329/01)**

Die in der rechtmäßigen Genehmigung genannte(n) Person(en), deren ankommender und abgehender Fernmeldeverkehr überwacht und aufgezeichnet werden soll.

**ÜBERWACHTER TELEKOMMUNIKATIONSDIENST (Neu)**

ein der überwachten Person zugeordneter Dienst, der in der Regel in einer rechtmäßigen Überwachungsanordnung aufgeführt wird.

**VERBINDUNGSRELEVANTE DATEN (Glossar Abl. 96/C 329/01)**

Zeichengabeinformationen, die zwischen einem überwachten Telekommunikationsdienst und dem Netz oder einem anderen Teilnehmer ausgetauscht werden. Hierzu zählen Zeichengabeinformationen, die zum Aufbau und zur Steuerung der Verbindung verwendet werden (z.B. Halten einer Verbindung, Weiterreichen). Zu den verbindungsrelevanten Daten zählen auch die für den Netzbetreiber/Diensteanbieter verfügbaren Verbindungsdaten (z.B. Verbindungsdauer).

**VERFÜGBARKEIT (Neu)**

Die Eigenschaft, daß in der geforderten Weise auf Dateninformationen und Informations- und Kommunikationssysteme auf aktueller Basis zugegriffen werden kann und diese benützt werden können.

**VERSCHLÜSSELUNG (Neu)**

Die Umwandlung von Daten durch die Verwendung von Kryptographie zur Erzeugung von unvertändlichen (verschlüsselten) Daten, um deren Vertraulichkeit sicherzustellen.

**VERTRAULICHKEIT (Neu)**

Die Eigenschaft, daß Daten oder Informationen unbefugten Personen, Rechtssubjekten oder Prozessen nicht zur Verfügung gestellt oder offenbart werden.

**ZUGRIFF (Glossar Abl. 96/C 329/01)**

Die technische Möglichkeit, in einer Kommunikationseinrichtung, beispielsweise einer Leitung oder einer Vermittlungseinrichtung, eine Schnittstelle einzurichten, so daß eine gesetzlich ermächtigte Behörde den Fernmeldeverkehr und die von der Einrichtung abgewickelten verbindungsrelevanten Daten abfragen und überwachen kann.

**ZUVERLÄSSIGKEIT (Glossar Abl. 96/C 329/01)**

Die Wahrscheinlichkeit, daß ein System oder ein Dienst bei Einsatz unter spezifizierten Betriebsbedingungen für einen bestimmten Zeitraum zufriedenstellend arbeitet.