KOMMISSION DER EUROPÄISCHEN GEMEINSCHAFTEN

KOM(90) 314 endg.-SYN 287-288
Brüssel, den 13. September 1990

MITTEILUNG DER KOMMISSION
zum Schutz von Personen bei der Verarbeitung personenbezogener Daten in der Gemeinschaft und zur Sicherheit der Informationssysteme

---

Vorschlag für eine SYN 287
RICHTLINIE DES RATES
zum Schutz von Personen bei der Verarbeitung personenbezogener Daten

---

Entwurf einer
ENTSCHLIESSUNG DER IM RAT VEREINIGTEN VERTRETER DER REGIERUNGEN DER MITGLIEDSTAATEN DER EUROPÄISCHEN GEMEINSCHAFTEN

ERKLÄRUNG DER KOMMISSION
betreffend die Anwendung der Grundsätze der Richtlinie zum Schutz von Personen bei der Verarbeitung personenbezogener Daten auf die Organe und Einrichtungen der Europäischen Gemeinschaften

---

Vorschlag für eine SYN 288
RICHTLINIE DES RATES
zum Schutz personenbezogener Daten und der Privatsphäre in öffentlichen digitalen Telekommunikationsnetzen, insbesondere im dienstelntegrierenden digitalen Telekommunikationsnetz (ISDN) und in öffentlichen digitalen Mobilfunknetzen

---

Empfehlung für einen
BESCHLUSS DES RATES
zur Aufnahme von Verhandlungen über den Beitritt der Europäischen Gemeinschaften zum Übereinkommen des Europarats zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten

---

Vorschlag für einen
BESCHLUSS DES RATES
auf dem Gebiet der Informationssicherheit

(von der Kommission vorgelegt)

Mitteilung der Kommission zum Schutz von Personen bei der Verarbeitung personenbezogener Daten in der Gemeinschaft und zur Sicherheit der Informationssysteme

I. EINLEITUNG

1. Die immer häufigere Verarbeitung personenbezogener Daten in allen Bereichen wirtschaftlicher und sozialer Tätigkeit sowie der neue Bedarf am Austausch von Daten im Zusammenhang mit der Stärkung des Gemeinschaftsaufbaus machen die Einführung von Maßnahmen in der Gemeinschaft erforderlich, die darauf abzielen, den Schutz von Personen bei der Verarbeitung personenbezogener Daten zu gewährleisten und die Sicherheit der Verarbeitung von Daten insbesondere im Rahmen der Entwicklung offener Telekommunikationsnetze zu verstärken.

2. Zu einem Zeitpunkt, zu dem die Fortschritte der Informationstechniken die Verarbeitung und den Austausch von Daten aller Art beträchtlich erleichtern, ist der Stand des Schutzes von Personen bei dieser Verarbeitung in der Gemeinschaft durch die Vielfalt der einzelstaatlichen Ansätze gekennzeichnet. In den siebziger Jahren haben die Besorgnisse im Zusammenhang mit dem Schutz von Personen bei der Verarbeitung personenbezogener Daten in mehreren Mitgliedstaaten zu einem Gesetzgebungsprozeß geführt, mit dem die Verwendung dieser Art von Daten eingeschränkt und strukturiert werden sollte. Zur Zeit gibt es allerdings nur in sieben Mitgliedstaaten spezifische Rechtsvorschriften auf diesem Gebiet, obwohl die Zielsetzung dieser Rechtsvorschriften identisch ist, werden aber bisweilen unterschiedliche Lösungen, beispielsweise in der Frage des Anwendungsbereichs (Einbeziehung von Karteien, Schutz juristischer Personen) oder der Voraussetzungen für die Verarbeitungen (Ausmaß der Meldepflicht, Unterrichtung bei der Erhebung, Verarbeitung sensibler Daten), gewählt.

3. Abgesehen von den einzelstaatlichen Regeln und der Empfehlung des Rates der OECD vom 23. September 1980 hinsichtlich der Leitlinien über den Schutz der Privatsphäre und den grenzüberschreitenden Verkehr von personenbezogenen Daten, ist das Übereinkommen des Europarates vom 28. Januar 1981 zum Schutze des Menschen bei der automatischen Verarbeitung personenbezogener Daten das einzige Instrument internationalen Rechts in diesem Bereich. Es läßt allerdings viele Optionen für die Umsetzung der von ihm definierten Rahmengrundsätze offen und wurde nur von sieben Mitgliedstaaten ratifiziert, wobei es in einem immer noch keine innerstaatlichen Rechtsvorschriften gibt.

4. Angesichts dieser Situation sind in der Gemeinschaft bereits Besorgnisse laut geworden. So hat das Europäische Parlament bereits 1976 mehrere Entschließungen(1) angenommen, in denen es seine Bedenken hinsichtlich dieser Frage zum Ausdruck bringt und die Kommission auffordert, einen Richtlinienvorschlag zur Angleichung der Rechtsvorschriften im Bereich des Schutzes personenbezogener Daten auszuarbeiten.

5. In einer Entschließung vom 29. Juli 1981 hat die Kommission hervorgehoben, daß dieser Schutz den Charakter eines Grundrechts habe und es wünschenswert sei, daß eine Angleichung in diesem Bereich in allen Mitgliedstaaten ausgearbeitet wird. Sie hat den Mitgliedstaaten ferner empfohlen, vor Ende des Jahres 1982 das Übereinkommen des Europarates vom 28. Januar 1981 zum Schutze des Menschen bei der automatischen Verarbeitung personenbezogener Daten zu ratifizieren. Es wurde allerdings präzisiert, daß, "sollte es nicht binnen einer angemessenen Zeitspanne zu einer Unterzeichnung und Ratifizierung des Übereinkommens durch alle Mitgliedstaaten kommen, sich die Kommission vorbehält, dem Rat den Erlaß eines auf den EWG-Vertrag gestützten Rechtsaktes vorzuschlagen".

---

(1) ABl. Nr. C 100 vom 3.5.1976, S. 27;
ABl. Nr. C 140 vom 5.6.1979, S. 34;
ABl. Nr. C 87 vom 5.4.1982, S. 39.

6. Die unterschiedlichen Ansätze auf einzelstaatlicher Ebene und das Fehlen eines Schutzsystems auf Gemeinschaftsebene stellen ein Hemmnis für die Vollendung des Binnenmarkts dar. Sind die Grundrechte der betroffenen Personen, insbesondere das Recht auf Privatsphäre, nicht auf Gemeinschaftsebene gewährleistet, so könnte der grenzüberschreitende Datenfluß behindert werden, während er doch für die Tätigkeiten der Betriebe und Forschungseinrichtungen sowie für die Zusammenarbeit zwischen den Verwaltungen der Mitgliedstaaten im Rahmen des Raums ohne Binnengrenzen gemäß Artikel 8a des Vertrags unerläßlich geworden ist. So betonte der Europäische Rat von Straßburg am 8. und 9. Dezember 1989 im Rahmen der Maßnahmen für die Freizügigkeit der Personen und das Europa der Bürger die Notwendigkeit, "daß bei diesen Beratungen dafür Sorge getragen wird, daß in den Bestimmungen über die Zusammenarbeit zwischen den Verwaltungen der Persönlichkeitsschutz bei der Benutzung von Datenbanken mit personenbezogenen Angaben sichergestellt wird".

7. Ein Gemeinschaftsansatz für den Schutz von Personen bei der Verarbeitung personenbezogener Daten ist auch für die Entwicklung der Informatikindustrie und leistungsfähigerer Telematikdienste ein wesentliches Erfordernis. Die rasche Einführung harmonisierter Vorschriften für den Datenschutz und den Schutz der Privatsphäre im Rahmen der dienstintegrierenden digitalen Netze ist für die Verwirklichung des Binnenmarkts für Anlagen und Telekommunikationsdienste unabdingbar.

8. Das Eindringen der Informatik in alle Bereiche wirtschaftlicher und sozialer Tätigkeit und die Einführung globaler Kommunikationssysteme zur Erleichterung der Integration verschiedener Tätigkeiten sind ebenfalls eine neue Herausforderung, aufgrund derer ein an die Risiken angepaßter "Schutz" geboten werden muß, die mögliche technische oder menschliche, zufällige oder beabsichtigte Unzulänglichkeiten mit sich bringen. Eine wirksame Sicherheit der Informationssysteme ist ein wesentliches Element, mit dem ein tatsächlicher Schutz der Privatsphäre gewährleistet und die

Integrität der Güter gewahrt werden kann, die heute die gespeicherten und in elektronischer Form übermittelten Daten darstellen. Die Gemeinschaftspolitiken und -programme für die Entwicklung der Informations- und Telekommunikationsindustrie und die Verwirklichung des Binnenmarkts drohen ernsthaft behindert zu werden, wenn nicht eine aktive Politik der Einführung, Entwicklung und Förderung von Sicherheitsnormen für die Informationssysteme betrieben wird. Da das Fernmeldewesen heute einen weltweiten Datenaustausch ermöglicht, hat eine derartige Politik diese Dimension zu berücksichtigen. Wesentlich ist auch, daß die nationalen Politiken im Bereich der Informationssicherheit kein Hemmnis für die Förderung der harmonischen Entwicklung der Gemeinschaft und der Beziehungen zu den Drittländern werden.

II. VORGESCHLAGENES VORGEHEN

9. Mit dem vorgeschlagenen Ansatz soll über ein gemeinschaftliches Schutzsystem, das auf einem Paket von sich gegenseitig ergänzenden Maßnahmen beruht, ein hohes Schutzniveau gewährleistet werden.

A Ein hohes Schutzniveau

10. Da die einzelstaatlichen Rechtsvorschriften das Ziel verfolgen, die Grundrechte der Personen, insbesondere das Recht auf Privatsphäre, zu garantieren, und die Gemeinschaft selbst insbesondere in Absatz 3 der Präambel der Einheitlichen Europäischen Akte ihre Bindung an die Grundrechte zum Ausdruck gebracht hat, darf die Maßnahme der Gemeinschaft nicht zu einer Verringerung des Schutzes führen, sondern muß ein hohes Schutzniveau in der gesamten Gemeinschaft sicherstellen. Durch eine Gemeinschaftsmaßnahme läßt sich in allen Mitgliedstaaten der Gemeinschaft ein gleichwertiges hohes Schutzniveau garantieren und damit können Hemmnisse für die Errichtung des Binnenmarkts gemäß Artikel 100a aufgehoben werden.

11. Neben der Angleichung der anerkannten Rechte der Personen auf einer hohen Ebene ist es unerläßlich, eine aktive Politik im Bereich der Sicherheit der Informationssysteme einzuleiten. Die Sicherheit der Informationssysteme ist für die Personen wie für den Handel, die Industrie und die Verwaltung lebenswichtig. Im wesentlichen geht es darum, eine wirksame, praktische Sicherheit der in elektronischer Form gespeicherten Information zu gewährleisten und dabei die Bildung neuer technischer Hemmnisse zwischen Mitgliedstaaten oder gegenüber Drittländern zu vermeiden. Dieses Erfordernis macht eine Prüfung des Bedarfs und der möglichen Optionen auf Gemeinschaftsebene in enger Zusammenarbeit mit den Verantwortlichen des Bereichs und der Mitgliedstaaten erforderlich.

B Ein globaler Ansatz

12. Für die Einführung eines Systems des Schutzes von Personen bei der Verarbeitung personenbezogener Daten in der Gemeinschaft sind mehrere Maßnahmen vorzusehen, mit denen die verschiedenen Aspekte dieser Frage abgedeckt werden können.

13. Intern wird über eine Rahmenrichtlinie zur Angleichung bestimmter Rechts- und Verwaltungsvorschriften der Mitgliedstaaten für den Schutz von Personen bei der Verarbeitung personenbezogener Daten (Allgemeine Richtlinie) - das zentrale Schutzsystem - hinaus ein Paket weiterer ergänzender Maßnahmen vorgeschlagen, um einen möglichst vollständigen Schutz sicherzustellen. Jede der vorgeschlagenen Maßnahmen ist einer spezifischen Situation angepaßt, aber alle gehen von denselben Schutzprinzipien aus, die in der allgemeinen Richtlinie enthalten sind. So verfolgen eine Entschließung der im Rat vereinigten Vertreter der Regierungen der Mitgliedstaaten und eine Erklärung der Kommission das Ziel, die Grundsätze der Richtlinie auf Dateien anwendbar zu machen, die nicht in den Anwendungsbereich der Richtlinie fallen. Eine sektorielle Richtlinie ist im Rahmen der öffentlichen digitalen Telekommunikationsnetze erforderlich. Die Sicherheit der Informationssysteme schließlich macht einen gemeinschaftlichen Aktionsplan notwendig.

14. Nach außen hin hat die Europäische Gemeinschaft bei ihren Partnern die Einführung angemessener Schutzbestimmungen zu fördern und die einschlägigen Bemühungen des Europarats zu unterstützen. Hier ist es insbesondere wünschenswert, daß die Kommission Verhandlungen mit dem Ziel ihres Beitritts zu dem Übereinkommen 108 des Europarats einleitet.

Diese Vorschläge lassen sich nicht voneinander trennen, ohne die Geschlossenheit und Kohärenz des vorgeschlagenen Schutzsystems zu beeinträchtigen.

C Vorlage der Vorschläge

15. Der Vorschlag für eine allgemeine Richtlinie verfolgt das Ziel, in allen Mitgliedstaaten der Gemeinschaft ein gleichwertiges hohes Schutzniveau einzuführen, um die Hemmnisse für den Austausch von Daten abzubauen, der für das Funktionieren des Binnenmarktes unerläßlich ist. Dazu müssen die in dem Entwurf eines Richtlinienvorschlags genannten Grundsätze von den Mitgliedstaaten garantiert werden. Diese Grundsätze beziehen sich insbesondere auf die Bedingungen, unter denen eine Verarbeitung personenbezogener Daten rechtmäßig ist, die Rechte der betroffenen Person (Recht auf Unterrichtung, Auskunftsrecht, Recht auf Berichtigung, Einspruchsrecht usw.), die nötige Qualität der Daten (sie müssen richtig, nach Treu und Glauben, für bestimmte rechtmäßige Zweckbestimmungen gespeichert sein usw.), die Einsetzung einer Gruppe für den Schutz personenbezogener Daten, die die Kommission in Fragen des Datenschutzes berät. Der Richtlinienvorschlag gilt für den privaten wie für den öffentlichen Bereich, dessen Tätigkeiten in den Anwendungsbereich des Gemeinschaftsrechts fallen. Da jeder in jedem Mitgliedstaat bei der Verarbeitung personenbezogener Daten den gleichen hohen Schutz genießen können wird, werden die Mitgliedstaaten die Freizügigkeit dieser Daten in der Gemeinschaft nicht mehr mit der Begründung des Schutzes der betroffenen Person einschränken können.

16. Der Entschließungsentwurf der im Rat vereinigten Vertreter der Mitgliedstaaten der Europäischen Gemeinschaften verfolgt das Ziel, die Geltung der Grundsätze der allgemeinen Richtlinie auf die Dateien des öffentlichen Bereichs auszudehnen, für die sie nicht gilt, d.h. die Dateien der Verwaltungen, deren Tätigkeiten nicht in den Anwendungsbereich des Gemeinschaftsrechts fallen. Im Sinne stärkerer Kohärenz wäre es wünschenswert, daß für alle Dateien von Verwaltungen, auchwenn sie nicht unter die allgemeine Richtlinie fallen,dieselben Schutzprinzipien gelten. Dazu müßten sich die Mitgliedstaaten verpflichten, die erforderlichen Gesetzgebungsverfahren auf einzelstaatlicher Ebene einzuleiten.

17. Die Erklärung der Kommission betreffend die Anwendung der Bestimmungen der allgemeinen Richtlinie auf die Organe und Einrichtungen der Gemeinschaft bringt den Wunsch zum Ausdruck, daß die Grundsätze der Richtlinie für die Organe und Einrichtungen der Gemeinschaft gelten. Dazu ist vorgesehen, daß die Kommission die erforderlichen Maßnahmen trifft und vorschlägt; in der Zwischenzeit wird sie die Bestimmungen der Richtlinie auf ihre eigenen Dateien anwenden.

18. Der Vorschlag für eine Richtlinie des Rates zum Schutz personenbezogener Daten und der Privatsphäre in öffentlichen digitalen Telekommunikationsnetzen, insbesondere im dienstintegrierenden digitalen Telekommunikationsnetz (ISDN) und in öffentlichen digitalen Mobilfunknetzen vervollständigt die allgemeine Richtlinie durch die Anwendung der allgemeinen Grundsätze des Datenschutzes auf den spezifischen Bedarf der neuen Telekommunikationsnetze. Die Richtlinie zielt darauf ab, den Telekommunikationsbenutzern in allen Mitgliedstaaten ein Basisschutzniveau durch Maßnahmen zu garantieren, die in die von den neuen Netzen gebotenen Dienste zu integrieren sind. Der Rat und das Europäische Parlament haben wiederholt die Bedeutung geeigneter Maßnahmen für die Sicherstellung des Schutzes der Daten und der Privatsphäre im Hinblick auf die neuen Entwicklungen der Telekommunikation und insbesondere des ISDN[1] hervorgehoben. Dieses Anliegen ist von den Datenschutzbeauftragten der Mitgliedstaaten bei ihrem Jahrestreffen in Berlin im August 1989 mit Nachdruck vorgebracht worden.

---

(1) ABl. Nr. C 257 vom 4.10.1988, S. 1; ABl. Nr. C 196 vom 1.8.1989, S. 4; ABl. Nr. C 7 vom 12.1.1987, S. 334; ABl. Nr. C. 12 vom 16.1.1989, S. 66; ABl. Nr. C 12 vom 16.1.1989, S. 69.

19. Die Empfehlung für einen Beschluß des Rates betreffend den Beitritt der Europäischen Gemeinschaft zum Übereinkommen des Europarats zum Schutze des Menschen bei der automatischen Verarbeitung personenbezogener Daten ist einer der Bestandteile des Ansatzes der Gemeinschaft im Bereich des Schutzes personenbezogener Daten. Der Beitritt zu dem Übereinkommen wird in den Beziehungen zwischen der Gemeinschaft und den Drittländern, die Vertragspartner sind, den Schutz der betroffenen Personen und den grenzüberschreitenden Verkehr personenbezogener Daten gewährleisten.

20. Der Vorschlag für eine Entscheidung des Rates über die Annahme eines zwei-Jahres-Aktionsprogramms im Bereich der Sicherheit der Informationssysteme wird die Instrumente ergänzen, mit denen die Rechte der Personen bei der Verarbeitung personenbezogener Daten verstärkt werden sollen. Die Sicherheit der Information, d.h. der Schutz der gespeicherten, verarbeiteten und in elektronischer Form übermittelten Daten vor allen möglichen (zufälligen oder beabsichtigten) Gefährdungen ist für die tatsächliche Wahrnehmung der Rechte der Personen bei der Verarbeitung personenbezogener Daten von wesentlicher Bedeutung. Dabei handelt es sich ganz allgemein um ein wichtiges Erfordernis für den Schutz von Gütern und Personen, der im Rahmen der Erweiterung der offenen Telekommunikationsnetze die Entwicklung einer globalen Strategie, konzertierter Aktionen auf Gemeinschaftsebene im Bereich der Technologie, Normen und Verfahren zur Genehmigung und Prüfung sowie technologische Entwicklungen erforderlich macht, die eine Zusammenarbeit auf dem Gebiet der vorwettbewerblichen Forschung und Entwicklung voraussetzen.

21. Das vorgeschlagene Aktionsprogramm sieht vor: die Entwicklung eines strategischen Rahmens für die Sicherheit der Informationssysteme, die Analyse des Bedarfs im Bereich Sicherheit, die Ausarbeitung von Lösungen für bestimmte Bereiche mit vorrangigem Bedarf, die Ausarbeitung von Spezifikationen, Normen und Eignungsprüfungen, die Einbeziehung der technischen und betrieblichen Entwicklungen im Bereich der Sicherheit der Informationssysteme in einen allgemeinen strategischen Rahmen und die Einbeziehung bestimmter Sicherheitsfunktionen in die Informationssysteme.

Vorschlag für eine SYN 287

RICHTLINIE DES RATES

zum Schutz von Personen bei der Verarbeitung

personenbezogener Daten

INHALTSVERZEICHNIS

Zusammenfassung

Dieser Vorschlag der allgemeinen Richtlinie verfolgt das Ziel, in allen Mitgliedstaaten der Gemeinschaft ein gleichwertiges hohes Schutzniveau einzuführen, um die Hemmnisse für den Austausch von Daten abzubauen, der für das Funktionieren des Binnenmarktes unerläßlich ist. Dazu müssen die in dem Entwurf eines Richtlinienvorschlags genannten Grundsätze von den Mitgliedstaaten garantiert werden. Diese Grundsätze beziehen sich insbesondere auf die Bedingungen, unter denen eine Verarbeitung personenbezogener Daten rechtmäßig ist, die Rechte der betroffenen Person (Recht auf Unterrichtung, Auskunftsrecht, Recht auf Berichtigung, Einspruchsrecht usw.), die nötige Qualität der Daten (sie müssen richtig nach Treu und Glauben, für bestimmte rechtmäßige Zweckbestimmungen gespeichert sein usw.), die Einsetzung einer Gruppe für den Schutz personenbezoger Daten, die die Kommission in Fragen des Datenschutzes berät. Der Entwurf des Richtlinienvorschlags gilt für den privaten wie für den öffentlichen Bereich, dessen Tätigkeiten in den Anwendungsbereich des Gemeinschaftsrechts fallen. Da jeder in jedem Mitgliedstaat bei der Verarbeitung personenbezogener Daten den gleichen hochwertigen Schutz genießen können wird, werden die Mitgliedstaaten die Freizügigkeit dieser Daten in der Gemeinschaft nicht mehr mit der Begründung des Schutzes der betroffenen Person einschränken können.

Begründung

I. EINLEITUNG

Die Besorgnisse hinsichtlich des Schutzes von Personen bei der Verarbeitung personenbezogener Daten, die in den letzten fünfzehn Jahren geäußert wurden, wurden zum einen ausgelöst durch die Möglichkeiten, die die technischen Fortschritte im Bereich der Datenverarbeitung eröffnen und zum anderen durch die immer häufigere Verwendung personenbezogener Daten in einer Vielzahl von Bereichen. Diese Besorgnisse wurden bei verschiedenen Gelegenheiten vorgetragen und haben in mehreren Mitgliedstaaten zu gesetzgeberischen Initiativen geführt. Auf internationaler Ebene ist das Übereinkommen des Europarates vom 28. Januar 1981 für den Schutz von Personen bei der automatischen Verarbeitung personenbezogener Daten gegenwärtig das einzige Instrument internationalen Rechts auf diesem Gebiet. Die OECD hat in einer Empfehlung vom 23. September 1980 Leitlinien über den Schutz der Privatsphäre und die grenzüberschreitende Weitergabe von personenbezogenen Daten aufgestellt, und die Vereinten Nationen erarbeiten zur Zeit ebenfalls solche Leitlinien.

Besorgnisse wurden auch auf der Ebene der Gemeinschaft geäußert. So hat das Europäische Parlament bereits 1976 mehrere Entschließungen verabschiedet[1], in denen es seine Beunruhigung in dieser Frage erklärt und die Kommission auffordert, einen Richtlinienvorschlag zur Harmonisierung der Rechtsvorschriften auf dem Gebiet des Schutzes personenbezogener Daten auszuarbeiten.

Die Kommission hat in einer Empfehlung vom 29. Juli 1981 darauf hingewiesen, daß dieser Schutz den Charakter eines Grundrechts hat und daß eine Annäherung auf diesem Gebiet für alle Mitgliedstaaten anzustreben ist. Sie hat den Mitgliedstaaten außerdem empfohlen, vor Ablauf des Jahres

---

(1) ABl. Nr. C 100 vom 3.5.1976, S. 27; ABl. Nr. C 140 vom 5.6.1979, S. 34; ABl. Nr. C 87 vom 5.4.1982, S. 39.

1982 das Übereinkommen des Europarates vom 28. Januar 1981 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten zu ratifizieren. Sie hat allerdings hinzugefügt, daß "sich die Kommission das Recht vorbehält, wenn nach Ablauf einer angemessenen Frist nicht alle Mitgliedstaaten dieses Übereinkommen unterzeichnet und ratifiziert haben sollten, dem Rat vorzuschlagen, einen Rechtsakt auf der Grundlage des EWG-Vertrags zu verabschieden."

Der Europäische Rat von Straßburg vom 8. und 9. Dezember 1989 hat im Zusammenhang mit den Maßnahmen zugunsten des freien Personenverkehrs und des Europas der Bürger auf die Notwendigkeit hingewiesen, "dafür zu sorgen, daß die Verfahren der Zusammenarbeit zwischen den Verwaltungen die Gewährleistung des Schutzes der Bürger bei der Benutzung personenbezogener Datenbanken vorsehen".

Es ist darauf hinzuweisen, daß sich diese Besorgnisse neben diesen Stellungnahmen zur Notwendigkeit eines generellen Schutzes auch im Rahmen spezieller oder sektoraler Maßnahmen der Gemeinschaft insbesondere im Bereich der neuen Informationstechnologien niedergeschlagen haben.

Angesichts der gegenwärtigen Situation im Bereich der Verarbeitung personenbezogener Daten sowie der Erfordernisse des gemeinschaftlichen Aufbauwerks ist eine Richtlinie, die den Personenschutz bei der Verarbeitung dieser Daten gewährleistet, dringend notwendig.

II. DIE NOTWENDIGKEIT EINES SCHUTZES AUF DER EBENE DER GEMEINSCHAFT

Die unterschiedlichen nationalen Rechtsvorschriften und das Fehlen eines angemessenen Schutzes in der Gemeinschaft

Der Schutz von Personen im Zusammenhang mit personenbezogenen Daten ist Gegenstand einer Vielzahl von Initiativen in den Mitgliedstaaten. Diese Vielzahl unterschiedlicher Maßnahmen ist das Ergebnis zum einen der Tatsache, daß einige Mitgliedstaaten keine speziellen Rechtsvorschriften auf diesem Gebiet erlassen haben, und zum anderen der Tatsache, daß diese, wo sie vorhanden sind, unterschiedlichen Inhalts sind.

Gegenwärtig haben sieben Mitgliedstaaten spezielle Rechtsvorschriften (Deutschland, Dänemark, Frankreich, Irland, Luxemburg, Niederlande und Vereinigtes Königreich). In einigen anderen Mitgliedstaaten werden zur Zeit Rechtsvorschriften ausgearbeitet.

Die Zielsetzung dieser nationalen Rechtsvorschriften - der Schutz der betroffenen Personen - ist zwar die gleiche, allerdings werden angesichts der Vielfalt der möglichen Wege, um diesen Schutz zu gewährleisten, unterschiedliche Lösungen gewählt. So sind unterschiedliche Regelungen beispielsweise für die Einbeziehung von Karteien, den Schutz juristischer Personen, die Verfahren vor der Einrichtung von Datenbanken, den Anwendungsbereich der Mitteilungspflicht, die Information bei der Erhebung der Daten, die Behandlung schützenswerter Daten und die Übermittlung in andere Länder möglich. Außerdem kann die technologische Entwicklung dazu führen, daß die Mitgliedstaaten anders reagieren und so die Disparitäten verstärken.

Durch das Übereinkommen des Europarates vom 28. Januar 1981 für den Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten konnten die Disparitäten nicht reduziert werden, da dieses zum einen eine Vielzahl von Möglichkeiten bei der Umsetzung der darin festgelegten Grundprinzipien offenläßt und zum anderen nur von sieben Mitgliedstaaten (Deutschland, Dänemark, Spanien, Frankreich, Irland, Luxemburg und Vereinigtes Königreich) ratifiziert wurde, von denen einer (Spanien) noch immer keine innerstaatlichen Rechtsvorschriften erlassen hat. Die Empfehlung der Kommission vom 29. Juli 1981, in der die Mitgliedstaaten der Gemeinschaft aufgefordert werden, das Übereinkommen des Europarates zu ratifizieren, hat an dieser Situation nichts geändert.

Angesichts der unterschiedlichen nationalen Konzepte ist der Schutz von Personen bei der Verarbeitung personenbezogener Daten nicht in allen Mitgliedstaaten gleichwertig, so daß der Grad des Schutzes von Mitgliedstaat zu Mitgliedstaat unterschiedlich sein kann.

Folgen dieser Situation für die Gemeinschaft

Für die Gemeinschaft verursacht diese Situation Probleme in drei Bereichen:

- Das Fehlen spezieller nationaler Rechtsvorschriften oder deren Lücken sind nicht mit dem Engagement der Gemeinschaft für die Wahrung der Grundrechte vereinbar, auf das in der gemeinsamen Erklärung des Europäischen Parlamentes, des Rates und der Kommission zu den Grundrechten vom 5. April 1977 und in Absatz 3 der Präambel der Einheitlichen Europäischen Akte hingewiesen wurde. Außerdem ist der Schutz der Grundrechte im Rahmen des Gemeinschaftsrechts Teil der allgemeinen Rechtsgrundsätze, deren Beachtung der Gerichtshof der Europäischen Gemeinschaften gewährleistet.

- Die Weitergabe personenbezogener Daten erscheint soweit sie unter Beachtung der Rechte der betroffenen Person erfolgt, im Rahmen der Verwirklichung und des ordnungsgemäßen Funktionierens des Binnenmarkts als notwendig. Im Zusammenhang mit der technologischen Entwicklung im Bereich der Datenverarbeitung, insbesondere des Ausbaus der Datenkommunikationsnetze in der Gemeinschaft ist die grenzüberschreitende Übermittlung von Daten auf drei Ebenen von Bedeutung:

  . Der Verwendung personenbezogener Daten, die in vielen Bereichen des Wirtschaftslebens erforderlich ist. Der freie Verkehr von Waren, Personen, Dienstleistungen und Kapital macht es erforderlich, daß personenbezogene Daten zwischen den Wirtschaftsteilnehmern, die grenzüberschreitend tätig sind, übermittelt werden können.

  . Im Zuge des Integrationsprozesses der Gemeinschaft, insbesondere im Zusammenhang mit der Beseitigung der Grenzen, muß die Zusammenarbeit zwischen den nationalen Verwaltungen verstärkt werden. Die nationalen Verwaltungen werden dann Aufgaben übernehmen müssen, die in den Zuständigkeitsbereich einer Verwaltung eines anderen Mitgliedstaates fallen. Unter diesen Umständen wird die Übermittlung von Daten zu einer notwendigen Voraussetzung für die Zusammenarbeit. Die Verpflichtung zur Zusammenarbeit oder Information,

die für die Verwaltungen durch das Gemeinschaftsrecht entsteht, setzt voraus, daß gleichzeitig für einen angemessenen Schutz für die betroffenen Personen gesorgt wird.

. Der Datenaustausch ist außerdem für die Zusammenarbeit auf dem Gebiet der Wissenschaft erforderlich.

Dieser Notwendigkeit, den Austausch von Daten zwischen den Mitgliedstaaten zu ermöglichen, steht gegenwärtig die Verschiedenartigkeit der nationalen Vorschriften auf dem Gebiet des Schutzes von Personen bei der Verarbeitung personenbezogener Daten entgegen. Diese Verschiedenartigkeit kann dazu führen, daß ein Mitgliedstaat den Datenaustausch behindert und sich dabei auf einen fehlenden oder unzureichenden Schutz im Ausgangs- oder Bestimmungsland beruft.

- Diese Verschiedenartigkeit kann auch in bestimmten Fällen den Wettbewerb zwischen den privaten Wirtschaftsteilnehmern verfälschen, wenn diese in ihrem Land unterschiedlich strengen Vorschriften unterliegen.

III. DIE VORGESEHENEN MASSNAHMEN

Ein gleichwertiger Schutz in der Gemeinschaft

Um für jede Person mit Wohnsitz in der Gemeinschaft einen Schutz bei der Verarbeitung personenbezogener Daten zu gewährleisten und den Austausch dieser Art von Daten zwischen den Mitgliedstaaten zu ermöglichen, muß ein gleichwertiger Schutz in allen Teilen der Gemeinschaft erreicht werden. Eine Angleichung der Rechtsvorschriften ist daher notwendig. Das Arbeitsprogramm der Kommission für 1990 sieht im übrigen vor, daß der Datenschutz im Rahmen der Vollendung des Binnenmarkts Priorität genießt(1).

---

(1) Bull. EG, Beilage 1/90, Seite 18, 26 und 28.

Da ein gleichwertiger Schutz auf hohem Niveau für die Vollendung des Binnenmarkts erforderlich ist, ist Artikel 100 a des Vertrags als geeignete Rechtsgrundlage anzusehen. Die Vollendung und das ordnungsgemäße Funktionieren des Binnenmarkts, der in Artikel 8 a als "ein Raum ohne Binnengrenzen" definiert wird, "in dem der freie Verkehr von Waren, Personen, Dienstleistungen und Kapital gemäß den Bestimmungen dieses Vertrages gewährleistet ist", erfordert aus den bereits genannten Gründen eine Angleichung der Rechtsvorschriften in diesem Bereich.

Bei der Vorbereitung dieses Vorschlags hat die Kommission den Erfordernissen des Artikels 8 c des Vertrages Rechnung getragen und ist zu dem Schluß gelangt, daß Sonderbestimmungen oder Ausnahmeregelungen in diesem Stadium weder erforderlich erscheinen noch zu rechtfertigen wären.

Die Kommission hat auch der Frage des nach dem Wortlaut von Artikel 100 a Absatz 3 des Vertrages erforderlichen hohen Schutzniveaus in den Bereichen Gesundheit, Sicherheit, Umweltschutz und Verbraucherschutz Beachtung geschenkt.

Ein hohes Schutzniveau

Da durch die nationalen Rechtsvorschriften auf diesem Gebiet ein Schutz der Grundrechte, insbesondere des Rechts auf den Schutz der Privatsphäre sichergestellt werden soll, muß die Angleichung dieser Rechtsvorschriften dem Ziel dienen, ein hohes Schutzniveau zu garantieren. Abgesehen von den Anpassungen, die jede Rechtsangleichung mit sich bringt, darf diese Angleichung nicht zu einer Verringerung des Schutzniveaus führen, das in den Mitgliedstaaten bereits gewährleistet wird.

Die allgemeinen Grundsätze, die im Übereinkommen des Europarates niedergelegt sind, können als Referenz dienen, da sie bereits eine gemeinsame Basis für die Länder darstellen, die es ratifiziert haben. Die Richtlinie enthält daher Regelungen, die mit denen des Übereinkommens vereinbar sind, ergänzt diese allgemeinen Grundsätze jedoch, um einen gleichwertigen Schutz auf hohem Niveau herzustellen.

Ein hohes Schutzniveau setzt voraus, daß die Richtlinie einen möglichst breiten Schutz gewährleistet und daß alle Fälle abgedeckt werden, in denen die Verarbeitung personenbezogener Daten für die betroffenen Personen ein Risiko darstellt. Die Richtlinie gilt daher sowohl für Kartelen als auch für Datenbanken und für die Dateien des öffentlichen Bereichs ebenso wie für die des privaten Bereichs.

Durch die in der Richtlinie enthaltenen Grundsätze, insbesondere den der Rechtmäßigkeit der Verarbeitung, der Weitergabe der Daten an Dritte, der Meldepflichten, der Rechte der betroffenen Personen sowie der Qualität der Daten soll ein hohes Schutzniveau sichergestellt werden, wobei die verschiedenen Regelungen des nationalen Rechts als Referenz dienen. Außerdem wurde den Mitteln zur Gewährleistung einer effektiven Anwendung der Bestimmungen der Richtlinie, die über die üblichen Mechanismen zur Kontrolle der Anwendung des Gemeinschaftsrechts hinausgehen, besondere Aufmerksamkeit gewidmet. Die Bestimmungen über die Verantwortlichkeit und die Einsetzung einer Gruppe für den Schutz personenbezogener Daten sind das Ergebnis dieser Bestrebungen.

Die Grundsätze der Richtlinie können gegebenenfalls ergänzt werden. Die Richtlinie sieht zu diesem Zweck in mehreren Bestimmungen vor, daß die Mitgliedstaaten näher regeln können, welche Dateien ihren Rechtsvorschriften unterliegen. Ergänzende Maßnahmen können auch im Rahmen der Anwendung bestimmter allgemeiner Grundsätze auf Sektoren mit ausgeprägten Besonderheiten erforderlich sein.

IV. ERÖRTERUNG DER ARTIKEL

KAPITEL I

Allgemeine Bestimmungen

Artikel 1

Gegenstand der Richtlinie

Dieser Artikel sieht vor, daß die Mitgliedstaaten verpflichtet sind, den Schutz von Personen bei der Verarbeitung von personenbezogenen Daten gemäß den Bestimmungen dieser Richtlinie zu gewährleisten. Da durch diese Richtlinie der Schutz nach den gleichen Grundsätzen in allen Mitgliedstaaten sichergestellt wird und daher gleichwertig ist, dürfen diese den freien Verkehr von Daten in den von der Richtlinie abgedeckten Bereichen aus Gründen des Schutzes der betroffenen Person nicht mehr einschränken. Der Schutz von Personen und der freie Verkehr von Daten wird jedoch durch die Richtlinie nur in den Bereichen gewährleistet, die von dieser abgedeckt sind. Dateien, die für private Zwecke oder von gemeinnützigen Vereinigungen unterhalten werden, fallen nicht in den Anwendungsbereich der Bestimmungen dieses Artikels, soweit sie gemäß Artikel 3 Absatz 2 vom Anwendungsbereich der Richtlinie ausgeschlossen sind.

Artikel 2

Begriffsbestimmungen

In diesem Artikel werden die wichtigsten Begriffe definiert, die in der Richtlinie verwendet werden. Die Definitionen entsprechen denen des Übereinkommens 108 des Europarates, allerdings wurden die Anpassungen und näheren Ausführungen vorgenommen, die notwendig sind, um einen gleichwertigen Schutz auf hohem Niveau in der Gemeinschaft zu gewährleisten.

a) "Personenbezogene Daten". Ebenso wie im Übereinkommen 108 wurde eine Definition im weiten Sinne gewählt, die alle Informationen einschließt, die mit einer Person in Verbindung gebracht werden können. Tatsächlich können alle Daten im Zusammenhang mit einer Person, selbst wenn diese scheinbar harmlos sind, bei entsprechender Verwendung sensiblen Charakter haben (eine einfache Postanschrift beispielsweise). Um zu verhindern, daß Mittel zur indirekten Identifizireung eine Umgehung dieser Definition ermöglichen, wird darauf hingewiesen, daß eine Person als bestimmbar angesehen wird, die durch die Zuordnung zu einer Kennnummer oder einer ähnlichen Information identifiziert werden kann.

b) "Anonymisieren". Durch diesen Begriff soll der Ausschluß von Daten, die nicht mehr zugeordnet werden können, von der Anwendung bestimmter Vorschriften der Richtlinie ermöglicht werden. Daten können als anonymisiert gelten, auch wenn sie theoretisch mit einem unverhältnismäßig großen technischen und finanziellen Aufwand wieder einer Person zugeordnet werden können.

c) "Datei mit personenbezogenen Daten". Die Definition basiert auf dem Kriterium der Zugangsmöglichkeit zu den personenbezogenen Daten entweder durch eine manuelle Verarbeitung im Rahmen einer Erfassung strukturierter Daten oder durch eine automatisierte Verarbeitung, die eine Verknüpfung verstreuter Daten ermöglicht oder das Auffinden von Daten aus einem fortlaufenden Text mit Hilfe einer Suchroutine ermöglicht, die der einer Datei entspricht.

Die Definition deckt daher elektronische Dateien und strukturierte Karteien ab. Individuelle Akten, insbesondere Verwaltungsakten, die keine strukturierte personenbezogene Datensammlung enthalten, sind angesichts der für diese geltenden unterschiedlichen Sonderbestimmungen in den Mitgliedstaaten nicht eingeschlossen.

d) "Verarbeitung". In dieser Definition werden die wichtigsten Verarbeitungsvorgänge aufgezählt und im Sinne eines weitgefaßten Anwendungsbereichs des Begriffs Datei an die des Übereinkommens angepaßt. Das Verknüpfen der Daten fällt in den Anwendungsbereich, da dadurch neue Daten ermittelt werden können (beispielsweise ein elektronisches Profil). Die Sperrung von Daten betrifft den Fall, daß der Zugang zu Daten über die üblichen Sicherheitsmaßnahmen hinaus gesperrt wird, ohne daß dies jedoch dem Löschen gleichkommt.

e) "Verantwortlicher der Datei". Der Begriff des "Betreibers der Datei" des Übereinkommens wurde in zwei Punkten angepaßt : zum einen wurde auf das Gemeinschaftsrecht in den Fällen hingewiesen, in denen bestimmte Richtlinien materielle Bestimmungen über den Schutz personenbezogener Daten enthalten; zum anderen wird festgestellt, daß der Verantwortliche der Datei, insbesondere bei direkten Abfragen, derjenige ist, der den Zugang genehmigt.

f) "Kontrollbehörde". In dieser Definition wird darauf hingewiesen, daß die Behörde unabhängig sein muß; außerdem wird auf Artikel 26 verwiesen, der die Aufgaben der Kontrollbehörde regelt.

g) und h)
"öffentlicher Bereich" und "privater Bereich". Die Unterscheidung zwischen öffentlichem und privatem Bereich in der Richtlinie ist dadurch begründet, daß bestimmte Definitionen nur für den einen oder den anderen Bereich gelten (Kapitel II und III über die Rechtmäßigkeit der Verarbeitung von personenbezogenen Daten im öffentlichen Bereich und im privaten Bereich). Diese Definitionen basieren auf der Art der Dienstleistungen, die vom betreffenden Organ erbracht werden, unabhängig davon, ob dessen Rechtsform privat oder öffentlich ist. Wenn das Organ eine kommerzielle Tätigkeit ausübt, sind die besonderen Regelungen für den privaten Bereich anzuwenden, und wenn es an der Ausübung der Staatsgewalt beteiligt ist, sind die besonderen Regelungen für den öffentlichen Bereich anzuwenden.

Artikel 3

Anwendungsbereich

Die Richtlinie gilt für alle Dateien, deren Verantwortliche dem privaten Bereich oder dem öffentlichen Bereich zuzuordnen sind. Im Falle der letztgenannten Organe ist zur Ausübung zahlreicher Verwaltungstätigkeiten in Anwendung des Gemeinschaftsrechts eine Zusammenarbeit zwischen den Verwaltungen der Mitgliedstaaten erforderlich. Nicht abgedeckt sind jedoch die Dateien des öffentlichen Bereichs, wenn die Tätigkeit dieser Organe nicht in den Anwendungsbereich des Gemeinschaftsrechts fällt. Dies betrifft insbesondere die Dateien, die ausschließlich für Tätigkeiten verwendet werden, die nicht dem Anwendungsbereich des Gemeinschaftsrechts zuzuordnen sind (wie die Geheimdienste).

Absatz 2 sieht zwei Ausnahmen vor, die durch die Tatsache gerechtfertigt sind, daß Eingriffe in die Privatsphäre unwahrscheinlich sind, weil es sich entweder um die Verwendung von Daten für rein private Zwecke, wie ein

persönliches Telefonnummernverzeichnis, oder um das Verzeichnis der Mitglieder einer Vereinigung handelt, deren Einverständnis mit der Aufnahme in das Verzeichnis durch ihren Beitritt vorausgesetzt werden kann, und weil die in diesem Verzeichnis enthaltenen Informationen nicht an Dritte weitergegeben werden.

Artikel 4

Anwendbares Recht

In diesem Artikel werden die Zuordnungskriterien festgelegt, die für die Anwendung der Bestimmungen dieser Richtlinie in den einzelnen Mitgliedstaaten ausschlaggebend sind. Die Kriterien in Absatz 1 wurden so ausgewählt, daß vermieden wird, daß der betroffenen Person jeder Schutz, insbesondere im Falle der Umgehung der Gesetze, entzogen wird. Aus diesem Grund wurde das zusätzliche Kriterium des Ortes, an dem sich die Datei befindet, vorgesehen. In diesem Zusammenhang ist jeder Teil einer Datei, die sich auf mehrere Orte oder Mitgliedstaaten verteilt, als eine eigenständige Datei anzusehen.

Um den Schutz von Personen auch im Falle einer Verlegung der Datei zu gewährleisten, wurde eine Bestimmung eingeführt, nach der ein Benutzer, der eine in einem Drittland befindliche Datei von einem in einem Mitgliedstaat befindlichen Datenendgerät aus abfragt, die Bestimmungen der Richtlinie über die Rechtmäßigkeit der Verarbeitung, die Information der betroffenen Person im Falle der Weitergabe der Daten, die sensiblen Daten, die Sicherheit der Daten und die Haftung zu beachten hat. Diese Verpflichtung gilt nicht in den Fällen, in denen es sich nur um eine vereinzelte Abfrage handelt.

Da Dateien leicht transferiert werden können, stellt die vorübergehende Verlegung einer Datei keinen Wechsel des Standorts dar. Die Verlegung von Datenträgern, auf denen die Daten aufgezeichnet wurden, erfordert keine zusätzliche Formalitäten zu denen, die in dem Migliedstaat erfüllt wurden, in dem die Datei sich ständig befindet.

Durch diesen Artikel soll auch eine Kumulierung der geltenden Gesetze verhindert werden.

KAPITEL II

Rechtmäßigkeit der Verarbeitung im öffentlichen Bereich

Die personenbezogenen Daten dürfen nur dann Gegenstand einer Verarbeitung sein, wenn diese rechtmäßig ist. In diesem Kapitel werden ebenso wie in Kapitel III die Voraussetzungen festgelegt, unter denen eine Verarbeitung rechtmäßig ist. Die Rechtmäßigkeit kann sich im Einzelfall auf die Zustimmung der betroffenen Person, eine Bestimmung der Richtlinie oder des Gemeinschaftsrechts oder auf einen nationalen Rechtsakt stützen.

Artikel 5

Grundsätze

Dieser Artikel sieht vor, daß die Errichtung einer Datei des öffentlichen Bereichs und jede andere Verarbeitung personenbezogener Daten nur in dem Maße rechtmäßig ist, in dem sie für die Wahrnehmung der Aufgaben der für diese Datei verantwortlichen Behörde erforderlich ist.

In vier Fällen ist vorgesehen, daß die Verarbeitung der Daten für einen anderen Zweck ist als den, für den die Datei erstellt worden ist, durchgeführt werden kann : wenn die betroffene Person dafür ihre Einwilligung erteilt oder die Verarbeitung sich auf eine Rechtsgrundlage stützt, wenn nach Abwägung der vorhandenen Interessen festgestellt wird, daß dieser Verarbeitung kein berechtigtes Interesse der betroffenen Person entgegensteht, und schließlich im Fall einer drohenden Gefahr für die öffentliche Ordnung oder einer schwerwiegenden Verletzung des Rechtes Dritter.

Diese Grundsätze betreffen nicht den besonderen Fall der Weitergabe der Daten an Dritte, die Gegenstand der Betimmungen in Artikel 6 ist.

Artikel 6

Weitergabe personenbezogener Daten bei der Datenverarbeitung im öffentlichen Bereich.

Eine Bestimmung für den besonderen Fall der Weitergabe der Daten an Dritte ist erforderlich, da diese Art der Verarbeitung mit den größten Risiken für die betroffene Person verbunden ist. Der betreffende Absatz sieht zwei Fälle vor, in denen die Daten an Dritte übermittelt werden können; dabei wird unterschieden, ob der Empfänger dem öffentlichen Bereich oder dem privaten Bereich zuzurechnen ist. Im ersten Fall muß die Weitergabe für die Wahrnehmung von Aufgaben der Verwaltungsdienststelle, die diese Daten anfordert oder weitergibt, erforderlich sein, und im zweiten Fall sind die Interessen abzuwägen, um festzustellen, ob der Antragsteller ein berechtigtes Interesse geltend macht und ob nicht das Interesse der betroffenen Person überwiegt.

Die Mitgliedstaaten können in ihren Rechtsvorschriften im Rahmen der beiden obengenannten Grundsätze festlegen, unter welchen Bedingungen die Weitergabe rechtmäßig ist. So können sie beispielsweise für bestimmte Bereiche festlegen, in welchen Fällen das Interesse der betroffenen Person überwiegt.

Um zu gewährleisten, daß von der Möglichkeit der Weitergabe an den privaten Bereich nicht entgegen den Interessen der betroffenen Person Gebrauch gemacht wird, ist ein Verfahren zur Information dieser Person vorgesehen. Eine Ausnahme von dieser Verpflichtung ist möglich, wenn diese von der Kontrollbehörde genehmigt wird. Diese Behörde kann die Genehmigung von Bedingungen abhängig machen oder beschließen, die betroffene Person selbst zu informieren.

Artikel 7

Meldepflicht bei der Kontrollbehörde

Die in diesem Artikel vorgesehene Meldepflicht gegenüber einem Register der Kontrollbehörde beschränkt sich auf die Dateien des öffentlichen Bereichs,

deren Daten gegebenfalls weitergegeben werden können. Diese Regelung zielt darauf ab, das Mindestmaß an Transparenz zu gewährleisten, das für die Ausübung der Rechte der betroffenen Person erforderlich ist, während gleichzeitig die Meldeformalitäten verringert werden, die eine erhebliche Belastung für die Kontrollbehörde darstellen könnten, insbesondere angesichts des weitgefaßten Begriffs der Datei. Die Mitgliedstaaten haben jedoch die Möglichkeit, die Meldepflicht auf andere Dateien des öffentlichen Bereichs auszuweiten.

KAPITEL III

Zulässigkeit der Verarbeitung im privaten Bereich

Artikel 8

Grundsätze

Die Rechtmäßigkeit der Verarbeitung personenbezogener Daten im privaten Bereich kann auf dem Einverständnis der betroffenen Person beruhen. Dieses Einverständnis muß gemäß den Bestimmungen in Artikel 12 über die Einwilligung nach Unterrichtung und Artikel 13 über die Unterrichtung bei der Datenerhebung erklärt werden.

Ohne das Einverständnis der betroffenen Person kann die Rechtmäßigkeit der Verarbeitung dadurch begründet sein, daß ein vertragsähnliches Verhältnis zwischen dem Verantwortlichen der Datei und der betroffenen Person besteht und soweit die Verarbeitung zur Erfüllung des Vertrages (beispielsweise zur Auftragsbearbeitung oder Fakturierung) erforderlich ist.

Die Rechtmäßigkeit der Verarbeitung kann auch durch die Tatsache begründet sein, daß die Daten aus allgemein zugänglichen Quellen stammen (der Öffentlichkeit zugängliche Verzeichnisse) und ihre Verarbeitung ausschließlich Korrespondenzzwecken dient.

Schließlich kann die Rechtmäßigkeit der Verarbeitung auf einer Abwägung der Interessen beruhen, aus der sich ergibt, daß der Verantwortliche der Datei ein berechtigtes Interesse verfolgt und daß das Interesse der betroffenen Person nicht überwiegt.

Die Übermittlung von Daten ist nur rechtmäßig, wenn sie mit dem Zweck der Datei vereinbar ist, der gemäß Artikel 11 Ziffer 2 mitzuteilen und bei der Speicherung der Daten (Artikel 16 Ziffer 1 Buchstabe b) zu beachten ist. Im Falle der Übermittlung von Daten ist der Verantwortliche der Datei außerdem verpflichtet, die betroffene Person gemäß Artikel 9 und 10 zu informieren. Die Mitgliedstaaten können in ihren Rechtsvorschriften die Bedingungen festlegen, unter denen die Verarbeitung personenbezogener Daten im Rahmen der obengenannten Grundsätze rechtmäßig ist. So können sie beispielsweise für bestimmte Bereiche festlegen, in welchen Fällen das Interesse der betroffenen Person überwiegt.

Artikel 9

Pflicht zur Benachrichtigung

Um der betroffenen Person die Ausübung ihrer Rechte zu ermöglichen, ist der Verantwortliche der Datei nach Ziffer 1 verpflichtet, die betroffene Person zu unterrichten, daß die sie betreffenden Daten weitergegeben wurden. Die betroffene Person kann dann ihr Auskunftsrecht ausüben und Einwände gegen die Fortsetzung der betreffenden Verarbeitung geltend machen. Die Verpflichtung, die betroffene Person zu unterrichten, gilt nicht in den Fällen, in denen die Daten aus allgemein zugänglichen Quellen stammen und ihre Verarbeitung ausschließlich Korrespondenzzwecken dient.

Artikel 10

Besondere Ausnahmen von der Pflicht zur Benachrichtigung der betroffenen Person

Dieser Artikel räumt den Mitgliedstaaten die Möglichkeit ein, in ihren Rechtsvorschriften vorzusehen, daß die Aufsichtsbehörde in den Fällen, in denen der Benachrichtigung der betroffenen Person größere praktische

Schwierigkeiten oder ein überwiegendes berechtigtes Interesse des Verantwortlichen der Datei oder ein ähnliches Interesse eines Dritten entgegenstehen, auf Antrag des Verantwortlichen der Datei eine Ausnahme von der Verpflichtung zur Benachrichtigung der betroffenen Person genehmigen kann. Die Kontrollbehörde kann im Rahmen der Rechtsvorschriften, die sie dazu ermächtigen, Bedingungen für die Anwendung der Ausnahmeregelung festlegen und beschließen, die betroffene Person selbst zu unterrichten. Größere praktische Schwierigkeiten sind beispielsweise im Falle von Daten zu Personen gegeben, deren persönliche Anschrift nicht bekannt ist.

Artikel 11

Meldepflicht bei der Kontrollbehörde

Aus dem gleichen Grund wie im Falle der Meldepflicht im öffentlichen Bereich (Artikel 7) gilt die Meldepflicht im privaten Bereich nicht für Dateien, die nicht für die Weitergabe bestimmt sind oder die aus allgemein zugänglichen Quellen stammen. Die Meldung ist zu aktualisieren, wenn sich die Zweckbestimmung der Datei ändert.

Die zu meldenden Informationen haben die Angaben zu umfassen, die für die Kontrolle der Anwendung der Bestimmungen dieser Richtlinie erforderlich sind (mindestens Namen und Anschrift des Verantwortlichen der Datei, die Zweckbestimmung der Datei, eine Beschreibung der Arten der gespeicherten Daten, die Dritten, denen die Daten möglicherweise übermittelt werden, sowie eine Beschreibung der Datenschutzmaßnahmen). Die Mitgliedstaaten können den Anwendungsbereich der Meldepflicht ausweiten.

KAPITEL IV : RECHTE DER BETROFFENEN PERSON

Artikel 12

Einwilligung nach Unterrichtung der betroffenen Person

Diese Bestimmung legt fest, unter welchen Voraussetzungen die Einwilligung der betroffenen Person zu einer Verarbeitung der sie betreffenden Daten des öffentlichen sowie des privaten Bereichs rechtlich wirksam ist.

Die Einwilligung der betroffenen Person zu einer Verarbeitung der sie betreffenden Daten ist eine wichtige Grundlage für die Rechtmäßigkeit der Verarbeitung personenbezogener Daten durch den Verantwortlichen der Datei. Der Begriff der "Einwilligung" im Sinne von Artikel 12 basiert auf der Information der betroffenen Person. Damit die betroffene Person die Risiken und die Vorteile der geplanten Verarbeitung abwägen und ihre Rechte gemäß Artikel 14 des Richtlinienentwurfs (Berichtigung, Löschen und Sperrung) ausüben kann, hat der Verantwortliche der Datei der betroffenen Person die Informationen zur Verfügung zu stellen, die für die Entscheidung der betroffenen Person relevant sind, so z.B. Name und Anschrift des Verantwortlichen, Zweckbestimmung der Datei, in der Datei gespeicherte Daten usw.

Der Richtlinienentwurf sieht aus praktischen Gründen nicht vor, daß die betroffene Person ihr Einverständnis in schriftlicher Form zu erklären hat. Die Einwilligung muß jedoch ausdrücklich geäußert werden. Das Einverständnis der betroffenen Person muß für den besonderen Fall erteilt werden, d.h. es muß sich auf die Verarbeitung der Daten der betroffenen Person durch einen bestimmten Verantwortlichen einer Datei oder für einen bestimmten Zweck oder bestimmte Zwecke beziehen. Darüber hinaus hat die Einwilligung die Art der zu verarbeitenden Daten, die Form der Verarbeitung und die möglichen Empfänger, im Falle der Weitergabe von Daten an Dritte, genau zu bestimmen.

Nach Artikel 12 Buschstabe c) kann die Einwilligung von der betroffenen Person jederzeit widerrufen werden. Dieser Widerruf hat jedoch keine rückwirkende Gültigkeit, da sonst eine zuvor rechtmäßige Verarbeitung personenbezogener Daten nachträglich unrechtmäßig würde.

Artikel 13

Unterrichtung bei der Datenerhebung

Ein effektiver Datenschutz erfordert eine umfassende Information der betroffenen Person über die Verarbeitung der sie betreffenden personenbezogenen Daten nicht nur, wenn diese Daten bereits in einer Datei gespeichert und verarbeitet werden, sondern bereits vor der Verarbeitung der Daten zum Zeitpunkt der Erhebung der personenbezogenen Daten.

Nach Artikel 16 Ziffer 1 Buchstabe a) sind die Daten nach Treu und Glauben und in zulässiger Art und Weise zu erheben und zu verarbeiten. Diese Anforderungen werden in Artikel 13 für den Fall näher bestimmt, daß die Daten bei der betroffenen Person selbst gesammelt werden.

Eine Erhebung personenbezogener Daten nach Treu und Glauben und in zulässiger Art und Weise setzt voraus, daß die betroffene Person ihre Entscheidung darüber, ob sie die Daten den Erhebern der Daten in sachlich zuverlässiger Form im Sinne des Zwecks der Verarbeitung offenlegt, auf der Grundlage sachlich zuverlässiger Informationen über den Zweck der Verarbeitung, die Identität des Verantwortlichen der Datei und die Frage, ob sie rechtlich verpflichtet ist, die sie betreffenden Daten offen zu legen, oder ob es ihr freisteht, diese offen zu legen, trifft. Um ihre Rechte gemäß Artikel 14 des Richtlinienentwurfs ausüben zu können und die Verwendung der sie betreffenden Daten effektiv kontrollieren zu können, sollte sie auch über ihr Recht auf Auskunft und Berichtigung sowie über die Empfänger, an die die Daten weitergegeben werden, informiert werden. Nach Artikel 13 Ziffer 1 des Richtlinienentwurfs sind die Mitgliedstaaten verpflichtet, in ihren innerstaatlichen Datenschutzbestimmungen vorzusehen, daß der betroffenen Person diese Informationen zur Verfügung gestellt werden.

Die Personen, die die Erhebung der Daten durchführen, sind häufig nicht mit dem Verantwortlichen der Datei, der diese gegebenenfalls speichert und

verarbeitet, identisch. Damit die betroffene Person ihre Rechte gegen diese Person geltend machen kann, ist es wichtig, daß der betroffenen Person deren Name und Anschrift bereits bei der Erhebung der Daten mitgeteilt werden.

Nach Artikel 13 Ziffer 2 sind die Mitgliedstaaten befugt, die Pflicht zur Information der betroffenen Person bei der Erhebung der Daten zum Schutz vorherrschender öffentlicher Interessen einzuschränken. Im Sinne dieser Bestimmung gilt die Pflicht zur Unterrichtung der betroffenen Person gemäß Artikel 13 Ziffer 1 nicht, wenn die Unterrichtung die ordnungsgemäße Ausübung der Kontroll- und Überprüfungsaufgaben einer staatlichen Behörde oder die Aufrechterhaltung der öffentlichen Ordnung verhindert.

Artikel 14

Ergänzende Rechte der betroffenen Person

Artikel 14 des Richtlinienentwurfs regelt die Rechte und Ansprüche der betroffenen Person gegenüber dem Verantwortlichen der Datei. Der Datenschutz dient dem Ziel der Gewährleistung des Rechts der betroffenen Person auf ihre Privatsphäre. Die Rechte und Ansprüche dieser Person gegenüber dem Verantwortlichen der Datei sind daher ein wichtiger Bestandteil des Datenschutzes.

Nach Artikel 14 Ziffer 1 hat die betroffene Person das Recht, aus berechtigten Gründen gegen eine Verarbeitung der sie betreffenden Daten Einspruch zu erheben.
Berechtigte Gründe im Sinne dieser Bestimmung sind eine unzureichende Rechtsgrundlage für eine bestimmte Verarbeitung, z.B. weil die Voraussetzungen in Kapitel II und III des Richtlinienentwurfs für die Rechtsmäßigkeit dieser Verarbeitung im Hinblick auf eine bestimmte Verarbeitung von Daten nicht gegeben sind.

Artikel 14 Ziffer 2 schützt die betroffene Person dagegen, Gegenstand einer Entscheidung zu sein, die eine Beurteilung ihres menschlichen Verhaltens impliziert und sich allein auf eine rechnergestützte Verarbeitung

personenbezogener Daten stützt, die eine Beschreibung des Profils oder der Persönlichkeit des Betroffenen vermittelt. Durch diese Bestimmung soll das Interesse der betroffenen Person an der Beteiligung an den Prozessen im Zusammenhang mit den für sie wichtigen Entscheidungen geschützt werden. Die Verwendung umfangreicher Datenprofile von Privatpersonen durch mächtige öffentliche und private Einrichtungen entzieht dem Einzelnen die Möglichkeit, Entscheidungsprozesse innerhalb dieser Institutionen zu beeinflussen, wenn die Entscheidungen ausschließlich auf der Grundlage seines "Datenschattens" getroffen werden.

Um ihr Recht auf Berichtigung, Löschen oder Sperrung der Daten gegenüber dem Verantwortlichen der Datei effektiv geltend machen zu können, muß die betroffene Person ein Auskunftsrecht über die Daten der Datei gemäß Artikel 14 Ziffer 3 und 4 haben. Artikel 14 Ziffer 3 gewährt der betroffenen Person das Recht, über die für die Verarbeitung relevanten Tatsachen der sie betreffenden Daten durch den Verantwortlichen der Datei informiert zu werden, damit sie ihre Ansprüche auf Berichtigung, Löschen und Sperrung geltend machen und eine effektive Kontrolle der Verarbeitung der sie befreffenden Daten ausüben kann. Artikel 14 Ziffer 4 gewährt der betroffenen Person das Recht, in angemessenen Abständen, unverzüglich und ohne überhöhte Kosten die Bestätigung der Existenz sie betreffender personenbezogener Daten in einer Datei sowie, falls Daten über die betroffene Person in der Datei gespeichert sind, über die Weitergabe dieser Daten in einer verständlichen Form zu erhalten.

Artikel 14 Ziffer 3 und 4 überläßt es den Mitgliedstaaten, zu entscheiden, ob diese Informationen der betroffenen Person zur Verfügung gestellt werden. Die Interpretation des Begriffs "angemessene Abstände" ist ebenfalls dem innerstaatlichen Recht der Mitgliedstaaten überlassen. Unter Berücksichtigung der Interessen der betroffenen Person und des Verantwortlichen der Datei können die innerstaatlichen Rechtsvorschriften der Mitgliedstaaten vorsehen, daß der Verantwortliche der Datei der betroffenen Person, die ihr Recht auf Auskunft wahrnimmt, nur die damit verbundenen Kosten in Rechnung stellt, die nicht überhöht sein dürfen.

Nach Artikel 14 Ziffer 4 können die Mitgliedstaaten eine besondere Regelung anwenden, nach der das Recht auf Auskunft zu Daten medizinischer Art eingeschränkt wird. Um einem psychischen Schock der betroffenen Person vorzubeugen, der in Extremfällen zu einem Selbstmordversuch führen kann, ist die Information gegebenenfalls Sache eines Arztes.

Artikel 14 Ziffer 5 des Richtlinienentwurfs gewährt der betroffenen Person das Recht auf Berichtigung, Löschen und Sperrung der Daten, falls die Verarbeitung dieser Daten nicht mit den Bestimmungen des Richtlinienentwurfs im Einklang steht. Die betroffenen Personen können einen Anspruch auf Berichtigung geltend machen, falls die sie betreffenden Daten unrichtig, unvollständig, ungenau, irreführend oder überholt sind. Das Recht der betroffenen Person, die Daten löschen oder sperren zu lassen, setzt voraus, daß diese Daten entgegen den Bestimmungen des Richtlinienentwurfs verarbeitet wurden. Artikel 14 Ziffer 5 bezieht sich daher auf alle Bestimmungen des Richtlinienentwurfs, die die Erhebung, Speicherung, Verarbeitung und Verwendung personenbezogener Daten regeln.

Der Begriff der Sperrung wurde aus dem Datenschutzgesetz der Bundesrepublik Deutschland (§§ 14, 27 und 35 BDSG: Sperrung) übernommen. Werden Daten gesperrt, weil sie entgegen den Vorschriften des Richtlinienentwurfs erhoben, gespeichert, verarbeitet oder verwendet wurden, kann der Verantwortliche der Datei diese weiterhin in seiner Datei speichern, es ist ihm jedoch untersagt, diese zu verarbeiten oder zu verwenden und insbesondere, sie an Dritte zu übermitteln. Die gesperrten Daten müssen in der Datei gekennzeichnet werden, um den Benutzer der Datei über die Sperrung zu informieren.

Die Verwendung des Begriffs "gegebenenfalls" überläßt die konkrete Fassung des Rechts der betroffenen Person auf Löschen, Sperrung oder Berichtigung im Hinblick auf die verschiedenen Situationen, in denen personenbezogene Daten entgegen den Bestimmungen des Richtlinienentwurfs verarbeitet und verwendet werden können, dem Datenschutzrecht der Mitgliedstaaten.

Häufig werden die Daten nicht nur von einem Verantwortlichen einer Datei verarbeitet, sondern an Dritte weitergegeben. Wenn der Verantwortliche der Datei Daten zu berichtigen, zu löschen oder zu sperren hat, weil diese unrichtig sind oder unrechtmäßig verarbeitet oder verwendet wurden, liegt es im Interesse der betroffenen Person, daß Dritten, denen diese Daten übermittelt wurden, die Berichtigung, Löschung oder Sperrung der Daten gemeldet wird, so daß diese Dritten ebenfalls die Daten berichtigen, löschen oder sperren können. Dieses Interesse der betroffenen Person ist Gegenstand von Artikel 14 Ziffer 7.

Artikel 14 Ziffer 6 gibt der betroffenen Person das Recht, das Löschen der sie betreffenden Daten zu erreichen, die in Dateien für kommerzielle Zwecke oder für die Zwecke der Briefkastenwerbung gespeichert sind. Die betroffene Person kann sich somit gegen lästige Postwurfsendungen schützen.

Artikel 14 Ziffer 8 schließlich verpflichtet die Mitgliedstaaten, der betroffenen Person ein effektives Rechtsmittel für den Fall zur Verfügung zu stellen, daß der Verantwortliche der Datei oder eine andere Person die Rechte und Ansprüche der betroffenen Person im Sinne von Artikel 14 des Richtlinienentwurfs verletzt.

Artikel 15

Ausnahmen vom Auskunftsrecht der betroffenen Person bei Dateien des öffentlichen Bereichs.

Nach Artikel 15 können die Mitgliedstaaten das Recht der betroffenen Person auf Auskunft aus Dateien zum Schutz vorherrschender öffentlicher Interessen oder der Interessen von Privatpersonen einschränken, die dem Recht auf Schutz der Privatsphäre der betroffenen Person gleichwertig sind, wenn es sich um Dateien des öffentlichen Bereichs handelt. Es bleibt den Mitgliedstaaten überlassen, zu entscheiden, bis zu welchem Grad sie Ausnahmen gemäß Artikel 15 in ihrem innerstaatlichen Datenschutzrecht vorsehen. Die in diesem Artikel vorgesehenen Ausnahmen beschränken sich

jedoch auf solche, die zum Schutz der Grundwerte einer demokratischen Gesellschaft erforderlich sind, und müssen daher Gegenstand einer formellen gesetzlichen Regelung sein. Die Aufzählung der Interessen, die eine Einschränkung des Auskunftsrechts gemäß Artikel 15 des Richtlinienentwurfs rechtfertigen, ist erschöpfend.

Der Begriff der "Sicherheit des Staates" ist als der Schutz der nationalen Souveränität gegen innere und äußere Bedrohungen zu interpretieren. "Strafverfolgung" bezeichnet die Verfolgung von Straftaten, die bereits begangen wurden, während der Begriff "öffentliche Sicherheit" alle Polizeifunktionen der staatlichen Organe einschließlich der Verhinderung von Straftaten umfaßt.

Der Begriff "schwerwiegendes wirtschaftliches oder finanzielles Interesse eines Mitgliedstaats oder der Europäischen Gemeinschaft" bezieht sich auf alle Mittel der Wirtschaftspolitik und der Finanzierung der Politik eines Mitgliedstaates oder der Gemeinschaft, z.B. Devisenkontrollen, Außenhandelskontrollen und Steuererhebung. Nur ein schwerwiegendes Interesse dieser Art rechtfertigt jedoch die Einschränkung des Auskunftsrechts.

Schließlich kann ein dem Auskunftsrecht der betroffenen Person gleichwertiges Recht eines Dritten bzw. die Rechte und Freiheiten anderer Personen als Begründung für die Einschränkung des Auskunftsrechts anerkannt werden. Von Bedeutung sind in diesem Zusammenhang Interessen wie Geschäftsgeheimnisse anderer Personen oder die Pressefreiheit.

Wird der betroffenen Person die Auskunft über die sie betreffenden Daten in einer Datei verweigert, weil ein Interesse im Sinne von Artikel 15 Ziffer 1 dem entgegensteht, ist die Datenschutzbehörde auf Antrag verpflichtet, die erforderlichen Überprüfungen und Kontrollen der Datei durchzuführen, in der diese Daten gespeichert sind.
Artikel 15 Ziffer 3 ermächtigt die Mitgliedstaaten, Beschränkungen des Auskunftsrechts für Daten einzuführen, die nur vorübergehend gespeichert werden, um statistische Auskünfte zu entnehmen, da dies nur mit geringen Risiken für die betroffene Person verbunden ist.

KAPITEL V : Qualität der Daten

Die in diesem Kapitel vorgesehenen Grundsätze des Datenschutzes gehen über den Titel hinaus; sie betreffen nicht nur die Qualität der Daten (Artikel 16), sondern auch die Verarbeitung bestimmter Kategorien von Daten, die als besonders sensibel für die Interessen der betroffenen Person (Artikel 17) anzusehen sind, und die geeigneten Datenschutzmaßnahmen (Artikel 18).

Artikel 16

Grundsätze

Nach Artikel 16 des Richtlinienentwurfs sind die Mitgliedstaaten verpflichtet, die wesentlichen Grundsätze des Datenschutzes hinsichtlich der Qualität personenbezogener Daten in ihre inländische Datenschutzgesetzgebung zu übernehmen. Diese Grundsätze sollen das Recht der betroffenen Person auf Schutz der Privatsphäre durch bestimmte Beschränkungen der Erhebung und Verarbeitung personenbezogener Daten ebenso wie des zulässigen Inhalts personenbezogener Dateien gewährleisten.

Artikel 16 Ziffer 1 Buchstabe a) sieht vor, daß die personenbezogenen Daten nach Treu und Glauben sowie auf rechtmäßige Art und Weise zu erheben und zu verarbeiten sind. Diese Bestimmung betrifft die Verarbeitung personenbezogener Daten im Sinne von Artikel 2 Buchstabe d) ebenso wie deren Erhebung. Die Regelung in Artikel 16 Ziffer 1 Buchstabe a) schließt z.B. den Einsatz vor der betroffenen Person versteckter technischer Geräte aus, die dazu dienen, Daten insgeheim und ohne das Wissen der betroffenen Person zu erheben, wie beispielsweise durch Abhören, heimliches Belauschen und ähnliche Methoden. Diese Bestimmung soll auch verhindern, daß der Verantwortliche der Datei geheime Dateien, die personenbezogene Daten enthalten, aufbaut und verwendet.

Artikel 16 Ziffer 1 Buchstabe b) enthält den Grundsatz der Zweckbestimmung. Nach diesem Grundsatz sind personenbezogene Daten nur für bestimmte, ausdrücklich festgelegte und rechtmäßige Zweckbestimmungen zu speichern. Die Zweckbestimmung der Speicherung personenbezogener Daten ist in dem Sinne festzulegen, daß das Ziel, dem die Speicherung und Verwendung der Daten dient, so eng wie möglich definiert und bestimmt wird. Eine allgemeine oder unbestimmte Definition oder Beschreibung der Zweckbestimmung einer Datei (z.B. die Datei dient "Geschäftszwecken") wird dem Grundsatz der Zweckbestimmung im Sinne von Artikel 16 Ziffer 1 Buchstabe b) nicht gerecht.

Die Zweckbestimmung ist anzugeben, bevor die Speicherung durchgeführt wird. Für den Fall, daß die Daten bei der betroffenen Person erhoben werden, sieht Artikel 13 vor, daß der Zweck bereits bei der Erhebung der Daten zu bestimmen ist.

Eine spätere Änderung der Zweckbestimmung einer Verarbeitung ist nur zulässig, falls diese nicht mit der früheren Zweckbestimmung unvereinbar ist.

Artikel 16 Ziffer 1 Buchstabe b) sieht auch vor, daß der Verantwortliche der Datei die Zweckbestimmung der Speicherung und Verwendung der Daten ausdrücklich festlegt. Der Grundsatz der Ausdrücklichkeit soll verhindern, daß personenbezogene Daten für geheime Zwecke verwendet werden. Der Grundsatz der Rechtmäßigkeit der Zweckbestimmung der Speicherung und Verwendung personenbezogener Daten beschränkt die potentiellen Zweckbestimmungen, denen eine Datei dienen darf; eine solche Datei darf nur für die Zwecke erstellt und verwendet werden, die mit den Bestimmungen dieses Richtlinienentwurfs und des innerstaatlichen Rechts der Mitgliedstaaten vereinbar sind. Außerdem sind nur solche Verarbeitungen rechtmäßig, die der administrativen Funktion der Verantwortlichen der Datei des öffentlichen Bereichs und dem Bereich der Geschäftstätigkeit der Verantworlichen der Datei des privaten Bereichs entsprechen. In Artikel 16 Ziffer 1

Buchstabe b) wird ausdrücklich darauf hingewiesen, daß der Grundsatz der Zweckbestimmung nicht nur für die Verarbeitung personenbezogener Daten gilt; auch die Verwendung dieser Daten muß der Zweckbestimmung der Datei entsprechen.

Artikel 16 Ziffer 1 Buchstabe c) sieht vor, daß die Daten einer Datei den Zweckbestimmungen, für die sie gespeichert wurden, entsprechen, dafür erheblich sein müssen und nicht darüber hinausgehen dürfen. Dieser Grundsatz soll gewährleisten, daß der Inhalt einer Datei mit seiner Zweckbestimmung übereinstimmt.

Die Bestimmung in Artikel 16 Ziffer 1 Buchstabe d) steht in engem Zusammenhang mit den Anforderungen in Artikel 16 Ziffer 1 Buchstabe b). Personenbezogene Daten, die in einer Datei gespeichert sind, müssen richtig sein und gegebenenfalls aktualisiert werden. Falls die Daten im Sinne der Zweckbestimmung nicht zutreffend oder unvollständig sind, sieht Artikel 16 Ziffer 1 Buchstabe d) vor, daß diese zu löschen oder zu berichtigen sind.

Artikel 16 Ziffer 1 Buchstabe e) sieht eine Begrenzung des Zeitraums vor, für den die personenbezogenen Daten gespeichert werden. Im Sinne dieser Bestimmung dürfen die Daten in einer Form, die die Identifizierung der betroffenen Person ermöglicht, nur während des Zeitraums aufbewahrt werden, der für die Zweckbestimmung, für die die Daten gespeichert wurden, erforderlich ist.

Es kann jedoch in bestimmten Fällen, beispielsweise für statistische Zwecke, erforderlich sein, die Daten über diesen Zeitraum hinaus aufzubewahren. Zum Schutz der betroffenen Person muß dann jedoch die Verknüpfung zwischen dem Namen und den übrigen Daten beseitigt werden.

Artikel 16 Ziffer 2 verpflichtet den Verantwortlichen der Datei, für die Einhaltung der in Artikel 16 Ziffer 1 vorgesehenen Bestimmungen über die Qualität der Daten zu sorgen.

Artikel 17

Besondere Datenarten

Es wird allgemein akzeptiert, daß das Recht auf Schutz der Privatsphäre durch den Inhalt personenbezogener Daten nicht gefährdet wird, sondern vielmehr durch Bedrohungen, die durch den Zusammenhang entstehen, in dem die Verarbeitung personenbezogener Daten durchgeführt wird. Unter den Mitgliedstaaten besteht ein breiter Konsens, daß es dagegen bestimmte Kategorien von Daten gibt, die durch ihren Inhalt - unabhängig vom Kontext ihrer Verarbeitung - mit der Gefahr einer Verletzung des Rechts auf Schutz der Privatsphäre der betroffenen Person verbunden sind. Artikel 17 des Richtlinienentwurfs sieht daher strenge Beschränkungen der elektronischen Verarbeitung und der Verwendung sensibler Informationen in Dateien mit personenbezogenen Daten vor.

Als sensibel werden in Artikel 17 folgende Kategorien von Daten bezeichnet: rassische Herkunft (einschließlich Angaben zur Hautfarbe), politische Meinung, religiöse oder philosophische Überzeugungen (auch die Information, daß eine Person keine religiöse Überzeugung hat, fällt in diese Kategorie), (diese Kategorien schließen die Informationen über Aktivitäten der betroffenen Person im Zusammenhang mit politischen, religiösen oder philosophischen Überzeugungen ein) sowie Angaben zur Gewerkschaftszugehörigkeit, Informationen über den Gesundheitszustand der betroffenen Person (einschließlich Informationen über den früheren, gegenwärtigen und zukünftigen Zustand physischer und geistiger Gesundheit und Informationen über Drogen- und Alkoholmißbrauch) und Informationen über das Sexualleben.

Artikel 17 Ziffer 1 untersagt generell die automatisierte Verarbeitung sensibler Daten. Ausnahmen von dieser Regel sind mit freier, ausdrücklicher schriftlicher Einwilligung der betroffenen Person und gemäß Artikel 17 Ziffer 2 möglich.

Im Sinne dieser Bestimmung können die Mitgliedstaaten die rechnergestützte Verarbeitung sensibler Daten aus wichtigen Gründen des öffentlichen Interesses zulassen. Eine solche Ausnahme setzt jedoch als Rechtsgrundlage die Verabschiedung einer formellen Rechtsvorschrift voraus, die die Arten speicherfähiger sensibler Daten, die Personen, die Zugang zu den Daten haben, sowie die entsprechenden Schutzmaßnahmen gegen mißbräuchliche Verwendungen und unzulässigen Zugang bestimmen. Artikel 17 Ziffer 3 enthält eine besondere Regelung für die Speicherung von Informationen über strafrechtliche Verurteilungen. Die Speicherung dieser Informationen in automatisierten Dateien ist daher nur in Dateien des öffentlichen Bereichs zulässig.

Der Anwendungsbereich von Artikel 17 ist begrenzt; betroffen sind nur Daten, die mit elektronischen Hilfsmitteln verarbeitet werden. Artikel 17 betrifft auch nicht die elektronische Speicherung und Verarbeitung von Daten über die politische Meinung, religiöse und philosophische Überzeugungen und die Gewerkschaftszugehörigkeit, sofern diese Daten von gemeinnützigen Vereinigungen im Sinne von Artikel 3 Ziffer 2 Buchstabe b) verarbeitet werden.

Artikel 18

Sicherheit der Daten

Das Recht der betroffenen Person auf Schutz der Privatsphäre wird nicht nur dadurch bedroht, daß der Verantwortliche der Datei Daten über den Einzelnen für seine eigenen Zwecke erhebt, speichert, verarbeitet und übermittelt. Sein Recht auf Schutz der Privatsphäre wird auch beeinträchtigt, wenn die ihn betreffenden Daten von Dritten durch unbefugten Zugang zu den Daten und unbefugte Verwendung der Daten mißbraucht werden.

Artikel 18 Ziffer 1 Absatz 1 sieht vor, daß die Mitgliedstaaten den Verantwortlichen der Datei verpflichten, die geeigneten technischen oder organisatorischen Maßnahmen zu treffen, die für den Schutz der Daten in der

Datei vor der Gefahr eines unbefugten Eindringens Dritter in eine Datei oder eines zufälligen Verlusts von Daten, einschließlich zufälliger oder nicht genehmigter Zerstörung, Zufallsverlust sowie unzulässiger Änderung oder unzulässigen Zugang zu den Daten und jede weitere nicht genehmigte Verarbeitung personenbezogener Daten erforderlich sind.

Die technischen Maßnahmen für die Sicherheit der Daten umfassen: Sicherheitsmaßnahmen für den Zugang zur Datenverarbeitung und zu den Speichermedien, Sicherheitscodes für die Personen mit Zugangsberechtigung zu diesen Orten, informationstechnische Schutzmaßnahmen wie die Verwendung von Passworten für den Zugang zu elektronisch verarbeiteten Dateien, die Verschlüsselung der Daten und die Überwachung von Hackeraktivitäten und sonstigen ungewöhnlichen Vorgängen in einer Datei. Durch organisatorische Maßnahmen trifft der Verantwortliche der Datei bestimmte Vorkehrungen innerhalb der Hierarchie seiner Behörde oder seines Unternehmens, beispielsweise die Verknüpfung des Zugangs zu den Daten mit bestimmten Positionen.

Artikel 18 Ziffer 1 Absatz 2 sieht einen Standard für geeignete Datenschutzmaßnahmen für automatisierte Dateien vor. Die Maßnahmen müssen zum einen unter Berücksichtigung des technischen Stands im Bereich des Datenschutzes und der Kosten für die Verwirklichung dieser Maßnahmen und zum anderen der Art der zu schützenden Daten und der Beurteilung potentieller Risiken, für diese Dateien ein geeignetes Sicherheitsniveau gewährleisten. Bei der Beurteilung der Angemessenheit der Datenschutzmaßnahmen hat der Verantwortliche der Datei die Empfehlungen für die DV-Sicherheit und die Verknüpfbarkeit der Netze in Betracht zu ziehen, die die Kommission nach den Modalitäten gemäß Artikel 29 des Richtlinienentwurfs ausgearbeitet hat.

Die Verpflichtung, geeignete Datenschutzmaßnahmen zu treffen, beschränkt sich nicht auf den Ort der Datenverarbeitung oder der für die Verarbeitung verwendeten Hard- und Software. Wenn eine Datenübertragung zwischen zwei Computern oder zwischen einem Computer und Terminals im Rahmen eines Telekommunikationsnetzes stattfindet, sind gemäß Artikel 18 Ziffer 2 auch im Hinblick auf das Netz Datenschutzmaßnahmen zu treffen, um eine sichere und ungestörte Datenübertragung zu gewährleisten.

Artikel 18 Ziffer 3 betrifft den direkten Zugang eines außenstehenden Benutzers einer Datei bei Online-Abfragen. Die Ermächtigung des Benutzers, Daten aus der Datei abzufragen, entspricht und beschränkt sich auf den Vertrag mit dem Verantwortlichen der Datei. Der Richtlinienentwurf sieht vor, daß der Verantwortliche der Datei die technischen Anlagen und die Software für Online-Abfragen so zu gestalten hat, daß der Zugang des Benutzers im Rahmen der Ermächtigung bleibt, die dem Benutzer vom Verantwortlichen der Datei erteilt wurde.

Artikel 18 Ziffer 4 regelt die Verantwortung für die Erfüllung der Verpflichtungen in Artikel 18 Ziff. 1 bis 3. Die Person, die - de facto oder aufgrund eines Vertrages - die Kontrolle über die Vorgänge im Zusammenhang mit einer Datei ausübt, ist auch für die Beachtung der Datenschutzvorschriften verantwortlich. Diese Bestimmung betrifft im Einzelfall den Verantwortlichen der Datei, den Benutzer, der Zugang zur Online-Abfrage hat, bzw. Datenverarbeitungsdienste, die Datenverarbeitungsoperationen für den Verantwortlichen der Datei durchführen.

Artikel 18 Ziffer 5 schließlich sieht ein Berufsgeheimnis für die Bediensteten des Verantwortlichen einer Datei und andere Personen vor, die im Rahmen ihrer beruflichen Tätigkeit Zugang zu den in den Dateien enthaltenen personenbezogenen Informationen haben. Diese Personen dürfen die Informationen, zu denen sie Zugang haben, Dritten nicht ohne das Einverständnis des Verantwortlichen der Datei mitteilen.

KAPITEL VI

Sonderbestimmungen für bestimmte Bereiche

Artikel 19

Die Mitgliedstaaten können Ausnahmen von den Bestimmungen dieser Richtlinie für Organe der Presse und der audiovisuellen Medien insofern vorsehen, als

diese erforderlich sind, um die Grundrechte der Personen, insbesondere das Recht auf Privatsphäre, mit den Regeln für die Informations- und Pressefreiheit in Einklang zu bringen.

Tatsächlich besteht die Gefahr eines Konflikts zwischen diesen beiden Kategorien von Grundrechten. Die Regelung sieht vor, daß die vorhandenen Interessen bei einer abweichenden Maßnahme gegeneinander abzuwägen sind. Bei dieser Abwägung sind gegebenenfalls vorhandene Einspruchmöglichkeiten der betroffenen Person oder ein mögliches Auskunftsrecht, vorhandene Grundsätze des Berufsethos, die Beschränkungen der Europäischen Menschenrechtskonvention und allgemeine Rechtsgrundsätze zu berücksichtigen.

Artikel 20

Dieser Artikel sieht vor, daß die Mitgliedstaaten die Berufskreise ermutigen, an der Ausarbeitung von Standesordnungen oder europäischen Verhaltenscodizes mitzuwirken, die geeignet sind, die Anwendung der Grundsätze der Richtlinie in bestimmten Bereichen zu erleichtern.
Die Kommission unterstützt ebenfalls solche Initiativen und berücksichtigt diese gegebenenfalls bei der Ausübung ihrer Regelungsbefugnisse oder bei der Ausarbeitung neuer Vorschläge.

KAPITEL VII

Haftung und Sanktionen

Artikel 21

Haftung

Für den Fall, daß ein Schaden auf die Mißachtung der Bestimmungen dieser Richtlinie zurückzuführen ist, sieht dieser Artikel vor, daß der Verantwortliche der Datei dafür haftet und daß die betroffene Person von diesem Schadenersatz fordern kann. Der Begriff des Schadens bezieht sich

auf einen materiellen ebenso wie auf einen immateriellen Schaden. Eine Einschränkung der Haftung des Verantwortlichen der Datei ist vorgesehen, falls er im Falle des Verlusts, der Zerstörung oder des unbefugten Zugangs nachweist, daß die Datenschutzvorschriften beachtet wurden.

Artikel 22

Verarbeitung im Auftrag des Verantwortlichen der Datei

Durch diesen Artikel soll verhindert werden, daß eine Verarbeitung durch einen Dritten im Auftrag des Verantwortlichen der Datei zu einer Schwächung des Schutzes der betroffenen Person führt. Um dies zu gewährleisten, muß der Verantwortliche der Datei ebenso wie der Dritte, der die Verarbeitung durchführt, Auflagen beachten.

Artikel 23

Sanktionen

Um die Einhaltung der in Anwendung dieser Richtlinie erlassenen Vorschriften zu gewährleisten, sind die Mitgliedstaaten verpflichtet, wirksame abschreckende Sanktionen (beispielsweise im Bereich des Strafrechts) zu erlassen, die insbesondere der Tatsache Rechnung tragen, daß die Nichtbeachtung der Grundsätze des Schutzes der betroffenen Person eine Verletzung eines Grundrechts darstellt.

KAPITEL VIII

Übermittlung personenbezogener Daten in Drittländer

Artikel 24

Grundsätze

Dieser Artikel sieht den Grundsatz vor, daß der Transfer personenbezogener Daten aus einem Mitgliedstaat in ein Drittland nur stattfinden kann, wenn

dieses Land ein angemessenes Schutzniveau gewährleistet. Die Mitgliedstaaten und gegebenenfalls die Kommission legen fest, ob ein Land ein angemessenes Schutzniveau garantiert. Die Mitgliedstaaten müssen der Kommission Fälle mitteilen, in denen ein einführendes Drittland dieses Niveau nicht gewährleistet. In diesem Fall kann die Kommission Verhandlungen mit dem betreffenden Drittland einleiten.

Die Kommission kann im Rahmen ihrer Durchführungsbefugnisse gemäß Artikel 29 entscheiden, daß ein Land ein angemessenes Schutzniveau bietet; sie stützt sich dabei auf dessen innerstaatliches Recht und die von diesem eingegangenen internationalen Verpflichtungen. Das Übereinkommen des Europarats vom 28. Januar 1981 über den Schutzes des Menschen bei der Verarbeitung personenbezogener Daten ist Teil der Verpflichtungen, die die Kommission berücksichtigt. Sie kann außerdem die Gruppe für den Schutz personenbezogener Daten in dieser Frage anhören.

Artikel 25

Ausnahmebestimmung

Falls ein Land ein angemessenes Schutzniveau nicht gewährleistet, ist eine Ausnahme möglich, die den Datentransfer für eine bestimmte Ausfuhr ermöglicht. Der Mitgliedstaat, in dem sich die Datei befindet, kann diesen Transfer genehmigen, wenn der Verantwortliche der Datei ein angemessenes Schutzniveau für diese Ausfuhr garantieren kann und wenn die anderen Mitgliedstaaten oder die Kommission keine Einwände geltend machen. Zu diesem Zweck ist ein Informationsverfahren mit einer Frist von zehn Tagen für die Meldung eines Einspruchs vorgesehen. Bei Meldung eines Einspruchs kann die Kommission geeignete Maßnahmen erlassen, insbesondere kann sie beschließen, den Transfer zu untersagen.

KAPITEL IX

Kontrollbehörden und Gruppe für den Schutz personenbezogener Daten

Artikel 26

Die Kontrollbehörde

Dieser Artikel sieht vor, daß eine Kontrollbehörde geschaffen wird, deren Unabhängigkeit gewährleistet ist und die über Mittel für die Untersuchung und Eingriffsmöglichkeiten verfügt, die ihren Kontrollaufgaben entsprechen. Die nationalen Rechtsvorschriften müssen diese beiden Eigenschaften sicherstellen. Der Begriff "Kontrollbehörde" steht nicht der Entscheidung für eine interne Struktur entgegen, die auch andere Aufgaben vorsieht und dem Rechtssystem des betreffenden Mitgliedstaates entspricht.

Artikel 27

Gruppe für den Schutz personenbezogener Daten

Um den besonderen Gegebenheiten des Personenschutzes bei der Verarbeitung personenbezogener Daten Rechnung zu tragen, sieht dieser Artikel eine beratende Gruppe vor, die Gruppe für den Schutz personenbezogener Daten. Diese unabhängige Gruppe setzt sich aus Vertretern der nationalen Aufsichtsbehörden zusammen. Den Vorsitz in dieser Gruppe führt ein Vertreter der Kommission.

Artikel 28

Aufgaben der Gruppe für den Schutz personenbezogener Daten

Dieser Artikel bestimmt die Aufgaben der Gruppe für den Schutz personenbezogener Daten. Die Gruppe unterstützt die Kommission mit ihren Kenntnissen und ihrem Sachverstand im Bereich des Personenschutzes bei der Verarbeitung personenbezogener Daten. Sie trägt somit zur homogenen

Auslegung der einzelstaatlichen Durchführungsbestimmungen dieser Richtlinie bei; sie beurteilt das Schutzniveau in der Gemeinschaft und in den Drittländern und unterrichtet die Kommission darüber; schließlich kann sie die Kommission bei der Ausarbeitung zusätzlicher Maßnahmen beraten.
Die Gruppe für den Schutz personenbezogener Daten kann Empfehlungen aussprechen, die gegebenenfalls auf ihr Ersuchen dem Beratenden Ausschuß übermittelt werden, der im Rahmen der Durchführungsbefugnisse der Kommission angehört wird.

Die Gruppe für den Schutz personenbezogener Daten erstellt einen Jahresbericht über die Situation im Bereich des Schutzes personenbezogener Daten in der Gemeinschaft und in den Drittländern. Dieser Bericht wird der Kommission vorgelegt.

KAPITEL X

Rechtssetzungsbefugnis der Kommission

Artikel 29 und 30

Ausübung der Rechtssetzungsbefugnis
Beratender Ausschuß

Artikel 29 überträgt der Kommission die Durchführungsbefugnisse hinsichtlich der ergänzenden Maßnahmen, die angesichts des Umfangs und der technischen Spezialisierung des Bereichs der Verarbeitung personenbezogener Daten erforderlich sind.

Da die Richtlinie zur Vollendung des Binnenmarkts beitragen soll, sieht Artikel 30 vor, daß ein Ausschuß mit beratender Funktion eingesetzt wird, um die Kommission bei der Ausübung ihrer Durchführungsbefugnisse zu unterstützen; dabei sind die Verfahren der Entscheidung des Rates vom 13. Juli 1987 über die Modalitäten der Ausübung der Durchführungsbefugnisse der Kommission anzuwenden.

Vorschlag für eine **SYN 287**

RICHTLINIE DES RATES

zum Schutz von Personen bei der Verarbeitung personenbezogener Daten

---

DER RAT DER EUROPÄISCHEN GEMEINSCHAFTEN -

gestützt auf den Vertrag zur Gründung der Europäischen Wirtschaftsgemeinschaft, insbesondere auf die Artikel 100 a und Artikel 113,

auf Vorschlag der Kommission (1),

in Zusammenarbeit mit dem Europäischen Parlament (2),

nach Stellungnahme des Wirtschafts- und Sozialausschusses (3),

in Erwägung nachstehender Gründe:

(1) Die in dem durch die Einheitliche Europäische Akte geänderten Vertrag genannten Ziele der Gemeinschaft bestehen darin, einen immer engeren Zusammenschluß der europäischen Völker zu schaffen, immer engere Beziehungen zwischen den in der Gemeinschaft zusammengeschlossen Staaten herzustellen, durch gemeinsames Handeln den wirtschaftlichen und sozialen Fortschritt zu sichern, indem die Europa trennenden Schranken beseitigt werden, die ständige Besserung der Lebensbedingungen ihrer Völker zu fördern, Frieden und Freiheit zu wahren und zu festigen und für die Demokratie einzutreten, und sich dabei auf die in den Verfassungen und Gesetzen der Mitgliedstaaten sowie in der Europäischen Konvention zum Schutze der Menschenrechte und Grundfreiheiten anerkannten Grundrechte zu stützen.

(2) Für die Errichtung und das Funktionieren des Binnenmarkts, in dem gemäß Artikel 8a des Vertrags der freie Verkehr von Waren, Personen, Dienstleistungen und Kapital gewährleistet ist, ist nicht nur erforderlich, daß

personenbezogene Daten unabhängig von den Mitgliedstaaten, in denen sie verarbeitet oder in denen sie angefordert werden, übermittelt werden können, sondern auch, daß in Anbetracht der wachsenden Inanspruchnahme der Verarbeitung personenbezogener Daten in den verschiedenen wirtschaftlichen und sozialen Tätigkeitsbereichen in der Gemeinschaft die Grundrechte gewahrt werden.

(3) Der Binnenmarkt umfaßt einen Raum ohne Binnengrenzen; aus diesem Grunde sind die nationalen Verwaltungen der einzelnen Mitgliedstaaten aufgrund der Anwendung des Gemeinschaftsrechts immer häufiger aufgerufen, zusammenzuarbeiten und untereinander personenbezogene Daten auszutauschen, um ihren Auftrag erfüllen oder Aufgaben für die Verwaltung eines anderen Mitgliedstaats durchführen zu können.

(4) Die verstärkte wissenschaftliche und technische Zusammenarbeit sowie die koordinierte Einführung neuer Netze im Fernmeldeverkehr in der Gemeinschaft machen den grenzüberschreitenden Verkehr personenbezogener Daten erforderlich und erleichtern ihn.

(5) Das unterschiedliche Niveau des Schutzes der Privatsphäre bei der Verarbeitung personenbezogener Daten in den Mitgliedstaaten kann die Übermittlung dieser Daten aus dem Gebiet eines Mitgliedstaates nach dem eines anderen Mitgliedstaates verhindern; mithin kann dieses unterschiedliche Schutzniveau ein Hemmnis für die Ausübung einer Reihe von Wirtschaftstätigkeiten auf Gemeinschaftsebene darstellen, den Wettbewerb verfälschen und den Auftrag der sich im Anwendungsbereich des Gemeinschaftsrechts einschaltenden Verwaltungen behindern; dieses unterschiedliche Schutzniveau ergibt sich aus den Unterschieden in den einzelstaatlichen Rechts- und Verwaltungsvorschriften.

(6) Für die Beseitigung der Hemmnisse für den Verkehr personenbezogener Daten ist ein gleichwertiges Schutzniveau der Privatsphäre bei der Verarbeitung dieser Daten in allen Mitgliedstaaten unerläßlich; dementsprechend sind die einschlägigen geltenden Rechtsvorschriften anzugleichen.

(7) Gegenstand der einzelstaatlichen Rechtsvorschriften über die Verarbeitung personenbezogener Daten ist die Gewährleistung der Achtung der Grundrechte insbesondere des auch in Artikel 8 der Konvention zum Schutze der Menschenrechte und Grundfreiheiten und in den allgemeinen Grundsätzen des Gemeinschaftsrechts anerkannten Rechts auf die Privatspäre; deshalb darf die Angleichung dieser Rechtsvorschriften nicht zu einer Verringerung des durch sie garantierten Schutzes führen, sondern muß darauf abzielen, in der Gemeinschaft ein hohes Schutzniveau sicherzustellen.

(8) Die Grundsätze des Schutzes der Privatsphäre bei der Verarbeitung personenbezogener Daten, die Gegenstand der Richtlinie sind, können - insbesondere für bestimmte Bereiche - durch mit diesen Grundsätzen im Einklang stehende besondere Regeln ergänzt oder präzisiert werden.

(9) Die Grundsätze des Schutzes müssen für alle Dateien gelten, sobald die Tätigkeiten des Verantwortlichen der Datei in den Anwendungsbereich des Gemeinschaftsrechts fallen; für die nicht in den Anwendungsbereich des Gemeinschaftsrechts fallenden Dateien des öffentlichen Bereichs sollten die gleichen Grundsätze des Schutzes gelten, die gemäß der Entschließung der im Rat vereinigten Vertreter der Regierungen der Mitgliedstaaten der Europäischen Gemeinschaften vom ..... in die einzelstaatlichen Rechtsvorschriften aufgenommen werden sollen; auszunehmen sind allerdings Dateien wie persönliche Adressendateien, die ausschließlich in den Bereich der Ausübung des Rechtes auf die Privatsphäre einer natürlichen Person fallen.

(10) Jede Verarbeitung personenbezogener Daten in der Gemeinschaft muß die Rechtsvorschriften des Mitgliedstaates achten, in dem sich die Datei befindet, um zu vermeiden, daß eine Person den Schutz, der ihr gemäß dieser Richtlinie gewährt werden muß, nicht erhält; in diesem Zusammenhang ist jeder Teil einer in mehreren Mitgliedstaaten befindlichen Datei als eine Datei anzusehen, und die Verbringung in ein Drittland darf diesen Schutz nicht verhindern.

(11) Jede Verarbeitung personenbezogener Daten muß rechtmäßig sein; diese Rechtmäßigkeit muß sich auf das Einverständnis der betroffenen Person, das Gemeinschaftsrecht oder auf die einzelstaatlichen Rechtsvorschriften stützen.

(12) Die einzelstaatlichen Rechtsvorschriften können unter den in der Richtlinie vorgesehenen Bedingungen die Regeln für die Rechtmäßigkeit der Verarbeitung festlegen; eine solche Möglichkeit darf allerdings nicht als Begründung für eine Kontrolle eines anderen Mitgliedstaats als des Staats dienen, in dem die Datei sich befindet, da letzterer verpflichtet ist, gemäß dieser Richtlinie zu gewährleisten, daß die Privatspäre bei der Verarbeitung personenbezogener Daten im Hinblick auf das Gemeinschaftsrecht ausreichend geschützt wird, um den freien Verkehr der Daten zu ermöglichen.

(13) Die Meldeverfahren für die Dateien des öffentlichen oder privaten Bereichs und die Benachrichtigungsverfahren bei der ersten Übermittlung für die Dateien des privaten Bereichs sollen die Transparenz gewährleisten, die für die Ausübung des Rechtes auf Zugang der betroffenen Person zu den sie betreffenden Daten unerläßlich ist.

(14) Die betroffene Person muß vollständig informiert werden, damit ihre Einwilligung wirksam ist; dies gilt auch, wenn die sie betreffenden Daten bei ihr erhoben werden.

(15) Die betroffene Person muß das Recht auf Auskunft über die sie betreffenden Daten haben, um sich der Rechtmäßigkeit der Verarbeitung der und ihrer Qualität vergewissern zu können.

(16) Um Gegenstand einer Verarbeitung zu sein, müssen die Daten bestimmten Anforderungen genügen; die Verarbeitung der Daten, die aufgrund ihrer Art geeignet sind, das Recht auf den Schutz der Privatsphäre zu beeinträchtigen, ist ohne ausdrückliche Einwilligung der betroffenen Person zu untersagen; aus Gründen wichtigen öffentlichen Interesses können allerdings insbesondere für die medizinischen Berufe Ausnahmeregelungen auf der Grundlage einer Rechtsvorschrift vorgesehen werden, die die Bedingungen und Beschränkungen der Verarbeitung dieser Art von Daten genau und strikt festlegt.

(17) Für den Schutz der Privatsphäre im Hinblick auf personenbezogene Daten müssen sowohl auf der Planungs- als auch auf der technischen Ebene der Verarbeitung geeignete Sicherheitsmaßnahmen getroffen werden, um jede nicht genehmigte Verarbeitung zu verhindern.

(18) Im Medienbereich können die Mitgliedstaaten Ausnahmen von den Bestimmungen dieser Richtlinie vorsehen, sofern diese darauf abzielen, das Recht auf die Privatsphäre mit dem Recht auf Information und dem Recht, Informationen zu empfangen oder zu übermitteln, zu vereinbaren, das insbesondere in Artikel 10 der Konvention zum Schutze der Menschenrechte und Grundfreiheiten garantiert ist.

(19) Die Mitgliedstaaten haben die Ausarbeitung von Standesordnungen oder europäischen freiwilligen Verhaltensregeln für bestimmte Einzelbereiche durch die Berufskreise zu fördern; die Kommission wird derartige Initiativen unterstützen und berücksichtigen, wenn sie prüft, ob für bestimmte Bereiche neue spezifische Maßnahmen erforderlich sind.

(20) Bei Nichteinhaltung der in dieser Richtlinie vorgesehenen Vorschriften ist der Verantwortliche der Datei bei einer Schadensersatzklage als Verantwortlicher anzusehen; zur Abschreckung sind Sanktionen anzuwenden, um einen wirksamen Schutz zu gewährleisten.

(21) Personenbezogene Daten müssen in ein Drittland mit einem angemessenen Schutzniveau übermittelt werden können; fehlt ein solcher Schutz in Drittländern, so sieht diese Richtlinie insbesondere Verhandlungsverfahren mit letzteren vor.

(22) Die in dieser Richtlinie enthaltenen Grundsätze konkretisieren und erweitern die in dem Übereinkommen des Europarats vom 26. Januar 1981 zum Schutze des Menschen bei der automatischen Verarbeitung personenbezogener Daten enthaltene Grundsätze.

(23) Die Existenz einer unabhängigen Kontrollstelle in jedem Mitgliedstaat ist ein wesentliches Element des Schutzes der Personen bei der Verarbeitung personenbezogener Daten; auf Gemeinschaftsebene muß eine aus Vertretern der einzelstaatlichen Kontrollbehörden zusammengesetzte Gruppe eingesetzt werden und ihre Aufgaben in völliger Unabhängigkeit wahrnehmen; in Anbetracht dieses besonderen Charakters hat sie die Kommission zu beraten und zu der einheitlichen Anwendung der zur Durchführung dieser Richtlinie erlassenen einzelstaatlichen Bestimmungen beizutragen.

(24) Die Verabschiedung der ergänzenden Maßnahmen für die Anwendung der Grundsätze dieser Richtlinie macht es notwendig, der Kommission Befugnisse zu ihrer Durchführung zu übertragen und gemäß den in Beschluß des Rates 87/373/EWG vom 13. Juli 1987[1] festgelegten Modalitäten einen Beratenden Ausschuß einzusetzen -

HAT FOLGENDE RICHTLINIE ERLASSEN:

KAPITEL I

ALLGEMEINE BESTIMMUNGEN

Artikel 1

Gegenstand der Richtlinie

1. Die Mitgliedstaaten gewährleisten nach den Bestimmungen dieser Richtlinie den Schutz der Privatsphäre von Personen bei der Verarbeitung personenbezogener Daten, die in Dateien enthalten sind.

2. Die Mitgliedstaaten beschränken oder untersagen nicht den freien Verkehr personenbezogener Daten zwischen Mitgliedstaaten aus Gründen des gemäß Absatz 1 gewährleisteten Schutzes.

---

(1) ABl. Nr. L 197 vom 18.8.1987, S. 33.

Artikel 2

Begriffsbestimmungen

Für die Zwecke dieser Richtlinie bedeuten:

a) "Personenbezogene Daten": alle Informationen über eine bestimmte oder bestimmbare natürliche Person ("betroffene Person"); als bestimmbar wird insbesondere eine Person angesehen, die durch die Zuordnung zu einer Kennummer oder einer vergleichbaren Information identifiziert werden kann.

b) "Anonymisieren": das Verändern personenbezogener Daten derart, daß die darin enthaltenen Angaben nicht mehr oder nur mit einem unverhältnismäßig großen Aufwand an Arbeitskraft, Kosten und Zeit einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können.

c) "Datei mit personenbezogenen Daten" (Datei): jede Sammlung personenbezogener Daten, die zentral oder an mehreren Standorten geführt wird, Gegenstand einer automatisierten Verarbeitung ist oder, falls sie mittels nicht-automatisierter Verfahren verarbeitet werden, geordnet und in einer Sammlung zugänglich ist, die nach bestimmten Kriterien organisiert ist, die die Benutzung oder Verknüpfung der Daten erleichtern.

d) "Verarbeitung": die mit oder ohne Hilfe automatisierter Verfahren vorgenommenen Vorgänge: Speichern, Aufbewahrung, Verknüpfung von Daten, ihre Veränderung, Benutzung und Weitergabe, insbesondere die Übermittlung, Verbreitung, Erstellung von Auszügen sowie das Sperren und Löschen.

e) "Verantwortlicher der Datei": die natürliche oder juristische Person, Behörde, Dienststelle oder jede andere Einrichtung, die nach dem Gemeinschaftsrecht oder den einzelstaatlichen Rechtsvorschriften eines

Mitgliedstaats zuständig ist, darüber zu entscheiden, welche Zweckbestimmung die Datei verfolgt, welche Arten personenbezogener Daten gespeichert und mit welchen Vorgängen sie verarbeitet werden sollen sowie welche Dritte Zugang zu den Dateien haben dürfen.

f) "Kontrollbehörde": die unabhängige Behörde oder jede andere unabhängige Instanz, die von jedem Mitgliedstaat gemäß Artikel 26 dieser Richtlinie bestimmt wird.

g) "öffentlicher Bereich": die Gesamtheit der öffentlich-rechtlichen Verwaltungen, Organisationen und Einrichtungen eines Mitgliedstaats, mit Ausnahme derer, die an einer gewerblichen oder kommerziellen Tätigkeit teilnehmen, sowie die privatrechtlichen Einrichtungen und Rechtssubjekte, wenn sie an der Ausübung der Staatsgewalt beteiligt sind.

h) "privater Bereich": jede natürliche oder juristische Person oder Vereinigung, sowie die Behörden, Organisationen und Rechtssubjekte des öffentlichen Bereichs, soweit diese eine gewerbliche oder kommerzielle Tätigkeit ausüben.

Artikel 3

Anwendungsbereich

1. Die Mitgliedstaaten wenden die Bestimmungen dieser Richtlinie auf die Dateien des privaten und des öffentlichen Bereichs an mit Ausnahme der Dateien des öffentlichen Bereichs, wenn dessen Tätigkeiten nicht in den Anwendungsbereich des Gemeinschaftsrechts fallen.

2. Die Bestimmungen dieser Richtlinie finden keine Anwendung auf Dateien:

   (a) einer natürlichen Person, die ausschließlich privaten und persönlichen Zwecken dienen oder

(b) von gemeinnützigen, insbesondere politischen, philosophischen, religiösen, kulturellen, gewerkschaftlichen, Sport- oder Freizeitvereinigungen im Rahmen ihres zulässigen Zwecks und unter der Voraussetzung, daß sie sich nur auf die Mitglieder und Korrespondenzpartner der Vereinigung beziehen, die ihre Einwilligung zur Aufnahme in die Datei erteilt haben, und sofern sie nicht an Dritte weitergeben werden.

Artikel 4

Anwendbares Recht

1. Jeder Mitgliedstaat wendet die Bestimmungen dieser Richtlinie an auf:

   (a) alle in seinem Hoheitsgebiet befindlichen Dateien.

   (b) den Verantwortlichen der Datei, der in seinem Hoheitsgebiet ansässig ist, und der von diesem aus eine in einem Drittland angesiedelte/befindliche Datei benutzt, dessen Rechtsvorschriften kein angemessenenes Schutzniveau garantieren, sofern diese Benutzung nicht nur vereinzelt erfolgt.

2. Jeder Mitgliedstaat wendet die Bestimmungen der Artikel 5, 6, 8, 9, 10, 17, 18 und 21 auf den Benutzer an, der von einem im Hoheitsgebiet eines Mitgliedstaats befindlichen Datenendgerät aus eine außerhalb der Gemeinschaft befindliche Datei abfragt, sofern es sich dabei nicht um eine vereinzelte Abfrage handelt.

3. Wird eine Datei vorübergehend von einem Mitgliedstaat in einen anderen Mitgliedstaat verbracht, so wird dies von diesem Mitgliedstaat weder behindert noch wird irgendeine zusätzliche Förmlichkeit verlangt, die über die Regelungen in dem Mitgliedstaat hinausgeht, in dem die Datei sich ständig befindet.

KAPITEL II

RECHTMÄSSIGKEIT DER VERARBEITUNG IM ÖFFENTLICHEN BEREICH

Artikel 5

Grundsätze

1. Vorbehaltlich der Bestimmungen in Artikel 6 sehen die Mitgliedstaaten in ihren Rechtsvorschriften für die Dateien des öffentlichen Bereichs folgendes vor:

(a) Die Einrichtung einer Datei und jede andere Verarbeitung personenbezogener Daten sind rechtmäßig, insoweit sie für die Wahrnehmung der Aufgaben der für diese Datei verantwortlichen Behörde erforderlich sind;

(b) Die Verarbeitung von Daten zu einem anderen Zweck als dem, zu dem die Datei errichtet worden ist, ist rechtmäßig, wenn:

- die betroffene Person dafür ihre Einwilligung erteilt oder

- sie auf der Grundlage des Gemeinschaftsrechts, eines Gesetzes oder eines Rechtsakts in Anwendung eines Gesetzes eines Mitgliedstaats erfolgt, wenn diese Rechtsgrundlage im Einklang mit dieser Richtlinie steht, ihn zu dieser Verarbeitung ermächtigt und deren Grenzen festlegt oder
- dieser Zweckänderung kein berechtigtes Interesse der betroffenen Person entgegensteht oder
- sie erforderlich ist, um einer drohenden Gefahr für die öffentliche Sicherheit und Ordnung oder einer schwerwiegenden Verletzung der Rechte Dritter vorzubeugen.

Artikel 6

Weitergabe personenbezogener Daten bei der Datenverarbeitung im öffentlichen Bereich

1. Die Mitgliedstaaten sehen in ihren Rechtsvorschriften vor, daß die Weitergabe personenbezogener Daten aus Dateien einer öffentlichen Stelle nur rechtmäßig ist, wenn:

   (a) sie für die Wahrnehmung von Aufgaben der öffentlichen Stelle, die sie weitergibt oder um die Weitergabe dieser Daten ersucht, erforderlich ist oder

   (b) auf Anfrage einer natürlichen oder juristischen Person des privaten Bereichs, die ein berechtigtes Interesse geltend macht, sofern nicht das Interesse der betroffenen Person überwiegt.

2. Unbeschadet der Bestimmungen des Absatzes 1 können die Mitgliedstaaten die Voraussetzungen näher bestimmen, unter denen die Weitergabe personenbezogener Daten rechtmäßig ist.

3. Die Mitgliedstaaten sehen in ihren Rechtsvorschriften vor, daß der für die Datei Verantwortliche die betroffenen Personen in den in Absatz 1 Buchstabe b genannten Fällen über die Weitergabe der personenbezogenen Daten benachrichtigt. Die Mitgliedstaaten können festlegen, daß diese Information durch eine vorherige Genehmigung der Kontrollbehörde ersetzt wird.

Artikel 7

Meldepflicht bei der Kontrollbehörde

1. Die Mitgliedstaaten sehen in ihren Rechtsvorschriften vor, daß die Einrichtung einer Datei des öffentlichen Bereichs, deren personenbezogene Daten für eine Weitergabe in Frage kommen, zuvor der Kontrollbehörde gemeldet werden muß, die dies in ein Register einträgt. Das Register kann von jedermann eingesehen werden.

2. Die Mitgliedstaaten legen fest, welche Angaben der Kontrollbehörde zu melden sind. Diese Angaben haben mindestens Namen und Anschrift des Verantwortlichen der Datei, ihre Zweckbestimmung, eine Beschreibung der Art des gespeicherten Daten, die Dritten, denen die Daten möglicherweise weitergegeben werden, sowie eine Beschreibung der in Anwendung von Artikel 18 getroffenen Maßnahmen zu umfassen.

3. Die Mitgliedstaaten können vorsehen, daß die Bestimmungen der Absätze 1 und 2 auf andere Dateien des öffentlichen Bereichs Anwendung finden und die Einsicht in das Register aus den in Artikel 15 Absatz 1 genannten Gründen eingeschränkt werden kann.

KAPITEL III

ZULÄSSIGKEIT DER VERARBEITUNG IM PRIVATEN BEREICH

Artikel 8

Grundsätze

1. Die Mitgliedstaaten sehen in ihren Rechtsvorschriften vor, daß ohne die Einwilligung der betroffenen Person das Erfassen personenbezogener Daten in einer Datei und jede andere Verarbeitung nur im Einklang mit den Bestimmungen dieser Richtlinie zulässig sind und wenn:

   a. die Verarbeitung im Rahmen eines Vertrages mit oder eines vertragsähnlichen Vertrauensverhältnisses zu dem Betroffenen erfolgt und für dessen Durchführung erforderlich ist oder

   b. die Daten aus jedermann zugänglichen Quellen stammen und ihre Verarbeitung ausschließlich Korrespondenzzwecken dient oder

   c. der für die Datei Verantwortliche ein berechtigtes Interesse verfolgt, sofern nicht das Interesse der betroffenen Person überwiegt;

2. Die Mitgliedstaaten sehen in ihren Rechtsvorschriften vor, daß sich der für die Datei Verantwortliche zu vergewissern hat, daß jede Weitergabe mit dem Zweck der Datei vereinbar ist und die öffentliche Sicherheit und Ordnung nicht beeinträchtigt. Bei einem Datenabruf im automatisierten Verfahren obliegen dem Benutzer dieselben Pflichten.

3. Unbeschadet der Bestimmungen in Absatz 1 können die Mitgliedstaaten die Bedingungen näher festlegen, unter denen die Verarbeitung personenbezogener Daten rechtmäßig ist.

Artikel 9

Die Pflicht zur Benachrichtigung der betroffenen Person

1. Für den privaten Bereich sehen die Mitgliedstaaten in ihren Rechtsvorschriften vor, daß der Verantwortliche die betroffene Person bei der ersten Weitergabe oder bei der Eröffnung einer Möglichkeit des automatisierten Datenabrufs benachrichtigt und dabei die Zweckbestimmung der Datei, die Arten der darin gespeicherten Daten, seinen Namen und seine Anschrift angibt.

2. Die in Absatz 1 vorgesehene Benachrichtigung ist in dem in Artikel 8 Absatz 1 Buchstabe b genannten Fall nicht zwingend. Die Benachrichtigungspflicht besteht in den Fällen nicht, in denen die Übermittlung gesetzlich vorgeschrieben ist.

3. Erhebt die betroffene Person Einwände gegen die Weitergabe oder jede andere Form der Verarbeitung, so hat der Verantwortliche der Datei die strittige Verarbeitung einzustellen, wenn nicht eine gesetzliche Bestimmung ihm diese erlaubt.

Artikel 10

Besondere Ausnahmen von der Pflicht zur Benachrichtigung der betroffenen Person

Erweist sich die Benachrichtigung der betroffenen Person nach Artikel 9 Absatz 1 als unmöglich oder ist mit unverhältnismäßigen Bemühungen verbunden oder steht ihr ein überwiegendes berechtigtes Interesse des Verantwortlichen der Datei oder ein vergleichbares Interesse eines Dritten entgegen, so können die Mitgliedstaaten in ihren Rechtsvorschriften vorsehen, daß die Kontrollbehörde eine Ausnahme erteilen kann.

Artikel 11

Meldepflicht bei der Kontrollbehörde

1. Die Mitgliedstaaten sehen in ihren Rechtsvorschriften vor, daß der Verantwortliche der Datei die Einrichtung einer Datei mit personenbezogenen Daten meldet, soweit die Daten zur Weitergabe bestimmt sind und nicht aus jedermann zugänglichen Quellen stammen. Die Meldung hat bei der Kontrollbehörde des Mitgliedstaats zu erfolgen, in dem die Datei sich befindet, oder, falls sie sich in keinem Mitgliedstaat befindet, bei der Kontrollbehörde des Mitgliedstaats, in dem der Verantwortliche der Datei ansässig ist. Der Verantwortliche der Datei hat den zuständigen einzelstaatlichen Behörden jede Änderung seiner Anschrift oder der Zweckbestimmung der Datei zu melden.

2. Die Mitgliedstaaten legen fest, welche Angaben der Kontrollbehörde zu melden sind. Diese Angaben umfassen mindestens Namen und Anschrift des Verantwortlichen der Datei, ihre Zweckbestimmung der Datei, eine Beschreibung der Arten der gespeicherten Daten, die Dritten, denen die Daten möglicherweise weitergegeben werden, sowie eine Beschreibung der in Anwendung von Artikel 18 getroffenen Maßnahmen.

3. Die Mitgliedstaaten können vorsehen, daß die Bestimmungen in Absatz 1 und 2 auf andere Dateien des privaten Bereichs Anwendung finden und die Angaben nach Absatz 2 der Öffentlichkeit zugänglich sind.

KAPITEL IV

RECHTE DER BETROFFENEN PERSON

Artikel 12

Einwilligung nach Unterrichtung der betroffenen Person

Die Einwilligung einer betroffenen Person zu einer Verarbeitung sie betreffender personenbezogener Daten im Sinne dieser Richtlinie ist nur wirksam, wenn:

(a) die Person über die nachstehenden Informationen verfügt:
- Zweckbestimmung der Datei und Art der gespeicherten Daten;
- Art der Verwendung und gegebenenfalls Empfänger der in der Datei gespeicherten personenbezogenen Daten;
- Name und Anschrift des Verantwortlichen der Datei;

(b) die Einwilligung muß konkret sein und ausdrücklich erklärt werden; sie hat die Art der Daten, die Form der Verarbeitung und die möglichen Empfänger, auf die sie sich erstreckt, genau zu bestimmen;

(c) sie kann von der betroffenen Person jederzeit widerrufen werden. Der Widerruf hat keine Rückwirkung.

Artikel 13

Unterrichtung bei der Datenerhebung

1. Die Mitgliedstaaten stellen sicher, daß die Personen, bei denen personenbezogene Daten erhoben werden, das Recht haben, zumindest über folgendes unterrichtet zu werden:

(a) Zweckbestimmung der Datei, für die die Angaben bestimmt sind;

(b) darüber, ob sie zur Beantwortung der Fragen, die Gegenstand der Erhebung sind, verpflichtet sind oder nicht;

(c) über die sie betreffenden Konsequenzen einer unterlassenen Beantwortung;

(d) über die Empfänger der Angaben,

(e) über die Rechte auf Auskunft und auf Berichtigung der sie betreffenden Daten und

(f) über Namen und Anschrift des Verantwortlichen der Datei.

2. Die Bestimmungen des Absatzes 1 gelten nicht für die Datenerhebung, wenn die Unterrichtung der betroffenen Person die Ausübung der Kontroll- und Überprüfungsaufgaben einer Behörde oder die Aufrechterhaltung der öffentlichen Sicherheit und Ordnung verhindert.

Artikel 14

Ergänzende Rechte der betroffenen Person

Die Mitgliedstaaten erkennen nachstehende Rechte der betroffenen Person an:

1. aus berechtigten Gründen dagegen Einspruch zu erheben, daß sie betreffende personenbezogene Daten Gegenstand einer Verarbeitung sind;

2. keiner Verwaltungsmaßnahme oder Entscheidung im privaten Bereich unterworfen zu werden, die eine Beurteilung ihres Verhaltens enthält und sich dabei allein auf eine rechnergestützte Verarbeitung personenbezogener Daten stützt, die ein Persönlichkeitsprofil des Betroffenen herstellt;

3. die Existenz einer Datei, ihre wichtigsten Zweckbestimmungen sowie die Identität und den gewöhnlichen Aufenthalt, den Sitz oder die Niederlassung des für die Datei Verantwortlichen zu kennen;

4. in angemessenen Abständen, unverzüglich, in verständlicher Form und ohne überhöhte Kosten die Bestätigung des Vorhandenseins sie betreffender personenbezogener Daten in einer Datei sowie diese Daten selbst in einer verständlichen Form zu erhalten.

   Die Mitgliedstaaten können vorsehen, daß das Auskunftsrecht bei medizinischen Daten nur über einen Arzt wahrgenommen werden kann;

5. gegebenenfalls die Berichtigung dieser Daten oder ihre Löschung oder ihre Sperrung zu erreichen, wenn ihre Verarbeitung nicht mit den Bestimmungen dieser Richtlinie im Einklang steht;

6. auf Antrag die kostenlose Löschung der sie betreffenden Daten zu erreichen, die in Dateien für Zwecke der Marktforschung oder Werbezwecke gespeichert sind;

7. bei Anwendung von Absatz 5 dieses Artikels und soweit Daten an Dritte weitergegeben sind, zu erreichen, daß letzteren die Berichtigung, Löschung oder Sperrung mitgeteilt wird;

8. bei Verletzung der in diesem Artikel garantierten Rechte bei Gericht einen Rechtsbehelf einlegen zu können.

Artikel 15

Ausnahmen vom Auskunftsrecht der betroffenen Personen bei Dateien des öffentlichen Bereichs

1. Die Mitgliedstaaten können die in Artikel 14 Nummern 3 und 4 vorgesehenen Rechte aus nachstehenden Gründen durch Gesetz einschränken:

(a) Sicherheit des Staates,

(b) Landesverteidigung,

(c) Strafverfolgung,

(d) öffentliche Sicherheit und Ordnung,

(e) ordnungsgemäß begründetes, zwingendes wirtschaftliches und finanzielles Interesse eines Mitgliedstaats oder der Europäischen Gemeinschaft,

(f) Notwendigkeit der Erfüllung behördlicher Kontroll- oder Überwachungsaufgaben, oder

(g) ein gleichwertiges Recht einer anderen Person und Rechte und Freiheiten eines Dritten.

2. In den in Absatz 1 genannten Fällen muß die Kontrollbehörde auf Antrag der betroffenen Person die notwendigen Überprüfungen der Datei vornehmen können.

3. Die Mitgliedstaaten können das Auskunftsrecht der betroffenen Person für Daten einschränken, die nur vorübergehend zur Ermittlung statistischer Informationen gespeichert werden.

KAPITEL V

Qualität der Daten

Artikel 16

Grundsätze

1. Die Mitgliedstaaten bestimmen wie folgt:

a) Personenbezogene Daten sind nach Treu und Glauben sowie auf rechtmäßige Art und Weise zu erheben und zu verarbeiten;

b) die Daten sind für bestimmte, ausdrücklich festgelegte und rechtmäßige Zwecke zu speichern und in einer mit diesen Zweckbestimmungen zu vereinbarenden Art zu verwenden;

c) die Daten müssen den Zwecken, für die sie gespeichert wurden, entsprechen, dafür erheblich sein und nicht darüber hinausgehen;

d) die Daten müssen richtig und gegebenenfalls auf dem neuesten Stand sein; nicht zutreffende oder unvollständige Daten sind zu löschen oder zu berichtigen;

e) die Daten müssen so aufbewahrt werden, daß die betroffene Person nicht länger identifiziert werden kann, als es die Zwecke der Speicherung erfordern.

2. Der Verantwortliche der Datei hat für die Einhaltung der Bestimmungen des Absatzes 1 zu sorgen.

Artikel 17

Besondere Datenarten

1. Die Mitgliedstaaten untersagen die automatisierte Verarbeitung von Daten, aus denen rassische und ethnische Herkunft, politische Meinung, religiöse oder philosophische Überzeugungen sowie Gewerkschaftszugehörigkeit hervorgehen, sowie von Informationen über Gesundheit und Sexualleben, für die keine freie, ausdrückliche und schriftliche Einwilligung der betroffenen Person vorliegt.

2. Die Mitgliedstaaten können aus wichtigen Gründen des öffentlichen Interesses Ausnahmen von den Bestimmungen des Absatzes 1 auf der Grundlage eines Gesetzes vorsehen, das die speicherbaren Datenarten, die Personen, die Zugang zu der Datei haben, sowie die entsprechenden Sicherungsvorkehrungen gegen mißbräuchliche Verwendung und unzulässigen Zugang näher bestimmt.

3. Daten über strafrechtliche Verurteilungen dürfen nur in Dateien des öffentlichen Bereichs gespeichert werden.

Artikel 18

Sicherheit der Daten

1. Die Mitgliedstaaten sehen in ihren Rechtsvorschriften vor, daß der Verantwortliche der Datei verpflichtet ist, die angemessenen technischen und organisatorischen Maßnahmen zu treffen, die für den Schutz der Datei gegen die zufällige oder nicht genehmigte Zerstörung, den zufälligen Verlust sowie die nicht genehmigte Veränderung, den nicht genehmigten Zugriff oder Zugang und jede andere Form der nicht genehmigten Verarbeitung personenbezogener Daten erforderlich sind.

   Diese Maßnahmen müssen für automatisierte Dateien unter Berücksichtigung des Standes der Technik, der Kosten für ihre Verwirklichung, der Art der zu schützenden Daten sowie der Beurteilung potentieller Risiken ein angemessenes Sicherheitsniveau gewährleisten. Dazu hat der Verantwortliche der Datei die Empfehlungen für die DV-Sicherheit und die Verknüpfbarkeit von Netzen zu berücksichtigen, die die Kommission nach dem in Artikel 29 vorgesehenen Verfahren ausgearbeitet hat.

2. Für die Übertragung personenbezogener Daten über Netze sind Verfahren zu wählen, die eine angemessene Sicherheit gewährleisten.

3. Bei dem Datenabruf im automatischen Verfahren sind die Geräte und die Programme so zu gestalten, daß die Abfrage sich im Rahmen der vom Dateiverantwortlichen erteilten Berechtigung hält.

4. Die in den Absätzen 1 bis 3 genannten Pflichten obliegen auch den Personen, die tatsächlich oder aufgrund eines Vertrages die auf Dateien bezogenen Verarbeitungsvorgänge kontrollieren.

5. Jede Person, die im Rahmen ihrer beruflichen Tätigkeit Zugang zu in den Dateien gespeicherten Informationen hat, darf diese Dritten nicht ohne das Einverständnis des Verantwortlichen der Datei mitteilen.

KAPITEL VI

SONDERBESTIMMUNGEN FÜR BESTIMMTE BEREICHE

Artikel 19

Die Mitgliedstaaten können für Presseorgane und audiovisuelle Medien von dieser Richtlinie abweichende Bestimmungen vorsehen, soweit diese erforderlich sind, um das Recht auf Privatsphäre mit den für die Informations- und Pressefreiheit geltenden Vorschriften in Einklang zu bringen.

Artikel 20

Die Mitgliedstaaten ermutigen die Berufs- und Standesvertretungen auf der Grundlage der in dieser Richtlinie enthaltenen Prinzipien an der Ausarbeitung von europäischen Standes- oder Verhaltensregeln für bestimmte Bereiche mitzuwirken.

KAPITEL VII

Haftung und Sanktionen

Artikel 21

Haftung

1. Die Mitgliedstaaten sehen in ihren Rechtsvorschriften vor, daß jede Person, deren personenbezogene Daten in einer Datei gespeichert sind und die wegen der Verarbeitung oder jeder anderen mit den Bestimmungen dieser Richtlinie unvereinbaren Maßnahmen einen Schaden erleidet, das Recht hat, von dem Verantwortlichen der Datei Schadensersatz zu verlangen.

2. Die Mitgliedstaaten können bestimmen, daß Schäden wegen Verlusts oder Zerstörung von Daten oder wegen unbefugtem Zugangs dem Verantwortlichen der Datei nicht zugerechnet werden können, wenn er nachweist, daß er angemessene Maßnahmen getroffen hat, um den in Artikel 18 und 22 genannten Anforderungen zu genügen.

Artikel 22

Verarbeitung im Auftrag des Dateiverantwortlichen

1. Die Mitgliedstaaten sehen in ihren Rechtsvorschriften vor, daß sich der Verantwortliche der Datei im Fall einer Verarbeitung in seinem Auftrag vergewissern muß, daß die erforderlichen Sicherheits- und organisatorischen Maßnahmen getroffen werden; er muß eine Person oder ein Unternehmen wählen, die bzw. das in dieser Hinsicht ausreichende Gewähr bietet.

2. Jede Person, die personenbezogene Daten im Auftrag des Verantwortlichen der Datei erhebt oder verarbeitet, hat den Pflichten nach Artikel 16 und 18 dieser Richtlinie nachzukommen.

3. Der Vertrag bedarf der Schriftform und hat insbesondere die Bestimmung zu enthalten, daß die personenbezogenen Daten durch den Auftragnehmer oder seine Beschäftigten nur mit Zustimmung des Verantwortlichen der Datei weitergegeben werden dürfen.

Artikel 23

Sanktionen

Jeder Mitgliedstaat sieht in seinen Rechtsvorschriften die Anwendung von ausreichenden Sanktionen vor, um die Einhaltung der zur Durchführung dieser Richtlinie erlassenen Bestimmungen zu gewährleisten.

KAPITEL VIII

Weitergabe personenbezogener Daten in Drittländer

Artikel 24

Grundsätze

1. Die Mitgliedstaaten sehen in ihren Rechtsvorschriften vor, daß die vorübergehende oder endgültige Weitergabe personenbezogener Daten, die Gegenstand einer Verarbeitung oder zu diesem Zweck gesammelt sind, in ein Drittland nur stattfinden kann, wenn dieses Land ein angemessenes Schutzniveau gewährleistet.

2. Die Mitgliedstaaten teilen der Kommission Fälle mit, in denen ein Daten einführendes Drittland kein angemessenes Schutzniveau gewährleistet.

3. Stellt die Kommission auf der Grundlage von Informationen der Mitgliedstaaten oder auf der Grundlage anderer Informationen fest, daß ein Drittland kein angemessenes Schutzniveau aufweist und dies für die Interessen der Gemeinschaft oder eines Mitgliedstaats nachteilig ist, so kann sie Verhandlungen einleiten, um eine Lösung für diese Situation herbeizuführen.

4. Die Kommission kann nach dem Verfahren gemäß Artikel 30 Absatz 2 dieser Richtlinie feststellen, daß ein Drittland aufgrund der von ihm eingegangenen internationalen Verpflichtungen oder seiner innerstaatlichen Rechtsvorschriften ein angemessenes Schutzniveau gewährleistet.

5. Die im Rahmen dieses Artikels getroffenen Maßnahmen entsprechen den Pflichten der Gemeinschaft aufgrund bilateraler und multilateraler internationaler Abkommen, die den Schutz von Personen im Hinblick auf die automatisierte Verarbeitung personenbezogener Daten regeln.

Artikel 25

Ausnahmebestimmung

1. Ein Mitgliedstaat kann von den Bestimmungen des Artikels 24 Absatz 1 für eine bestimmte Datenübermittlung ins Ausland abweichen, wenn der Verantwortliche der Datei ausreichend glaubhaft macht, daß die Einhaltung eines angemessenen Schutzniveaus sichergestellt ist. Der Mitgliedstaat kann eine Ausnahme nur nach vorheriger Unterrichtung der Kommission und der Mitgliedstaaten gewähren, wenn weder ein Mitgliedstaat noch die Kommission innerhalb einer Frist von zehn Tagen Widerspruch erheben.

2. Wird Widerspruch erhoben, so trifft die Kommission gemäß dem Verfahren nach Artikel 30 Absatz 2 die geeigneten Maßnahmen.

KAPITEL IX

KONTROLLBEHÖRDEN UND GRUPPE FÜR DEN SCHUTZ PERSONENBEZOGENER DATEN

Artikel 26

Die Kontrollbehörde

1. Die Mitgliedstaaten tragen dafür Sorge, daß eine unabhängige Behörde den Schutz personenbezogener Daten kontrolliert. Diese Behörde hat den Auftrag, die Anwendung der in Durchführung dieser Richtlinie erlassenen einzelstaatlichen Bestimmungen zu überwachen und alle Aufgaben wahrzunehmen, die ihr durch diese Richtlinie zugewiesen sind.

2. Diese Behörde verfügt über Untersuchungsbefugnisse und wirksame Eingriffsmöglichkeiten gegen die Einrichtung und Nutzung von Dateien, die den Bestimmungen dieser Richtlinie nicht entsprechen. Dazu verfügt sie

insbesondere über das Zugriffsrecht auf die Dateien, die unter diese Richtlinie fallen; sie muß dafür alle für die Erfüllung ihrer Kontrollaufgabe erforderlichen Informationen sammeln können.

3. Jedermann kann sich an diese Behörde wenden mit einer Eingabe oder Beschwerde in bezug auf den Schutz von Personen im Hinblick auf die Verarbeitung personenbezogener Daten.

Artikel 27

Gruppe für den Schutz personenbezogener Daten

1. Es wird eine Gruppe für den Schutz personenbezogener Daten eingesetzt. Diese unabhängige Gruppe mit beratender Funktion setzt sich aus Vertretern der in Artikel 26 vorgesehenen Kontrollbehörden aus allen Mitgliedstaaten zusammen; den Vorsitz führt ein Vertreter der Kommission.

2. Das Sekretariat der Gruppe für den Schutz personenbezogener Daten führen die Dienststellen der Kommission.

3. Die Gruppe für den Schutz personenbezogener Daten gibt sich ihre Geschäftsordnung.

4. Die Gruppe für den Schutz personenbezogener Daten prüft die Fragen, die ihr Vorsitzender von sich aus oder auf begründeten Antrag eines Vertreters der Kontrollbehörden auf die Tagesordnung gesetzt hat und die sich auf die Anwendung der gemeinschaftsrechtlichen Bestimmungen im Bereich des Schutzes personenbezogener Daten beziehen.

Artikel 28

Aufgaben der Gruppe für den Schutz personenbezogener Daten

1. Die Gruppe für den Schutz personenbezogener Daten hat die Aufgabe

a) zur einheitlichen Anwendung der zur Durchführung dieser Richtlinie erlassenen einzelstaatlichen Vorschriften beizutragen;

b) zum Schutzniveau in der Gemeinschaft und den Drittländern Stellung zu nehmen;

c) die Kommission zu Vorhaben zusätzlicher oder besonderer Maßnahmen zur Erhaltung des Schutzes der Privatsphäre zu beraten.

2. Stellt die Gruppe für den Schutz personenbezogener Daten fest, daß sich im Bereich des Schutzes personenbezogener Daten zwischen den Rechtsvorschriften oder der Praxis der Mitgliedstaaten schwerwiegende Unterschiede ergeben, die die Gleichwertigkeit des Schutzes in der Gemeinschaft zu beeinträchtigen drohen, so teilt sie dies der Kommission mit.

3. Die Gruppe für den Schutz personenbezogener Daten kann zu allen Fragen, die den Schutz von Personen im Hinblick auf personenbezogene Daten in der Gemeinschaft betreffen, Empfehlungen abgeben. Diese Empfehlungen werden in den Sitzungsbericht aufgenommen und können dem in Artikel 30 genannten Beratenden Ausschuß übermittelt werden. Die Kommission teilt der Gruppe für den Schutz personenbezogener Daten mit, wie sie mit den Empfehlungen weiter verfahren ist.

4. Die Gruppe für den Schutz personenbezogener Daten erstellt einen Jahresbericht über den Stand des Schutzes der Personen im Hinblick auf die Verarbeitung personenbezogener Daten in der Gemeinschaft und in den Drittländern, den sie der Kommission übermittelt.

KAPITEL X

RECHTSETZUNGSBEFUGNIS DER KOMMISSION

Artikel 29

Ausübung der Rechtsetzungsbefugnis

Gemäß dem Verfahren nach Artikel 30 Absatz 2 trifft die Kommission die für die Anwendung dieser Richtlinie auf die Besonderheiten bestimmter Bereiche erforderlichen ergänzenden Maßnahmen unter Berücksichtigung des einschlägigen technischen Standes und der Verhaltensregeln.

Artikel 30

Beratender Ausschuß

1. Die Kommission wird durch einen Beratenden Ausschuß unterstützt, der sich aus Vertretern der Mitgliedstaaten zusammensetzt und dessen Vorsitz der Vertreter der Kommission führt.

2. Der Vertreter der Kommission unterbreitet dem Ausschuß einen Entwurf der zu treffenden Maßnahmen. Der Ausschuß gibt seine Stellungnahme zu diesem Entwurf innerhalb einer Frist, die der Vorsitzende unter Berücksichtigung der Dringlichkeit der betreffenden Frage - erforderlichenfalls durch eine Abstimmung - festsetzen kann. Die Stellungsnahme wird in das Protokoll aufgenommen; darüber hinaus hat jeder Mitgliedstaat das Recht zu verlangen, daß sein Standpunkt im Protokoll festgehalten wird. Die Kommission berücksichtigt soweit wie möglich die Stellungnahme des Ausschusses. Sie unterrichtet den Ausschuß darüber, inwieweit sie seine Stellungnahme berücksichtigt hat.

SCHLUSSBESTIMMUNGEN

Artikel 31

1. Die Mitgliedstaaten erlassen die erforderlichen Rechts- und Verwaltungsvorschriften, um dieser Richtlinie spätestens am 1. Januar 1993 nachzukommen.

   Die aufgrund des ersten Unterabsatzes erlassenen Vorschriften enthalten eine ausdrückliche Verweisung auf diese Richtlinie.

2. Die Mitgliedstaaten teilen der Kommission den Wortlaut der innerstaatlichen Rechtsvorschriften mit, die sie auf dem unter diese Richtlinie fallenden Gebiet erlassen.

Artikel 32

Die Kommission legt dem Rat und dem Europäischen Parlament regelmäßig einen Bericht über die Durchführung dieser Richtlinie vor, den sie gegebenenfalls mit geeigneten Änderungsvorschlägen verbindet.

Artikel 33

Diese Richtlinie ist an die Mitgliedstaaten gerichtet.

Geschehen zu Brüssel am

Im Namen des Rates
Der Präsident

Fiche Financière

PROPOSITION DE DIRECTIVE DU CONSEIL VISANT AU RAPPROCHEMENT DE CERTAINES DISPOSITIONS LEGISLATIVES, REGLEMENTAIRES ET ADMINISTRATIVES DES ETATS MEMBRES RELATIVES A LA PROTECTION DES PERSONNES A L'EGARD DU TRAITEMENT DES DONNEES A CARACTERE PERSONNEL

1. Ligne budgétaire concernée (éventuellement à créer) :

   A 2511 : Frais de réunions de comités dont la consultation n'est pas un élément obligatoire de la procédure de formation d'actes communautaires.

2. Base légale (ou autre) :

   Article 100 A

3. Proposition de classification en dépense obligatoire/non obligatoire

   (avec justification succincte en vertu de la déclaration commune du 30 juin 1982) :
   non-obligatoire

4. Description et justification de l'action :

   4.1. Objectifs : - assurer la protection des personnes à l'égard des données à caractère personnel,
   - permettre la circulation transfrontière de données à caractère personnel dans la Communauté,
   - permettre le bon fonctionnement du marché intérieur.

   4.2. Création de 2 comités compétents en matière de protection des personnes à l'égard des données à caractère personnel (Art. 27,30)

   personnes concernées : 1. Pour le Comité de protection des données à caractère personnel (Art. 27) : représentants de l'autorité de contrôle de tous les Etats membres (groupe 4)

   2. Pour le Comité consultatif (Art.30) : représentants des Etats membres (groupe 3)

   4.3. Un représentant de la Commission préside le Comité de protection des données à caractère personnel et le Comité consultatif. Le secrétariat du Comité de protection des données à caractère personnel est assuré par les services de la Commission.

5. Nature de la dépense et mode de calcul :

5.1. Nature : réunions
(frais de participation des membres des 2 Comités)

5.2. Calcul : - Comité de protection des données :
24 membres (non-gouvernementals) x 3 réunions
a 2 jours x 1180 ECU (590 ECU/jour) = 84.960 ECU*
- Comité consultatif :
.24 membres (gouvernemental) x 1 réunion a 2 jours x
780 ECU (390 ECU/jour) = 18.720 ECU*

6. Incidence financière de l'action sur les crédits d'intervention :

6.1. Echéancier des crédits d'engagement et de paiement

CE-CP

1993 : 103.680 ECU
1994 : " "
1995 : " "
1996 : " "
1997 : " "

6.2. Part du financement communautaire dans le coût total : 100%

7. Observations :

1. Le Comité de protection des données à caractère personnel (Art. 27) :

Il est institué ce Comité à caractère consultatif et indépendant et est composé de représentants de l'autorité de contrôle de tout les Etats membres, présidé par un représentant de la Commission.

Ce Comité établit son règlement intérieur. Le secrétariat du Comité est assuré par les services de la Commission.

Missions de ce Comité : voir Art.28.

2. Le Comité consultatif (Art.30) :

Il est institué un Comité consultatif composé des représentants des Etats membres, présidé par le représentant de la Commission.

La Commission est assistée par ce Comité afin de prendre les éventuelles mesures complémentaires nécessaires pour adapter les dispositions de la directive aux spécificités de certaines secteurs.

---

* estimation

FICHE D'IMPACT SUR LA COMPETITIVITE ET L'EMPLOI

I. Quelle est la justification principale de la mesure ?

- Assurer la protection des personnes à l'égard des données à caractère personnel.

- Permettre la circulation transfrontière de données à caractère personnel dans la Communauté.

- Permettre le bon fonctionnement du marché intérieur.

II. Caractéristiques des entreprises concernées.

La proposition concerne toutes les entreprises qui utilisent des fichiers de données à caractère personnel quel que soit leur taille ou leur secteur d'activité.

III. Quelles sont les obligations imposées directement aux entreprises ?

Se conformer aux dispositions applicables aux traitements de données à caractère personnel, notamment celles relatives à la légitimité de ces traitements dans le secteur privé.

IV. Quelles sont les obligations susceptibles d'être imposées indirectement aux entreprises via les autorités locales ?

Aucune.

V. Y a-t-il des mesures spéciales pour les PME ?

Non.

VI. Quel est l'effet prévisible ?

a) sur la compétitivité des entreprises ?

Les règles de protection s'appliquent à toutes les entreprises et élimineront les distorsions de concurrence dûes à l'actuelle disparité des législations nationales. En ce qui concerne leur compétitivité internationale, la directive prévoit des négociations avec les pays tiers qui n'assurent pas encore un niveau de protection adéquat.

b) sur l'emploi ?

La directive prévoit la création d'instances de contrôle nationales.

VII. Les partenaires sociaux ont-ils été consultés sur cette proposition ?

Non.

Entwurf einer

ENTSCHLIESSUNG DER IM RAT VEREINIGTEN VERTRETER DER REGIERUNGEN DER MITGLIEDSTAATEN DER EUROPÄISCHEN GEMEINSCHAFTEN

Die im Rat vereinigten Vertreter der Regierungen der Mitgliedstaaten der Europäischen Gemeinschaften

in der Erwägung, daß die Richtlinie des Rates zum Schutz von Personen bei der Verarbeitung personenbezogener Daten den Schutz der Privatsphäre von Personen gewährleistet in bezug auf die Verarbeitung von personenbezogenen Daten, die in Dateien des privaten und des öffentlichen Sektors enthalten sind mit Ausnahme der Dateien des öffentlichen Sektors, insoweit seine Tätigkeiten nicht in den Anwendungsbereich des Gemeinschaftsrechts fallen;

in dem Bestreben, die Zusammenarbeit zwischen den Verwaltungen der Mitgliedstaaten in den Bereichen zu erleichtern, die nicht in den Anwendungsbereich des Gemeinschaftsrechts fallen, und dabei ein hohes Schutzniveau der Privatsphäre der betroffenen Personen sicherzustellen:

in der Erwägung, daß die in der Richtlinie enthaltenen Grundsätze die Prinzipien konkretisieren und erweitern, die in dem Übereinkommen des Europarats vom 26. Januar 1981 zum Schutze des Menschen bei der automatischen Verarbeitung personenbezogener Daten enthalten sind -

kommen wie folgt überein:

Die Regierungen der Mitgliedstaaten verpflichten sich, die erforderlichen Gesetzgebungsverfahren einzuleiten, um die Grundsätze, die in der Richtlinie des Rates zum Schutz von Personen bei der Verarbeitung personenbezogener Daten enthalten sind, auf den öffentlichen Bereich anzuwenden, der nicht in den Anwendungsbereich des Gemeinschaftsrechts fällt.

Erklärung der Kommission betreffend die Anwendung der Grundsätze der Richtlinie zum Schutz von Personen bei der Verarbeitung personenbezogener Daten auf die Organe und Einrichtungen der Europäischen Gemeinschaften

1. Die Kommission bringt den Wunsch zum Ausdruck, daß die Grundsätze der Richtlinie zum Schutz von Personen bei der Verarbeitung personenbezogener Daten ("die Richtlinie") auf die Organe und Einrichtungen der Europäischen Gemeinschaften Anwendung finden.

2. Dazu wird die Kommission sobald wie möglich die erforderlichen Maßnahmen treffen und vorschlagen.

3. Bis diese Maßnahmen getroffen sind, verpflichtet sich die Kommission, die in der Richtlinie enthaltenen Grundsätze auf die Verarbeitung personenbezogener Daten in ihrem Zuständigkeitsbereich anzuwenden.

4. Die Kommission äußert den Wunsch, daß die anderen Organe der Gemeinschaften sich ebenfalls verpflichten, die in der Richtlinie enthaltenen Grundsätze auf die Verarbeitung personenbezogener Daten in ihrem Zuständigkeitsbereich anzuwenden.

VORSCHLAG FÜR EINE SYN 288

RICHTLINIE DES RATES

ZUM SCHUTZ PERSONENBEZOGENER DATEN UND DER PRIVATSPHÄRE IN ÖFFENTLICHEN DIGITALEN TELEKOMMUNIKATIONSNETZEN,

INSBESONDERE IM DIENSTEINTEGRIERENDEN DIGITALEN TELEKOMMUNIKATIONSNETZ (ISDN) UND IN ÖFFENTLICHEN DIGITALEN MOBILFUNKNETZEN

INHALT

A. ZUSAMMENFASSUNG

Die Einführung öffentlicher digitaler Telekommunikationsnetze ist nunmehr in der Gemeinschaft voll angelaufen. Zu Beginn dieses Jahrzehnts werden über 70 % der Fernübertragung, über 50 % der Fernvermittlungsstellen und mehr als 30 % der Ortsvermittlungsstellen auf Digitaltechnologie umgestellt sein.

Die breit angelegte Einführung öffentlicher Digitalkommunikationsnetze in der Gemeinschaft wird, insbesondere mit dem diensteintegrierenden digitalen Telekommunikationsnetz (ISDN) und den neuen digitalen Mobilfunkdiensten, der Allgemeinheit stark verbesserte Kommunikationsfunktionen bieten, erfordert jedoch gleichzeitig ein gemeinschaftsweites gemeinsames Konzept für den Schutz der Privatsphäre und der personenbezogenen Daten sowie für die Datensicherheit im Hinblick auf die spezifischen Anforderungen des neuen digitalen Kommunikationsumfelds.

Der Rat und das Europäische Parlament haben wiederholt die zentrale Bedeutung geeigneter Maßnahmen zum Schutz der Daten und der Privatsphäre bei der künftigen Entwicklung der Kommunikationsdienste in der Europäischen Gemeinschaft anerkannt. Insbesondere forderte das Europäische Parlament in seinen Entschließungen vom 14. Dezember 1988 "Maßnahmen zur Sicherung des Datenschutzes und zur Wahrung der Vertraulichkeit" und erinnerte die Kommission daran, "daß sie die politische Verantwortung dafür trägt, daß gleichzeitig mit der Vorlage der Gesetzgebungsvorschläge zur Öffnung der Telekommunikationsmärkte in den geeigneten juristischen Formen Initiativen zustandekommen, um in der Gemeinschaft personenbezogene Daten ... zu schützen."

In der Gemeinschaft rücken die Auswirkungen digitaler Netze auf den Schutz personenbezogener Daten und der Privatsphäre immer mehr in den Brennpunkt. In einer im August 1989 in Berlin verabschiedeten Entschließung forderten die Datenschutzbeauftragten der Mitgliedstaaten, dem Schutz personenbezogener Daten und der Privatsphäre im Rahmen des ISDN besondere Aufmerksamkeit zu widmen.

Der beigefügte Vorschlag soll diesen spezifischen Anforderungen an den Schutz personenbezogener Daten und der Privatsphäre im Bereich der neuen öffentlichen Digitalkommunikationsnetze gerecht werden. Er wird im Zusammenhang mit - und als Ergänzung zu - den Vorschlägen der Kommission zur Festlegung allgemeiner Rahmenbedingungen für den Datenschutz in der Gemeinschaft unterbreitet.

Der wirksame Schutz personenbezogener Daten und der Privatsphäre wird immer mehr zu einer wesentlichen Voraussetzung für die gesellschaftliche Akzeptanz der neuen Digitalnetze und -dienste. Er muß wesentlicher Bestandteil der gemeinschaftlichen Telekommunikationspolitik sein, die darauf abzielt, dem europäischen Bürger die Vorteile moderner Kommunikationsdienste uneinge
schränkt zu sichern, da sich die Gemeinschaft einem Umfeld nähert, das durch wesentlich mehr Informationen gekennzeichnet sein wird als zuvor.

Der beigefügte Vorschlag für eine Richtlinie des Rates wurde im Hinblick auf dieses Globalziel erarbeitet.

B. BEGRÜNDUNG

I. EINLEITUNG

Die derzeitige breit angelegte Einführung öffentlicher digitaler Telekommunikationsdienste in der Gemeinschaft, insbesondere die Implementierung des diensteintegrierenden digitalen Telekommunikationsnetzes (ISDN)[1] und neuer digitaler Mobilfunkdienste[2] wird der Allgemeinheit stark verbesserte Kommunikationsfunktionen bieten, erfordert jedoch gleichzeitig ein europaweites gemeinsames Konzept für den Schutz der Privatsphäre und der personenbezogenen Daten sowie für die Datensicherheit im Hinblick auf die spezifischen Anforderungen des neuen digitalen Kommunikationsumfelds.

In seiner Entschließung vom 12. Dezember 1986[3] zur koordinierten Einführung des diensteintegrierenden digitalen Telekommunikationsnetzes (ISDN) in der Europäischen Gemeinschaft stellte das Europäische Parlament fest, daß "das künftige diensteintegrierende digitale Telekommunikationsnetz (ISDN) als Fortentwicklung des Telefonnetzes geschäftlichen und privaten Teilnehmern eine Vielzahl zusätzlicher Dienste anbieten wird ...", forderte die Kommission jedoch auf, "Vorschläge zu unterbreiten, wie zweckmäßigerweise vorgegangen werden sollte, um in dem im Entstehen begriffenen europaweiten ISDN-Netz ein einheitliches und den gesteigerten technischen Möglichkeiten dieses neuen Systems angemessenes Niveau des Datenschutzes zu gewährleisten". Das Europäische Parlament unterstrich dieses Anliegen ferner in einem allgemeineren Kontext in seinen Entschließungen vom 14. Dezember 1989[4], in denen es "Maßnahmen zur Sicherung des Datenschutzes und zur Wahrung der Vertraulichkeit" bei der Nutzung von Telekommunikationsnetzen fordert und die Kommission daran erinnert, "daß sie die politische Verantwortung dafür trägt, daß gleichzeitig mit der Vorlage der Gesetzgebungsvorschläge zur Öffnung der Telekommunikationsmärkte in den geeigneten juristischen Formen Initiativen zustandekommen, um in der Gemeinschaft personenbezogene Daten ... zu schützen".

In seiner Entschließung vom 30. Juni 1988[5] billigte der Rat die Grundsätze des Grünbuchs über die Entwicklung des gemeinsamen Marktes für Telekommunikationsdienstleistungen und Telekommunikationsgeräte[6], unterstützte

---

(1) Empfehlung des Rates vom 22. Dezember 1986 über die koordinierte Einführung des diensteintegrierenden digitalen Telekommunikationsnetzes (ISDN) in der Europäischen Gemeinschaft (86/659/EWG).
Das ISDN ist als organische Weiterentwicklung des Telefonnetzes zu sehen. Es ermöglicht über einen einzigen Anschluß und die vorhandene Teilnehmerleitung die Übertragung von Sprache (Telefondienst), Text, Daten und Bildern durch eine Vielzahl effizienterer bzw. neuer Dienste (siehe auch Empfehlung des Rates 86/659/EWG sowie Kapitel II).
Der Ratsempfehlung entsprechend wurden der Kommission bislang zwei Zwischenberichte über die Einführung des ISDN vorgelegt (KOM(88) 589; KOM(90) 123).

(2) Empfehlung des Rates vom 25. Juni 1987 für die koordinierte Einführung eines europaweiten öffentlichen zellularen digitalen terrestrischen Mobilfunkdienstes in der Gemeinschaft (87/371/EWG, Abl. Nr. L 196 vom 17. Juli 1987, S. 81) und Richtlinie des Rates vom 25. Juni 1987 über die Frequenzbänder, die für die koordinierte Einführung eines europaweiten öffentlichen zellularen digitalen terrestrischen Mobilfunkdienstes in der Gemeinschaft bereitzustellen sind (87/372/EWG, ABl. Nr. L 196 vom 17. Juli 1987, S. 85) sowie spätere Vorschläge der Kommission für den Bereich der öffentlichen digitalen Mobilfunkdienste.

(3) Entschließung zur Empfehlung des Rates 86/659/EWG, ABl. C 7 vom 12. Januar 1987, S.334.

(4) Entschließung zur Post und Telekommunikation, ABl. Nr. C 12 vom 16. Januar 1989, S. 69. Entschließung zur Notwendigkeit, die Zersplitterung im Bereich der Telekommunikation zu überwinden, ABl. Nr. C 12 vom 16. Januar 1989, S. 66.

(5) Entschließung des Rates vom 30. Juni 1988 über die Entwicklung des gemeinsamen Marktes für Telekommunikationsdienste und -geräte bis 1992 (ABl. Nr. C 257 vom 4.10.1988, S. 1).

(6) KOM(87) 290.

generell die in der Mitteilung vom 9. Februar 1988[7] aufgeführten Ziele des Aktionsprogramms und nannte als eines der Hauptziele, "die personenbezogenen Daten zu schützen und den Zugang des einzelnen - auf dem Wege über die Kommunikationsmedien - zu einem Umfeld sicherzustellen, das durch weitaus mehr Informationen als zuvor gekennzeichnet sein wird".

In seiner Entschließung über eine verstärkte Koordinierung bei der Einführung des diensteintegrierenden digitalen Telekommunikationsnetzes (ISDN) in der Europäischen Gemeinschaft bis 1992[8] erläuterte der Rat sein Anliegen in bezug auf das ISDN und nannte als notwendige Maßnahme "weitere Diskussionen auf europäischer Ebene über die Anforderungen des Schutzes der Privatsphäre der Nutzer und der Sicherheit des Nachrichtenverkehrs im Zusammenhang mit den neuen Diensten, im Sinne der Entschließung des Europäischen Parlaments vom 12. Dezember 1986 zur Empfehlung 86/659/EWG".

Die Vertreter der Datenschutz-Kontrollinstanzen der Mitgliedstaaten verabschiedeten auf ihrer elften internationalen Konferenz vom 28. bis 31. August 1989 in Berlin eine Entschließung, in der gefordert wird, daß dem Schutz der Daten und der Privatsphäre im Zusammenhang mit dem ISDN besondere Aufmerksamkeit zu widmen ist.

Mit dem beigefügten Vorschlag erfüllt die Kommission diese Forderung nach gemeinschaftsweiten spezifischen Maßnahmen zum Schutz personenbezogener Daten und der Privatsphäre bei der Einführung der neuen öffentlichen digitalen Telekommunikationsnetze, insbesondere des diensteintegrierenden digitalen Telekommunikationsnetzes und der öffentlichen digitalen Mobilfunknetze. Sie berücksichtigt die Tatsache, daß eine tiefe - und begründete - Besorgnis hinsichtlich der unmittelbaren Auswirkungen digitaler Netze auf den Schutz personenbezogener Daten und der Privatsphäre besteht. Die Kommission hat ferner den Schutz der Daten und der Privatsphäre als grundlegende Voraussetzung bei der Entwicklung eines Umfeldes für offenen Netzzugang in der Gemeinschaft anerkannt[9].

Der Vorschlag ist vor dem Hintergrund der Diskussionen und allgemeinen Grundsätze für den Schutz personenbezogener Daten zu sehen, die in Europa durch das Übereinkommen des Europarates von 1981 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten festgelegt worden sind. Dieses Übereinkommen ist bislang von sieben Mitgliedstaaten der Gemeinschaft ratifiziert worden. Der Vorschlag wird im Zusammenhang mit - und als Ergänzung zu - den Vorschlägen der Kommisson zur Festlegung allgemeiner Rahmenbedingungen für den Datenschutz in der Gemeinschaft vorgelegt. Dabei handelt es sich insbesondere um den Entwurf eines Vorschlages einer Ratsrichtlinie über die Angleichung bestimmter Rechts- und Verwaltungsvorschriften der Mitgliedstaaten zum Schutz des Menschen bei der Verarbeitung personenbezogener Daten, den Entwurf eines Vorschlags einer Ratsentscheidung über die Eröffnung von Verhandlungen im Hinblick auf den Beitritt der Europäischen Wirtschaftsgemeinschaft, im Rahmen ihrer Zuständigkeiten, zu dem Übereinkommen des Europarates zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten, sowie den Entwurf eines Vorschlags einer Ratsentscheidung über die Sicherheit von Informationssystemen; zusätzlich wird die

---

(7) Auf dem Wege zu einem wettbewerbsfähigen EG-weiten Telekommunikationsmarkt im Jahre 1992: Zur Verwirklichung des Grünbuches über die Entwicklung des gemeinsamen Marktes für Telekommunikationsdienstleistungen und Telekommunikationsgeräte. Stand der Diskussionen und Vorschläge der Kommission (KOM(88) 48).

(8) ABl. Nr. C 196 vom 1. August 1989, S. 4.

(9) Gemeinsamer Standpunkt des Rates vom 05.02.1990 im Hinblick auf die Genehmigung der Richtlinie zur Verwirklichung des Binnenmarktes für Telekommunikationsdienste durch Einführung eines Offenen Netzzugangs (ONP), ABl. .....

Kommission interne Regelungen erarbeiten, die darauf abzielen, den Betroffenen ein Niveau des Datenschutzes zu garantieren, das den Grundsätzen der oben genannten Ratsrichtlinie entspricht.

Die beigefügte Richtlinie fügt sich in diesen allgemeinen Rahmen ein und enthält die notwendigen Sonderbestimmungen zur Angleichung der Rechts- und Verwaltungsvorschriften der Mitgliedstaaten zum Schutz personenbezogener Daten und der Privatsphäre im Zusammenhang mit öffentlichen, ortsfesten und mobilen Digitalkommunikationsnetzen und den neuen "intelligenten" Funktionen, die damit bereitgestellt werden.

II. DIE NEUEN SPEZIFISCHEN ANFORDERUNGEN AN DEN SCHUTZ PERSONENBEZOGENER DATEN UND DER PRIVATSPHÄRE IM TELEKOMMUNIKATIONSSEKTOR

Die "Digitalisierung" der öffentlichen Telekommunikationsnetze ist nunmehr in der Gemeinschaft voll angelaufen. Zu Beginn dieses Jahrzehnts werden über 70 % der Fernübertragung, über 50 % der Fernvermittlungsstellen und mehr als 30 % der Ortsvermittlungsstellen auf Digitaltechnologie umgestellt sein.

Digitalisierung bedeutet Einführung der EDV bei allen Vermittlungsvorgängen sowie bei der Verarbeitung und Übertragung sämtlicher Informationen (Sprache, Daten, Bilder) in Form von Binärziffern[10] über Telekommunikationsnetze. Auf die so erzeugten "Bitströme" kann durch die Intelligenz der Computer direkt zugegriffen werden, sowohl innerhalb des Netzes als auch im Teilnehmer-Endgerät. Dies führt zu einem höheren Qualitätsniveau der Dienste, das mit den herkömmlichen "Analogtechniken" nicht erreicht wird, sowie zu einer Vielzahl "intelligenter" Funktionen, die ein breites Spektrum neuer Aktivitäten über Telekommunikationsnetze ermöglichen. Eine vollständig vom Endgerät zu Endgerät durchlaufende digitale Kommunikation wird mit dem künftigen diensteintegrierenden digitalen Telekommunikationsnetz und den neuen öffentlichen digitalen Mobilfunksystemen[11] angeboten.

In bezug auf den Datenschutz ergeben sich aus der Einführung öffentlicher Digitalnetze hauptsächlich zwei Konsequenzen.

Einerseits bieten die voll computergestützten Techniken, wie sie heute zur Verfügung stehen, einen wesentlich höheren Grad an Datensicherheit für individuelle Anforderungen wie hochwertige Verschlüsselungstechniken.

Andererseits besteht aufgrund der Digitalverarbeitung sowohl operationeller als auch anrufbezogener Daten und der Bearbeitung durch computergestützte Vermittlungsstellen theoretisch - d.h. ohne entsprechende Datenschutzmaßnahmen - die Möglichkeit, anrufspezifische Daten wie etwa die Herkunft des Anrufs systematisch zu speichern und zu verfolgen. Dies ließ sich bei den herkömmlich analogen, "nichtintelligenten" Netzen nur mit erheblichem technischen Aufwand erreichen; daher wurde von dieser Möglichkeit nur unter außergewöhnlichen Umständen Gebrauch gemacht.

Gleichzeitig ermöglichen die neuen intelligenten Kommunikationsfunktionen, wie sie im Rahmen der ISDN-"Zusatzdienste"[12] definiert sind, wesentliche zusätzliche

---

(10) Der Computer verarbeitet sämtliche Informationen in Form von "Binärziffern", d.h. er zerlegt sie in elementare Informationseinheiten (Bits) mit dem Wert 0 bzw. 1.

(11) Siehe auch Empfehlung des Rates 86/659/EWG und 87/371/EWG, obige Fußnoten 1 und 2.

(12) Einzelheiten siehe Empfehlung des Rates 86/659/EWG, obige Fußnote 1.

Dienstmerkmale für den Teilnehmer, die mehr Dienstqualität und Verbraucherschutz bieten, wie z.B. den Einzelgebührennachweis. Diese Funktionen erfordern jedoch spezielle Maßnahmen und Vorschriften, um den Schutz der Privatsphäre in dem neuen Umfeld zu gewährleisten.

Daher wirft die Einführung digitaler Kommunikationsnetze in der Gemeinschaft in bezug auf den Schutz personenbezogener Daten grundlegende spezielle Fragen auf, die zu lösen sind, z.B. die Behandlung:

- von personenbezogenen Informationen, die in zunehmendem Maße in elektronischen Teilnehmerdateien gespeichert werden;
- von Verkehrs- und sonstigen Betriebsdaten;
- von Daten für Einzelgebührennachweise;
- der Rufnummeranzeige (Identifizierung der Herkunft des Anrufs);
- der Anrufweiterschaltung zu dritten Teilnehmern;
- unerbetener Anrufe;
- spezieller technischer Merkmale von Endgeräten und sonstigen Einrichtungen, die gegebenenfalls erforderlich sind, um einen angemessenen Schutz zu gewährleisten.

Die allgemeinen Bestimmungen über den Schutz personenbezogener Daten, die im Übereinkommen des Europarats vorgesehen sind und mit der obenerwähnten Initiative der Kommission auch in der Gemeinschaft eingeführt werden sollen, bilden zwar einen generellen Rahmen, sehen jedoch nicht die spezifischen Einzelmaßnahmen vor, die zur Lösung der obigen Probleme erforderlich sind.

Die allgemeinen Bestimmungen über den Schutz personenbezogener Daten können nicht verhindern, daß in den Mitgliedstaaten laufend abweichende Rechts- und Verwaltungsvorschriften für den Betrieb der künftigen Digitalnetze erlassen werden, die den Gemeinsamen Markt sowohl für Telekommunikationsdienste als auch für Endgeräte sehr bald in Frage stellen könnten.

Beispielsweise sehen einige Mitgliedstaaten für die Anzeige der Rufnummer vor, daß der Anrufer diese Funktion von Fall zu Fall unterdrücken kann. Falls dies über eine Taste am Telefonapparat erfolgen soll, während andere Betreiber beschließen, die Funktion über einen Code vor der Wahl der Rufnummer zu eliminieren, würde dies Probleme für den freien Verkehr der Endgeräte in der Gemeinschaft aufwerfen.

Ein Vergleich der bestehenden einzelstaatlichen Bestimmungen zeigt erhebliche Diskrepanzen in bezug auf Inhalt und Art der verwendeten rechtlichen Kodifizierung. Unter diesen Umständen entwickelt sich in der Gemeinschaft eine rechtliche Unsicherheit im Bereich der Kommunikationsnetze und -dienste, die das grenzüberschreitende Angebot an Diensten erheblich zu behindern droht.

Ohne eine Richtlinie über die notwendigen speziellen Bestimmungen zur Umsetzung der allgemeinen Grundsätze für den Schutz der Daten und der Privatsphäre in öffentlichen, digitalen, ortsfesten und mobilen Netzen wäre es unmöglich, abweichende Entwicklungen in der Gemeinschaft zu verhindern.

Gleichzeitig werden gemeinschaftsweite Vorkehrungen für den wirksamen Schutz personenbezogener Daten und der Privatsphäre zu einer wesentlichen Voraussetzung

für die gesellschaftliche Akzeptanz der neuen Digitalnetze und -dienste. Dies wurde vom Rat auf seiner Sitzung vom 7. November 1989 bestätigt, indem er zu den sozialen Aspekten der Telekommunikationsdienste feststellte, daß der Schutz der Privatsphäre und der personenbezogenen Daten in einer europäischen Perspektive erhalten bleiben muß.

Der beiliegende Vorschlag für eine Richtlinie des Rates soll diesen spezifischen Anforderungen gerecht werden.

III. DAS VORGESCHLAGENE KONZEPT: DIE BESTIMMUNGEN DES RICHTLINIENENTWURFS

Globalziel der vorgeschlagenen Richtlinie ist es, gemeinschaftsweit ein Mindestniveau für den Schutz personenbezogener Daten und der Privatsphäre des europäischen Bürgers zu gewährleisten. Dieses sollte im allgemeinen Angebot an neuen digitalen Telekommunikationsdiensten vorgesehen sein, wobei für Anforderungen an ein erhöhtes Niveau der Datensicherheit für besondere Fälle und Anwendungen spezifische Maßnahmen im Rahmen des Arbeitsplans zu entwickeln sind, der im obengenannten Vorschlag der Kommission für einen Ratsbeschluß über die Sicherheit in Informationssystemen festgelegt worden ist.

Die vorgeschlagene Richtlinie zielt auf die Sicherung eines Mindestumfangs an Schutzmaßnahmen für den Teilnehmer in der neuen Digitalumgebung ab. Hierzu werden zwei Hauptprinzipien herausgearbeitet:

- Minimierung des Mißbrauchrisikos. Hierzu sind die bei öffentlichen Telekommunikationsdiensten verarbeiteten und gespeicherten Daten auf das strikte Minimum zu begrenzen, das zur Gewährleistung eines ordnungsgemäßen Betriebs, sowie einer angemessenen Qualität der Dienste und der Teilnehmereinrichtungen notwendig ist.

- Gewährleistung des uneingeschränkten Rechts des Teilnehmers auf informationelle Selbstbestimmung, sowohl gegenüber der Telekommunikationsorganisation, die die Dienste erbringt, als auch gegenüber dem zweiten Teilnehmer einer Fernsprechverbindung sowie gegenüber Dritten, die Zugang zu den über ein öffentliches Kommunikationsnetz übertragenen oder bereitgestellten Daten haben wollen.

Da die tiefgreifendsten Auswirkungen des neuen Kommunikationsumfelds auf den Teilnehmer den Telefondienst betreffen, konzentriert sich der Richtlinienvorschlag auf diesen Bereich. Er sieht jedoch vor, die Bestimmungen für den Fernsprechdienst gegebenenfalls auf andere öffentliche digitale Telekommunikationsdienste anzuwenden; dies gilt beispielsweise für öffentliche Datenübertragungsdienste im Rahmen des ISDN sowie für öffentliche paket- und leitungsvermittelte Datennetze und sonstige öffentliche Kommunikationsdienste.

Angesichts der Übergangsphase, in der sich die öffentlichen Kommunikationsnetze in der Gemeinschaft derzeit befinden, und insbesondere aufgrund der Tatsache, daß bestimmte "speicherprogrammierte" Vermittlungsstellen (SPC), wenngleich noch nicht vollständig digitalisiert, die betreffenden intelligenten Funktionen bereits teilweise anbieten, sieht der Richtlinienvorschlag vor, daß Mitgliedstaaten, die das diensteintegrierende digitale Telekommunikationsnetz bzw. öffentliche digitale Mobilfunknetze noch nicht eingeführt haben, die Bestimmungen der Richtlinie insoweit anwenden, als sie auch für Dienste in Analognetzen gelten.

Auf der Basis dieser allgemeinen Grundsätze geht es in der vorgeschlagenen Richtlinie insbesondere um folgendes: die Erfassung, Speicherung und Verarbeitung personenbezogener Daten in der Teilnehmerdatei; die Speicherung und Verarbeitung von Verkehrs- und Gebührendaten, insbesondere zur Erstellung von Einzelgebührennachweisen; das Problem der Rufnummernanzeige; Zugriff auf die Daten durch Dritte; unerbetene Anrufe und die gegebenenfalls notwendigen Verfahren zur Festlegung spezieller technischer Normen.

Nachstehend werden die Artikel der Richtlinie kurz erläutert:

Artikel 1 und 2 beschreiben die Globalziele der Richtlinie und ihre Anwendung auf den Schutz personenbezogener Daten und der Privatsphäre bei der Erbringung öffentlicher Telekommunikationsdienste in öffentlichen digitalen Telekommunikationsnetzen der Gemeinschaft.

Artikel 3 enthält Definitionen wichtiger Begriffe im Sinne der obengenannten Gemeinsamen Position des Rates zu einer Richtlinie zur Einführung eines offenen Netzzugangs (ONP)[13].

Der allgemeine Grundsatz in Artikel 4, wonach die Erfassung, Speicherung und Verarbeitung personenbezogener Daten durch eine Telekommunikationsorganisation nur im Hinblick auf die Bereitstellung des betreffenden Dienstes zulässig ist und diese Daten nicht ohne besondere Rechtsgrundlage oder ohne vorherige registrierte Zustimmung des Teilnehmers für andere Zwecke verwendet werden dürfen, wird in Artikel 5 auf das Anlegen von Teilnehmerdateien angewandt. Wie in den Erwägungsgründen ausgeführt, darf die Erfassung, Speicherung und Verarbeitung personenbezogener Daten vor allem nicht dazu dienen, einer Telekommunikationsorganisation einen unzulässigen Wettbewerbsvorteil gegenüber anderen Diensteanbietern zu verschaffen.

Artikel 6 nennt die Rechte des Teilnehmers in bezug auf seine personenbezogenen Daten, die bei einer Telekommunikationsorganisation gespeichert sind. In Artikel 7 ist der Grundsatz niedergelegt, daß diese Daten ohne Zustimmung des Teilnehmers oder Rechtsgrundlage nicht an Dritte weitergegeben werden dürfen.

Artikel 8 soll einen angemessenen Schutz der Daten gegen unbefugten Zugriff gewährleisten.

Mit Artikel 9 und 10 wird die Erfassung, Speicherung und Verarbeitung personenbezogener Daten, soweit sie für Telekommunikationszwecke benötigt werden, auf Gebühren- und Verkehrsdaten beschränkt. Mit Artikel 11 soll die Privatsphäre der Teilnehmer, d.h. das Recht auf Anonymität des angerufenen Teilnehmers, in bezug auf Einzelgebührennachweise geschützt werden.

Artikel 12 und 13 enthalten ausführliche Bestimmungen hinsichtlich der Anzeige der Nummer des anrufenden Teilnehmers. Die Möglichkeit, die Rufnummernanzeige auszuschließen, sollte angeboten werden, da u.a. Teilnehmer, die Rehabilitationszentren für Drogen- und Alkoholabhängige, Unterkünfte für mißhandelte Familienmitglieder oder psychologische Beratungsstellen anrufen, ein berechtigtes Interesse daran haben, daß ihre Anonymität nicht durch diese Funktion preisgegeben wird; gleiches gilt für Notrufdienste für Selbstmordgefährdete und AIDS-Kranke.

Der angerufene Teilnehmer kann jedoch ein legitimes Interesse daran haben, nur identifizierte Anrufe zu erhalten. Um das Recht auf informationelle Selbstbestimmung

(13) Siehe Fußnote 9.

sowohl für den Anrufer als auch für den angerufenen Teilnehmer zu sichern, muß letzterer die Entgegennahme ankommender Verbindungen auf diejenigen beschränken können, die die Nummer des anrufenden Teilnehmers angeben.

Ferner sollten die Telekommunikationsorganisationen eine Blockierfunktion vorsehen, die die Eliminierung der Anzeige bei Störanrufen verhindert; diese Funktion ist auch für die Verfolgung von Straftaten sowie bei Notrufdiensten, insbesondere für Feuerwehren, bereitzustellen, um einen Mißbrauch dieser Dienste zu verhindern.

Artikel 14 gewährleistet den Schutz der Privatsphäre sowohl des rufenden als auch des angerufenen Teilnehmers bei Anrufweiterschaltung.

Artikel 15 zielt darauf ab, mit technischen Mitteln zu verhindern, daß der Inhalt von Telefongesprächen gespeichert und/oder Dritten zugänglich gemacht wird, ohne daß der Anrufer zuvor darüber informiert wird.

Artikel 16 und 17 sollen die unzulässige Verwendung personenbezogener Daten zur Erstellung von Verbraucherprofilen durch Teleshopping- und Videotext-Dienste verhindern und die Privatsphäre des Teilnehmers gegen unerbetene Anrufe, z.B. zu Werbungszwecken, schützen.

Artikel 18 soll verhindern, daß die Einführung technischer Funktionen aufgrund von Datenschutzanforderungen zu unzulässigen Einschränkungen des freien Verkehrs von Telekommunikationsgeräten und -diensten in der Gemeinschaft führt. Hierzu sind gegebenenfalls gemeinsame europäische Normen für die Implementierung technischer Sondermerkmale zu erarbeiten. Im Sinne der Richtlinie des Rates zur Angleichung der Rechtsvorschriften der Mitgliedstaaten über Telekommunikationsendgeräte einschließlich der gegenseitigen Anerkennung ihrer Konformität[14] und des Ratsbeschlusses 87/95/EWG vom 22. Dezember 1986 über die Normung auf dem Gebiet der Informationstechnik und der Telekommunikation[15] sind mit den technischen Arbeiten die entsprechenden europäischen Normungsgremien, insbesondere das Europäische Institut für Telekommunikationsnormen (ETSI) und CEN/CENELEC zu beauftragen.

Die Schlußbestimmungen in Artikel 19 bis 25 betreffen den Geltungsbereich, die notwendigen Verfahren zur Anpassung dieser Richtlinie an neue technische Entwicklungen sowie die Konsultationsverfahren. Vorgesehen ist, daß die Kommission bei der Durchführung der Richtlinie von einem Ausschuß aus Vertretern der Datenschutzbeauftragten der Mitgliedstaaten und einem Ausschuß aus Vertretern der Mitgliedstaaten unterstützt wird. Diese Ausschüsse sind dem Vorschlag zufolge diejenigen, die für die Zwecke des parallel hierzu vorgelegten Vorschlags einer Ratsrichtlinie über die Angleichung bestimmter Rechts- und Verwaltungsvorschriften der Mitgliedstaaten zum Schutz des Menschen bei der Verarbeitung personenbezogener Daten vorgesehen sind, werden jedoch speziell für die Zwecke dieser Richtlinie eingesetzt.

---

(14) KOM(89) 289 - SYN 204 vom 27.7.1989.

(15) ABl. Nr. L 36 vom 7. Februar 1987, S. 31.

IV. SCHLUSSFOLGERUNGEN

Ein wirksamer, gemeinschaftsweiter Schutz der personenbezogenen Daten und der Privatsphäre wird immer mehr zu einer wesentlichen Voraussetzung für die gesellschaftliche Akzeptanz der neuen digitalen Netze und Dienste.

Ohne eine Richtlinie über die notwendigen speziellen Bestimmungen zur Verwirklichung der allgemeinen Grundsätze des Schutzes personenbezogener Daten und der Privatsphäre in bezug auf die spezifischen Anforderungen öffentlicher, ortsfester und mobiler Digitalnetze lassen sich abweichende Entwicklungen in der Gemeinschaft nicht verhindern, die den gemeinsamen Markt für Telekommunikationsdienste und Endgeräte sehr bald in Frage stellen würden.

Diese speziellen Bestimmungen sind im beiliegenden Richtlinienentwurf vorgesehen.

Der Rat wird daher gebeten, den beiliegenden Vorschlag für eine Richtlinie anzunehmen.

VORSCHLAG FÜR EINE RICHTLINIE DES RATES ZUM SCHUTZ PERSONENBEZOGENER DATEN UND DER PRIVATSPHÄRE IN ÖFFENTLICHEN DIGITALEN TELEKOMMUNIKATIONSNETZEN, INSBESONDERE IM DIENSTEINTEGRIERENDEN DIGITALEN TELEKOMMUNIKATIONSNETZ (ISDN) UND IN ÖFFENTLICHEN DIGITALEN MOBILFUNKNETZEN

SYN 288

DER RAT DER EUROPÄISCHEN GEMEINSCHAFTEN -

Gestützt auf den Vertrag zur Gründung der Europäischen Wirtschaftsgemeinschaft, insbesondere auf Artikel 100a,

auf Vorschlag der Kommission[1],

in Zusammenarbeit mit dem Europäischen Parlament[2],

nach Stellungnahme des Wirtschafts- und Sozialausschusses[3],

in Erwägung nachstehender Gründe:

1. Die Richtlinie des Rates ..... zum Schutz von Personen bei der Verarbeitung personenbezogener Daten sieht vor, daß die Mitgliedstaaten den Schutz der Privatsphäre sicherstellen.

2. Gegenwärtig werden in der Europäischen Gemeinschaft zukunftsorientierte öffentliche digitale Telekommunikationsnetze eingeführt, die spezielle Anforderungen an den Schutz personenbezogener Daten und der Privatsphäre des Benutzers mit sich bringen.

3. Dies gilt insbesondere für die Einführung des diensteintegrierenden digitalen Telekommunikationsnetzes (ISDN) und öffentlicher digitaler Mobilfunknetze.

4. In seiner Entschließung vom 30. Juni 1988 über die Entwicklung des gemeinsamen Marktes für Telekommunikationsdienste und -geräte bis 1992[4] hat der Rat Maßnahmen zum Schutz personenbezogener Daten gefordert, um ein geeignetes Umfeld für die künftige Entwicklung der Telekommunikationsdienste in der Gemeinschaft zu schaffen. In seiner Entschließung vom 18. Juli 1989 über eine verstärkte Koordinierung bei der Einführung des diensteintegrierenden digitalen Telekommunikationsnetzes (ISDN) in der Europäischen Gemeinschaft[5] betonte der Rat erneut die Bedeutung des Schutzes personenbezogener Daten und der Privatsphäre.

---

(1) ...
(2) ...
(3) ...
(4) ABl. Nr. C 257 vom 4.10.1988, S. 1.
(5) ABl. Nr. C 196 vom 1.8.1989, S. 4.

5. Das Europäische Parlament hat auf die Bedeutung des Schutzes personenbezogener Daten und der Privatsphäre in Telekommunikationsnetzen, insbesondere bei der Einführung des diensteintegrierenden digitalen Telekommunikationsnetzes (ISDN)[6][7][8], hingewiesen.

6. In der Empfehlung der Kommission 81/679/EWG werden die Mitgliedstaaten aufgefordert, die Konvention des Europarates zum Schutz von Personen hinsichtlich der automatischen Verarbeitung personenbezogener Daten anzunehmen und zu ratifizieren, in der allgemeine Grundsätze für den Schutz personenbezogener Daten festgelegt sind.

7. Mehrere Mitgliedstaaten haben diese Konvention angenommen und ratifiziert.

8. Die Entscheidung des Rates .....[9] sieht die Aufnahme von Verhandlungen im Hinblick auf einen Beitritt der Europäischen Wirtschaftsgemeinschaft - im Bereich ihrer Kompetenzen - zu dem Übereinkommen des Europarats zum Schutz der Menschen bei der automatischen Verarbeitung personenbezogener Daten vor.

9. Die Richtlinie des Rates ..... zum Schutz von Personen bei der Verarbeitung personenbezogener Daten übernimmt diese allgemeinen Grundsätze für die Gemeinschaft.

10. Öffentliche Digitalnetze erfordern spezielle rechtliche, ordnungspolitische und technische Vorschriften, um die personenbezogenen Daten und die Privatsphäre der Benutzer gegenüber den zunehmenden Risiken zu schützen, die mit der elektronischen Speicherung und Verarbeitung personenbezogener Daten in diesen Netzen verbunden sind.

11. Die Mitgliedstaaten arbeiten gegenwärtig abweichende Vorschriften für diesen Bereich aus.

12. Angesichts der Hindernisse, die sich aus diesen abweichenden rechtlichen, ordnungspolitischen und technischen Vorschriften für den Schutz personenbezogener Daten und der Privatsphäre bei der Einführung öffentlicher digitaler

---

(6) ABl. Nr. C 7 vom 12.1.1987, S. 334.
(7) ABl. Nr. C 12 vom 16.1.1989, S. 69
(8) ABl. Nr. C 12 vom 16.1.1989, S. 66
(9) ABl. Nr.

Telekommunikationsnetze in der Gemeinschaft, insbesondere des diensteintegrierenden digitalen Telekommunikationsnetzes (ISDN) und öffentlicher digitaler Mobilfunknetze ergeben, erfordert die Vollendung eines gemeinschaftsweiten Marktes für Telekommunikationsdienste und -geräte die rasche Einführung harmonisierter Vorschriften.

13. Mit dieser Richtlinie soll festgelegt werden, in welchem Umfang personenbezogene Daten bei der Bereitstellung von Kommunikationsdiensten erfaßt, gespeichert und verarbeitet werden dürfen.

14. Die Erfassung, Speicherung und Verarbeitung personenbezogener Daten durch eine Telekommunikationsorganisation ist nur im Hinblick auf die Bereitstellung des betreffenden Dienstes gerechtfertigt; diese Daten dürfen ohne besondere Rechtsgrundlage oder vorherige schriftliche Zustimmung des Teilnehmers zu keinem anderen Zweck verwendet werden. Die Erfassung, Speicherung und Verarbeitung personenbezogener Daten darf vor allem nicht dazu dienen, einer Telekommunikationsorganisation einen unzulässigen Wettbewerbsvorteil gegenüber anderen Anbietern von Diensten zu verschaffen.

15. Mit dieser Richtlinie sollen die allgemeinen Grundsätze hinsichtlich der Rechte des Teilnehmers auf den Bereich der Telekommunikation angewendet werden, wonach er sich darüber informieren kann, welche seine Person betreffende Daten gespeichert sind und, falls erforderlich, deren Berichtigung oder Löschung verlangen kann, sowie deren unberechtigte Weitergabe an Dritte verhindern kann.

16. Diese Richtlinie muß auf eine Harmonisierung der Vorschriften der Mitgliedstaaten in bezug auf den Schutz der Privatsphäre bei Einzelgebührennachweisen hinwirken.

17. Bei der Anzeige der Rufnummer des Anrufers sind sowohl dessen Recht auf Anonymität als auch die Privatsphäre des angerufenen Teilnehmers in bezug auf nicht identifizierte Anrufe zu schützen.

18. Es sind Sicherheitsvorkehrungen zu treffen, um Benutzer von Teleshopping- und Videotext-Diensten gegen die unberechtigte Verwendung ihrer personenbezogenen Daten sowie allgemein die Teilnehmer gegen das Eindringen in ihre Privatsphäre durch unerbetene Anrufe zu schützen.

19. Es muß gewährleistet sein, daß die aus Gründen des Datenschutzes erforderliche Einführung von technischen Merkmalen der Telekommunikationsgeräte harmonisiert wird, damit sie der Vollendung des Binnenmarktes bis 1992 nicht entgegensteht.

20. Bei der Umsetzung dieser Richtlinie in bezug auf Drittländer ist das Niveau des Schutzes personenbezogener Daten und der Privatsphäre in diesen Ländern zu berücksichtigen, das in der Richtlinie des Rates ..... zur Angleichung bestimmter Rechts- und Verwaltungsvorschriften der Mitgliedstaaten für den Personenschutz bei der Verarbeitung personenbezogener Daten behandelt wird.

21. Falls Angelegenheiten des Schutzes personenbezogener Daten und der Privatsphäre in öffentlichen digitalen Telekommunikationsnetzen von den Vorschriften dieser speziellen Richtlinie nicht erfaßt werden, so gilt die oben erwähnte Ratsrichtlinie.

22. Diese Richtlinie bezieht sich nicht auf Fragen des Schutzes personenbezogener Daten und der Privatsphäre, die in den Bereich der nationalen Sicherheit fallen.

23. Es ist sinnvoll, bei der Vorbereitung von Maßnahmen, die zur Durchführung oder Änderung dieser Richtlinie getroffen werden sollen, auf die Erfahrung der Gruppe zurückzugreifen, der gemäß Artikel 27 der Richtlinie des Rates ..... zum Schutz von Personen bei der Verarbeitung personenbezogener Daten aus Vertretern der für den Schutz personenbezogener Daten zuständigen Kontrollbehörden der Mitgliedstaaten zusammengesetzt ist.

24. Diese Maßnahmen sind unter Mitwirkung des Ausschusses vorzubereiten, der sich gemäß Artikel 30 der Richtlinie des Rates ..... zum Schutz von Personen bei der Verarbeitung personenbezogener Daten aus Vertretern der Mitgliedstaaten zusammensetzt.

HAT FOLGENDE RICHTLINIE ERLASSEN:

Artikel 1

1. Diese Richtlinie dient der Harmonisierung der Vorschriften, die erforderlich sind, um einen gleichmäßigen Schutz der Privatsphäre in der gesamten Gemeinschaft zu gewährleisten und sowohl innerhalb der Mitgliedstaaten als auch grenzüberschreitend den freien Verkehr von Telekommunikationsgeräten und -diensten sicherzustellen.

2. Die Mitgliedstaaten erlassen die notwendigen besonderen Vorschriften, um den Schutz personenbezogener Daten und der Privatsphäre im Telekommunikationssektor zu gewährleisten.

Artikel 2

1. Unbeschadet der allgemeinen Vorschriften der Richtlinie des Rates ..... zum Schutz von Personen bei der Verarbeitung personenbezogener Daten gilt diese Richtlinie speziell für die Erfassung, Speicherung und Verarbeitung personenbezogener Daten durch Telekommunikationsorganisationen in Verbindung mit der Bereitstellung öffentlicher Telekommunikationsdienste über öffentliche digitale Telekommunikationsnetze in der Gemeinschaft, insbesondere über das diensteintegrierende digitale Telekommunikationsnetz (ISDN) und öffentliche digitale Mobilfunknetze.

2. Falls ein Mitgliedstaat das diensteintegrierende digitale Telekommunikationsnetz (ISDN) oder öffentliche digitale Mobilfunknetze noch nicht eingeführt hat, gelten die Vorschriften dieser Richtlinie, soweit sie auch auf Dienste in analogen Netzen anwendbar sind.

Artikel 3

Im Sinne dieser Richtlinie bedeuten:

1. "Personenbezogene Daten": alle Informationen über eine bestimmte oder bestimmbare Person.

2. "Telekommunikationsorganisation": eine staatliche oder private Einrichtung, der ein Mitgliedstaat besondere oder ausschließliche Rechte zur

Bereitstellung von öffentlichen Telekommunikationsnetzen und gegebenenfalls zur Erbringung von öffentlichen Telekommunikationsdiensten gewährt.

3. "Öffentliches Telekommunikationsnetz": die öffentliche Telekommunikationsinfrastruktur, mit der Signale zwischen definierten Netzabschlußpunkten über Draht, über Richtfunk, auf optischem oder anderem elektromagnetischem Weg übertragen werden.

4. "Öffentlicher Telekommunikationsdienst": eine Telekommunikationsdienst, mit dessen Erbringung die Mitgliedstaaten insbesondere eine oder mehrere Telekommunikationsorganisationen ausdrücklich betraut haben.

Artikel 4

1. Die Erhebung, Speicherung und Verarbeitung personenbezogener Daten durch eine Telekommunikationsorganisation ist nur für Telekommunikationszwecke zulässig, insbesondere wenn sie zum Aufbau von Verbindungen für Sprach-, Daten- oder Bildübertragung, zur Gebührenberechnung, zur Herstellung von Teilnehmerverzeichnissen oder zu sonstigen zulässigen betrieblichen Zwecken dient, z.B. Störungsbeseitigung, Vermeidung des Mißbrauchs der Anlagen der Telekommunikationsorganisationen oder Feststellung ankommender Verbindungen in Übereinstimmung mit Art. 13 Absatz 1.

2. Die Telekommunikationsorganisationen dürfen diese Daten nicht verwenden, um elektronische Profile der Teilnehmer zu erstellen oder einzelne Teilnehmer nach Kategorien zu sortieren.

Artikel 5

1. Personenbezogene Daten des Teilnehmers dürfen nur gespeichert werden, soweit dies zum Abschluß, zur Durchführung, zur Änderung oder Beendigung des Vertrages mit der Telekommunikationsorganisation notwendig ist. Nach Ablauf des Vertrages sind die Daten zu löschen, es sei denn, sie werden noch benötigt, um Beschwerden zu bearbeiten, Gebühren einzuziehen oder sonstige Verpflichtungen zu erfüllen, die in den Mitgliedstaaten dem Gemeinschaftsrecht entsprechend gesetzlich vorgeschrieben sind.

2. Die Inhalte der übertragenen Information dürfen nach Beendigung der Übertragung nicht von der Telekommunikationsorganisation gespeichert werden, es sei denn, dies

ist aufgrund von Verpflichtungen erforderlich, die in den Mitgliedstaaten dem Gemeinschaftsrecht entsprechend gesetzlich vorgeschrieben sind.

Artikel 6

Der Teilnehmer ist berechtigt,

- in angemessenen Zeitabständen und ohne unzumutbare Verzögerung oder übermäßige Kosten die Bestätigung zu erhalten, ob personenbezogene Daten über ihn gespeichert sind, sowie zu erwirken, daß ihm diese Daten in verständlicher Form mitgeteilt werden;

- gegebenenfalls diese Daten berichtigen oder löschen zu lassen, wenn sie entgegen den in Übereinstimmung mit dem Gemeinschaftsrecht bestehenden Vorschriften des Mitgliedstaates verarbeitet worden sind.

Artikel 7

1. Grundsätzlich sind alle personenbezogenen Daten, die bei der Bereitstellung von Telekommunikationsnetzen und -diensten verarbeitet werden, vertraulich zu behandeln.

2. Personenbezogene Daten dürfen außerhalb der Dienste oder des Netzes der Telekommunikationsorganisation nur aufgrund besonderer gesetzlicher Grundlage oder vorheriger schriftlicher Zustimmung des Teilnehmers weitergegeben werden. Eine solche Zustimmung des Teilnehmers gilt nur dann als erteilt, wenn sie ausdrücklich als Antwort auf ein Ersuchen der Telekommunikationsorganisation gegeben wurde. Ohne vorherige schriftliche Zustimmung des Teilnehmers dürfen diese personenbezogenen Daten Personen, die der Telekommunikationsorganisation angehören und sich nicht mit den betreffenden Diensten befassen, nicht zugänglich gemacht werden.

3. Die Telekommunikationsorganisation darf die Bereitstellung ihrer Dienste nicht von einer solchen Zustimmung abhängig machen.

Artikel 8

1. Die Telekommunikationsorganisation muß einen dem Stand der Technik entsprechenden, angemessenen Schutz der personenbezogenen Daten gegen unbefugten Zugriff und unbefugte Verwendung gewährleisten.

2. Besteht ein besonderes Risiko der Verletzung der Netzsicherheit, z.B. im Bereich des Mobilfunks, so hat die Telekommunikationsorganisation die Teilnehmer darüber zu informieren und ihnen eine Verschlüsselung von Endgerät zu Endgerät anzubieten.

Artikel 9

1. Zulässig ist die Speicherung und Verarbeitung von Daten für die Gebührenabrechnung, wie Telefonnummer oder Identifikation des Teilnehmerendgerätes, Teilnehmeranschrift und Art des Endgerätes, Gesamtzahl der für den Abrechnungszeitraum zu berechnenden Einheiten, die Rufnummern der angerufenen Teilnehmer, Art und Dauer der Anrufe, und/oder der Umfang der übertragenen Daten sowie sonstige Informationen, die für die Abrechnung benötigt werden, z.B. Vorauszahlungen, Ratenzahlungen, Sperren des Anschlusses und Mahnungen.

2. Diese generelle Speicherung von Gebührendaten ist für die Dauer der gesetzlichen Frist zulässig, während derer die Rechnung angefochten werden kann.

Artikel 10

1. Verkehrsdaten einschließlich der zum Verbindungsaufbau oder für die Gebührenabrechnung und für sonstige betriebliche Zwecke benötigten personenbezogenen Daten wie Telefonnummer des anrufenden und des angerufenen Teilnehmers, Beginn und Ende des Anrufs und der in Anspruch genommene Telekommunikationsdienst können erhoben, gespeichert und verarbeitet werden, soweit dies zur Bereitstellung des entsprechenden Dienstes erforderlich ist.

2. Verkehrsdaten, die in den Vermittlungsstellen der Telekommunikationsorganisation gespeichert werden, sind nach Beendigung des Anrufs zu löschen, sofern sie nicht anonymisiert worden sind oder für die Gebührenabrechnung oder sonstige zulässige Zwecke gemäß Artikel 4 benötigt werden.

Artikel 11

1. Auf Antrag des Teilnehmers kann ein Einzelgebührennachweis erstellt werden, der unter anderem die Rufnummer der angerufenen Teilnehmer ohne die letzten vier Ziffern enthält.

Artikel 12

1. Bei Verbindungen zwischen Teilnehmern, die an digitale Vermittlungsstellen angeschlossen sind, muß der anrufende Teilnehmer die Möglichkeit haben, über eine einfache technische Einrichtung die Anzeige seiner Telefonnummer auf dem Display des Endgeräts des angerufenen Teilnehmers bzw. die Aufzeichnung in einem Speicher dieses Endgeräts von Fall zu Fall auszuschließen.

   Die Übertragung der Telefonnummer kann auf Antrag des anrufenden Teilnehmers von der Telekommunikationsorganisation auch permanent ausgeschlossen werden.

2. Der angerufene Teilnehmer kann den permanenten Ausschluß der Rufnummernanzeige bei sämtlichen ankommenden Verbindungen beantragen; er muß ferner die Möglichkeit haben, die Anzeige an seinem Endgerät abzuschalten oder die Aufzeichnung in einem Speicher des Endgeräts auszuschließen, um die Rufnummernanzeige von Fall zu Fall zu verhindern.

   Der angerufene Teilnehmer muß die Entgegennahme ankommender Verbindungen auf diejenigen beschränken können, bei denen die Nummer des anrufenden Teilnehmers angegeben ist.

3. Bei Verbindungen zwischen einem an eine analoge Vermittlungsstelle und den an digitale Vermittlungsstellen angeschlossenen Teilnehmern muß ersterer über die Rufnummernanzeige informiert werden und die Möglichkeit erhalten, diese Funktion auf Antrag permanent auszuschließen. Dieser Teilnehmer muß ebenfalls die Möglichkeit haben, die Rufnummernanzeige von Fall zu Fall auszuschließen.

Artikel 13

1. Die Telekommunikationsorganisation kann für einen begrenzten Zeitraum den Ausschluß der Rufnummernanzeige verhindern, wenn

   a) ein Teilnehmer die Feststellung von belästigenden Anrufen beantragt hat. In diesem Fall werden die Daten mit der Rufnummer des Anrufers von der

Telekommunikationsorganisation gespeichert und auf Verlangen der Behörde zur Verfügung gestellt, die für die Verhinderung oder Verfolgung strafbarer Handlungen in dem betreffenden **Mitgliedstaat zuständig ist;**

b) **eine gerichtliche Anordnung vorliegt, mit der schwere Straftaten verhindert oder verfolgt werden sollen.**

2. Auf Antrag muß

a) Organisationen, die von einem Mitgliedstaat anerkannt sind und Notrufe beantworten und bearbeiten sowie

b) den von einem Mitgliedstaat betriebenen oder anerkannten Feuerwehren

die Möglichkeit geboten werden, **den Ausschluß der Rufnummernanzeige auf Dauer zu verhindern.**

3. Die Telekommunikationsorganisationen unternehmen die notwendigen Schritte, um zu gewährleisten, daß die Verhinderung **des Anzeigeausschlusses landes- und** gemeinschaftsweit bereitgestellt wird.

Artikel 14

1. Der angerufene Teilnehmer darf Anrufe nur dann zu einem dritten Teilnehmer weiterschalten lassen, wenn dieser zugestimmt hat; der Dritte kann die Weiterschaltung auf diejenigen Anrufe beschränken, bei denen die Nummer des anrufenden Teilnehmers angezeigt wird; der Dritte muß durch ein bestimmtes Signal darauf aufmerksam gemacht werden, daß es sich um einen weitergeschalteten Anruf handelt.

2. Der anrufende Teilnehmer muß bei Aufbau der Verbindung automatisch darüber informiert werden, daß der Anruf an einen Dritten weitergeschaltet wird.

Artikel 15

1. Wird der Inhalt von Telefongesprächen über technische Geräte wie Lautsprecher oder sonstige angeschlossene Geräte Dritten zugänglich gemacht oder für eigene Zwecke bzw. zur Verwendung durch Dritte auf Band gespeichert, so ist dafür zu sorgen, daß die betroffenen Parteien in geeigneter Form von dieser Weitergabe oder Speicherung

unterrichtet werden, bevor der Vorgang der Weitergabe oder Speicherung eingeleitet wird und solange er andauert.

2. Absatz 1 gilt nicht in den in Artikel 13 Absatz 1 geregelten Fällen.

Artikel 16

1. Die Telekommunikationsorganisation muß sicherstellen, daß die Rufnummer sowie sonstige personenbezogene Daten des Teilnehmers, insbesondere Art und Menge seiner Bestellungen über einen Teleshopping-Dienst oder die über einen Videotext-Dienst angeforderte Informationen nur gespeichert werden, soweit dies unbedingt zur Erbringung des Dienstes notwendig ist, und daß diese Informationen vom Anbieter der Dienste ausschließlich für die vom Teilnehmer gestatteten Zwecke verwendet werden.

2. Vorbehaltlich der Bestimmungen des Artikels 20, darf der Anbieter der Dienste ohne vorherige schriftliche Zustimmung der Teilnehmer keine elektronischen Profile von ihnen erstellen und sie nicht nach Kategorien sortieren.

Artikel 17

1. Teilnehmer, die unerbetene Anrufe erhalten, mit denen Werbung betrieben oder Angebote für die Lieferung von Waren oder Erbringung von Dienstleistungen unterbreitet werden, können der Telekommunikationsorganisation, die diese Anrufe vermittelt, förmlich mitteilen, daß derartige Anrufe unerwünscht sind.

2. Die Telekommunikationsorganisation unternimmt die notwendigen Schritte, um die Übertragung solcher Nachrichten an den betreffenden Teilnehmer zu unterbinden. Darüberhinaus führt die Telekommunikationsorganisation eine detaillierte und von der Aufsichtsbehörde überprüfbare Liste der förmlichen Mitteilungen, damit solche Anrufe in Zukunft unterbunden werden können.

Artikel 18

1. Bei der Durchführung der Bestimmungen dieser Richtlinie stellen die Mitgliedstaaten vorbehaltlich der Absätze 2 und 3 dieses Artikels sicher, daß keine zwingenden Anforderungen in bezug auf spezielle technische Merkmale für Endgeräte oder sonstige Telekommunikationsgeräte gestellt werden, die deren Vermarktung und deren freien Vertrieb in und zwischen den Mitgliedstaaten behindern.

2. Soweit die Bestimmungen dieser Richtlinie nur mit Hilfe von speziellen technischen Merkmalen durchgeführt werden können, unterrichten die Mitgliedstaaten die Kommission darüber gemäß der Richtlinie 83/189/EWG des Rates [10] über ein Informationsverfahren auf dem Gebiet der Normen und technischen Vorschriften.

3. Soweit erforderlich, sorgt die Kommission für die Erarbeitung gemeinsamer europäischer Normen zur Einführung spezieller technischer Merkmale im Sinne der Richtlinie ...../EWG des Rates zur Angleichung der Rechtsvorschriften der Mitgliedstaaten über Telekommunikationsendgeräte einschließlich der gegenseitigen Anerkennung ihrer Konformität [11] und der Richtlinie 87/95/EWG des Rates vom 22. Dezember 1986 über die Normung auf dem Gebiet der Informationstechnik und der Telekommunikation [12].

Artikel 19

1. Die Bestimmungen dieser Richtlinie in bezug auf den Telefondienst gelten ebenfalls für andere öffentliche digitale Telekommunikationsdienste, soweit diese ähnliche Risiken für die Privatsphäre des Benutzers beinhalten.

2. Die notwendigen Maßnahmen zur Durchführung des obigen Absatzes werden von der Kommission nach Anhörung des in Artikel 22 erwähnten Ausschusses gemäß dem in Artikel 23 festgelegten Verfahren beschlossen.

Artikel 20

Erfordert die Verwirklichung der Ziele dieser Richtlinie die Anwendung ihrer Bestimmungen auf andere Anbieter der Dienste als Telekommunikationsorganisation, so kann die Kommission die erforderlichen Maßnahmen zur Anwendung dieser Richtlinie auf diese Anbieter der Dienste nach Anhörung des in Artikel 22 erwähnten Ausschusses gemäß dem in Artikel 23 festgelegten Verfahren beschließen.

---

(10) ABl. Nr. L 109 vom 26.4.1983, S. 8.
(11) ABl. Nr. C
(12) ABl. Nr. L 36 vom 7.2.1987, S. 31.

Artikel 21

Einzelheiten der Anwendung dieser Richtlinie und der notwendigen Änderungen zur Anpassung der Richtlinie an neue technische Entwicklungen werden von der Kommission nach Anhörung des in Artikel 22 erwähnten Ausschusses gemäß dem in Artikel 23 vorgeschriebenen Verfahren festgelegt.

Artikel 22

1. Die Gruppe für den Schutz personenbezogener Daten, die gemäß Artikel 27 der Richtlinie des Rates ..... zum Schutz von Personen bei der Verarbeitung personenbezogener Daten eingesetzt wird, nimmt ihre Aufgaben gemäß Artikel 28 der erwähnten Richtlinie ebenfalls bezüglich der Maßnahmen zum Schutz personenbezogener Daten, die Gegenstand dieser Richtlinie sind, wahr.

2. Die Gruppe wird für die Zwecke dieser Richtlinie speziell zusammengesetzt.

Artikel 23

1. Das in Artikel 30 der Richtlinie des Rates ..... zum Schutz von Personen bei der Verarbeitung personenbezogener Daten festgelegte Verfahren findet ebenfalls auf diese Richtlinie Anwendung.

2. Der Ausschuß, der im Rahmen des Verfahrens gemäß Absatz 1 eingesetzt wird, wird für die Zwecke dieser Richtlinie speziell zusammengesetzt.

Artikel 24

1. Die Mitgliedstaaten erlassen die erforderlichen Rechts- und Verwaltungsvorschriften, um dieser Richtlinie spätestens am 1. Januar 1993 nachzukommen.

   Die aufgrund des ersten Unterabsatzes erlassenen Vorschriften enthalten eine ausdrückliche Bezugnahme auf diese Richtlinie.

2. Die Mitgliedstaaten teilen der Kommission den Wortlaut der innerstaatlichen Rechtsvorschriften mit, die sie auf dem unter diese Richtlinie fallenden Gebiet erlassen.

Artikel 25

Diese Richtlinie ist an die Mitgliedstaaten gerichtet.

Geschehen zu Brüssel am

Im Namen des Rates

Der Präsident

FICHE FINANCIERE

PROPOSITION DE DIRECTIVE DU CONSEIL CONCERNANT LA PROTECTION DES DONNEES A CARACTERE PERSONNEL ET DE LA VIE PRIVEE DANS LE CONTEXTE DES RESEAUX DE TELECOMMUNICATIONS NUMERIQUES PUBLICS, ET EN PARTICULIER DU RESEAU NUMERIQUE A INTEGRATION DE SERVICES (RNIS) ET DES RESEAUX NUMERIQUES MOBILES PUBLICS.

1. Ligne budgétaire concernée

En 1990 : B 7700

En 1991 et exercices ultérieurs : B5-4010

2. Base légale

Article 100 A

3. Proposition de classification en dépense obligatoire /non obligatoire

non -obligatoire

4. Description et justification de l'action :

4.1. Objectifs : - assurer la protection des personnes à l'égard des données à caractère personnel,

- permettre la circulation transfrontalière de données à caractère personnel dans la Communauté,

- permettre le bon fonctionnement du marché intérieur.

4.2. Réunions spécifiques du groupe de protection des données à caractère personnel (Art. 22) et du Comité consultatif (Art. 23), créés par la directive, représentant les Etats membres .

4.3. Un représentant de la Commission préside le groupe de protection des données à caractère personnel et le Comité consultatif. Le secrétariat du groupe et du Comité de protection des données à caractère personnel est assuré par les services de la Commission.

5. Nature de la dépense et mode de calcul :

5.1. Nature : réunions

(frais de participation des membres des 2 Comités)

5.2. Calcul : - Groupe de protection des données : (cf. fiche financière de la directive générale)

- Comité consultatif :

24 membres (gouvernementaux) x 3 réunions x 2 jours x 390 ECU/jour = 56.160 ECU *

6. Incidence financière de l'action sur les crédits d'intervention :

6.1. Echéancier des crédits d'engagement et de paiement

CE-CP

1993 : 56.160 ECU

1994 : 56.160 *

1995 : 56.160 *

1996 : 56.160 *

1997 : 56.160 *

6.2. Part du financement communautaire dans le coût total : 100 %

---

* estimation

7. Observations :

1. Le groupe de protection des données à caractère personnel (Art. 22):

Il est institué ce groupe à caractère consultatif et indépendant et est composé de représentants de l'autorité de contrôle de tous les Etats membres, présidé par un représentant de la Commission.

Ce groupe établit son règlement intérieur. Le secrétariat du groupe est assuré par les services de la Commission.

Missions de ce groupe : voir Art. 22

2. Le Comité consultatif (Art . 23)

Il est institué un Comité consultatif composé des représentants des Etats Membres, présidé par le représentant de la Commission.

La Commission est assistée par ce Comité afin de prendre les éventuelles mesures complémentaires nécessaires pour adapter les dispositions de la directive aux spécificités de certains secteurs.

Empfehlung für einen Beschluß des Rates zur Aufnahme von Verhandlungen über den Beitritt der Europäischen Gemeinschaften zum Übereinkommen des Europarats zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten

BEGRÜNDUNG:

1. Der Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten ist zugleich ein Persönlichkeitsrecht und eine Grundvoraussetzung für die Weiterentwicklung des internationalen Handelsverkehrs.

2. Die automatische Verarbeitung personenbezogener Daten ist für den internationalen Waren- und Dienstleistungsverkehr und eine engere Zusammenarbeit zwischen den einzelnen Ländern unerläßlich.

3. Die Kommission hat dem Rat einen Richtlinienvorschlag unterbreitet, mit dem überall in der Gemeinschaft hinsichtlich der automatischen Verarbeitung personenbezogener Daten für Personen ein hohes Schutzniveau erreicht werden soll. Es wäre wünschenswert, wenn diese Maßnahme analog auf den Datenaustausch zwischen der Gemeinschaft und Drittländern ausgedehnt würde.

4. Im Jahre 1981 wurde im Rahmen des Europarats ein Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten abgeschlossen. Zweck dieses Übereinkommens ist es, im Hoheitsgebiet jeder Vertragspartei für jedermann ungeachtet seiner Staatsangehörigkeit oder seines Wohnorts sicherzustellen, daß seine Grundrechte und Grundfreiheiten, insbesondere sein Recht auf Schutz der Privatsphäre, bei der automatischen Verarbeitung personenbezogener Daten geschützt werden. Das Übereinkommen sieht auch vor, daß eine Vertragspartei nicht allein zum Zweck des Schutzes der Privatsphäre den grenzüberschreitenden Verkehr personenbezogener Daten in das Hoheitsgebiet einer anderen Vertragspartei verbieten oder von einer besonderen Genehmigung abhängig machen kann.

5. In ihrer Empfehlung vom 29. Juli 1981 hat die Kommission die Mitgliedstaaten der Gemeinschaft aufgerufen, das Übereinkommen des Europarats zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten zu ratifizieren, wobei sie sich ausdrücklich das Recht vorbehalten hat, dem Rat einen Rechtsakt auf der Grundlage des EWG-Vertrages vorzuschlagen, falls die Mitgliedstaaten dieses Übereinkommen nicht innerhalb einer angemessenen Frist unterzeichnen und ratifizieren.

6. Bis zum heutigen Tage haben noch nicht alle EG-Mitgliedstaaten dieses Übereinkommen ratifiziert (1). Es wäre nicht nur wünschenswert, sondern notwendig, daß die Gemeinschaft der Konvention beitritt, damit der Schutz und die grenzüberschreitende Übermittlung personenbezogener Daten in Drittländer nicht beeinträchtigt und die Attraktivität des Übereinkommens für Drittländer gesteigert wird, denen an einem möglichst ungehinderten Datenaustausch mit der Gemeinschaft gelegen ist.

7. Daher empfiehlt die Kommission dem Rat, die Kommission dazu zu ermächtigen, ein Zusatzprotokoll mit dem Europarat und den Vertragsparteien des Übereinkommens auszuhandeln, welches den Europäischen Gemeinschaften die Möglichkeit eröffnet, diesem Übereinkommen in den Bereichen der Gemeinschaftszuständigkeit beizutreten.

8. Die Kommission wird die Verhandlungen in Abstimmung mit den Vertretern der Mitgliedstaaten führen, und zwar unter Beachtung der beigefügten oder gegebenfalls vom Rat an sie gerichteten Verhandlungsdirektiven.

9. Die Mitgliedstaaten der Gemeinschaft, die auch Mitglieder des Europarats sind, werden das Vorgehen der Gemeinschaft bei den Beitrittsverhandlungen uneingeschränkt unterstützen, wenn diese Frage von den Organen des Europarats behandelt wird.

Anhang: Verhandlungsdirektiven

---

1 Von den EG-Mitgliedstaaten haben Belgien, Griechenland, Irland, Italien, die Niederlande und Portugal das Übereinkommen (STE 108 vom 28. Januar 1981) unterzeichnet. Ratifiziert wurde sie von Dänemark, Frankreich, der Bundesrepublik Deutschland, Luxemburg, Spanien und dem Vereinigten Königreich Großbritannien.

ANHANG

VERHANDLUNGSDIREKTIVEN

1. Die Verhandlungen sollen zum Abschluß eines Zusatzprotokolls führen, das der Gemeinschaft die Möglichkeit eröffnet, in den Bereichen ihrer Zuständigkeit Vertragspartei des Übereinkommens zu werden; dabei sind die nachstehend aufgeführten Grundsätze zu beachten:

2. In dem gemäß Artikel 18 des Übereinkommens eingesetzten Beratenden Ausschuß wird die Europäische Gemeinschaft als Mitglied von der Kommission der Europäischen Gemeinschaften vertreten.

   Nach einer auf Initiative der Kommission erfolgten Koordinierung auf Gemeinschaftsebene verfügt der Vertreter der Europäischen Gemeinschaften über eine Stimmenzahl, die der Summe der Stimmen aller nationalen Delegationen der EG-Mitgliedstaaten entspricht, die zugleich Vertragspartei des Übereinkommens sind. Diese Regelung gilt für alle Fragen im Zusammenhang mit der automatischen Verarbeitung personenbezogener Daten in den Bereichen der Gemeinschaftszuständigkeit.

   In allen anderen Fragen geben die nationalen Delegationen ihre Stimmen getrennt ab.

3. Um das Inkrafttreten des Zusatzprotokolls über den Beitritt der Gemeinschaft zu dem Übereinkommen innerhalb einer angemessenen Frist zu gewährleisten, wird die Kommission mit Unterstützung der Mitgliedstaaten vorschlagen, eine "Ablehnungsklausel" (opting out procedure) für die Annahme des Zusatzprotokolls in den Text des Protokolls aufzunehmen.

Vorschlag für einen Beschluß des Rates

auf dem Gebiet der

Informationssicherheit

Zusammenfassung

Informationen in unterschiedlicher Form bilden immer mehr eine Bereicherung des einzelnen, der Unternehmen und Staaten. Wachstum und Leistung von annähernd zwei Dritteln der Wirtschaft basieren auf Produktionen bzw. Diensten, die stark von Informationstechnologien, Telekommunikation und Rundfunk abhängig sind, und sind damit wesentlich auf die Präzision, Sicherheit und "Vertrauenswürdigkeit" der Informationen angewiesen. Dieser Umstand ist für Privatpersonen ebenso wie für den Handel, die Industrie und öffentliche Verwaltungen maßgebend. Daher ist der umfassende Schutz der Informationen, nachstehend als "Informationssicherheit"1) bezeichnet, zu einer zentralen politischen Frage und einem wichtigen weltweiten Anliegen geworden.

In den letzten Jahrzehnten sind grundlegende Veränderungen eingetreten; diejenigen, die auf uns zukommen, könnten jedoch noch tiefgreifender sein. Supercomputer für den Schreibtisch, direkt strahlender Satellitenrundfunk, digitaler Mobilfunk, integrierte Breitbandkommunikation und andere neue Anwendungen von Technologien werden derzeit entwickelt und eröffnen Möglichkeiten für die weltweite, kostengünstige, mobile Hochleistungskommunikation in einem bislang unerreichten Maßstab. Mit der Einführung effizienter globaler Kommunikationsdienste wurde der Schwerpunkt verstärkt auf die Notwendigkeit eines angemessenen "Schutzes" gelegt, der durch Zugangsrechte, Nachrichtenintegrität und Schutz der Privatsphäre entsprechend dem voraussichtlichen Grad der administrativen oder technischen Risiken zu gewährleisten ist.

Dieses Thema ist für die sozioökonomische Entwicklung der Europäischen Gemeinschaft und die Vollendung des Binnenmarktes 1992 von zentraler Bedeutung. Ein kohärentes Konzept auf europäischer Ebene sollte zunehmendes Vertrauen in den Einsatz neuer Informationstechnologien und Telekommunikationsdienste schaffen und dazu beitragen, die Entstehung neuer Schranken zwischen einzelnen Mitgliedstaaten und gegenüber Drittländern zu vermeiden. Daher sind umgehend die Anforderungen und Optionen Im Hinblick auf eine gemeinschaftsweite Aktion in enger Zusammenarbeit mit den betreffenden Akteuren und Mitgliedstaaten zu prüfen. Bei allen Maßnahmen sind die kommerziellen, rechtlichen und technischen Entwicklungen auf einzelstaatlicher und internationaler Ebene zu berücksichtigen. Da Informationssicherheit nicht nur den Schutz des Menschen und des Eigentums, sondern auch den Schutz der Gesellschaft als solche umfaßt, ist sie für die Mitgliedstaaten ein Thema, das die nationale Souveränität berührt.

Gleichzeitig ist es für die Gemeinschaft und die Mitgliedstaaten von entscheidender Bedeutung, daß die Informationssicherheit die Förderung der harmonischen Entwicklung in der Gemeinschaft und die Beziehungen zu anderen Ländern nicht behindert. Die Entwicklung eines harmonisierten Konzepts der Informationssicherheit muß wesentlicher Bestandteil der Gemeinschaftspolitiken zum Ausbau der sozioökonomischen Leistungen der Europäischen Gemeinschaft, der internationalen Wettbewerbsfähigkeit und zur Vollendung des Binnenmarktes sein.

In erster Linie geht es darum, Privatbenutzern, Verwaltungen und Unternehmen eine wirksame und praktikable Sicherheit der elektronisch gespeicherten Informationen zu bieten, ohne die Interessen der breiten Öffentlichkeit zu beeinträchtigen.

1) Informationssicherheit (IS) bedeutet Schutz der elektronisch gespeicherten, verarbeiteten oder übertragenen Informationen gegen beabsichtigte und unbeabsichtigte Risiken. Elektronische Informationsdienste benötigen eine sichere Kommunikationsinfrastruktur, sichere Endgeräte (einschließlich Prozessoren und Datenbanken) und sichere Nutzungsmöglichkeiten.

Eine Aktion auf Gemeinschaftsebene erfordert konzertierte Maßnahmen zur Entwicklung der notwendigen Technologien, Normen, Prüf- und Zertifizierungsverfahren und gegebenenfalls Regelungen im Rahmen der Gemeinschaftspolitik.

Die Kommission möchte eine Diskussion über Fragen der Informationssicherheit mit den betreffenden Akteuren in der Gemeinschaft fördern und einen Konsens hinsichtlich der geeigneten Schritte, die zu erwägen sind, herbeiführen. Diese Diskussion könnte aufgrund der im Anhang erläuterten Themen und Aktionslinien eingeleitet werden. Dabei muß sich die Gemeinschaftsinitiative angesichts der Verantwortlichkeit der Mitgliedstaaten in diesem Bereich unbedingt auf eine enge Zusammenarbeit mit hohen Beamten der Mitgliedstaaten stützen können.

Daher wird vorgeschlagen, die Kommission durch einen Beratenden Ausschuß zu unterstützen, der sich aus Vertretern der Mitgliedstaaten zusammensetzt und dessen Vorsitz ein Vertreter der Kommission führt. Die Arbeitsweise dieses Ausschusses muß den Besonderheiten des Bereichs entsprechen. Er würde die Bezeichnung "Gruppe hoher Beamter Informationssicherheit (SOG-IS)" führen.

Die Kernfrage des Schutzes persönlicher Daten wird in einem Vorschlag für eine Richtlinie behandelt, der parallel zu dieser Mitteilung vorgelegt wird.

A. Die neuen Herausforderungen und die gesellschaftliche, wirtschaftliche, strategische und politische Bedeutung der Informationssicherheit

1. Die Verwaltung und Nutzung von Informationen mit Hilfe der Informationstechnologien und Informatikdienste setzt sich in allen Bereichen des wirtschaftlichen, gesellschaftlichen und politischen Lebens durch. Sie hat die Integration von Tätigkeiten über ein globales Kommunikationssystem ermöglicht, an das Fertigungsanlagen, Forschungsinstitute, Datenbanken, Rechenzentren und Diensteanbieter ebenso wie politische und wirtschaftliche Entscheidungsträger angeschlossen sind.

2. Diese verstärkte Integration getrennter Tätigkeiten schafft einen erheblichen Mehrwert durch Einsparungen oder Effizienzsteigerung. Sie ist daher ein Schlüsselfaktor der internationalen Wettbewerbsfähigkeit. Daraus ergibt sich jedoch auch in zunehmendem Maße die Notwendigkeit, die legitimen Interessen von Privatpersonen, der breiten Öffentlichkeit, des Handels, der Industrie, der Netzbetreiber, der Diensteanbieter und der einzelstaatlichen Verwaltungen zu schützen.

3. Um eine Expansion des Dienstebereichs und damit Investitionen in elektronische Anlagen, Telekommunikation, Rundfunk und Fernsehen, Computer und Endgeräte und eine breite Palette von Telematikanwendungen zu ermöglichen, ist ein sicheres europäisches Umfeld für elektronische Informationsver- und bearbeitung zu schaffen. Eine breite Akzeptanz und Zustimmung aller Parteien sind wichtig, um legitime Interessen zu wahren und den Mißbrauch von Informationen zu verhindern. Dies muß in einer Weise geschehen, die für Benutzer in verschiedenen Rechtssystemen sowohl effizient als auch angemessen ist. Darüber hinaus müssen Informationssicherheitssysteme die Privatsphäre, das geistige Eigentum, den lauteren Wettbewerb, die nationale Sicherheit und sonstige Interessen schützen.

4. Mit der Einführung der Mikrocomputer hat sich der Einsatz von Informationstechnologien, Telekommunikation und Rundfunk-Techniken über den professionellen Bereich hinaus ausgedehnt und ist zu einer "Verbraucheraktivität" mit entsprechenden "Verbraucherdiensten" geworden. Mit dieser quantitativen Veränderung ging eine wesentliche qualitative Verbesserung einher: Telekommunikationsdienste ermöglichen heute den Dialog und die Kommunikation weltweit.

5. Wesentliche Veränderungen sind in den letzten Jahrzehnten eingetreten; diejenigen, die noch vor uns liegen, könnten jedoch noch tiefgreifender sein. Schreibtisch-Supercomputer, direktstrahlender Satellitenrundfunk, digitaler Mobilfunk, integrierte Breitbandkommunikation und weitere neue Anwendungen werden derzeit entwickelt und Möglichkeiten für eine weltweite, kostengünstige, mobile Hochleistungskommunikation in nie dagewesenem Maßstab eröffnen.

6. Die Einführung effizienter globaler Kommunikationsdienste bildet qualitativ und quantitativ eine neue Herausforderung, d.h. es muß ein angemessener Schutz durch Zugangsrechte, Nachrichtenintegrität und Schutz der Privatsphäre geboten werden, der den voraussichtlichen administrativen und technischen Risiken entspricht.

7. Angesichts der zunehmenden Bereitschaft der Industrie, der Regierungen und der Gesellschaft insgesamt, Informationsdienste in Anspruch zu nehmen, sind diese wesentlicher Bestandteil der Grundstruktur des täglichen Lebens geworden. Allgemeine Steuerungs-, Kommunikations- und Kontrollfunktionen, Prozeßsteuerung in der Fertigung, Verkehrswesen, Finanzdienste, Büroautomation u.a. erfordern ausnahmslos Zugangsrechte und eine funktionelle Robustheit, die bei der ursprünglichen Konzeption der Dienste oder Geräte noch nicht vorgesehen waren.

8. Neue Anwendungen werden künftig definiert und implementiert, die sich unter Umständen innerhalb der derzeitigen Rahmenarchitektur der IBC nicht realisieren lassen. Eine grundlegende Neudefinition der Architektur und der Leistungsnormen (einschließlich Konformitätsanforderungen) für Dienste und Hardware wird gegebenenfalls erforderlich sein.

9. Neue Disziplinen und entsprechende Tätigkeiten und Organisationen sind zu entwickeln, um diesen gestiegenen funktionellen Erwartungen gerecht zu werden. Der Hauptbedarf wird jedoch nicht durch technische, sondern durch kulturelle Veränderungen bestimmt. Die umfassende Nutzung von Informationsdiensten über weitgespannte Telekommunikationsnetze wird den Begriff der organisatorischen und menschlichen Beziehungen in der Gesellschaft verändern.

10. Die Kommunikation wird in zunehmendem Maße über Vermittler abgewickelt, wie es z.B. auf den verschiedenen Stufen Iinformationstechnologie-gestützter Mehrwertdienste der Fall ist, oder findet unmittelbar statt, nachdem Vermittler die Verbindung zugelassen haben. Unter diesen Umständen muß "Vertrauen" im Zusammenhang mit organisatorischen Beziehungen, Behörden, Privilegien und zahlreichen "Qualitätskontrollen" von Diensten und Produkten ausdrücklich definiert werden. in einer solchen Gesellschaft ist sorgfältig darauf zu achten, daß die Rechte von Privatpersonen und Organisationen in der Gesetzgebung und bei ordnungspolitischen Rahmenbedigungen voll berücksichtigt werden. Parallel dazu müssen die Technologien so ausgelegt und realisiert sein, daß sie den Sicherheitsanforderungen gerecht werden.

B. Notwendigkeit einer gemeinschaftsweiten Aktion in Zusammenarbeit mit den Mitgliedstaaten

11. Soweit der Schutz des Eigentums, der Personen und sogar der Gesellschaft auf dem Spiel steht, unterliegt die Informationssicherheit eindeutig der obersten Zuständigkeit der Mitgliedstaaten. Sowohl im Bereich der Verteidigung als auch in bezug auf die normale Arbeitsweise seiner Institutionen ist jeder Mitgliedstaat unmittelbar für die Sicherheit verantwortlich. Angesichts dieser innerstaatlichen Anliegen haben die Verwaltungen historisch gesehen eine solide, langfristige Kompetenz im Bereich der Informationssicherheit erworben und kontrollieren die entsprechenden Technologien und Techniken, um die Weitergabe vertraulicher Informationen zu verhindern. Wenngleich jeder Benutzer für seine eigene Sicherheit verantwortlich ist, basieren seine Entscheidungen wesentlich auf den Garantien, die letztlich von den Behörden, beispielsweise durch rechtliche Einschränkungen, geboten werden.

12. Die Politiken und Programme der EG zur Entwicklung der Informations- und Kommunikationsindustrien und zur Vollendung des Binnenmarktes könnten ernstlich in Frage gestellt werden, wenn nicht eine aktive Politik zur Einführung, Entwicklung und Förderung von Sicherheitsnormen für Informationsdienste festgelegt wird. Im Interesse der Gemeinschaft darf die Informationssicherheit die Förderung der harmonischen Entwicklung innerhalb der Gemeinschaft und die Beziehungen zu anderen Ländern nicht behindern. Die Entwicklung eines harmonisierten Konzepts der Informationssicherheit muß wesentlicher Bestandteil der Gemeinschaftspolitiken zum Ausbau der sozioökonomischen Leistungen und der internationalen Wettbewerbsfähigkeit der europäischen Industrie und zur Vollendung des Binnenmarktes sein.

13. Sie erfordert insbesondere konzertierte Maßnahmen zur Festlegung der erforderlichen Normen, Prüf- und Zertifizierungsverfahren, der technologischen Entwicklungen und gegebenenfalls Regelungen im Rahmen der Gemeinschaftspolitik. Da es sich um überaus technische Fragen handelt, erfordert die Konzertierung der Maßnahmen eine Zusammenarbeit der Akteure im vorwettbewerblichen Stadium der Forschung und Entwicklung.

14. Die Einführung "offener Normen" durch die Regierungen (GOSIP in den USA und im UK), die westliche Verteidigungsgemeinschaft (NATO/NOSI), die Computer- und Telekommunikationsindustrie und Netzbetreiber (OSI-Normen der ISO) führte zu einer stärkeren Betonung der Sicherheitsfragen bei Informationssystemen, Architekturen, Normen, Kommunikationsprotokollen und Techniken.

15. Nur schätzungsweise 2 % der Dienste, die bis zum Jahr 2000 in der Gemeinschaft bereitstehen werden, sind heute schon verfügbar. Bis dahin werden die Dienste generell auf den Benutzerbedarf eingehen können und ein Spektrum an integrierten Merkmalen mit flexibler Kombination von Sprach-, Daten- und Bildübertragung bieten. Dementsprechend wird es wesentlich schwieriger sein, den Benutzeranforderungen an die Informationssicherheit wie Datenschutz, Schutz der Privatsphäre, Authentifizierung, Genehmigung, Fakturierung usw. gerecht zu werden. Daher sind die Informationssicherheit und entsprechende technische Merkmale wie Integrität u.a. systematisch zu entwickeln und zu untersuchen. Die US-Behörden finanzieren Programme für sichere Computersysteme, offene Systemarchitekturen, Protokolle und Techniken, die den Einsatz anwenderspezifischer Sicherheitslösungen international beschleunigen. Die Mitgliedstaaten müssen in erster Linie bestrebt sein, ein gleichberechtigter Partner bei der Lösung von Normungsfragen in diesem Bereich zu sein. Die Übernahme einer De- facto-Normung würde zu neuen technologischen Abhängigkeiten führen, die die internationale Wettbewerbsfähigkeit der EG-Wirtschaft ernsthaft gefährden könnten. Daher sind in der Gemeinschaft entsprechende Maßnahmen zu treffen, die die Voraussetzung für eine konstruktive Interaktion mit Drittländern, insbesondere den USA, bilden.

16. Kurz, die Gemeinschaft und ihre Mitgliedstaaten sind angesichts ihrer jeweiligen Verantwortlichkeit an folgenden Kernfragen besonders interessiert:

    - Wie sind wirksame Spezifikationen und Normen der Informationssicherheit festzulegen und zu verbreiten?

    - Wie sind die formale Bewertung und Zertifizierung der Normenkonformität von Produkten und Systemen (sowohl funktional als auch hinsichtlich der Qualitätssicherung) zu realisieren?

    - Wie sind Sicherheitsprodukte und -systeme zu realisieren, bereitzustellen und einzusetzen?

17. Informationssicherheit ist ein typisches Beispiel für eine Politik, bei der angesichts der Komplexität des Themas, der Beteiligung zahlreicher Akteure und der Notwendigkeit, eine Reihe politischer Werkzeuge einzusetzen, das Prinzip der Subsidiarität zum Tragen kommt. In einem Aktionsplan wird im wesentlichen festgelegt, was von wem und wie zu tun ist. Einerseits müssen die Mitgliedstaaten diese Fragen bearbeiten; andererseits ist die Gemeinschaft sehr daran interessiert, Bedingungen auszuarbeiten, die sowohl die Kompatibilität zwischen der Vollendung des Binnenmarktes, der Schaffung des Europas der Bürger, der Einführung einer Telekommunikationspolitik, der Wettbewerbsfähigkeit der europäischen Elektronikindustrie und Informationsdienste als auch die Erfüllung grundlegender Anforderungen von Einzelpersonen und Geschäftsleuten an die Informationssicherheit gewährleistet. Daher werden nachstehend im Hinblick auf die Konzentration der Maßnahmen verschiedene Aktionstypen und eine Verfahrensstruktur als Basis für weitere eingehende Studien vorgeschlagen, aufgrund derer Maßnahmen auf den jeweiligen Ebenen getroffen werden können.

VORSCHLAG FÜR EINEN BESCHLUSS DES RATES AUF DEM GEBIET DER INFORMATIONSSICHERHEIT

DER RAT DER EUROPÄISCHEN GEMEINSCHAFTEN -

gestützt auf den Vertrag zur Gründung der Europäischen Wirtschaftsgemeinschaft, insbesondere auf Artikel 235,

auf Vorschlag der Kommission (1) ,

nach Stellungnahme des Europäischen Parlaments (2)

nach Stellungnahme des Wirtschafts- und Sozialausschusses (3),

in Erwägung nachstehender Gründe:

Aufgabe der Gemeinschaft ist es, durch Schaffung eines Gemeinsamen Marktes und stufenweise Annäherung der Wirtschaftspolitiken der Mitgliedstaaten gemeinschaftsweit eine harmonische Entwicklung der Wirtschaftstätigkeit, eine stetige und ausgewogene Expansion, erhöhte Stabilität, eine beschleunigte Anhebung der Lebensqualität und engere Beziehungen zwischen den Mitgliedstaaten zu fördern.

Elektronisch gespeicherte, verarbeitete und übertragene Informationen spielen bei den sozialen und wirtschaftlichen Tätigkeiten eine immer wichtigere Rolle.

Mit der Einführung effizienter globaler Kommunikationsdienste und der immer weiter verbreiteten elektronischen Informationsverarbeitung wächst der Bedarf an angemessenen Schutzmaßnahmen.

Das Europäische Parlament hat in seinen Beratungen und Beschlüssen wiederholt auf die Bedeutung der Informationssicherheit hingewiesen.

---

(1) ABl. Nr. C
(2) ABl. Nr. C
(3) ABl. Nr. C

Der Wirtschafts- und Sozialausschuß hat auf die Notwendigkeit hingewiesen, im Rahmen der Gemeinschaftsaktionen Fragen der Informationssicherheit zu behandeln, wobei insbesondere die Auswirkungen der Vollendung des Binnenmarkt zu berücksichtigen sind.

Es muß eine umfassende Strategie der Informationssicherheit entwickelt werden, um die Sicherheit des Benutzers auf Gemeinschaftsebene zu gewährleisten und die Entstehung neuer technischer Hindernisse für das Kommunikationswesen zu vermeiden. Die Komplexität der Informationssicherheit erfordert Subsidiarität, Beteiligung verschiedener Akteure und die konzertierte Durchführung mehrerer Politiken.

Aktionen auf nationaler, internationaler und Gemeinschaftsebene bilden hierfür eine solide Basis.

Es besteht eine enge Verbindung zu den Politiken in den Bereichen Telekommunikation, Normung, Informationsmarkt und Forschung und Entwicklung und zu der Arbeit, die die Europäische Gemeinschaft auf diesen Gebieten bereits geleistet hat.

Die Konzertierung der Maßnahmen sollte unter Zugrundelegung der laufenden Arbeiten auf nationaler und internationaler Ebene und durch Förderung der Zusammenarbeit der wichtigsten Akteure gewährleistet werden. Dies sollte im Rahmen eines kohärenten Aktionsplans geschehen.

Die Verantwortlichkeit der Mitgliedstaaten auf diesem Gebiet beinhaltet einen konzertierten Ansatz, der auf einer engen Zusammenarbeit mit hohen Beamten der Mitgliedstaaten basiert .

BESCHLIESST:

Artikel 1

1. Es wird ein Aktionsplan auf dem Gebiet der Informationssicherheit (INFOSEC) über einen Zeitraum von 24 Monaten verabschiedet, beginnend (....).

2. Der Aktionsplan dient der Entwicklung einer umfassenden Strategie, die für Benutzer von elektronisch gespeicherten, verarbeiteten oder übertragenen Informationen den Schutz der Daten und seines Informationssystems gegen beabsichtigte oder unbeabsichtigte Risiken gewährleistet.

3. Die Aktion berücksichtigt und unterstützt die laufenden europäischen und weltweiten Normungstätigkeiten auf diesem Gebiet.

Artikel 2

Der Aktionsplan gemäß Artikel 1, dessen Einzelheiten im Anhang aufgeführt sind, umfaßt folgende Aktionslinien:

I. Entwicklung einer Rahmenstrategie für Informationssicherheit
II. Anforderungen an die Informationssicherheit
III. Lösungen für den kurz- und mittelfristigen Bedarf
IV. Spezifikation, Normung und Überprüfung der Informationssicherheit
V. Technologische und funktionale Entwicklungen im Hinblick auf die Informationssicherheit
VI. Maßnahmen zur Gewährleistung der Informationssicherheit

Artikel 3

Der Aktionsplan wird von der Kommission in Zusammenarbeit mit den betroffenen Organisationen und Unternehmen und in enger Abstimmung mit den Mitgliedsstaaten durchgeführt.

Artikel 4

Die dieser Aktion zugewiesenen Mittel werden im Rahmen des jährlichen Haushaltsverfahrens bestimmt.

Artikel 5

Die Kommission legt dem Europäischen Parlament und dem Rat innerhalb von drei Monaten nach Abschluß des Aktionsplans einen Bericht über dessen Ergebnisse vor.

Artikel 6

Bei der Durchführung des Aktionsplans konsultiert die Kommission nach Bedarf die Gruppe hoher Beamter Informationssicherheit (SOGIS). Diese setzt sich aus jeweils zwei Vertretern der Mitgliedstaaten und der Kommission zusammen. Den Vorsitz führt ein Vertreter der Kommission.

Die Mitglieder der Gruppe können sich entsprechend der Art der zu erörternden Fragen von Sachverständigen oder Beratern unterstützen lassen.

Die Arbeiten der Gruppe sind vertraulich. Die Gruppe gibt sich ihre eigene Geschäftsordnung. Das Sekretariat wird von der Kommission wahrgenommen.

Geschehen zu Brüssel am

Im Namen des Rates
Der Präsident

ANHANG 1

Übersicht über die Aktionslinien

1. Aktionslinie I - Entwicklung einer Rahmenstrategie für Informationssicherheit

1.1 Problematik

1. Informationssicherheit gilt unbestritten als eine Dimension, die in allen Bereichen der modernen Gesellschaft vorhanden sein muß. Elektronische Informationsdienste erfordern eine sichere Kommunikationsinfrastruktur, sichere Endgeräte (einschließlich Prozessoren und Datenbanken) sowie sichere Anwendungen. Es muß eine Gesamtstrategie entwickelt werden, die alle Aspekte der Informationssicherheit berücksichtigt und somit ein aufgesplittertes Konzept vermeidet. Jegliche Strategie für die Sicherheit der elektronisch verarbeiteten Informationen muß den Wunsch der Gesellschaft berücksichtigen, effizient zu arbeiten und sich gleichzeitig in einem sich rasch wandelnden Umfeld zu schützen.

1.2 Zielsetzung

2. Es muß eine Rahmenstrategie geschaffen werden, um die gesellschaftlichen, wirtschaftlichen und politischen Ziele mit den technischen, operationellen und legislativen Optionen in Einklang zu bringen. Das empfindliche Gleichgewicht zwischen verschiedenen Anliegen, Zielen und Sachzwängen muß von den Akteuren des Bereichs ermittelt werden, die bei der Entwicklung eines gemeinsamen Standpunkts und einer abgestimmten Strategie zusammenarbeiten. Dies sind die Voraussetzungen, um Interessen und Bedürfnisse sowohl im politischen Bereich als auch bei industriellen Entwicklungen zu vereinen.

1.3 Derzeitiger Stand und Tendenzen

3. Charakteristisch für die Lage ist das zunehmende Bewußtsein der Notwendigkeit zu handeln. In Ermangelung einer Konzertierungsinitiative ist es jedoch sehr wahrscheinlich, daß verstreut Maßnahmen in verschiedenen Bereichen ergriffen werden und damit in der Praxis eine widersprüchliche Situation entsteht, die nach und nach zu ernsthaften rechtlichen, gesellschaftlichen und wirtschaftlichen Problemen führt.

1.4 Anforderungen, Optionen und Prioritäten

4. Innerhalb eines solchen Rahmens wären Risikoanalyse und Risikomanagement zu behandeln und abzugrenzen. Diese betreffen: die Schwachstellen der Informationsdienste, die Angleichung von Gesetzen und Regelungen im Zusammenhang mit dem Mißbrauch von Computern und Telekommunikationsdiensten, Verwaltungsinfrastrukturen einschließlich Sicherheitspolitiken und die Frage, wie sich diese in verschiedenen Industrien/Disziplinen effizient einführen lassen, und schließlich soziale und private Anliegen (z.B. die Einführung von Plänen für Identifizierung, Authentifizierung und gegebenenfalls Zugangsberechtigung in einem demokratischen Umfeld).

5. Es bedarf einer klaren Ausrichtung für die Entwicklung physischer und logischer Architekturen für sichere verteilte Informationsdienste, Normen, Leitlinien und Definitionen für Sicherheitsprodukte und -dienste, Pilotprojekte und Prototypen, um die Brauchbarkeit verschiedener Verwaltungsstrukturen, Architekturen und Normen, gemessen an dem Bedarf spezifischer Bereiche, zu ermitteln.

6. Es muß ein Sicherheitsbewußtsein geschaffen werden, damit die Benutzer die Sicherheit in der Informationstechnologie und in Telekommunikationssystemen zu ihrem eigenen Anliegen machen.

2. Aktionslinie II - Anforderungen an die Informationssicherheit

2.1 Problematik

7. Informationssicherheit ist die unerläßliche Voraussetzung für den Schutz der Privatsphäre, des geistigen Eigentums, des gewerblichen Rechtsschutzes und der nationalen Sicherheit. Dies führt unweigerlich zu einem empfindlichen Gleichgewicht und erfordert gelegentlich eine Wahl zwischen einem Engagement für den freien Handel und einem Engagement für den Schutz der Privatsphäre und des geistigen Eigentums. Diese Entscheidungen und Kompromisse müssen auf einer Gesamteinschätzung des Bedarfs und der Auswirkungen möglicher Informationssicherheitsoptionen basieren, die sich zur Deckung dieses Bedarfs anbieten.

8. Die Benutzeranforderungen umfassen Funktionalitäten in Verbindung mit technologischen, operationellen und ordnungspolitischen Aspekten. Daher ist eine systematische Untersuchung der Anforderungen an die Informationssicherheit für die Entwicklung geeigneter und wirksamer Maßnahmen unerläßlich.

2.2 Zielsetzung

9. Ermittlung der Benutzeranforderungen (Art und Merkmale) und ihre Beziehung zu Informationssicherheitsmaßnahmen.

2.3 Derzeitiger Stand und Tendenzen

10. Bislang wurden keine konzertierten Maßnahmen ergriffen, um den Bedarf der Hauptakteure im Bereich der Informationssicherheit zu ermitteln, der sich rasch weiterentwickelt und ständig verändert. Die EG-Mitgliedstaaten haben den Harmonisierungsbedarf der nationalen Tätigkeiten (insbesondere in bezug auf "IT-Sicherheitskriterien") festgelegt. Einheitliche Bewertungskriterien und Regeln für die gegenseitige Anerkennung der Bewertungsergebnisse und Zertifikate sind von grundlegender Bedeutung.

2.4 Anforderungen, Optionen und Prioritäten

11. Als Grundlage für eine kohärente und transparente Behandlung der fundierten Bedürfnisse der Akteure ist eine abgestimmte Klassifizierung der Benutzeranforderungen und ihrer Beziehungen zu den Maßnahmen zur Gewährleistung der Informationssicherheit zu entwickeln.

12. Ferner sind die Anforderungen an Rechts- und Verwaltungsvorschriften und Verfahrensregeln festzulegen. Dabei sind die aktuellen Trends der Dienstmerkmale und Technologien zu berücksichtigen, um alternative Strategien zur Erreichung der Ziele durch administrative, dienstspezifische, operationelle und technische Bestimmungen zu entwickeln. Ferner sind die Wirksamkeit, Benutzerfreundlichkeit und Kosten alternativer Optionen und Strategien der Informationssicherheit für Benutzer, Diensteanbieter und Netz-Betreiber einzuschätzen.

3. Aktionslinie III - Lösungen für den kurz- und mittelfristigen Bedarf

3.1 Problematik

13. Computer können heutzutage gegen unberechtigten externen Zugriff durch "Isolierung", d.h. konventionelle organisatorische und technische Maßnahmen, hinreichend geschützt werden. Dies gilt auch für die elektronische Kommunikation, die innerhalb einer geschlossenen Benutzergruppe über ein dediziertes Netz abgewickelt wird. Eine ganz andere Situation ergibt sich, wenn Informationen mehreren Benutzergruppen zur Verfügung stehen oder über ein öffentliches bzw. allgemein zugängliches Netz ausgetauscht werden. Hier stehen grundsätzlich weder die Technologien, Endgeräte und Dienste noch die entsprechenden Normen und Verfahren zur Verfügung, um eine vergleichbare Informationssicherheit zu gewährleisten.

3.2 Zielsetzung

14. Ziel ist es, kurzfristig Lösungen zu erarbeiten, die dem dringendsten Benutzerbedarf gerecht werden. Sie sollten "offen" konzipiert sein, um auch künftige Anforderungen und Lösungen zu berücksichtigen.

3.3 Derzeitiger Stand und Tendenzen

15. Einige Benutzergruppen haben Techniken und Verfahren für ihre speziellen Anwendungen entwickelt, die insbesondere dem Bedarf an Authentifizierung, Integrität und Nachweisbarkeit gerecht werden. In der Regel werden Magnet- oder Chipkarten verwendet. Teilweise bedient man sich mehr oder weniger ausgefeilter Verschüsselungstechniken. Hierzu sind häufig Benutzergruppen spezifischer "Instanzen" zu definieren. Eine Anpassung dieser Techniken und Verfahren an die Anforderungen einer offenen Umgebung erweist sich jedoch als schwierig.

16. Die ISO entwickelt derzeit eine OSI-Informationssicherheitsnorm (ISO DiS 7498-2), während der CCITT diese Frage im Zusammenhang mit dem X.400 bearbeitet. Eine Möglichkeit besteht darin, Sicherheitssegmente in die Nachrichten zu integrieren. Authentifizierung, Integrität und Akzeptanz werden als Teil der Nachrichten (EDIFACT) und des Systems X.400 MHS behandelt.

17. Gegenwärtig befindet sich der rechtliche Rahmen für den elektronischen Datenaustausch noch in der Entwicklungsphase. Die internationale Handelskammer hat einheitliche Verhaltensregeln für den Austausch von kommerziellen Daten über Telekommunikationsnetze veröffentlicht.

18. Mehrere Länder (z.B. Deutschland, Frankreich, UK und USA) haben Kriterien zur Bewertung der Vertrauenswürdigkeit von IT- und Telekommunikationsprodukten und -systemen sowie entsprechende Bewertungsverfahren entwickelt bzw. in Arbeit. Diese Kriterien wurden mit den nationalen Herstellern koordiniert und werden in zunehmendem Maße die Entwicklung sicherer Produkte und Systeme, ausgehend von einfachen Produkten, ermöglichen. Dieser Trend wird durch die Einrichtung nationaler Organisationen unterstützt, die Bewertungen durchführen und Zertifikate erteilen.

19. Maßnahmen zur Wahrung der Vertraulichkeit werden von den meisten Benutzern für weniger dringend erachtet. Künftig wird sich diese Lage jedoch angesichts der allgemeinen Verbreitung moderner Kommunikationsdienste, insbesondere der Mobilfunkdienste, voraussichtlich ändern.

3.4 Anforderungen, Optionen und Prioritäten

20. Die Verfahren, Normen, Produkte und Werkzeuge zur Gewährleistung der Informationssicherheit in öffentlichen Kommunikationsnetzen müssen umgehend entwickelt werden. Hohe Prioritat kommt dabei der Authentifizierung, Integrität und Nachweisbarkeit zu. Pilotprojekte sind durchzuführen, um die vorgeschlagenen Lösungen auf ihre Eignung zu prüfen. Lösungen für prioritäre Anforderungen im Bereich des elektronischen Datenaustausches werden mit dem Programm TEDIS angestrebt, das sich in den breiteren Rahmen dieses Aktionsplans einfügt.

4. Aktionslinie IV - Spezikation, Normung und Überprüfung der Informationssicherheit

4.1 Problematik

21. Anforderungen an die Informationssicherheit stellen sich in allen Bereichen; daher sind gemeinsame Spezifikationen und Normen unerläßlich. Solange keine abgestimmten Normen und Spezifikationen vorliegen, können sich daraus wesentliche Hindernisse für den Fortschritt informationsgestützter Vorgänge und Dienste in der gesamten Wirtschaft und Gesellschaft ergeben. Es müssen Maßnahmen ergriffen werden, um die Entwicklung und den Einsatz von Technologien und Normen in verschiedenen zusammenhängenden Kommunikations- und Computernetzen zu beschleunigen, die für Benutzer, Industrieunternehmen und Verwaltungen von ausschlaggebender Bedeutung sind.

4.2 Zielsetzung

22. Es sind Maßnahmen zu treffen, um die Unterstützung und Durchführung spezieller Funktionen in den allgemeinen Bereichen OSI, ONP, ISDN/IBC, Netzmanagement und Netzsicherheit für nicht klassifizierte, jedoch sensitive Informationen zu ermöglichen. In engem Zusammenhang mit der Normung und Spezifikation stehen die notwendigen Überprüfungstechniken und -konzepte.

4.3 Derzeitiger Stand und Tendenzen

23. Vor allem die USA haben größere Initiativen zur Frage der Informationssicherheit im nichtmilitärischen Bereich ergriffen. In Europa wird dieses Thema von ETSI und CEN/CENELEC im Zusammenhang mit der IT- und Telekommunikationsnormung als Vorbereitung der entsprechenden Arbeiten des CCITT und der ISO behandelt.

24. Da dieses Thema immer mehr in den Brennpunkt rückt, werden die Arbeiten in den USA zügig vorangetrieben; Hersteller und Diensteanbieter verstärken ihre Bemühungen in diesem Bereich. in Europa haben Frankreich, die Bundesrepublik Deutschland und das Vereinigte Königreich unabhängig voneinander ähnliche Tätigkeiten aufgenommen; ein gemeinsamer Vorstoß wie in den USA zeichnet sich jedoch nur zögernd ab.

4.4 Anforderungen, Optionen und Prioritäten

25. Im Bereich der Informationssicherheit besteht zwangsläufig eine enge Verbindung zwischen ordnungspolitischen, operationellen, administrativen und technischen Aspekten. Staatliche Vorschriften sind in Normen zu berücksichtigen; Maßnahmen zur Gewährleistung der Informationssicherheit müssen nachweislich den Normen und Vorschriften entsprechen. In mehrfacher Hinsicht erfordern Vorschriften Spezifikationen, die über den traditionellen Bereich der Normung hinausgehen, d.h. Verfahrensregeln beinhalten. Anforderungen an Normen und Verfahrensregeln gibt es in allen Bereichen der Informationssicherheit. Dabei ist zu unterscheiden zwischen den Schutzanforderungen, die den Sicherheitszielen entsprechen, und einigen technischen Anforderungen, mit deren Erfüllung die zuständigen europäischen Normungsgremien (CEN/CENELEC/ETSI) beauftragt werden können.

26. Spezifikationen und Normen müssen zahlreiche Bereiche abdecken: die der Informationssicherheitsdienste (Authentifizierung von Personen und Unternehmen, Protokolle für die Nachweisbarkeit, rechtlich zulässige elektronische Belege, Berechtigungskontrolie>, Kommunikationsdienste (Schutz der Privatsphäre bei Bild-, Mobil- und Datenkommunikation, Schutz von Daten- und Bildbanken, Sicherheit integrierter Dienste), Kommunikations- und Sicherheitsmanagement (öffentliche/private Schlüsselsysteme für "offenen" Netzbetrieb, Schutz des Netzmanagements, Schutz der Diensteanbieter) und Zertifizierung (Kriterien und Stufen der Informationssicherheit, Verfahren zur Gewährleistung der Sicherheit).

5. Aktionslinie V - Technologische und funktionale Entwicklungen im Hinblick auf die Informationssicherheit

5.1 Problematik

27. Voraussetzung für die Entwicklung des Dienstemarktes und der Wettbewerbsfähigkeit der Europäischen Wirtschaft insgesamt ist die systematische Erforschung und Entwicklung der Technologien, um wirtschaftlich rentable und operationell zufriedenstellende Lösungen für eine Reihe gegenwärtiger und künftiger Anforderungen an die Informationssicherheit zu erarbeiten.

28. Bei technologischen Entwicklungen im Hinblick auf die Sicherheit der Informationssysteme sind grundsätzlich Aspekte sowohl der Computersicherheit als auch der Kommunikationssicherheit zu berücksichtigen, da es sich bei den heutigen Systemen überwiegend um verteilte Systeme handelt und der Zugang über Kommunikationsdienste erfolgt.

5.2 Zielsetzung

29. Systematische Erforschung und Entwicklung der Technologien, um wirtschaftlich rentable und operationell zufriedenstellende Lösungen für eine Reihe gegenwärtiger und künftiger Anforderungen zu erarbeiten.

5.3 Anforderungen, Optionen und Prioritäten

30. Die Arbeiten im Bereich der Informationssicherheit betreffen Entwicklungs- und Implementierungsstrategien, Technologien, Integration und Überprüfung.

31. Die strategischen FuE-Arbeiten müssen theoretische Modelle für sichere Systeme, Modelle der Funktionsanforderungen, Risikomodelle und Sicherheitsarchitekturen abdecken.

32. Die technologischen FuE-Arbeiten müssen die Authentifizierung von Benutzern und Nachrichten (z.B. durch Stimmerkennung und elektronische Unterschriften), technische Schnittstellen und Protokolle für die Verschlüsselung, Zugriffskontrollmechanismen und Implementierungsverfahren für nachweislich sichere Systeme abdecken.

33. Integrations- und Überprüfungsprojekte dienen der Verifikation und Validierung der technischen Systemsicherheit und ihrer Anwendbarkeit.

34. Über die Entwicklung und Konsolidierung von Sicherheitstechnologien hinaus sind eine Reihe von flankierenden Maßnahmen notwendig. Diese betreffen die Erstellung, Aktualisierung und konsequente Anwendung von Normen sowie die Validierung und Zertifizierung von IT- und Telekommunikationsprodukten in bezug auf ihre Sicherheitsmerkmale; dazu gehören auch die Validierung und Zertifizierung von Verfahren zum Entwurf und zur Implementierung der Systeme.

35. Aufgrund des dritten FuE-Rahmenprogramms der Gemeinschaft können kooperative Projekte auf vorwettbewerblicher und pränormativer Ebene gefördert werden.

6. Aktionslinie VI - Maßnahmen zur Gewährleistung der Informationssicherheit

6.1 Problematik

36. Je nach Art der erforderlichen Sicherheitsmerkmale sind die Funktionen an verschiedenen Stellen der Kommunikationssysteme zu integrieren. Hierzu gehören Endgeräte/Computer/Dienste, Netzmanagement ebenso wie Verschlüsselungsgeräte, Chipkarten, öffentliche und private Schlüssel usw. Einige Funktionen können voraussichtlich vom Hersteller in die Hard- oder Software integriert werden, während andere Bestandteil verteilter Systeme sind (z.B. Netzmanagement), sich im Besitz des einzelnen Benutzers befinden (z.B. Chipkarten) oder von einer besonderen Organisation geliefert werden (z.B. öffentliche/private Schlüssel).

37. Informationssicherheitsprodukte und -dienste dürften überwiegend von Herstellern, Diensteanbietern oder Netz-Betreibern bereitgestellt werden. Für spezielle Funktionen, z.B. die Zuteilung öffentlicher/privater Schlüssel, Überwachung oder Berechtigungskontrolle müssen ggf. entsprechende Organisationen bestimmt und beauftragt werden.

38. Gleiches gilt für die Zertifizierung, Bewertung und Überprüfung der Dienstqualität. Diese Aufgaben müssen von Organisationen wahrgenommen werden, die von den Interessen der Hersteller, Diensteanbieter und Netz-Betreiber nicht beeinflußt werden. Dies können private oder staatliche Organisationen sein oder solche, die eine staatliche Lizens zur Ausübung bestimmter Funktionen besitzen.

6.2 Zielsetzung

39. Um die harmonische Entwicklung der Informationssicherheit in der Gemeinschaft im Hinblick auf den Schutz öffentlicher und geschäftlicher Interessen zu fördern, ist ein kohärentes Konzept zu entwickeln. Soweit damit unabhängige Organisationen beauftragt werden müssen, sind ihre Funktionen und Bedingungen festzulegen und abzustimmen und nach Bedarf in den ordnungspolitischen Rahmen zu integrieren. Ziel ist es, eine klar definierte und abgestimmte Verteilung der Zuständigkeiten unter den verschiedenen Akteuren auf Gemeinschaftsebene als Voraussetzung für die gegenseitige Anerkennung zu erreichen.

6.3 Derzeitiger Stand und Tendenzen

40. Zum gegenwärtigen Zeitpunkt sind Informationssicherheitsmaßnahmen nur in bestimmten Bereichen durchorganisiert und beschränken sich auf spezielle Bedürfnisse. Die Organisation auf europäischer Ebene ist zumeist informell und die gegenseitige Anerkennung der Überprüfung und Zertifizierung, ausgenommen in geschlossenen Gruppen, noch nicht eingeführt. Mit der zunehmenden Bedeutung der Informationssicherheit wird die Festlegung eines kohärenten Konzepts der Informationssicherheitsmaßnahmen in Europa und international zu einem dringenden Anliegen.

6.4 Anforderungen, Optionen und Prioritäten

41. Angesichts der Zahl der betroffenen Akteure und des engen Zusammenhangs mit ordnungspolitischen und rechtlichen Fragen muß in erster Linie eine Einigung über die Grundsätze erzielt werden, die für den Bereich der Informationssicherheit gelten sollen.

Bei der Entwicklung eines kohärenten Konzepts zu dieser Frage sind die Aspekte der Festlegung und Spezifikation von Funktionen zu prüfen, die eine unabhängige Organisation (bzw. kooperierende Organisationen) erfordern. Dies gilt unter anderem für Funktionen wie die Verwaltung eines öffentlichen/privaten Schlüsselsystems.

Ferner sind zu einem frühen Zeitpunkt die Funktionen festzulegen und zu spezifizieren, die im öffentlichen Interesse einer unabhängigen Organisation (bzw. kooperierenden Organisationen) übertragen werden müssen. Dies gilt beispielsweise für Überwachung, Qualitätssicherung, Überprüfung, Zertifizierung und ähnliche Funktionen.

FINANCIAL STATEMENT

Information Security (INFOSEC)
Preparatory Action

1. **BUDGET HEADING**

Subsection B6, Item 8104

2. **LEGAL BASE AND PROPOSED CLASSIFICATION**

Article [235]

Non compulsory expenditure.

3. DESCRIPTION

Collaboration in the development of proposals and actions relating to information security as far as they require or significantly benefit from a concerted approach at Community level. The focus of the work is to relate to the needs of the general public, commerce, service providers and administrations and addresses the requirements for a collaborating approach to technological research, standardisation and related issues as relevant for the development or a consistent European approach to information security with particular reference to the completion of the internal market in 1992.

The goal of the INFOSEC action is to make a major contribution to the objective of the

"development of actions to providing effective and practical security for information held in an electronic form to the general users, administrations and business community without compromising the interest of the public at large."

The present proposal is the result of the preliminary investigations by experts, consultations and on-going related work.

The scope of the preparatory action is to focus on

I. development of an information security strategy framework
II. information security requirements
III. solutions for immediate and interim needs
IV. specifications, standardisation and verification of information security
V. technological and operational developments for information security
VI. information security provision.

4. JUSTIFICATION

Development of a harmonised approach to information security must form an integral part of the Community policies related to the completion of the Internal Market, strengthening of socio-economic performance and international competitiveness. It is vital that Information Security does not become a constraint to the promotion of harmonious development in the Community and to relations with other countries. In addition, information security systems must protect privacy, intellectual property, fair competition, national security and other interests.

The proposed action responds to an urgent need to facilitate and accelerate the emergence of generally accepted, effective and practicable measures in information security. The action will benefit from synergies with on-going programmes in the field of information technologies (ESPRIT) and telecommunications (RACE) as well as the on-going work on telecommunications, standardisation and information market policies.

5. INDICATIVE FINANCIAL PLANNING

5.0 *Implications for expenditure.*

5.0.0 Total cost over the whole of the expected duration of 2 years (in MioECU):

From the Budget of the Communities:	12.0
From the other sectors at the national level:	0.0
TOTAL	12.0

5.0.1 Multi-annual schedule (in MioECU):

	Commitment Appropriations	Payment Appropriations
1991	6	4
1992	6	6
1993	-	2
	12	12

5.0.2 Method of calculation

a) Expenditure by contract

This expenditure covers the Community's financial contribution to analytical work as required to support the development of specific actions proposals, for consultation and establishment of consensus.

b) Operational expenditure

Given the fact that the action is financed in Subsection 6 of the budget devoted to Research and Investment expenditure, administrative costs (Committee and working party meetings, consultation of experts, missions, document distribution or dissemination of techniques, use of data processing, telecommunication and broadcasting equipment) are covered directly by the budget item.

The following table fives the indicative breakdown over the various categories of expenditure (in MioECU):

			1991	1992
5.0.2	a)		4,823	4,100
5.0.2	b)	in total	1,177	1,900
of which		Experts	*0,400*	*0,600*
		Other operational expenditure	*0,500*	*0,725*
		Infrastructure	*0,050*	*0,100*
		Information and publication	*0,050*	*0,100*
		Statutory staff	*0,177*	*0,375*

6. FINANCIAL IMPLICATIONS FOR STAFF AND CURRENT ADMINISTRATIVE APPROPRIATIONS

The statutory research staff involved, i.e. 3 A, 1 B, 1 C, will be entered in the research staff table and is paid out of the appropriations entered onto Item B6-8104.

The administrative expenditure will be governed by the internal rules on mini-budgets decided by the Commission on 22 May 1990.

7. FINANCING OF EXPENDITURE

The appropriations to cover the Community's contribution to this project will be determined in the context of the annual budgetary procedure.

8. IMPLICATIONS FOR REVENUE

Contribution of the statutory research staff to the retirement scheme and the sickness insurance.

9. TYPE OF CONTROL

- Administrative control by the Director General for Financial Control as regards budget implementation;
- Control of achievement:
  - SOG-IS
  - control by officials of the Commission
  - audit by the Court of Auditors in accordance with provisions of the Treaty;
- In accordance with Article 2 of the Financial Regulations, the use of appropriations will be subject to analyses of cost-effectiveness and the realisation of quantified objectives will be monitored.