Bundesrat **Drucksache 966/96**

20. 12. 96

K - In - R - VP - Wi

Gesetzentwurf

der Bundesregierung

Entwurf eines Gesetzes zur Regelung der Rahmenbedingungen für Informations- und Kommunikationsdienste (Informations- und Kommunikationsdienste-Gesetz – IuKDG)

A. Zielsetzung

Der Gesetzentwurf trägt dem tiefgreifenden Wandel der Informations- und Kommunikationstechnologie Rechnung. Ziel des Gesetzes ist es, im Rahmen der Bundeskompetenzen eine verläßliche Grundlage für die Gestaltung der sich dynamisch entwickelnden Angebote im Bereich der Informations- und Kommunikationsdienste zu bieten und einen Ausgleich zwischen freiem Wettbewerb, berechtigten Nutzerinteressen und öffentlichen Ordnungsinteressen herbeizuführen.

Gesetzlicher Handlungsbedarf besteht in zwei Richtungen: Zum einen geht es um die Beseitigung von Hemmnissen für die freie Entfaltung der Marktkräfte im Bereich der neuen Informations- und Kommunikationsdienste und die Gewährleistung einheitlicher wirtschaftlicher Rahmenbedingungen für das Angebot und die Nutzung dieser Dienste. Zum anderen geht es um die Einführung notwendiger Regelungen im Datenschutz, in der Datensicherheit, im Urheberrecht, im Jugendschutz und Verbraucherschutz sowie zu Verantwortlichkeiten, die auch Änderungen in bestehenden Bundesgesetzen notwendig machen.

Der Gesetzentwurf berücksichtigt die Empfehlungen des Rates für Forschung, Technologie und Innovation (Technologierat), Vorschläge des „Petersberg Kreis" sowie Ergebnisse der Bund-Länder Arbeitsgruppe „Multimedia" und setzt die im Bericht der Bundesregierung „Info 2000 – Deutschlands Weg in die Informa-

---

Fristablauf: 31. 01. 97; vgl. jedoch Vorschlag eines Fristverlängerungsverlangens gemäß Artikel 76 Abs. 2 Satz 3 GG in Drucksache 966/1/96. Bei entsprechender Beschlußfassung läuft die Frist zur Stellungnahme am 21. 02. 97 ab.

Druck: Bonner Universitäts-Buchdruckerei, 53113 Bonn
Vertrieb: Bundesanzeiger Verlagsgesellschaft mbH, Postfach 13 20, 53003 Bonn, Telefon: 02 28/3 82 08 40, Telefax: 02 28/3 82 08 44
ISSN 0720-2946

tionsgesellschaft" aufgezeigten Handlungsoptionen um. Der Technologierat hat akuten Handlungsbedarf für einheitliche und angemessene, auf das notwendige Maß beschränkte Rahmenbedingungen für die neuen Informations- und Kommunikationsdienste gesehen und entsprechende Regelungen empfohlen.

B. Lösung

Der Gesetzesentwurf sieht folgende Regelungen vor:

- Artikel 1:
  Rahmenbedingungen für das Angebot und die Nutzung von Telediensten durch Sicherstellung der Zugangsfreiheit sowie Schließung von Regelungslücken im Verbraucherschutz und Klarstellung von Verantwortlichkeiten der Diensteanbieter.
- Artikel 2:
  Bereichsspezifische Regelungen zum Datenschutz bei Telediensten im Hinblick auf die erweiterten Risiken der Erhebung, Verarbeitung und Nutzung personenbezogener Daten.
- Artikel 3:
  Schaffung einer bundeseinheitlichen Sicherungsinfrastruktur für digitale Signaturen.
- Artikel 4 und 5:
  Klarstellungen des Schriftenbegriffs im Strafgesetzbuch und im Ordnungswidrigkeitengesetz im Hinblick auf die erweiterten Nutzungs- und Verbreitungsmöglichkeiten von rechtswidrigen Inhalten.
- Artikel 6:
  Kernbereich der spezifischen Jugendschutzregelungen des IuKDG mit dem Ziel einer effektiven Gewährleistung des Jugendschutzes und einer einheitlichen Anwendung des Schriftenbegriffs; außerdem Einführung technischer Sperrvorrichtungen im Zusammenhang mit der Verbreitung indizierter Angebote sowie die Bestellung von Jugendschutzbeauftragten als Anlaufstation für Nutzer und als Berater für die Diensteanbieter.
- Artikel 7:
  Umsetzung der Richtlinie des Europäischen Parlamentes und des Rates vom 11. März 1996 über den rechtlichen Schutz von Datenbanken (RL 96/9/EG) durch entsprechende Änderung des Urheberrechtes.
- Artikel 8 und 9:
  Erstreckung des Verbraucherschutzes im Preisangabengesetz und in der Preisangabenverordnung auf die erweiterten Nutzungsmöglichkeiten durch die neuen Dienste.
- Artikel 10 und 11:
  Gesetzestechnische Regelungen (Rückkehr zum einheitlichen Verordnungsrang und Inkrafttreten).

C. Alternativen

keine

D. Kosten der öffentlichen Haushalte

Mit diesem Gesetz sind folgende Kosten für den Bundeshaushalt verbunden (Vollzugsaufwand):

Kosten entstehen nur im Zusammenhang mit den Aufgaben der zuständigen Behörde nach § 3 Signaturgesetz (Regulierungsbehörde nach § 66 Telekommunikationsgesetz). Der Personalaufwand in der Regulierungsbehörde, die für die Aufgaben nach dem Signaturgesetz vorgesehen ist, wird bis zu vier Planstellen für Beamte des gehobenen Dienstes oder für vergleichbare Angestellte betragen. Der bei der Regulierungsbehörde für diese Aufgabe zu erwartende Sachaufwand wird DM 200 000,– nicht übersteigen.

Für öffentliche Leistungen nach dem Signaturgesetz ist eine aufwandsbezogene Kostenerhebung (Gebühren und Auslagen) durch die Regulierungsbehörde vorgesehen.

Eine Kostenaufstellung für den Zeitraum der mehrjährigen Finanzplanung des Bundes ist derzeit nicht möglich, da noch keine Festlegungen in bezug auf die Mittel für die zum 1. Januar 1998 zu errichtende Regulierungsbehörde getroffen worden sind.

Weitere Kosten der Ausführung des Informations- und Kommunikationsdienstegesetzes sind nicht zu erwarten.

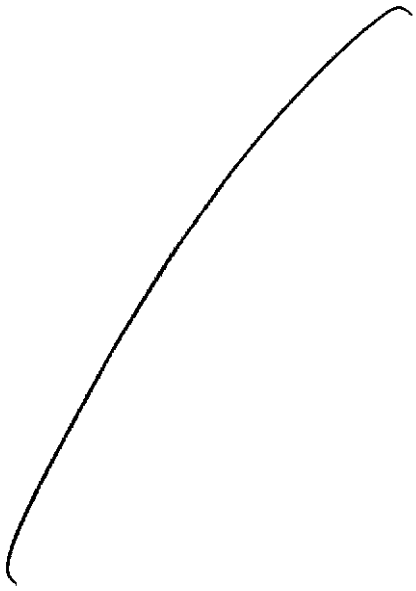
Länder und Gemeinden werden mit Kosten nicht belastet.

E. Sonstige Kosten

Die Wirtschaftsverbände und Unternehmen, auch der mittelständischen Wirtschaft, sind zu den mit der Umsetzung des Gesetzes (u.a. Datenschutz, Jugendschutz, digitale Signaturen) zu erwartenden Kosten um Stellungnahme gebeten worden. Diese Kosten können im Einzelfall erheblich sein. Sie sind abhängig von der Organisationsform und dem Grad der jeweiligen Inanspruchnahme und können – auch von der betroffenen Wirtschaft – gegenwärtig nicht eindeutig beziffert werden.

Die mit dem Gesetz verbundene Schaffung einheitlicher und verläßlicher Rahmenbedingungen sowie die Beseitigung von Investitionshemmnissen für die neuen Informations- und Kommunikationsdienste läßt erwarten, daß hiervon Impulse für ein verstärktes Wachstum in diesem Wirtschaftsbereich ausgehen. Die Regelungen führen daher bei einer Gesamtbetrachtung eher zu einer Entlastung der Wirtschaft. Von der Förderung des Wettbewerbes gehen tendenziell dämpfende Einflüsse auf Einzelpreise aus. Auswirkungen auf das Preisniveau, insbesondere das Verbraucherpreisniveau, sind jedoch nicht zu erwarten.

966/96



Bundesrat **Drucksache 966/96**

20. 12. 96

K - In - R - VP - Wi

Gesetzentwurf

der Bundesregierung

Entwurf eines Gesetzes zur Regelung der Rahmenbedingungen für Informations- und Kommunikationsdienste (Informations- und Kommunikationsdienste-Gesetz – IuKDG)

Bundesrepublik Deutschland
Der Bundeskanzler
031 (324) – 262 00 – Mu 5/96

Bonn, den 20. Dezember 1996

An den
Präsidenten des Bundesrates

Hiermit übersende ich gemäß Artikel 76 Abs. 2 des Grundgesetzes den von der Bundesregierung beschlossenen

> Entwurf eines Gesetzes zur Regelung der Rahmenbedingungen für Informations- und Kommunikationsdienste (Informations- und Kommunikationsdienste-Gesetz – IuKDG)

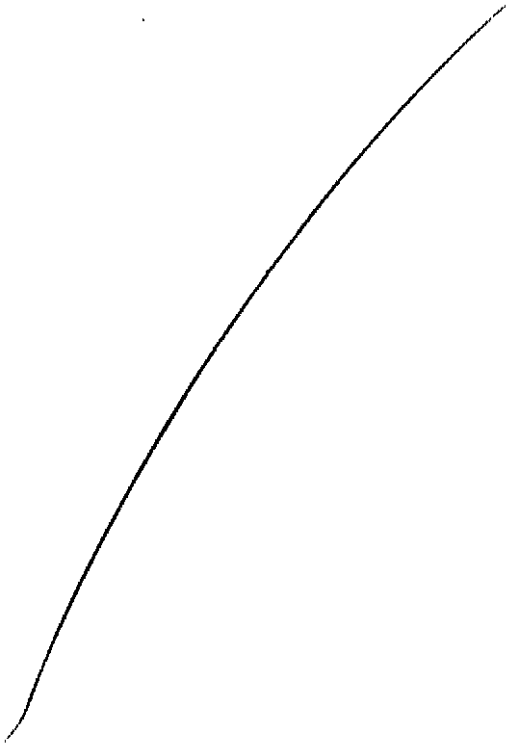
mit Begründung und Vorblatt.

Federführend ist das Bundesministerium für Bildung, Wissenschaft, Forschung und Technologie.

Dr. Helmut Kohl

Fristablauf: 31. 01. 97; vgl. jedoch Vorschlag eines Fristverlängerungsverlangens gemäß Artikel 76 Abs. 2 Satz 3 GG in Drucksache 966/1/96. Bei entsprechender Beschlußfassung läuft die Frist zur Stellungnahme am 21. 02. 97 ab.

966/96



Entwurf eines Gesetzes zur Regelung der Rahmenbedingungen für Informations- und Kommunikationsdienste (Informations- und Kommunikationsdienste-Gesetz – IuKDG)*)

Der Bundestag hat das folgende Gesetz beschlossen:

Inhaltsübersicht

Artikel 1

Gesetz über die Nutzung von Telediensten (Teledienstegesetz – TDG)

Artikel 2

Gesetz über den Datenschutz bei Telediensten (TDDSG)

Artikel 3

Gesetz zur digitalen Signatur (Signaturgesetz – SigG)

Artikel 4

Änderung des Strafgesetzbuches

Artikel 5

Änderung des Gesetzes über Ordnungswidrigkeiten

Artikel 6

Änderung des Gesetzes über die Verbreitung jugendgefährdender Schriften

Artikel 7

Änderung des Urheberrechtsgesetzes

Artikel 8

Änderung des Preisangabengesetzes

Artikel 9

Änderung der Preisangabenverordnung

Artikel 10

Rückkehr zum einheitlichen Verordnungsrang

Artikel 11

Inkrafttreten

*) Artikel 7 dieses Gesetzes dient der Umsetzung der Richtlinie 96/9/EG des Europäischen Parlaments und des Rates vom 11. März 1996 über den rechtlichen Schutz von Datenbanken (ABl. EG Nr. L 77 S. 20).

Artikel 1

Gesetz über die Nutzung von Telediensten (Teledienstegesetz – TDG)

§ 1

Zweck des Gesetzes

Zweck des Gesetzes ist es, einheitliche wirtschaftliche Rahmenbedingungen für die verschiedenen Nutzungsmöglichkeiten der elektronischen Informations- und Kommunikationsdienste zu schaffen.

§ 2

Geltungsbereich

(1) Die nachfolgenden Vorschriften gelten für alle elektronischen Informations- und Kommunikationsdienste, die für eine individuelle Nutzung von kombinierbaren Daten wie Zeichen, Bilder oder Töne bestimmt sind und denen eine Übermittlung mittels Telekommunikation zugrunde liegt (Teledienste).

(2) Teledienste im Sinne von Absatz 1 sind insbesondere

1. Angebote im Bereich der Individualkommunikation (zum Beispiel Telebanking, Datenaustausch),
2. Angebote zur Information oder Kommunikation, soweit nicht die redaktionelle Gestaltung zur Meinungsbildung für die Allgemeinheit im Vordergrund steht (Datendienste, zum Beispiel Verkehrs-, Wetter-, Umwelt- und Börsendaten, Verbreitung von Informationen über Waren und Dienstleistungsangebote),
3. Angebote zur Nutzung des Internets oder weiterer Netze,
4. Angebote zur Nutzung von Telespielen,
5. Angebote von Waren und Dienstleistungen in elektronisch abrufbaren Datenbanken mit interaktivem Zugriff und unmittelbarer Bestellmöglichkeit.

(3) Absatz 1 gilt unabhängig davon, ob die Nutzung der Teledienste ganz oder teilweise unentgeltlich oder gegen Entgelt möglich ist.

(4) Dieses Gesetz gilt nicht für

1. Telekommunikationsdienstleistungen und das geschäftsmäßige Erbringen von Telekommunikationsdiensten nach § 3 des Telekommunikationsgesetzes vom 25. Juli 1996 (BGBl. I S. 1120),

2. Rundfunk im Sinne des § 2 des Rundfunkstaatsvertrages.

(5) Presserechtliche Vorschriften bleiben unberührt.

§ 3

Begriffsbestimmungen

Im Sinne dieses Gesetzes sind

1. „Diensteanbieter" natürliche oder juristische Personen oder Personenvereinigungen, die eigene oder fremde Teledienste zur Nutzung bereithalten oder den Zugang zur Nutzung vermitteln,
2. „Nutzer" natürliche oder juristische Personen oder Personenvereinigungen, die Teledienste nachfragen.

§ 4

Zugangsfreiheit

Teledienste sind im Rahmen der Gesetze zulassungs- und anmeldefrei.

§ 5

Verantwortlichkeit

(1) Diensteanbieter sind für eigene Inhalte, die sie zur Nutzung bereithalten, nach den allgemeinen Gesetzen verantwortlich.

(2) Diensteanbieter sind für fremde Inhalte, die sie zur Nutzung bereithalten, nur dann verantwortlich, wenn sie von diesen Inhalten Kenntnis haben und es ihnen technisch möglich und zumutbar ist, deren Nutzung zu verhindern.

(3) Diensteanbieter sind für fremde Inhalte, zu denen sie lediglich den Zugang zur Nutzung vermitteln, nicht verantwortlich. Eine automatische und kurzzeitige Vorhaltung fremder Inhalte aufgrund Nutzerabfrage gilt als Zugangsvermittlung.

(4) Verpflichtungen zur Sperrung der Nutzung rechtswidriger Inhalte nach den allgemeinen Gesetzen bleiben unberührt, wenn der Diensteanbieter unter Wahrung des Fernmeldegeheimnisses gemäß § 85 des Telekommunikationsgesetzes von diesen Inhalten Kenntnis erlangt und eine Sperrung technisch möglich und zumutbar ist.

§ 6

Anbieterkennzeichnung

Diensteanbieter haben für ihre geschäftsmäßigen Angebote anzugeben

1. Namen und Anschrift sowie
2. bei Personenvereinigungen und -gruppen auch Namen und Anschrift des Vertretungsberechtigten.

Artikel 2

Gesetz über den Datenschutz bei Telediensten (Teledienstedatenschutzgesetz – TDDSG)

§ 1

Geltungsbereich

(1) Die nachfolgenden Vorschriften gelten für den Schutz personenbezogener Daten bei Telediensten im Sinne des Teledienstegesetzes.

(2) Soweit in diesem Gesetz nichts anderes bestimmt ist, sind die jeweils geltenden Vorschriften für den Schutz personenbezogener Daten anzuwenden, auch wenn die Daten nicht in Dateien verarbeitet oder genutzt werden.

§ 2

Begriffsbestimmungen

Im Sinne dieses Gesetzes sind

1. „Diensteanbieter" natürliche oder juristische Personen oder Personenvereinigungen, die Teledienste zur Nutzung bereithalten oder den Zugang zur Nutzung vermitteln,
2. „Nutzer" natürliche oder juristische Personen oder Personenvereinigungen, die Teledienste nachfragen.

§ 3

Grundsätze für die Verarbeitung personenbezogener Daten

(1) Personenbezogene Daten dürfen vom Diensteanbieter zur Durchführung von Telediensten nur erhoben, verarbeitet und genutzt werden, soweit dieses Gesetz oder eine andere Rechtsvorschrift es erlaubt oder der Nutzer eingewilligt hat.

(2) Der Diensteanbieter darf für die Durchführung von Telediensten erhobene Daten für andere Zwecke nur verwenden, soweit dieses Gesetz oder eine andere Rechtsvorschrift es erlaubt oder der Nutzer eingewilligt hat.

(3) Der Diensteanbieter darf die Erbringung von Telediensten nicht von einer Einwilligung des Nutzers in eine Verarbeitung oder Nutzung seiner Daten für andere Zwecke abhängig machen.

(4) Die Gestaltung und Auswahl technischer Einrichtungen für Teledienste hat sich an dem Ziel auszurichten, keine oder so wenige personenbezogene Daten wie möglich zu erheben, zu verarbeiten und zu nutzen.

(5) Der Nutzer ist vor der Erhebung über Art, Umfang, Ort und Zwecke der Erhebung, Verarbeitung und Nutzung personenbezogener Daten zu unterrichten. Bei automatisierten Verfahren, die eine spätere Identifizierung des Nutzers ermöglichen und eine Erhebung, Verarbeitung oder Nutzung personenbezogener Daten vorbereiten, ist der Nutzer vor

Beginn dieses Verfahrens zu unterrichten. Der Inhalt der Unterrichtung muß für den Nutzer jederzeit abrufbar sein. Der Nutzer kann auf die Unterrichtung verzichten. Die Unterrichtung und der Verzicht sind zu protokollieren. Der Verzicht gilt nicht als Einwilligung im Sinne von Absatz 1 und 2.

(6) Der Nutzer ist vor Erklärung seiner Einwilligung auf sein Recht auf jederzeitigen Widerruf mit Wirkung für die Zukunft hinzuweisen. Absatz 5 Satz 3 gilt entsprechend.

(7) Die Einwilligung kann auch elektronisch erklärt werden, wenn der Diensteanbieter sicherstellt, daß

1. sie nur durch eine eindeutige und bewußte Handlung des Nutzers erfolgen kann,
2. sie nicht unerkennbar verändert werden kann,
3. ihr Urheber erkannt werden kann,
4. die Einwilligung protokolliert wird und
5. der Inhalt der Einwilligung jederzeit vom Nutzer abgerufen werden kann.

§ 4

Datenschutzrechtliche Pflichten des Diensteanbieters

(1) Der Diensteanbieter hat dem Nutzer die Inanspruchnahme von Telediensten und ihre Bezahlung anonym oder unter Pseudonym zu ermöglichen, soweit dies technisch möglich und zumutbar ist. Der Nutzer ist über diese Möglichkeiten zu informieren.

(2) Der Diensteanbieter hat durch technische und organisatorische Vorkehrungen sicherzustellen, daß

1. der Nutzer seine Verbindung mit dem Diensteanbieter jederzeit abbrechen kann,
2. die anfallenden Daten über den Ablauf des Abrufs oder Zugriffs oder der sonstigen Nutzung unmittelbar nach deren Beendigung gelöscht werden, soweit nicht eine längere Speicherung für Abrechnungszwecke erforderlich ist,
3. der Nutzer Teledienste gegen Kenntnisnahme Dritter geschützt in Anspruch nehmen kann,
4. die personenbezogenen Daten über die Inanspruchnahme verschiedener Teledienste durch einen Nutzer getrennt verarbeitet werden; eine Zusammenführung dieser Daten ist unzulässig, soweit dies nicht für Abrechnungszwecke erforderlich ist.

(3) Die Weitervermittlung zu einem anderen Diensteanbieter ist dem Nutzer anzuzeigen.

(4) Nutzungsprofile sind nur bei Verwendung von Pseudonymen zulässig. Unter einem Pseudonym erfaßte Nutzungsprofile dürfen nicht mit Daten über den Träger des Pseudonyms zusammengeführt werden.

§ 5

Bestandsdaten

(1) Der Diensteanbieter darf personenbezogene Daten eines Nutzers erheben, verarbeiten und nutzen, soweit sie für die Begründung, inhaltliche Ausgestaltung oder Änderung eines Vertragsverhältnisses mit ihm über die Nutzung von Telediensten erforderlich sind (Bestandsdaten).

(2) Eine Verarbeitung und Nutzung der Bestandsdaten für Zwecke der Beratung, der Werbung, der Marktforschung oder zur bedarfsgerechten Gestaltung technischer Einrichtungen des Diensteanbieters ist nur zulässig, soweit der Nutzer in diese ausdrücklich eingewilligt hat.

(3) Diensteanbieter haben Bestandsdaten auf Ersuchen an die zuständigen Stellen zu übermitteln, soweit dies für die Verfolgung von Straftaten oder Ordnungswidrigkeiten, zur Abwehr von Gefahren für die öffentliche Sicherheit oder Ordnung oder für die Erfüllung der gesetzlichen Aufgaben der Verfassungsschutzbehörden des Bundes und der Länder, des Bundesnachrichtendienstes, des Militärischen Abschirmdienstes sowie des Zollkriminalamtes erforderlich ist.

§ 6

Nutzungs- und Abrechnungsdaten

(1) Der Diensteanbieter darf personenbezogene Daten über die Inanspruchnahme von Telediensten nur erheben, verarbeiten und nutzen, soweit dies erforderlich ist,

1. um dem Nutzer die Inanspruchnahme von Telediensten zu ermöglichen (Nutzungsdaten) oder
2. um die Nutzung von Telediensten abzurechnen (Abrechnungsdaten).

(2) Zu löschen hat der Diensteanbieter

1. Nutzungsdaten frühestmöglich, spätestens unmittelbar nach Ende der jeweiligen Nutzung, soweit es sich nicht um Abrechnungsdaten handelt,
2. Abrechnungsdaten, sobald sie für Zwecke der Abrechnung nicht mehr erforderlich sind; nutzerbezogene Abrechnungsdaten, die für die Erstellung von Einzelnachweisen über die Inanspruchnahme bestimmter Angebote auf Verlangen des Nutzers gemäß Absatz 4 gespeichert werden, sind spätestens 80 Tage nach Versendung des Einzelnachweises zu löschen, es sei denn, die Entgeltforderung wird innerhalb dieser Frist bestritten oder trotz Zahlungsaufforderung nicht beglichen.

(3) Die Übermittlung von Nutzungs- oder Abrechnungsdaten an andere Diensteanbieter oder Dritte ist unzulässig. Der Diensteanbieter, der den Zugang zur Nutzung von Telediensten vermittelt, darf anderen Diensteanbietern, deren Teledienste der Nutzer in Anspruch genommen hat, lediglich übermitteln

1. anonymisierte Nutzungsdaten zu Zwecken deren Marktforschung,
2. Abrechnungsdaten, soweit diese zum Zwecke der Einziehung einer Forderung erforderlich sind.

(4) Hat der Diensteanbieter mit einem Dritten einen Vertrag über die Abrechnung des Entgelts geschlossen, so darf er diesem Dritten Abrechnungsdaten übermitteln, soweit es für diesen Zweck erforderlich ist. Der Dritte ist zur Wahrung des Fernmeldegeheimnisses zu verpflichten.

(5) Die Abrechnung über die Inanspruchnahme von Telediensten darf Anbieter, Zeitpunkt, Dauer, Art, Inhalt und Häufigkeit bestimmter von einem Nutzer in Anspruch genommener Teledienste nicht erkennen lassen, es sei denn der Nutzer verlangt einen Einzelnachweis.

§ 7

Auskunftsrecht des Nutzers

Der Nutzer ist berechtigt, jederzeit die zu seiner Person oder zu seinem Pseudonym gespeicherten Daten unentgeltlich beim Diensteanbieter einzusehen. Die Auskunft ist auf Verlangen des Nutzers auch elektronisch zu erteilen. Das Auskunftsrecht ist im Falle einer kurzfristigen Speicherung im Sinne von § 33 Abs. 2 Nr. 5 Bundesdatenschutzgesetz nicht nach § 34 Abs. 4 Bundesdatenschutzgesetz ausgeschlossen.

§ 8

Datenschutzkontrolle

§ 38 Bundesdatenschutzgesetz findet mit der Maßgabe Anwendung, daß die Überprüfung auch vorgenommen werden darf, wenn Anhaltspunkte für eine Verletzung von Datenschutzvorschriften nicht vorliegen.

Artikel 3

Gesetz zur digitalen Signatur (Signaturgesetz – SigG) *)

§ 1

Zweck und Anwendungsbereich

(1) Zweck des Gesetzes ist es, Rahmenbedingungen für digitale Signaturen zu schaffen, unter denen diese als sicher gelten und Fälschungen digitaler Signaturen oder Verfälschungen von signierten Daten zuverlässig festgestellt werden können.

*) Die Mitteilungspflichten der Richtlinie 83/189/EWG des Rates vom 28. März 1983 über ein Informationsverfahren auf dem Gebiet der Normen und technischen Vorschriften (ABl. EG Nr. L 109 S. 8), zuletzt geändert durch die Richtlinie 94/10/EG des Europäischen Parlaments und des Rates vom 23. März 1994 (ABl. EG Nr. L 100 S. 30) sind beachtet worden.

(2) Die Anwendung anderer Verfahren für digitale Signaturen ist freigestellt, soweit nicht digitale Signaturen nach diesem Gesetz durch Rechtsvorschrift vorgeschrieben sind.

§ 2

Begriffsbestimmungen

(1) Eine digitale Signatur im Sinne dieses Gesetzes ist ein mit einem privaten Signaturschlüssel erzeugtes Siegel zu digitalen Daten, das mit Hilfe eines zugehörigen öffentlichen Schlüssels, der mit einem Signaturschlüssel-Zertifikat einer Zertifizierungsstelle oder der Behörde nach § 3 versehen ist, den Inhaber des Signaturschlüssels und die Unverfälschtheit der Daten erkennen läßt.

(2) Eine Zertifizierungsstelle im Sinne dieses Gesetzes ist eine natürliche oder juristische Person, die die Zuordnung von öffentlichen Signaturschlüsseln zu natürlichen Personen bescheinigt und dafür eine Lizenz gemäß § 4 besitzt.

(3) Ein Zertifikat im Sinne dieses Gesetzes ist eine mit einer digitalen Signatur versehene digitale Bescheinigung über die Zuordnung eines öffentlichen Signaturschlüssels zu einer natürlichen Person (Signaturschlüssel-Zertifikat) oder eine gesonderte digitale Bescheinigung, die unter eindeutiger Bezugnahme auf ein Signaturschlüssel-Zertifikat weitere Angaben enthält (Attribut-Zertifikat).

(4) Ein Zeitstempel im Sinne dieses Gesetzes ist eine mit einer digitalen Signatur versehene digitale Bescheinigung einer Zertifizierungsstelle, daß ihr bestimmte digitale Daten zu einem bestimmten Zeitpunkt vorgelegen haben

§ 3

Zuständige Behörde

Die Erteilung von Lizenzen und die Ausstellung von Zertifikaten, die zum Signieren von Zertifikaten eingesetzt werden, sowie die Überwachung der Einhaltung dieses Gesetzes und der Rechtsverordnung nach § 16 obliegen der Behörde nach § 66 des Telekommunikationsgesetzes.

§ 4

Lizenzerteilung für Zertifizierungsstellen

(1) Der Betrieb einer Zertifizierungsstelle bedarf einer Lizenz der zuständigen Behörde. Diese ist auf Antrag zu erteilen.

(2) Die Lizenz ist zu versagen, wenn Tatsachen die Annahme rechtfertigen, daß der Antragsteller nicht die für den Betrieb einer Zertifizierungsstelle erforderliche Zuverlässigkeit besitzt, wenn der Antragsteller nicht nachweist, daß die für den Betrieb einer Zertifizierungsstelle erforderliche Fachkunde vorliegt, oder wenn zu erwarten ist, daß bei Aufnahme des Betriebes die übrigen Voraussetzungen für den Betrieb der Zertifizierungsstelle nach diesem Gesetz

und der Rechtsverordnung nach § 16 nicht vorliegen werden.

(3) Die erforderliche Zuverlässigkeit besitzt, wer die Gewähr dafür bietet, als Lizenzinhaber die für den Betrieb der Zertifizierungsstelle maßgeblichen Rechtsvorschriften einzuhalten. Die erforderliche Fachkunde liegt vor, wenn die im Betrieb der Zertifizierungsstelle tätigen Personen über die dafür erforderlichen Kenntnisse, Erfahrungen und Fertigkeiten verfügen. Die übrigen Voraussetzungen für den Betrieb der Zertifizierungsstelle liegen vor, wenn die Maßnahmen zur Erfüllung der Sicherheitsanforderungen dieses Gesetzes und der Rechtsverordnung nach § 16 der zuständigen Behörde rechtzeitig in einem Sicherheitskonzept aufgezeigt und die Umsetzung durch eine von der zuständigen Behörde anerkannten Stelle geprüft und bestätigt worden ist.

(4) Die Lizenz kann mit Nebenbestimmungen versehen werden, soweit dies erforderlich ist um sicherzustellen, daß die Zertifizierungsstelle bei Aufnahme des Betriebes und im Betrieb die Voraussetzungen dieses Gesetzes und der Rechtsverordnung nach § 16 erfüllt.

(5) Die zuständige Behörde stellt für Signaturschlüssel, die zum Signieren von Zertifikaten eingesetzt werden, die Zertifikate aus. Die Vorschriften für die Vergabe von Zertifikaten durch Zertifizierungsstellen gelten für die zuständige Behörde entsprechend. Diese hat die von ihr ausgestellten Zertifikate jederzeit für jeden über öffentlich erreichbare Telekommunikationsverbindungen abrufbar zu halten. Dies gilt auch für Informationen über Anschriften und Rufnummern der Zertifizierungsstellen, die Sperrung von von ihr ausgestellten Zertifikaten, die Einstellung und die Untersagung der Ausübung lizenzierter Tätigkeit sowie den Widerruf von Lizenzen.

(6) Für öffentliche Leistungen nach diesem Gesetz und der Rechtsverordnung nach § 16 werden Kosten (Gebühren und Auslagen) erhoben.

§ 5
Vergabe von Zertifikaten

(1) Die Zertifizierungsstelle hat Personen, die ein Zertifikat beantragen, zuverlässig zu identifizieren. Sie hat die Zuordnung eines öffentlichen Signaturschlüssels zu einer identifizierten Person durch ein Signaturschlüssel-Zertifikat zu bestätigen und dieses sowie Attribut-Zertifikate jederzeit für jeden über öffentlich erreichbare Telekommunikationsverbindungen nachprüfbar und mit Zustimmung des Signaturschlüssel-Inhabers abrufbar zu halten.

(2) Die Zertifizierungsstelle hat auf Verlangen eines Antragstellers Angaben über seine Vertretungsmacht für eine dritte Person sowie zur berufsrechtlichen oder sonstigen Zulassung in das Signaturschlüssel-Zertifikat oder ein Attribut-Zertifikat aufzunehmen, soweit ihr die Einwilligung des Dritten zur Aufnahme dieser Vertretungsmacht oder die Zulassung zuverlässig nachgewiesen wird.

(3) Die Zertifizierungsstelle hat auf Verlangen eines Antragstellers im Zertifikat anstelle seines Namens ein Pseudonym aufzuführen.

(4) Die Zertifizierungsstelle hat Vorkehrungen zu treffen, damit Daten für Zertifikate nicht unbemerkt gefälscht oder verfälscht werden können. Sie hat weiter Vorkehrungen zu treffen, um die Geheimhaltung der privaten Signaturschlüssel zu gewährleisten. Eine Speicherung privater Signaturschlüssel bei der Zertifizierungsstelle ist unzulässig.

(5) Die Zertifizierungsstelle hat für die Ausübung der Zertifizierungstätigkeit zuverlässiges Personal einzusetzen. Für das Bereitstellen von Signaturschlüsseln sowie das Erstellen von Zertifikaten hat sie technische Komponenten gemäß § 14 einzusetzen. Dies gilt auch für technische Komponenten, die ein Nachprüfen von Zertifikaten nach Absatz 1 Satz 2 ermöglichen.

§ 6
Unterrichtungspflicht

Die Zertifizierungsstelle hat die Antragsteller nach § 5 Abs. 1 über die Maßnahmen zu unterrichten, die erforderlich sind, um zu sicheren digitalen Signaturen und deren zuverlässiger Prüfung beizutragen. Sie hat die Antragsteller darüber zu unterrichten, welche technischen Komponenten die Anforderungen nach § 14 Abs. 1 und 2 erfüllen, sowie über die Zuordnung der mit einem privaten Signaturschlüssel erzeugten digitalen Signaturen. Sie hat die Antragsteller darauf hinzuweisen, daß Daten mit digitaler Signatur bei Bedarf neu zu signieren sind, bevor der Sicherheitswert der vorhandenen Signatur durch Zeitablauf geringer wird.

§ 7
Inhalt von Zertifikaten

(1) Das Signaturschlüssel-Zertifikat muß mindestens folgende Angaben enthalten:

1. den Namen des Signaturschlüssel-Inhabers, der im Falle einer Verwechslungsmöglichkeit mit einem Zusatz zu versehen ist, oder ein dem Signaturschlüssel-Inhaber zugeordnetes unverwechselbares Pseudonym, das als solches kenntlich sein muß,
2. den zugeordneten öffentlichen Signaturschlüssel,
3. die Bezeichnung der Algorithmen, mit denen der öffentliche Schlüssel des Signaturschlüssel-Inhabers sowie der öffentliche Schlüssel der Zertifizierungsstelle benutzt werden kann,
4. die laufende Nummer des Zertifikates,
5. Beginn und Ende der Gültigkeit des Zertifikates,
6. den Namen der Zertifizierungsstelle und
7. Angaben, ob die Nutzung des Signaturschlüssels auf bestimmte Anwendungen nach Art und Umfang beschränkt ist.

(2) Angaben zur Vertretungsmacht für eine dritte Person sowie zur berufsrechtlichen oder sonstigen Zulassung können sowohl in das Signaturschlüssel-Zertifikat als auch in ein Attribut-Zertifikat aufgenommen werden.

§ 8

Sperrung von Zertifikaten

(1) Die Zertifizierungsstelle hat ein Zertifikat zu sperren, wenn ein Signaturschlüssel-Inhaber oder sein Vertreter es verlangen, das Zertifikat auf Grund falscher Angaben zu § 7 erwirkt wurde, sie ihre Tätigkeit beendet haben und diese nicht von einer anderen Zertifizierungsstelle fortgeführt wird oder die zuständige Behörde gemäß § 13 Abs. 5 Satz 2 eine Sperrung anordnet. Die Sperrung muß den Zeitpunkt enthalten, von dem an sie gilt. Eine rückwirkende Sperrung ist unzulässig.

(2) Enthält ein Zertifikat Angaben einer dritten Person, so kann auch diese eine Sperrung dieses Zertifikates verlangen.

(3) Die zuständige Behörde sperrt von ihr nach § 4 Abs. 5 ausgestellte Zertifikate, wenn eine Zertifizierungsstelle ihre Tätigkeit einstellt oder wenn die Lizenz widerrufen wird.

§ 9

Zeitstempel

Die Zertifizierungsstelle hat digitale Daten auf Verlangen mit einem Zeitstempel zu versehen. § 5 Abs. 5 Satz 1 und 2 gilt entsprechend.

§ 10

Dokumentation

Die Zertifizierungsstelle hat die Sicherheitsmaßnahmen zur Einhaltung dieses Gesetzes und der Rechtsverordnung nach § 16 sowie die ausgestellten Zertifikate so zu dokumentieren, daß die Daten und ihre Unverfälschtheit jederzeit nachprüfbar sind.

§ 11

Einstellung der Tätigkeit

(1) Die Zertifizierungsstelle hat, wenn sie ihre Tätigkeit einstellt, dies zum frühestmöglichen Zeitpunkt der zuständigen Behörde anzuzeigen und dafür zu sorgen, daß die bei Einstellung der Tätigkeit gültigen Zertifikate von einer anderen Zertifizierungsstelle übernommen werden, oder diese zu sperren.

(2) Sie hat die Dokumentation nach § 10 an die Zertifizierungsstelle, welche die Zertifikate übernimmt, oder andernfalls an die zuständige Behörde zu übergeben.

(3) Sie hat einen Antrag auf Eröffnung eines Konkurs- oder Vergleichsverfahrens der zuständigen Behörde unverzüglich anzuzeigen.

§ 12

Datenschutz

(1) Die Zertifizierungsstelle darf personenbezogene Daten nur unmittelbar beim Betroffenen selbst und nur insoweit erheben, als dies für Zwecke eines Zertifikates erforderlich ist. Eine Datenerhebung bei Dritten ist nur mit Einwilligung des Betroffenen zulässig. Für andere als die in Satz 1 genannten Zwecke dürfen die Daten nur verwendet werden, wenn dieses Gesetz oder eine andere Rechtsvorschrift es erlaubt oder der Betroffene eingewilligt hat.

(2) Bei einem Signaturschlüssel-Inhaber mit Pseudonym hat die Zertifizierungsstelle die Daten über dessen Identität auf Ersuchen an die zuständigen Stellen zu übermitteln, soweit dies für die Verfolgung von Straftaten oder Ordnungswidrigkeiten, zur Abwehr von Gefahren für die öffentliche Sicherheit oder Ordnung oder für die Erfüllung der gesetzlichen Aufgaben der Verfassungsschutzbehörden des Bundes und der Länder, des Bundesnachrichtendienstes, des Militärischen Abschirmdienstes oder des Zollkriminalamtes erforderlich ist. Die Auskünfte sind zu dokumentieren.

(3) § 38 des Bundesdatenschutzgesetzes findet mit der Maßgabe Anwendung, daß die Überprüfung auch vorgenommen werden darf, wenn Anhaltspunkte für eine Verletzung von Datenschutzvorschriften nicht vorliegen.

§ 13

Kontrolle und Durchsetzung von Verpflichtungen

(1) Die zuständige Behörde kann gegenüber Zertifizierungsstellen Maßnahmen zur Sicherstellung der Einhaltung dieses Gesetzes und der Rechtsverordnung treffen. Dazu kann sie insbesondere die Benutzung ungeeigneter technischer Komponenten untersagen und die Ausübung der lizenzierten Tätigkeit vorübergehend ganz oder teilweise untersagen. Personen, die den Anschein erwecken, über eine Lizenz nach § 4 zu verfügen, ohne daß dies der Fall ist, kann die Tätigkeit der Zertifizierung untersagt werden.

(2) Zum Zwecke der Überwachung nach Absatz 1 Satz 1 haben Zertifizierungsstellen der zuständigen Behörde das Betreten der Geschäfts- und Betriebsräume während der üblichen Betriebszeiten zu gestatten, auf Verlangen die in Betracht kommenden Bücher, Aufzeichnungen, Belege, Schriftstücke und sonstigen Unterlagen zur Einsicht vorzulegen, Auskunft zu erteilen und die erforderliche Unterstützung zu gewähren. Der zur Erteilung einer Auskunft Verpflichtete kann die Auskunft auf solche Fragen verweigern, deren Beantwortung ihn selbst oder einen der in § 383 Absatz 1 Nr. 1 bis 3 der Zivilprozeßordnung bezeichneten Angehörigen der Gefahr der Verfolgung wegen einer Straftat oder eines Verfahrens

nach dem Gesetz über Ordnungswidrigkeiten aussetzen würde. Der zur Auskunft Verpflichtete ist auf dieses Recht hinzuweisen.

(3) Bei Nichterfüllung der Pflichten aus diesem Gesetz oder der Rechtsverordnung oder bei Entstehen eines Versagungsgrundes für eine Lizenzerteilung hat die zuständige Behörde die Lizenz zu widerrufen, wenn Maßnahmen nach Absatz 1 Satz 2 keinen Erfolg versprechen.

(4) Im Falle der Rücknahme oder des Widerrufs einer Lizenz oder der Einstellung der Tätigkeit einer Zertifizierungsstelle hat die zuständige Behörde eine Übernahme der Tätigkeit durch eine andere Zertifizierungsstelle oder die Abwicklung der Verträge mit den Signaturschlüssel-Inhabern sicherzustellen. Dies gilt auch bei Antrag auf Eröffnung eines Konkurs- oder Vergleichsverfahrens, wenn die lizenzierte Tätigkeit nicht fortgesetzt wird.

(5) Die Gültigkeit der von einer Zertifizierungsstelle ausgestellten Zertifikate bleibt vom Widerruf einer Lizenz unberührt. Die zuständige Behörde kann eine Sperrung von Zertifikaten anordnen, wenn Tatsachen die Annahme rechtfertigen, daß Zertifikate gefälscht oder nicht hinreichend fälschungssicher sind oder daß zur Anwendung der Signaturschlüssel eingesetzte technische Komponenten Sicherheitsmängel aufweisen, die eine unbemerkte Fälschung digitaler Signaturen oder eine unbemerkte Verfälschung signierter Daten zulassen.

§ 14

Technische Komponenten

(1) Für die Erzeugung und Speicherung von Signaturschlüsseln sowie die Erzeugung und Prüfung digitaler Signaturen sind technische Komponenten mit Sicherheitsvorkehrungen erforderlich, die Fälschungen digitaler Signaturen und Verfälschungen signierter Daten zuverlässig erkennbar machen und gegen unberechtigte Nutzung privater Signaturschlüssel schützen.

(2) Für die Darstellung zu signierender Daten sind technische Komponenten mit Sicherheitsvorkehrungen erforderlich, die die Erzeugung einer digitalen Signatur vorher eindeutig anzeigen und feststellen lassen, auf welche Daten sich die digitale Signatur bezieht. Für die Überprüfung signierter Daten sind technische Komponenten mit Sicherheitsvorkehrungen erforderlich, die feststellen lassen, ob die signierten Daten unverändert sind, auf welche Daten sich die digitale Signatur bezieht und welchem Signaturschlüssel-Inhaber die digitale Signatur zuzuordnen ist.

(3) Bei technischen Komponenten, mit denen Signaturschlüssel-Zertifikate gemäß § 5 Abs. 1 Satz 2 nachprüfbar oder abrufbar gehalten werden, sind Vorkehrungen erforderlich, um die Zertifikatverzeichnisse vor unbefugter Veränderung und unbefugtem Abruf zu schützen.

(4) Bei technischen Komponenten nach Absatz 1 bis 3 ist es erforderlich, daß sie nach dem Stand der Technik hinreichend geprüft sind und die Erfüllung der Anforderungen durch eine von der zuständigen Behörde anerkannten Stelle bestätigt ist.

(5) Bei technischen Komponenten, die nach den in einem anderen Mitgliedstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum geltenden Regelungen oder Anforderungen rechtmäßig hergestellt oder in den Verkehr gebracht werden und die gleiche Sicherheit gewährleisten, ist davon auszugehen, daß die die sicherheitstechnische Beschaffenheit betreffenden Anforderungen nach Absatz 1 bis 3 erfüllt sind. In begründeten Einzelfällen ist auf Verlangen der zuständigen Behörde nachzuweisen, daß die Anforderungen nach Satz 1 erfüllt sind. Soweit zum Nachweis der die sicherheitstechnische Beschaffenheit betreffenden Anforderungen im Sinne der Absätze 1 bis 3 die Vorlage einer Bestätigung einer von der zuständigen Behörde anerkannten Stelle vorgesehen ist, werden auch Bestätigungen von in anderen Mitgliedstaaten der Europäischen Union oder in anderen Vertragsstaaten des Abkommens über den Europäischen Wirtschaftsraum zugelassenen Stellen berücksichtigt, wenn die den Prüfberichten dieser Stellen zugrundeliegenden technischen Anforderungen, Prüfungen und Prüfverfahren denen der durch die zuständige Behörde anerkannten Stellen gleichwertig sind.

§ 15

Ausländische Zertifikate

(1) Digitale Signaturen, die mit einem öffentlichen Signaturschlüssel überprüft werden können, für den ein ausländisches Zertifikat aus einem anderen Mitgliedstaat der Europäischen Union oder aus einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum vorliegt, sind, soweit sie gleichwertige Sicherheit aufweisen, digitalen Signaturen nach diesem Gesetz gleichgestellt.

(2) Absatz 1 gilt auch für andere Staaten, soweit überstaatliche oder zwischenstaatliche Vereinbarungen über die Anerkennung der Zertifikate getroffen sind.

§ 16

Rechtsverordnung

Die Bundesregierung wird ermächtigt, durch Rechtsverordnung die zur Durchführung der §§ 3 bis 15 erforderlichen Rechtsvorschriften zu erlassen über

1. die näheren Einzelheiten des Verfahrens der Erteilung, Übertragung und des Widerrufs einer Lizenz sowie des Verfahrens bei Einstellung lizenzierter Tätigkeit,
2. die gebührenpflichtigen Tatbestände nach § 4 Abs. 6 und die Höhe der Gebühr,
3. die nähere Ausgestaltung der Pflichten der Zertifizierungsstellen,

4. die Gültigkeitsdauer von Signaturschlüssel-Zertifikaten,

5. die nähere Ausgestaltung der Kontrolle der Zertifizierungsstellen,

6. die näheren Anforderungen an die technischen Komponenten sowie die Prüfung technischer Komponenten und die Bestätigung, daß die Anforderungen erfüllt sind,

7. den Zeitraum sowie das Verfahren, nach dem eine neue digitale Signatur angebracht werden sollte.

Artikel 4

Änderung des Strafgesetzbuches

Das Strafgesetzbuch in der Fassung der Bekanntmachung vom 10. März 1987 (BGBl. I S. 945, 1160), zuletzt geändert durch ... (BGBl. ...), wird wie folgt geändert:

1. § 11 Abs. 3 wird wie folgt gefaßt:

   „(3) Den Schriften stehen Ton- und Bildträger, Datenspeicher, Abbildungen und andere Darstellungen in denjenigen Vorschriften gleich, die auf diesen Absatz verweisen."

2. § 74 d wird wie folgt geändert:

   a) In Absatz 3 wird nach dem Wort „Schriften" die Angabe „(§ 11 Abs. 3)" eingefügt.

   b) In Absatz 4 werden nach dem Wort „wenn" die Wörter „die Schrift (§ 11 Abs. 3) oder" eingefügt.

3. In § 86 Abs. 1 werden nach dem Wort „ausführt" die Wörter „oder in Datenspeichern öffentlich zugänglich macht" eingefügt.

Artikel 5

Änderung des Gesetzes über Ordnungswidrigkeiten

Das Gesetz über Ordnungswidrigkeiten in der Fassung der Bekanntmachung vom 19. Februar 1987 (BGBl. I S. 602), zuletzt geändert durch ... (BGBl. ...), wird wie folgt geändert:

1. In § 116 Abs. 1, § 120 Abs. 1 Nr. 2 und § 123 Abs. 2 Satz 1 werden jeweils nach dem Wort „Bildträgern" ein Komma und das Wort „Datenspeichern" eingefügt.

2. § 119 wird wie folgt geändert:

   a) In Absatz 1 Nr. 2 werden nach dem Wort „Darstellungen" die Wörter „oder durch das öffentliche Zugänglichmachen von Datenspeichern" eingefügt.

   b) In Absatz 3 werden nach dem Wort „Bildträger" ein Komma und das Wort „Datenspeicher" eingefügt.

Artikel 6

Änderung des Gesetzes über die Verbreitung jugendgefährdender Schriften

Das Gesetz über die Verbreitung jugendgefährdender Schriften in der Fassung der Bekanntmachung vom 12. Juli 1985 (BGBl. I S. 1502), zuletzt geändert durch ... (BGBl. ...), wird wie folgt geändert:

1. Die Bezeichnung des Gesetzes wird wie folgt geändert:

   „Gesetz über die Verbreitung jugendgefährdender Schriften und Medieninhalte"

2. § 1 Abs. 3 wird wie folgt gefaßt:

   „(3) Den Schriften stehen Ton- und Bildträger, Datenspeicher, Abbildungen und andere Darstellungen gleich."

3. § 3 wird wie folgt geändert:

   a) In Absatz 1 wird am Ende der Nummer 3 der Punkt durch ein Komma ersetzt und folgende Nummer 4 angefügt:

      „4. durch Informations- und Kommunikationsdienste verbreitet, bereitgehalten oder sonst zugänglich gemacht werden."

   b) Dem Absatz 2 wird folgender Satz angefügt:

      „Absatz 1 Nr. 4 gilt nicht, wenn durch technische Vorkehrungen Vorsorge getroffen ist, daß das Angebot oder die Verbreitung im Inland auf volljährige Nutzer beschränkt werden kann."

4. § 5 Abs. 3 wird wie folgt gefaßt:

   „(3) Absatz 2 gilt nicht,

   1. wenn die Handlung im Geschäftsverkehr mit dem einschlägigen Handel erfolgt, oder

   2. wenn durch technische Vorkehrungen oder in sonstiger Weise eine Übermittlung an Kinder oder Jugendliche ausgeschlossen ist."

5. Nach § 7 wird folgender § 7a eingefügt:

   „§ 7a

   Jugendschutzbeauftragte

   Wer gewerbsmäßig elektronische Informations- und Kommunikationsdienste, denen eine Übermittlung mittels Telekommunikation zugrunde liegt, zur Nutzung bereithält, hat einen Jugendschutzbeauftragten zu bestellen, wenn diese allgemein angeboten werden und jugendgefährdende Inhalte enthalten können. Er ist Ansprechpartner für Nutzer und berät den Diensteanbieter in Fragen des Jugendschutzes. Er ist von dem Diensteanbieter an der Angebotsplanung und der Gestaltung der Allgemeinen Nutzungsbedingungen

zu beteiligen. Er kann dem Diensteanbieter eine Beschränkung von Angeboten vorschlagen. Die Verpflichtung des Diensteanbieters nach Satz 1 kann auch dadurch erfüllt werden, daß er eine Organisation der freiwilligen Selbstkontrolle zur Wahrnehmung der Aufgaben nach Satz 2 bis 4 verpflichtet."

6. Nach § 21 Abs. 1 Nr. 3 wird folgende Nummer 3 a eingefügt:

„3 a. entgegen § 3 Abs. 1 Nr. 4 verbreitet, bereithält oder sonst zugänglich macht,"

Artikel 7

Änderung des Urheberrechtsgesetzes

Das Urheberrechtsgesetz vom 9. September 1965 (BGBl. I S. 1273), zuletzt geändert durch ... (BGBl. ...), wird wie folgt geändert:

1. Nach § 69 g wird folgender Abschnitt eingefügt:

„Neunter Abschnitt
Besondere Bestimmungen für Datenbanken

§ 69 h
Begriff der Datenbank

Datenbank im Sinne dieses Gesetzes ist eine Sammlung von Werken, Daten oder anderen unabhängigen Elementen, die systematisch oder methodisch angeordnet und einzeln mit elektronischen Mitteln oder auf andere Weise zugänglich sind.

§ 69 i
Voraussetzung und Gegenstand des urheberrechtlichen Schutzes

(1) Datenbanken, die auf Grund der Auswahl oder Anordnung des Stoffes eine eigene geistige Schöpfung ihres Urhebers darstellen, werden als Werke geschützt.

(2) Dieser Schutz beschränkt sich auf die urheberrechtsfähige Ausdrucksform der Datenbank und erstreckt sich nicht auf deren Inhalt. Am Inhalt bestehende Schutzrechte, einschließlich des Rechts des Herstellers einer Datenbank (§ 87 a), bleiben unberührt.

§ 69 k
Mindestbefugnisse des rechtmäßigen Benutzers

Der zur Benutzung einer Datenbank oder eines Vervielfältigungsstücks einer Datenbank Berechtigte bedarf für Handlungen, die für den Zugang zum Inhalt der Datenbank und für deren normale Benutzung erforderlich sind, nicht der Einwilligung des Urhebers. Ist er nur zur Benutzung eines Teils der Datenbank berechtigt, so gilt dies nur für den Zugang zu diesem Teil und für dessen Benutzung. Entgegenstehende vertragliche Bestimmungen sind nichtig.

§ 69 l
Vervielfältigung zum privaten Gebrauch

§ 53 Abs. 1 Satz 1 findet auf die Vervielfältigung der urheberrechtsfähigen Ausdrucksform einer elektronischen Datenbank keine Anwendung."

2. Nach § 87 wird folgender Abschnitt eingefügt:

„Sechster Abschnitt
Schutz der Hersteller von Datenbanken

§ 87 a
Gegenstand des Schutzes und Verwertungsrechte

(1) Geschützt wird der Hersteller einer Datenbank (§ 69 h), der für die Beschaffung, Überprüfung oder Darstellung ihres Inhalts eine in qualitativer oder quantitativer Hinsicht wesentliche Investition vorgenommen hat.

(2) Der Hersteller hat das ausschließliche Recht, die Gesamtheit oder einen in qualitativer oder quantitativer Hinsicht wesentlichen Teil des Inhalts der Datenbank zu entnehmen oder weiterzuverwenden. Einer Entnahme oder Weiterverwendung eines wesentlichen Teils des Inhalts der Datenbank steht gleich die wiederholte und systematische Entnahme oder Weiterverwendung unwesentlicher Teile des Inhalts der Datenbank, die einer normalen Auswertung der Datenbank zuwiderläuft oder durch die die berechtigten Interessen des Herstellers unzumutbar beeinträchtigt werden.

(3) Entnahme ist die ständige oder vorübergehende Übertragung auf einen anderen Datenträger mit jedem Mittel und in jeder Form. Weiterverwendung ist jede Form öffentlicher Verfügbarmachung durch Verbreitung von Vervielfältigungsstücken, einschließlich der Vermietung, durch Online-Übermittlung oder durch andere Formen der Übermittlung.

(4) Ist ein Vervielfältigungsstück einer Datenbank mit Zustimmung des Rechtsinhabers im Gebiet der Europäischen Union oder eines anderen Vertragsstaates des Abkommens über den Europäischen Wirtschaftsraum im Wege der Veräußerung in Verkehr gebracht worden, so ist seine Weiterverbreitung mit Ausnahme der Vermietung zulässig. Im Falle des öffentlichen Verleihs (§ 27 Abs. 2) ist dem Hersteller eine angemessene Vergütung zu zahlen; § 27 Abs. 3 ist entsprechend anzuwenden.

(5) Der Hersteller kann die nach Absatz 2 gewährten Rechte an Dritte abtreten.

(6) Urheberrechte und sonstige Rechte an der Datenbank oder ihrem Inhalt bleiben unberührt.

§ 87 b
Schranken des Schutzes des Herstellers

(1) Ein wesentlicher Teil des Inhalts einer der Öffentlichkeit zugänglich gemachten Datenbank

kann durch den berechtigten Benutzer in folgenden Fällen ohne Zustimmung des Rechtsinhabers genutzt werden:

1. Entnahme des Inhalts einer nichtelektronischen Datenbank zum privaten Gebrauch;
2. Entnahme unter Angabe der Quelle zum eigenen wissenschaftlichen Gebrauch, wenn und soweit dies geboten ist;
3. Entnahme und Weiterverwendung zu Zwecken der öffentlichen Sicherheit und zur Verwendung in Verfahren vor einem Gericht, einem Schiedsgericht oder einer Behörde.

(2) Ist nach der Art einer Datenbank zu erwarten, daß ihr nach Absatz 1 Nr. 1 und 2 wesentliche Teile des Inhalts entnommen werden, gelten für den Anspruch des Datenbankherstellers auf Zahlung einer angemessenen Vergütung die §§ 54 bis 54 h entsprechend.

§ 87 c
Schutzdauer

(1) Das Recht nach § 87 a erlischt fünfzehn Jahre nach der Herstellung der Datenbank. Wird die Datenbank innerhalb dieser Frist erstmals der Öffentlichkeit zugänglich gemacht, erlischt der Schutz fünfzehn Jahre nach diesem Zeitpunkt. Die Frist ist nach § 69 zu berechnen.

(2) Jede in qualitativer oder quantitativer Hinsicht wesentliche Änderung des Inhalts der Datenbank, die als eine in qualitativer oder quantitativer Hinsicht wesentliche Neuinvestition in die Datenbank anzusehen ist, begründet für die Datenbank eine eigene Schutzdauer. Eine wesentliche Änderung kann sich auch aus einer Reihe aufeinanderfolgender Änderungen ergeben.

§ 87 d
Rechte und Pflichten des rechtmäßigen Benutzers

(1) Vertragliche Bestimmungen, die die Befugnis des berechtigten Benutzers einer der Öffentlichkeit zugänglich gemachten Datenbank ausschließen, in qualitativer oder quantitativer Hinsicht unwesentliche Teile des Inhalts der Datenbank ohne Zustimmung des Rechtsinhabers zu beliebigen Zwecken zu entnehmen und weiterzuverwenden, sind nichtig.

(2) Der Berechtigte darf keine Handlungen vornehmen, die der normalen Auswertung der Datenbank zuwiderlaufen oder durch die die berechtigten Interessen des Herstellers unzumutbar beeinträchtigt werden."

3. Dem § 96 Abs. 1 wird folgender Satz angefügt:

„Der rechtswidrig entnommene Inhalt einer Datenbank darf nicht weiterverwendet werden."

4. § 108 Abs. 1 wird wie folgt geändert:

a) In Nr. 7 wird das Komma durch das Wort „oder" ersetzt.

b) Nach Nr. 7 wird folgende Nummer angefügt:

„8. den Inhalt einer Datenbank entgegen § 87 a Abs. 2 entnimmt oder weiterverwendet,".

5. In § 119 Abs. 3 wird das Wort „und" nach dem Wort „Lichtbilder" durch ein Komma ersetzt und nach dem Wort „Tonträger" die Wörter „und die nach § 87 a geschützten Datenbanken" eingefügt.

6. Nach § 127 wird folgender § 127 a eingefügt:

„§ 127 a
Schutz des Herstellers von Datenbanken

(1) Den nach § 87 a gewährten Schutz genießen Hersteller, die Staatsangehörige eines Mitgliedstaates der Europäischen Union oder eines Vertragsstaates des Abkommens über den Europäischen Wirtschaftsraum sind oder die ihren gewöhnlichen Aufenthalt im Gebiet der Mitglied- und Vertragsstaaten haben. § 120 Abs. 2 Nr. 1 ist anzuwenden.

(2) Der Schutz steht auch nach den Rechtsvorschriften eines Mitglied- oder Vertragsstaates gegründeten Unternehmen zu, die ihren satzungsmäßigen Sitz, ihre Hauptverwaltung oder Hauptniederlassung im Gebiet der Mitglied- und Vertragsstaaten haben. Befindet sich lediglich der Satzungssitz in diesem Gebiet, muß die Tätigkeit des Unternehmens eine tatsächliche ständige Verbindung zu der Wirtschaft eines der Mitglied- oder Vertragsstaaten aufweisen.

(3) Andere Personen und Unternehmen genießen Schutz nach dem Inhalt der Staatsverträge."

7. Nach § 137 g wird folgender § 137 h eingefügt:

„§ 137 h
Übergangsregelung
bei Umsetzung der Richtlinie 96/9/EG

(1) Die Vorschriften des Neunten Abschnitts des Ersten Teils finden auch auf Datenbanken Anwendung, die vor dem 1. Januar 1998 geschaffen wurden.

(2) Die Vorschriften des Sechsten Abschnitts des Zweiten Teils sind auch auf Datenbanken anzuwenden, deren Herstellung zwischen dem 1. Januar 1983 und dem 31. Dezember 1997 abgeschlossen worden ist. Die Schutzfrist beginnt in diesen Fällen am 1. Januar 1998."

Artikel 8

Änderung des Preisangabengesetzes

Dem § 1 des Preisangabengesetzes vom 3. Dezember 1984 (BGBl. I S. 1429) wird folgender Satz angefügt:

„Bei Leistungen der Informations- und Kommunikationsdienste können auch Bestimmungen über die Angabe des Preisstandes fortlaufender Leistungen getroffen werden."

Artikel 9

Änderung der Preisangabenverordnung

Die Preisangabenverordnung vom 14. März 1985 (BGBl. I S. 580), zuletzt geändert durch ... (BGBl. ...), wird wie folgt geändert:

1. Dem § 3 Abs. 1 werden folgende Sätze angefügt:

   „Ort des Leistungsangebots ist auch die Bildschirmanzeige. Wird eine Leistung über Bildschirmanzeige erbracht und nach Einheiten berechnet, ist eine gesonderte Anzeige über den Preis der fortlaufenden Nutzung unentgeltlich anzubieten."

2. § 8 Abs. 2 Nr. 2 wird wie folgt gefaßt:

   „2. des § 3 Abs. 1 Satz 1, 2 oder 4 oder Abs. 2, jeweils auch in Verbindung mit § 2 Abs. 5, über das Aufstellen, das Anbringen oder das Bereithalten von Preisverzeichnissen oder über das Anbieten einer Anzeige des Preises,".

Artikel 10

Rückkehr zum einheitlichen Verordnungsrang

Die auf Artikel 8 beruhenden Teile der Preisangabenverordnung können auf Grund der Ermächtigung des § 1 Preisangabengesetz durch Rechtsverordnung geändert werden.

Artikel 11

Inkrafttreten

Dieses Gesetz tritt mit Ausnahme des Artikels 7, der am 1. Januar 1998 in Kraft tritt, am ... in Kraft.

Begründung

A. Allgemeiner Teil

Ausgangslage

Der Gesetzentwurf trägt dem tiefgreifenden Wandel der Informations- und Kommunikationstechnologie Rechnung. Die technischen Innovationen sind aus dem Zusammenwachsen von Computer-, Telekommunikations- und audiovisueller Technik entstanden. Seit den 70er Jahren haben sich durch Digitalisierung und Komprimierung von Daten die Formen der Speicherung und Übermittlung der Wissens- bzw. Informationsbestände nachhaltig verändert und den Wandel zur Informationsgesellschaft ausgelöst („Multimedia").

Der Markt für informationswirtschaftliche Produkte und Dienstleistungen gehört bereits heute zu einem der weltweit größten Wirtschaftszweige. Es werden in den nächsten Jahren für einzelne Marktsegmente zum Teil erhebliche Wachstumsraten erwartet. Es wird ebenfalls erwartet, daß hierdurch ein lang andauernder Wachstumsschub ausgelöst wird. Hierdurch können in Deutschland zukunftssichere und qualifizierte Arbeitsplätze geschaffen werden.

Wie die grundlegenden Innovationen der Neuzeit, z. B. der Übergang von der Handschriftenkultur zur Buchdruckkunst, bewirken auch die neuen Informations- und Kommunikationstechnologien und die hierdurch möglichen Anwendungen eine Neubewertung wirtschaftlicher Positionen. Nicht mehr die Produktion materieller Güter, sondern das Angebot von Informationen und Dienstleistungen bestimmt zunehmend das Wirtschaftsleben. Dieser Bereich hat sich zu einem eigenständigen Wirtschaftsgut entwikkelt, dem im nationalen und internationalen Standortwettbewerb eine immer größere Bedeutung zukommt.

Ziel des Gesetzes

Ziel des Gesetzes ist es, im Rahmen der Bundeskompetenzen eine verläßliche Grundlage für die Gestaltung der sich dynamisch entwickelnden Angebote im Bereich der Informations- und Kommunikationsdienste zu bieten und einen Ausgleich zwischen freiem Wettbewerb, berechtigten Nutzerbedürfnissen und öffentlichen Ordnungsinteressen herbeizuführen. Den erweiterten Möglichkeiten der Individualkommunikation und den zusätzlichen Formen wirtschaftlicher Betätigung im Wege der elektronischen Informations- und Kommunikationsdienste soll Rechnung getragen werden. Dabei sollen ein funktionsfähiger Wettbewerb gewährleistet, Nutzerbedürfnisse beachtet und öffentliche Interessen gewahrt werden. Deutschland kann im internationalen Wettbewerb nur bestehen und die Wachstums- und Beschäftigungschancen nur nutzen, wenn Hemmnisse auf dem Weg in die Informationsgesellschaft beseitigt werden.

Mit dem Gesetz soll der Wandel zur Informationsgesellschaft aktiv gestaltet und die durch die neuen Informations- und Kommunikationstechnologien gegebenen Chancen für Deutschland genutzt werden. Das Gesetz stützt sich dabei auf Feststellungen und Empfehlungen des Rates für Forschung, Technologie und Innovation (Technologierat), die Vorschläge des „Petersberg-Kreis" und die Ergebnisse der Bund-Länder-Arbeitsgruppe „Multimedia". Für die Entwicklung einer leistungsfähigen und zukunftsorientierten Informationsgesellschaft in Deutschland hat der Technologierat festgestellt, daß potentielle Investoren und Diensteanbieter einheitliche und angemessene, auf das notwendige Maß beschränkte Rahmenbedingungen benötigen. Er hat daher auch einen akuten Handlungsbedarf für die Schaffung eines national einheitlichen, klaren und verläßlichen Ordnungsrahmens für Multimediadienste in Deutschland gesehen und empfohlen, Regelungen über den Datenschutz, Schutz des geistigen Eigentums, Jugend- und Verbraucherschutz sowie Strafrecht und Datensicherheitsvorschriften an die neue technologische Entwicklung anzupassen und zu präzisieren. Die Bundesregierung hat diese Empfehlungen im Bericht „Info 2000 – Deutschlands Weg in die Informationsgesellschaft" aufgegriffen und entsprechende gesetzgeberische Maßnahmen angekündigt. Mit der Vorlage des Gesetzes wird dieser Teil des Aktionsplanes umgesetzt.

Notwendigkeit eines neuen Gesetzes

Gesetzlicher Handlungsbedarf besteht in zwei Richtungen: Zum einen geht es um die Beseitigung von Hemmnissen für die freie Entfaltung der Marktkräfte im Bereich der neuen Informations- und Kommunikationsdienste und die Gewährleistung einheitlicher wirtschaftlicher Rahmenbedingungen für das Angebot und die Nutzung dieser Dienste. Zum anderen geht es um die Einführung notwendiger Regelungen im Datenschutz, in der Datensicherheit, im Urheberrecht und im Jugendschutz, die teilweise auch Änderungen in bestehenden Bundesgesetzen erforderlich machen.

Zu den einzelnen Artikeln im Informations- und Kommunikationsdienste-Gesetz:

In Artikel 1 werden einheitliche wirtschaftliche Rahmenbedingungen für das Angebot und die Nutzung von Telediensten geregelt. Hierbei ist der freie Zugang zu diesen Diensten grundlegende Bedingung und Ausprägung des deregulierenden Charakters dieses Gesetzes. Tragende Elemente sind außerdem die Schließung von Regelungslücken im Verbraucherschutz sowie die Klarstellung von Verantwortlichkeiten der Diensteanbieter.

Artikel 2 betrifft den bereichsspezifischen Datenschutz. Er gilt für alle neuen Informations- und Kommunikationsdienste und trägt den erweiterten Risiken der Erhebung, Verarbeitung und Nutzung personenbezogener Daten Rechnung.

In Artikel 3 wird eine Sicherungsinfrastruktur geregelt und damit die rechtliche Grundlage für ein zuverlässiges Verfahren der digitalen Signaturen geschaffen (Signaturgesetz). Hierdurch wird ein Beitrag zur Akzeptanz der neuen Informations- und Kommunikationstechnologien im täglichen Rechts- und Geschäftsverkehr geleistet.

Artikel 4 und 5 enthalten Klarstellungen des Schriftenbegriffs im Strafgesetzbuch und im Ordnungswidrigkeitengesetz im Hinblick auf die erweiterten Nutzungs- und Verbreitungsmöglichkeiten von rechtswidrigen Inhalten.

Artikel 6 betrifft den Kernbereich der spezifischen Jugendschutzregelungen des Informations- und Kommunikationsdienste-Gesetzes. Die Anwendung des Gesetzes über die Verbreitung jugendgefährdender Schriften ist durch die einengende Interpretation in der Rechtsprechung der Verwaltungsgerichte auf Druckwerke und andere verkörperte Darstellungsformen beschränkt worden. Diese Einschränkung wird mit dem Ziel einer umfassenden Gewährleistung des Jugendschutzes und einer einheitlichen Anwendung des Schriftenbegriffs in der Verwaltungs- und strafgerichtlichen Rechtsprechung beseitigt.

Daneben ist die Verpflichtung zur Einführung technischer Sperrvorrichtungen im Zusammenhang mit der Verbreitung indizierter Angebote sowie die Bestellung von Jugendschutzbeauftragten als Ansprechpartner für Nutzer und als Berater der Diensteanbieter vorgesehen. Zusammen mit der Änderung des Schriftenbegriffs in den Artikeln 4 und 5 wird damit ein geschlossenes, effizientes Jugendschutzkonzept vorgelegt, das zugleich den verfassungsrechtlich gebotenen Ausgleich zwischen Meinungs- und Informationsfreiheit (Artikel 5 GG) und Jugendschutzauftrag gewährleistet.

Artikel 7 setzt die Richtlinie des Europäischen Parlamentes und des Rates vom 11. März 1996 über den rechtlichen Schutz von Datenbanken durch Änderung des Urheberrechtsgesetzes um.

Artikel 8 und 9 erstrecken den Verbraucherschutz im Preisangabengesetz und in der Preisangabenverordnung auf die neuen Nutzungsmöglichkeiten durch die Informations- und Kommunikationsdienste.

Die Anwendung bestimmter technischer Verfahren wird im Gesetz bewußt nicht vorgeschrieben; die gesetzlichen Regelungen beschränken sich auf Rahmenvorgaben, damit die verschiedenen technischen Verfahren zur Anwendung kommen und damit im Wettbewerb untereinander auf den Prüfstand gestellt werden können. Einzelne Experimentierklauseln enthält das Gesetz daher nicht; es sieht vielmehr Experimentierbereiche in diesem Sinne vor. Dabei handelt es sich um die Regelungen der digitalen Signaturen in Artikel 3.

Einordnung der neuen Informations- und Kommunikationsdienste

Das Gesetz regelt die erweiterten Formen der Individualkommunikation, d. h., die neuen, vom Benutzer individuell im Wege der neuen Informations- und Kommunikationstechnologien nutzbaren Dienste sowie die durch diese Technologien möglichen neuen Formen des Rechtsverkehrs mittels digitaler Signaturen. Die Nutzung der Informations- und Kommunikationsdienste macht neue Wege wirtschaftlicher Betätigung und eine verbilligte Geschäftskommunikation (z. B. Ergänzung / Ersatz bisheriger Vertriebsformen / „electronic commerce") möglich. Prägend für die Informations- und Kommunikationsdienste sind insbesondere die hierdurch möglichen Anwendungen im Sinne eines individuellen und frei kombinierbaren Umgangs mit digitalisierten Informationen verschiedener (interaktiv verwendbarer) Darstellungsformen (z. B. Text, Grafik, Sprache, Bild, Bildfolgen usw.). Von besonderer Wichtigkeit ist daneben der grenzüberschreitende Charakter dieser Dienste.

Aus dieser Wesensbeschreibung ergibt sich, daß Zielrichtung der Informations- und Kommunikationsdienste nicht die auf öffentliche Meinungsbildung angelegte massenmediale Versorgung ist, sondern die durch den Nutzer bestimmbare Kommunikation. Aus diesem Grunde ist der Anwendungsbereich des Rundfunks nach dem Rundfunkstaatsvertrag der Länder ausdrücklich vom Anwendungsbereich des Artikel 1 ausgenommen.

Die Informations- und Kommunikationsdienste setzen die Übermittlung von Inhalten mittels Telekommunikation im Sinne des § 3 Nr. 16 Telekommunikationsgesetz voraus. Das Informations- und Kommunikationsdienste-Gesetz regelt die Nutzung der mittels Telekommunikation übermittelten Inhalte, nicht die Telekommunikation selbst.

Gesetzgebungskompetenz des Bundes

Die Gesetzgebungskompetenz des Bundes für das Informations- und Kommunikationsdienste-Gesetz ergibt sich aus Artikel 74 Abs. 1 Nr. 11 Grundgesetz (Recht der Wirtschaft), insbesondere für die Zugangsfreiheit, Verbraucherschutz, Datenschutz und Datensicherheit sowie aus Artikel 73 Nr. 9 Grundgesetz für den gewerblichen Rechtsschutz und das Urheberrecht, aus Artikel 74 Abs. 1 Nr. 1 Grundgesetz für das Strafrecht und aus Artikel 74 Abs. 1 Nr. 7 Grundgesetz für den Jugendschutz.

Die besondere Bedeutung der Informations- und Kommunikationstechnologien für den Wirtschaftsstandort Deutschland und ihre grenzüberschreitenden Wirkungen machen einheitliche Rahmenbedingungen unabdingbar notwendig. Die Regelung durch Bundesgesetz ist deshalb zur Wahrung der Rechts- und Wirtschaftseinheit im gesamtstaatlichen Interesse erforderlich (Artikel 72 Abs. 2 GG).

Recht der Europäischen Union

Das Informations- und Kommunikationsdienste-Gesetz ist mit dem Recht der Europäischen Union ver-

einbar. Im Signaturgesetz ist vorgesehen, daß Signaturschlüssel-Zertifikate aus einem Mitgliedstaat der Europäischen Union digitalen Signaturen nach diesem Gesetz gleichgestellt sind. Artikel 7 setzt die Datenbankenrichtlinie der Europäischen Union um.

Das Signaturgesetz ist nach der Richtlinie der Europäischen Union über ein Informationsverfahren auf dem Gebiet der Normen und technischen Vorschriften bei der Europäischen Kommission zu notifizieren.

Finanzielle Auswirkungen

Mit diesem Gesetz sind folgende Kosten für den Bundeshaushalt verbunden (Vollzugsaufwand):

Kosten entstehen nur im Zusammenhang mit den Aufgaben der zuständigen Behörde nach § 3 Signaturgesetz (Regulierungsbehörde nach § 66 Telekommunikationsgesetz). Der Personalaufwand in der Regulierungsbehörde, die für die Aufgaben nach dem Signaturgesetz vorgesehen ist, wird bis zu vier Planstellen für Beamte des gehobenen Dienstes oder für vergleichbare Angestellte betragen. Der bei der Regulierungsbehörde für diese Aufgabe zu erwartende Sachaufwand wird DM 200 000,– nicht übersteigen.

Für öffentliche Leistungen nach dem Signaturgesetz ist eine aufwandsbezogene Kostenerhebung (Gebühren und Auslagen) durch die Regulierungsbehörde vorgesehen. Weitere Kosten der Ausführung des Informations- und Kommunikationsdienstegesetzes sind nicht zu erwarten. Länder und Gemeinden werden mit Kosten nicht belastet.

Die Wirtschaftsverbände und Unternehmen, auch der mittelständischen Wirtschaft, sind zu den mit der Umsetzung des Gesetzes (u. a. Datenschutz, Jugendschutz, digitale Signaturen) zu erwartenden Kosten um Stellungnahme gebeten worden. Diese Kosten können im Einzelfall erheblich sein. Sie sind abhängig von der Organisationsform und dem Grad der jeweiligen Inanspruchnahme und können – auch von der betroffenen Wirtschaft – gegenwärtig nicht eindeutig beziffert werden.

Weitere Auswirkungen

Die mit dem Informations- und Kommunikationsdienste-Gesetz verbundene Schaffung einheitlicher und verläßlicher Rahmenbedingungen sowie die Beseitigung von Investitionshemmnissen für die neuen Informations- und Kommunikationsdienste läßt erwarten, daß hiervon Impulse für ein verstärktes Wachstum in diesem Wirtschaftsbereich ausgehen. Die Regelungen führen daher bei einer Gesamtbetrachtung eher zu einer Entlastung der Wirtschaft. Von der Förderung des Wettbewerbes gehen tendenziell dämpfende Einflüsse auf Einzelpreise aus. Auswirkungen auf das Preisniveau, insbesondere das Verbraucherpreisniveau, sind jedoch nicht zu erwarten. Außerdem werden zum Schutz des Verbrauchers im Informations- und Kommunikationsdienste-Gesetz Regelungslücken im Hinblick auf die erweiterten Nutzungsmöglichkeiten von Angeboten der neuen Dienste geschlossen.

Die Schaffung einheitlicher und verläßlicher wirtschaftlicher Rahmenbedingungen für das Angebot und die Nutzung der neuen Dienste wird deren breite Nutzung fördern und damit auch einen Beitrag zur Entlastung von Verkehr und Umwelt leisten, in dem zunehmend bisherige Vertriebswege und weitere Transportmöglichkeiten ersetzt oder ergänzt werden.

B. Besonderer Teil

Zu Artikel 1 (Gesetz über die Nutzung von Telediensten)

Zur Ausgangslage und zur Zielsetzung des Teledienstegesetzes vgl. unter A. Allgemeiner Teil „Ziel des Gesetzes" und nachfolgend die Begründung zu § 1 des Teledienstegesetzes. Zur Gesetzgebungskompetenz des Bundes vgl. unter A. Allgemeiner Teil „Gesetzgebungskompetenz des Bundes".

Zu § 1 (Zweck des Gesetzes)

Der freie Zugang für Diensteanbieter und Nutzer sowie die Offenheit des Marktes im Bereich der neuen Informations- und Kommunikationsdienste sind grundlegende Bedingungen, um die internationale Wettbewerbsfähigkeit Deutschlands sicherzustellen. Die Regelungen dieses Gesetzes zielen deshalb darauf ab, Wettbewerbsverzerrungen zu vermeiden und Investitionshemmnisse durch Überregulierung zu verhindern.

Gleichzeitig soll das Gesetz einen Beitrag zur Akzeptanz der neuen Informations- und Kommunikationstechnik im täglichen Rechts- und Geschäftsverkehr leisten.

Zu § 2 (Geltungsbereich)

Zu Absatz 1

In diesem Absatz wird der Begriff „Teledienste" abstrakt definiert. Zur inhaltlichen Beschreibung der Teledienste siehe Ausführungen unter A. Allgemeiner Teil, Einordnung der neuen Informations- und Kommunikationsdienste.

Zu Absatz 2

Absatz 2 zählt beispielhaft die unterschiedlichen Dienste auf, die als Teledienste im Sinne des Absatzes 1 anzusehen sind und orientiert sich an den heute bekannten Diensten. Der Begriff „insbesondere" macht deutlich, daß das Gesetz auch für künftige Entwicklungen im Bereich der neuen Dienste offen ist.

Zu Absatz 2 Nr. 1

Bei den hier beschriebenen Diensten steht die Nutzung von Inhalten der Individualkommunikation im Vordergrund. Beispielhaft ist Telebanking für den wirtschaftlich geprägten Bereich der Individualkommunikation aufgeführt. Unter den ebenfalls genannten Datenaustausch ist ein breites Spektrum von individuell nutz- und gestaltbaren Inhalten zu subsumieren, die insbesondere Gegenstand des Angebots der neuen Dienste wie Meinungsforen oder der

neuen Formen der Zusammenarbeit sind, wie beispielsweise bei den Anwendungen Telearbeit, Telemedizin, Telelernen, Telematik und anderen erweiterten Formen der Individualkommunikation.

Zu Absatz 2 Nr. 2

Die hier erfaßten Dienste können unterschiedliche Informationen zum Inhalt haben. Beispielhaft aufgeführt sind für die individuelle Nutzung bestimmte Datendienste wie Verkehrs-, Wetter-, Umwelt- und Börsendaten; hierzu zählen aber auch Einzelwerbeangebote über Waren und Dienstleistungen sowie sonstige Angebote und Anzeigen (z. B. Homepages). Nicht erfaßt sind Datendienste, die mit dem Ziel der Meinungsbildung für die Allgemeinheit redaktionell aufbereitet sind, beispielsweise Textdienste im Rundfunk und in der elektronischen Presse.

Zu Absatz 2 Nr. 3

Es werden die von den Zugangsvermittlern – insbesondere Online-Anbietern – bereitgestellten Angebote zur Nutzung der neuen Dienste erfaßt (z. B. Navigationshilfen). Die Zuordnung der hierdurch vermittelten Angebote richtet sich nach den Nummern 1, 2, 4 und 5.

Zu Absatz 2 Nr. 4

Bei den Telespielen handelt es sich um eine besondere Form von Angeboten mit Bewegtbilddarstellungen (video-on-demand). Es wird erwartet, daß mit der fortschreitenden technischen Entwicklung diesem Bereich erhebliche wirtschaftliche Bedeutung zukommt.

Zu Absatz 2 Nr. 5

Mit dieser Regelung wird ein breites Spektrum wirtschaftlicher Betätigung mittels der neuen Dienste erfaßt. Dies betrifft sowohl die elektronischen Bestell-, Buchungs- und Maklerdienste als auch interaktiv nutzbare Bestell- und Buchungskataloge, Beratungsdienste und ähnliche Formen wirtschaftlicher Betätigung. Wesentliches Kennzeichen dieser Dienste ist, daß diese Angebote unmittelbar, d. h. ohne Medienbruch, in Anspruch genommen werden können.

Zu Absatz 3

In diesem Absatz wird klargestellt, daß es für die Anwendung dieses Gesetzes nicht darauf ankommt, ob die Teledienste entgeltlich oder unentgeltlich genutzt werden.

Zu Absatz 4

Der Absatz enthält die notwendige Abgrenzung zum Telekommunikationsgesetz sowie zum Rundfunk nach dem Rundfunkstaatsvertrag der Länder. Die Übermittlung der Teledienste setzt die Telekommunikation voraus, daher kommen sowohl das Teledienstegesetz als auch das Telekommunikationsgesetz funktionsbezogen zur Anwendung. Nummer 1 stellt klar, daß im Teledienstegesetz die inhaltlichen und nutzungsrelevanten Komponenten der bereitgestellten Angebote geregelt werden. Der technische Vorgang der Telekommunikation nach § 3 Nr. 16 Telekommunikationsgesetz, die Telekommunikationsdienstleistungen nach § 3 Nr. 18 Telekommunikationsgesetz und das geschäftsmäßige Erbringen von Telekommunikationsdiensten nach § 3 Nr. 5 Telekommunikationsgesetz bleiben unberührt.

Zu Absatz 5

Dieser Absatz hat klarstellende Funktion. Das Gesetz macht von der Rahmenkompetenz des Bundes für die Presse nach Artikel 75 Abs.1 Nr. 2 Grundgesetz keinen Gebrauch.

Zu § 3 (Begriffsbestimmungen)

Die Vorschrift definiert die Begriffe „Diensteanbieter" und „Nutzer".

Der Begriff des „Diensteanbieters" erfaßt drei wesentliche Handlungsformen. Diese drei Grundfunktionen können jeweils getrennt vorkommen, aber auch in der Person des Anbieters zusammenfallen. Hier ist bezogen auf die Rechtsfolgen jeweils aufgabenbezogen abzugrenzen (vgl. § 5). Die Vorschrift unterscheidet nicht nach der Art der Tätigkeit, die der Diensteanbieter ausübt; es ist daher unerheblich, ob er nur gelegentlich und privat oder geschäftsmäßig, also mit gewisser Nachhaltigkeit, auftritt.

Zu § 4 (Zugangsfreiheit)

Die Vorschrift stellt die Geltung der allgemeinen Handlungs- und Gewerbefreiheit (Artikel 2, 12 GG) auch für den Bereich der Teledienste klar. Eine besondere Anmeldung oder Zulassung ist deshalb nicht erforderlich. Die Einschränkung auf „besondere" macht deutlich, daß sonstige Anmelde- oder Zulassungserfordernisse des allgemeinen Rechts, etwa gewerberechtlicher oder wirtschaftsrechtlicher Art, unberührt bleiben. Hinsichtlich wettbewerbsrechtlicher Fragen gilt das Gesetz gegen Wettbewerbsbeschränkungen (GWB); ein zusätzlicher Wettbewerbsschutz durch das Teledienstegesetz ist nicht erforderlich. Anzeige oder Lizenzierungsvorschriften nach dem Telekommunikationsgesetz, soweit Anbieter von Telediensten zugleich einer Lizenz nach § 8 Telekommunikationsgesetz bedürfen, bleiben gleichfalls unberührt.

Zu § 5 (Verantwortlichkeit)

Zu Absatz 1

Absatz 1 der Vorschrift stellt den aus der allgemeinen Rechtsordnung folgenden Grundsatz der Eigenverantwortlichkeit der Diensteanbieter für die von ihnen angebotenen, eigenen Inhalte klar. Der Begriff der Verantwortlichkeit bezieht sich auf das Einstehenmüssen für eigenes Verschulden. Wer eigene Inhalte vorsätzlich oder fahrlässig so bereitstellt, daß sie über Teledienste zur Kenntnis genommen werden können, trägt die Verantwortung für diese Inhalte. Eigene Inhalte sind auch von Dritten hergestellte Inhalte, die sich der Anbieter zu eigen macht. Die Hersteller und Anbieter rechtswidriger Angebote, z. B. im Internet sind danach für diese im Rahmen der geltenden Straf- und Zivilrechtsordnung stets verantwortlich.

Zu Absatz 2

Stellt der Diensteanbieter fremde Inhalte in sein Angebot ein, bleibt auch hier in erster Linie der Urheber für diese Inhalte verantwortlich. Dennoch hat der Diensteanbieter selbst eine Mitverantwortung zu tragen, wenn ihm der einzelne, konkrete Inhalt bekannt ist und wenn er technisch in der Lage ist, diesen einzelnen Inhalt gegen weitere Nutzung zu sperren. Die Regelung dient der Klarstellung, daß dem Diensteanbieter, der rechtswidrige Inhalte Dritter in sein Diensteangebot, z. B. seinen eigenen News-Server oder in seinen eigenen Online-Dienst übernimmt, eine Garantenstellung für die Verhinderung der Übermittlung an Dritte trifft. Diese Verpflichtung soll allerdings nur dann greifen, wenn der Diensteanbieter die fremden rechtswidrigen Inhalte bewußt zum Abruf bereit hält. Diese Eingrenzung auf vorsätzliches Handeln entspricht der derzeitigen Rechtslage im allgemeinen Straf- und Ordnungswidrigkeitenrecht: Die geltende Rechtsordnung setzt im Strafrecht und Ordnungswidrigkeitenrecht für alle Äußerungsdelikte und sonstigen im Bereich der Teledienste durch bestimmte Inhalte begehbare Straftatbestände Vorsatz, also unbedingte oder bedingte Kenntnis der objektiven Tatbestandsverwirklichung voraus.

Auch im Hinblick auf die zivilrechtliche deliktische Haftung berücksichtigt die Einschränkung der Verantwortlichkeit auf vorsätzliches Handeln die Tatsache, daß der Diensteanbieter die fremden Inhalte nicht veranlaßt hat und es ihm aufgrund der technisch bedingten Vervielfachung von Inhalten und der Unüberschaubarkeit der in ihnen gebundenen Risiken von Rechtsgutverletzungen zunehmend unmöglich ist, alle fremden Inhalte im eigenen Dienstebereich zur Kenntnis zu nehmen und auf ihre Rechtmäßigkeit zu überprüfen. Dadurch, daß für die Verantwortlichkeit im Sinne des Absatz 2 Kenntnis von den Inhalten verlangt wird, erhalten die Diensteanbieter die erforderliche Rechtssicherheit. Wie für eigene Inhalte haben sie allerdings dann für die Bereitstellung fremder Inhalte voll einzustehen, wenn sie diese als eigene anbieten, d. h. sich den jeweiligen Inhalt in ihrem Dienstangebot zu eigen machen.

Die Einschränkung der Verantwortlichkeit für fremde Inhalte durch eine Zumutbarkeitsklausel stellt klar, daß hier nicht jeder denkbare Aufwand gemeint ist, sondern daß die Bedeutung des Einzelfalles und der Aufwand sowie die Auswirkung auf andere Teile des Dienstes im Verhältnis zueinander gesehen werden müssen. Die Zumutbarkeitsklausel nimmt in Betracht, daß Teledienste, z. B. Newsgruppen-Angebote im Server des Anbieters, besonders schnelle und umfangreiche Bereitstellung von Inhalten ermöglichen, damit zugleich aber von Dritten dazu benutzt werden können, rechtswidrige Inhalte einzufügen, ohne daß der den technischen/organisatorischen Rahmen setzende Diensteanbieter davon Kenntnis hat. Je nach Art des Teledienstes kann eine gezielte Sperrung oder Löschung nicht oder nur mit unverhältnismäßigem Aufwand möglich sein. Die Einschränkung durch die Zumutbarkeitsklausel gewährleistet, daß der Diensteanbieter nicht gezwungen wird, unzumutbaren Aufwand zu betreiben; dazu zählt z. B. die Sperrung der Nutzung für ganze Dienstebereiche oder die Einstellung des gesamten Teledienstes, obwohl nur ein einziger oder vereinzelte rechtswidrige Inhalte von Dritten eingestellt worden sind.

Liegen die Voraussetzungen der Verantwortlichkeit für rechtswidrige fremde Inhalte vor, bestimmen sich die Rechtsfolgen nach der geltenden Rechtsordnung; im Bereich des Strafrechts ist dies z. B. die Strafbarkeit, im Bereich der deliktischen Haftung die Schadensersatzpflicht des Diensteanbieters. Bei Vorliegen der Voraussetzungen genügt der Verweis auf die primäre Verantwortlichkeit des Urhebers der rechtswidrigen Inhalte nicht, um die Mitverantwortung des Diensteanbieters auszuschließen.

Die automatische und zeitlich begrenzte Vorhaltung fremder Inhalte aufgrund Nutzerabfrage gilt aufgrund der Fiktion des Abs. 3 Satz 2 – unter den dort genannten Voraussetzungen – als Anwendungsfall des Abs. 3 Satz 1.

Zu Absatz 3

Absatz 3 stellt klar, daß Diensteanbieter für fremde Inhalte dann nicht verantwortlich sind, wenn sie zu diesen fremden Inhalten lediglich den Weg öffnen. Es bleibt dabei, daß der Urheber und derjenige, der Inhalte in das Netz einstellt, für diese Inhalte einzustehen hat. Die technischen Möglichkeiten und Gegebenheiten der neuen Informations- und Kommunikationsdienste führen weder zu einer Haftungsverlagerung noch zu einer Haftungsausweitung. Dem Diensteanbieter, der fremde Inhalte lediglich, ohne auf sie Einfluß nehmen zu können zum abrufenden Nutzer durchleitet, obliegt es nicht, für diese Inhalte einzutreten. Er soll nicht anders behandelt werden als ein Anbieter von Telekommunikationsdienstleistungen. Denn der bloße Zugangsvermittler leistet ebenfalls keinen eigenen Tatbeitrag.

Absatz 3 Satz 2 geht auf Eigenschaften der Zugangsvermittlung ein, die zur Kostenvermeidung und Effizienzsteigerung üblich sind und in technischen Vorgaben wurzeln. Die Vorschrift stellt in diesem Zusammenhang durch eine Fiktion klar, daß die automatische Übernahme von fremden Inhalten in den eigenen Verfügungsbereich des Zugangsvermittlers (sog. Cache) aufgrund einer Nutzeranfrage zum Vermittlungsvorgang gehört, wenn diese übernommenen Inhalte nach begrenzter Zeit wieder gelöscht werden. Dies ist bei Zwischenspeicherungen auf sog. Proxy-Cache-Servern im Internet der Fall, die automatisch durch Nutzerabruf erfolgen und vom Diensteanbieter nicht im Einzelfall gesteuert werden können. Die Einschränkung der Fiktion auf eine kurzzeitige Zwischenspeicherung trägt dem Umstand Rechnung, daß Inhalte, die auf einem Cache-Speicher des Diensteanbieters gespeichert sind, mit zunehmender Verweildauer unter den Tatbestand des Abs. 2 fallen. Wegen der Verbindung zu den Fällen des Absatzes 2 ist hier aber nur ein Zeitraum von wenigen Stunden, nicht von Tagen gemeint.

Zu Absatz 4

Während Absatz 1 bis 3 die strafrechtliche und deliktische Verantwortlichkeit der Diensteanbieter für ei-

genes Verschulden zum Gegenstand haben, stellt Absatz 4 klar, daß die objektiven, d. h. keine Schuld voraussetzenden Verpflichtungen der Diensteanbieter zur Unterlassung von Rechtsgutverletzungen für alle Diensteangebote davon unberührt bleiben sollen. Dies gilt auch für die Diensteanbieter, die nur den Zugang zu fremden Inhalten vermitteln und dabei rechtswidrige Inhalte in ihrem Proxy-Cache-Server zwischenspeichern. Regelmäßig setzen Unterlassungspflichten im öffentlichen Recht, aber auch im Zivilrecht nur die Rechtswidrigkeit und eine andauernde Rechtsverletzung bzw. Wiederholungsgefahr voraus, nicht aber ein Verschulden. Eine selbständige verschuldensunabhängige Verpflichtung, Störungen der öffentlichen Ordnung und rechtswidrige Verletzungen privater Rechte zu unterlassen, enthält Absatz 4 nicht; die Vorschrift verweist insoweit auf die allgemeinen Vorschriften über die Verpflichtung des Störers zur Unterlassung bzw. Beseitigung der Störung der öffentlichen Sicherheit und Ordnung oder der Verletzung privater Rechte. Die Unterlassungspflichten, hier der Sperrung rechtswidriger Inhalte gegenüber den Nutzern, sollen nicht weiterreichen, als dem Diensteanbieter rechtlich und tatsächlich möglich ist. Die ausdrückliche Bezugnahme auf das Fernmeldegeheimnis nach § 85 Telekommunikationsgesetz – das selbstverständlich auch in den Fällen des Absatzes 1 bis 3 zu beachten ist – soll besonders hervorheben, daß Diensteanbieter, die lediglich den Zugang zur Nutzung vermitteln, mit dem Teledienst zugleich Telekommunikationsdienstleistungen erbringen und durch das Fernmeldegeheimnis gehindert sind, individuell abgerufene oder sonst nicht öffentlich übermittelte Inhalte von sich aus mitzulesen und Inhalt und Umstände der Telekommunikation von sich aus Dritten zu offenbaren. Die Pflicht zur Sperrung wird daher bei solchen nichtöffentlichen Inhalten durch die zuständigen Behörden oder Dritte angestoßen werden müssen, die den Anbieter auf die Zwischenspeicherung rechtswidriger Inhalte z. B. in seinem Internet-Server hinweisen.

Die Bezugnahme auf die technische Möglichkeit und Zumutbarkeit der Sperrung stellt wie in Absatz 2 klar, daß die verschuldensunabhängige Haftung des Diensteanbieters nicht weiter gehen kann als der vertretbare Aufwand.

Zu § 6 (Anbieterkennzeichnung)

Die Vorschrift dient dem Verbraucherschutz. Sie soll für den Nutzer ein Mindestmaß an Transparenz und Information über die natürliche oder juristische Person oder Personengruppe, die ihm einen Teledienst anbietet, sicherstellen. Durch die räumliche Trennung der möglichen Vertragspartner fehlt die unmittelbare Erfahrung über die Person des Anbieters; durch die Flüchtigkeit des Mediums fehlen – soweit keine Speicherung erfolgt – dauerhaft verkörperte Anhaltspunkte über dessen Identität. Die Pflicht zur Angabe von Identität und Anschrift dient damit auch als Anknüpfungspunkt für die Rechtsverfolgung im Streitfall. Die Vorschrift gilt nur für geschäftsmäßige Angebote, die aufgrund einer nachhaltigen Tätigkeit mit oder ohne Gewinnerzielungsabsicht abgegeben werden. Sie gilt dagegen nicht für private Gelegenheitsgeschäfte. Gelegentliche An- und Verkäufe z. B. über virtuelle „Schwarze Bretter" unterfallen daher nur dem allgemeinen Recht, so daß etwa bei Vertragsschluß die nach bürgerlichem Recht erforderlichen Angaben zu machen sind.

Zu Artikel 2 (Gesetz über den Datenschutz bei Telediensten)

Ausgangslage

Bei Telediensten können personenbezogene Daten in vielfältiger Weise anfallen, beliebig kombiniert, verändert oder ausgewertet werden; Erhebung, Verarbeitung und Nutzung personenbezogener Daten findet nicht nur in einer Datenverarbeitungsanlage, sondern im Netz mit vielen Beteiligten und ohne hinreichende Kontrollmöglichkeiten des Nutzers statt.

Ziel des Gesetzes

Ziel des Gesetzes ist es, eine verläßliche Grundlage für die Gewährleistung des Datenschutzes im Bereich der Teledienste zu bieten und einen Ausgleich zwischen dem Wunsch nach freiem Wettbewerb, berechtigten Nutzerbedürfnissen und öffentlichen Ordnungsinteressen zu schaffen.

Notwendigkeit eines neuen Gesetzes

Die Bestimmungen des Teledienstedatenschutzgesetzes knüpfen an das vorhandene Instrumentarium des Datenschutzrechts an. Ausgangspunkt für die Regelungen ist das verfassungsrechtlich verbürgte Recht auf informationelle Selbstbestimmung. Das traditionelle Datenschutzkonzept wird ergänzt, soweit die Risiken der neuen Teledienste dies erforderlich machen. Dabei berücksichtigen die gesetzlichen Regelungen die erweiterten Möglichkeiten moderner Informations- und Kommunikationstechnik.

Die gesetzlichen Bestimmungen im einzelnen

Zu § 1 (Geltungsbereich)

Zu Absatz 1

Das Teledienstedatenschutzgesetz gilt für alle Teledienste im Sinne des Teledienstegesetzes (Artikel 1 IuKDG).

Der Begriff „Übermittlung" beinhaltet die Vermittlung und Übertragung der Inhalte, die durch die Teledienste ermöglicht werden. Die Übermittlung erfolgt mittels Telekommunikation im Sinne von § 3 Nr. 16 Telekommunikationsgesetz.

Zu Absatz 2

Die Vorschrift stellt klar, daß die allgemeinen datenschutzrechtlichen Vorschriften für die Verarbeitung personenbezogener Daten gelten, soweit das Teledienstedatenschutzgesetz keine besondere Regelung trifft. Das Teledienstedatenschutzgesetz gilt auch für personenbezogene Daten, die nicht in Dateien im

Sinne von § 3 Abs. 2 Bundesdatenschutzgesetz verarbeitet oder genutzt werden.

Das Fernmeldegeheimnis (§ 85 Telekommunikationsgesetz) wird nicht berührt. Inhalte der Telekommunikation und ihre näheren Umstände, insbesondere die Tatsache, ob jemand an einem Telekommunikationsvorgang beteiligt ist, unterliegen dem Fernmeldegeheimnis. Zur weiteren Absicherung des Fernmeldegeheimnisses trifft das Teledienstedatenschutzgesetz in § 4 Abs. 2 Nr. 3 eine Regelung zu technischen und organisatorischen Maßnahmen der Datensicherung.

Zu § 2 (Begriffsbestimmungen)

Die Vorschrift definiert die Begriffe „Diensteanbieter" und „Nutzer".

Der Begriff des „Diensteanbieters" erfaßt die wesentlichen Handlungsformen. Diese Grundfunktionen können jeweils getrennt vorkommen, aber auch in der Person eines Anbieters zusammenfallen. Die Vorschrift unterscheidet entsprechend Artikel 1 § 2 Abs. 2 Informations- und Kommunikationsdienste-Gesetz nicht nach der Art der Tätigkeit, die der Diensteanbieter ausübt; es ist daher unerheblich, ob er nur gelegentlich und privat oder geschäftsmäßig, also mit gewisser Nachhaltigkeit, auftritt.

Der Begriff des „Nutzers" ist weit gefaßt, um die Schutzfunktionen des Gesetzes bereits im vorvertraglichen Bereich greifen zu lassen.

Zu § 3 (Grundsätze für die Verarbeitung personenbezogener Daten)

Zu Absatz 1

§ 3 Abs. 1 enthält die Befugnisnorm für die Erhebung, Verarbeitung und Nutzung personenbezogener Daten durch Diensteanbieter. Sie entspricht den in § 4 Abs. 1 Bundesdatenschutzgesetz festgelegten Voraussetzungen, bezieht aber auch die Erhebung in die Geltung des Gesetzesvorbehalts mit ein. Letzteres entspricht den Vorgaben der EG-Richtlinie zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr vom 23. November 1995, die bis 1998 in nationales Recht umzusetzen ist.

Zu Absatz 2

Diese Bestimmung ist Ausdruck des Grundsatzes der Zweckbindung. Daten über den Nutzer dürfen grundsätzlich nur für die Erbringung von Informations- und Kommunikationsdiensten verwendet werden. Eine Verwendung von Nutzerdaten für andere Zwecke ist nur zulässig, wenn ein Gesetz oder eine andere Rechtsvorschrift diese Verwendung erlauben oder der Nutzer eingewilligt hat.

Zu Absatz 3

Durch diese Vorschrift soll verhindert werden, daß die Nutzung von Telediensten von einer Einwilligung des Nutzers in eine Verarbeitung oder Nutzung seiner Daten für andere Zwecke abhängig gemacht wird.

Zu Absatz 4

Diese Regelung verankert die Grundsätze des Systemdatenschutzes und der Datenvermeidung. Bereits durch die Gestaltung der Systemstrukturen, in denen personenbezogene Daten erhoben und verarbeitet werden können, soll die Erhebung und Verwendung personenbezogener Daten vermieden und die Selbstbestimmung der Nutzer sichergestellt werden. Dies kann durch dateneinsparende Organisation der Übermittlung, der Abrechnung und Bezahlung sowie der Abschottung von Verarbeitungsbereichen unterstützt werden.

Normadressat ist der einzelne Diensteanbieter. Er soll das Angebot seiner Teledienste an dem Ziel ausrichten, keine oder jedenfalls so wenige personenbezogene Daten wie möglich zu erheben und zu verarbeiten. Dieser Grundsatz des Systemdatenschutzes findet seine Ausprägung in § 4 Abs. 1 mit der Ermöglichung der Inanspruchnahme von Telediensten in anonymer oder pseudonymer Form.

Zu Absatz 5

Der Nutzer ist vor der Erhebung umfassend zu unterrichten. Nur so kann der Nutzer sich einen umfassenden Überblick über die Erhebung, Verarbeitung und Nutzung seiner personenbezogenen Daten verschaffen. Zeitpunkt, Umfang und Form der Unterrichtung ergeben sich dabei aus den besonderen Risiken der Datenverarbeitung im Netz. Der Nutzer ist daher über Art, Umfang, Ort und Zweck der Verarbeitung seiner personenbezogenen Daten zu unterrichten; die Unterrichtung ist zu protokollieren und sie muß vom Diensteanbieter so abgelegt werden, daß der Nutzer sich jederzeit über den Inhalt der Unterrichtung informieren kann. Ein Verzicht auf die Unterrichtung ist möglich, darf aber nicht als Einwilligung in eine Verarbeitung im Sinne der Absätze 1 und 2 gedeutet werden.

Es wird klargestellt, daß sich die Unterrichtungspflicht auch auf automatisierte Verfahren bezieht, die eine Erhebung, Verarbeitung oder Nutzung ermöglichen (z. B. durch Speichern einzelner Nutzungsdaten auf der Festplatte des vom Nutzer benutzten PC), bei denen der Personenbezug aber erst zu einem späteren Zeitpunkt hergestellt werden kann.

Zu Absatz 6

Der Nutzer kann seine erteilte Einwilligung jederzeit widerrufen. Darauf ist der Nutzer hinzuweisen. Die jederzeitige Abrufbarkeit muß entsprechend Absatz 5 Satz 3 gewährleistet sein.

Zu Absatz 7

Eine Verarbeitung personenbezogener Daten ist auch mit Einwilligung des Nutzers (vgl. Absätze 1 und 2) zulässig. Der Einwilligung des Betroffenen kommt im Rahmen der alltäglichen Nutzung von Telediensten eine erhebliche praktische Bedeutung zu. Für eine wirksame Einwilligung ist nach § 4 Abs. 2 Bundesdatenschutzgesetz allerdings prinzipiell Schriftform erforderlich. Dieses Schutzerfordernis soll für den Bereich der Teledienste grundsätzlich

beibehalten werden; schriftlich erklärte Einwilligungen sollen weiterhin möglich sein. Daneben soll aber auch die elektronische Einwilligung ermöglicht werden.

Wegen der besonderen Risiken, denen elektronische Erklärungen mangels Verkörperung (keine Schriftform) und mangels biometrischer Kennzeichen (keine eigenhändige Unterschrift) ausgesetzt sind, bedürfen sie besonderer Verfahren, die ihre Wirksamkeit sicherstellen.

Zu Absatz 7 Nr. 1

Diese Voraussetzung soll den Schutz der Nutzer vor einer übereilten Einwilligung sicherstellen. Dieser Schutz ist in Anbetracht der besonderen technikspezifischen Gefahren, nämlich der Anwendung eines flüchtigen Mediums (Bildschirm) und des Handelns durch einfachen Knopfdruck oder Mausklick, das nicht zwischen wichtigen und unwichtigen Handlungen unterscheidet, von Bedeutung. In diesem Sinne autorisiert ist eine Einwilligung zum Beispiel durch eine bestätigende Wiederholung des Übermittlungsbefehls, während gleichzeitig die Einwilligungserklärung mindestens auszugsweise auf dem Bildschirm dargestellt wird. Sie verpflichtet den Diensteanbieter zu entsprechenden Maßnahmen nur, soweit seine Einflußnahmemöglichkeit reicht. Für die vom Nutzer eingesetzte Technik ist er nicht verantwortlich.

Zu Absatz 7 Nr. 2 und Nr. 3

Zum Nachweis von Authentizität und Urheberschaft der Einwilligung ist als geeignetes technisches Verfahren die Verwendung von digitalen Signaturen denkbar, die die Voraussetzung von Artikel 3 des Informations- und Kommunikationsdienste-Gesetzes erfüllt. Die Vorschrift ist aber bewußt auch für die Anwendung anderer geeigneter technischer Verfahren offen, soweit die Authentizität und Urheberschaft entsprechend sichergestellt sind.

Zu Absatz 7 Nr. 4 und Nr. 5

Diese Anforderungen dienen der Transparenz der vom Nutzer erlaubten Datenverarbeitung seiner personenbezogenen Daten. Sie schafft Akzeptanz für die Anwendung elektronischer Einwilligungen und sichert zugleich das informationelle Selbstbestimmungsrecht des Nutzers, der nachprüfen kann, wann, wem und in welchem Umfang er eine Einwilligung in die Verarbeitung seiner personenbezogenen Daten erteilt hat.

Zu § 4 (Datenschutzrechtliche Pflichten des Diensteanbieters)

Die Vorschrift konkretisiert im einzelnen die in § 3 aufgestellten datenschutzrechtlichen Grundsätze.

Zu Absatz 1

Absatz 1 konkretisiert das Ziel der Datenvermeidung (vgl. § 3 Abs. 4): Diensteanbieter haben im Rahmen der technischen Möglichkeiten den Nutzern anonymes oder pseudonymes Handeln zu ermöglichen. Das Gebot der Datenvermeidung gilt für den gesamten Nutzungsvorgang. Welche technischen Möglichkeiten dabei in Betracht kommen, ist von einer generellen, objektiven Sichtweise abhängig. Der Diensteanbieter soll aber nicht zu jedem möglichen technischen Angebot verpflichtet sein. Die Zumutbarkeit des Angebots setzt deshalb eine Grenze, bei der z. B. Größe und Leistungsfähigkeit des Diensteanbieters berücksichtigt werden können. Bestimmte technische Verfahren werden im Hinblick auf die weitere technische Entwicklung nicht vorgeschrieben. Denkbar ist z. B. das Angebot an den Nutzer, Teledienste mit vorbezahlten Wertkarten oder Chipkarten in Anspruch nehmen zu können. In jedem Fall ist der Nutzer entsprechend zu unterrichten.

Für das Erfordernis der Anonymität ist die faktische Anonymität im Sinne von § 3 Abs. 7, 2. Alternative Bundesdatenschutzgesetz ausreichend.

Pseudonymes Handeln ermöglicht nicht anonymes, sondern quasi-anonymes Handeln. Ein Pseudonym kann ein Name oder eine Kurzbezeichnung sein, die aus sich heraus die Identität des Nutzers nicht preisgeben, aber über eine Referenzliste beim Diensteanbieter mit der Identität des Nutzers zusammengeführt werden können.

Zu Absatz 2

Dieser Absatz konkretisiert die in § 3 festgelegten Grundsätze des Systemdatenschutzes und der Datenvermeidung. Der Diensteanbieter ist verpflichtet, durch entsprechende technische und organisatorische Maßnahmen die praktische Umsetzung dieser Grundsätze sicherzustellen.

Zu Absatz 2 Nr. 1

Durch die Anforderung nach Nummer 1 wird der Diensteanbieter verpflichtet, die technischen und organisatorischen Maßnahmen zu treffen, damit der Nutzer jederzeit seine Kommunikationsbeziehung abbrechen kann.

Zu Absatz 2 Nr. 2

Der Diensteanbieter ist verpflichtet, die technischen und organisatorischen Vorkehrungen zu treffen, damit die personenbezogenen Daten über die Inanspruchnahme von Telediensten unmittelbar gelöscht werden. Die Anforderung nach Nummer 2 flankiert das rechtliche Löschungsgebot nach § 6 hinsichtlich der Nutzungs- und Abrechnungsdaten.

Zu Absatz 2 Nr. 3

Der Diensteanbieter hat durch technische und organisatorische Maßnahmen sicherzustellen, daß der Nutzer Teledienste in Anspruch nehmen kann, ohne daß Dritte davon Kenntnis nehmen können. Auf diese Weise wird das Fernmeldegeheimnis im Bereich der Teledienste zusätzlich abgesichert.

Zu Absatz 2 Nr. 4

Nummer 4 statuiert ein technisch und organisatorisch zu gewährleistendes Trennungsgebot. Mit dieser Re-

gelung soll verhindert werden, daß der Diensteanbieter personenbezogene Daten über die Inanspruchnahme von verschiedenen Telediensten zusammenführt und auf diese Weise personenbezogene Nutzerprofile entstehen. Dem Interesse der Diensteanbieter an einer Zusammenführung der Daten für Abrechnungszwecke wird Rechnung getragen.

Zu Absatz 3

Zweck des Absatzes 3 ist es, dem Nutzer Transparenz über die Weiterschaltung zu einem weiteren Diensteanbieter zu ermöglichen. Ohne eine derartige Vorschrift können weder das Auskunftsrecht des Nutzers noch eine datenschutzrechtliche Kontrolle wirksam wahrgenommen werden.

Zu Absatz 4

Die Regelung ermöglicht einen Kompromiß zwischen dem Interesse des Nutzers an weitgehender Anonymität seines Konsumentenverhaltens und dem berechtigten wirtschaftlichen Interesse des Diensteanbieters, die Inanspruchnahme der Teledienste auszuwerten. Aus diesem Grund sind Nutzungsprofile der Nutzer pseudonym möglich.

Satz 2 soll eine Umgehung des Satzes 1 verhindern.

Zu § 5 (Bestandsdaten)

zu Absatz 1

Absatz 1 konkretisiert die in § 3 Abs. 1 festgeschriebene Befugnis zur Erhebung und Verwendung personenbezogener Daten unter dem Gesichtspunkt der Erforderlichkeit für sogenannte Bestandsdaten. Er regelt, in welchem Umfang und für welche Zwecke der Diensteanbieter personenbezogene Daten für die Bereitstellung und Vermittlung von Telediensten erheben, verarbeiten und nutzen darf. Die Vorschrift enthält keinen Katalog der Bestandsdaten; welche Daten zu den Bestandsdaten zu rechnen sind, ergibt sich aus dem Zweck des jeweiligen Vertragsverhältnisses; als Bestandsdaten sind aber in jedem Falle nur solche anzusehen, die für die Begründung, inhaltliche Ausgestaltung oder Änderung des Vertrages über die Inanspruchnahme von Telediensten mit dem Diensteanbieter unerläßlich sind.

Zu Absatz 2

Die Vorschrift ist Ausdruck des engen Zweckbindungsgrundsatzes in § 3 Abs. 2. Absatz 2 läßt eine Verarbeitung und Nutzung der Bestandsdaten für andere Zwecke als den nach Absatz 1, insbesondere für Zwecke der Beratung, Werbung, Marktforschung oder zur bedarfsgerechten Gestaltung technischer Einrichtungen des Diensteanbieters nur mit ausdrücklicher Einwilligung des Nutzers zu. Die Vorschrift entspricht der in § 89 Abs. 7 Telekommunikationsgesetz vorgesehenen Einwilligung.

Zu Absatz 3

Dieser Absatz entspricht der in § 89 Abs. 6 Satz 1 Telekommunikationsgesetz vorgesehenen Regel für die Übermittlung personenbezogener Daten zum Zwecke der Verfolgung von Straftaten und Ordnungswidrigkeiten, zur Abwehr von Gefahren für die öffentliche Sicherheit und Ordnung oder für die Erfüllung der gesetzlichen Aufgaben der Verfassungsschutzbehörden des Bundes und der Länder, des Bundesnachrichtendienstes, des Militärischen Abschirmdienstes und des Zollkriminalamtes. Der Anwendungsbereich ist auf Bestandsdaten im Sinne von Absatz 1 beschränkt. Die Vorschrift erlaubt dem Diensteanbieter eine zweckändernde Nutzung der Bestandsdaten; die Befugnisse der genannten Behörden werden davon nicht berührt.

Zu § 6 (Nutzungs- und Abrechnungsdaten)

Zu Absatz 1

Nutzungsdaten sind personenbezogene Daten, die dem Nutzer die Nachfrage nach Telediensten ermöglichen; es handelt sich dabei um Daten, die während der Nutzung eines Teledienstes, z. B. Interaktionen des Nutzers mit dem Diensteanbieter, entstehen.

Abrechnungsdaten sind Daten, die für die Abrechnung der Inanspruchnahme von Telediensten erforderlich sind.

Vom Teledienstedatenschutzgesetz nicht erfaßt werden Verbindungsdaten im Sinne von § 5 Abs. 1 der Verordnung über den Datenschutz für Unternehmen, die Telekommunikationsleistungen erbringen (Telekommunikationsdienstunternehmen-Datenschutzverordnung – TDSV), d. h. Daten, die zur Bereitstellung von Telekommunikationsdienstleistungen dienen. Nur bestimmte Verbindungsdaten dürfen nach diesen telekommunikationsrechtlichen Vorschriften erhoben und verarbeitet werden. Soweit bei der Inanspruchnahme von Telediensten Verbindungsdaten im Sinne der Telekommunikationsdienstunternehmen-Datenschutzverordnung anfallen, findet diese Anwendung.

Zu Absatz 2

Dieser Absatz schreibt Löschungspflichten für Nutzungs- und Abrechnungsdaten vor:

Zu Absatz 2 Nr. 1

Nutzungsdaten sind nach Ende der jeweiligen Nutzung des Teledienstes zu löschen, soweit sie nicht zu Abrechnungszwecken erforderlich sind.

Zu Absatz 2 Nr. 2

Personenbezogene Daten über Suchschritte, die im Hinblick auf das Nutzerverhalten und Konsumentenwünsche von Bedeutung sind, sind nach Beendigung der Nutzung des Teledienstes unmittelbar zu löschen. Abrechnungsdaten, die für die Erstellung von Einzelnachweisen erforderlich sind, müssen spätestens nach 80 Tagen nach Versendung der Einzelabrechnung gelöscht werden; Ausnahmen von dieser Löschungsfrist bestehen nur, wenn der Nutzer die Entgeltforderung innerhalb dieser Frist bestritten hat oder wenn der Nutzer seine Abrechnung nicht beglichen hat. Die vorgesehenen Speicherfristen sind abschließend im Teledienstedatenschutzgesetz geregelt.

Zu Absatz 3

Das Gesetz geht davon aus, daß Nutzungs- und Abrechnungsdaten aufgrund ihrer hohen Sensitivität beim jeweiligen Diensteanbieter verbleiben. Absatz 3 schließt daher eine Übermittlung von personenbezogenen Nutzungs- oder Abrechnungsdaten an andere Diensteanbieter oder Dritte grundsätzlich aus. Ausnahmen gelten nur für den Diensteanbieter, der den Zugang zur Nutzung von Telediensten vermittelt; dieser darf anderen Diensteanbietern oder Dritten Nutzungsdaten zu Zwecken der Marktforschung dieser Diensteanbieter in anonymisierter Form übermitteln, und er darf Abrechnungsdaten, soweit diese für die Einziehung einer Forderung dieses Diensteanbieters erforderlich sind, übermitteln.

Zu Absatz 4

Dem Interesse der Diensteanbieter an einer Abrechnung durch dritte Unternehmen soll dieser Absatz Rechnung tragen. Hat der Diensteanbieter mit einem Dritten einen Vertrag über die Abrechnung geschlossen, so darf er diesem Dritten Abrechnungsdaten zum Zwecke der Abrechnung übermitteln. Eine Übermittlung zu einer anderen Zweckbestimmung oder eine weitergehende Nutzung durch den Dritten sind unzulässig. Der Diensteanbieter hat den Dritten auf die Einhaltung des Fernmeldegeheimnisses (§ 85 Telekommunikationsgesetz) zu verpflichten.

Zu Absatz 5

Mit dieser Vorschrift soll verhindert werden, daß aufgrund der aufgeschlüsselten Abrechnung Nutzerprofile entstehen und von Dritten (z. B. Mitbenutzer, Betriebsangehörige) eingesehen werden können. Nur wenn der Nutzer einen Einzelentgeltnachweis verlangt, darf die Abrechnung über die Inanspruchnahme von Telediensten aufgeschlüsselt werden.

Zu § 7 (Auskunftsrecht des Nutzers)

§ 7 stellt sicher, daß der Nutzer, über das nach dem Bundesdatenschutzgesetz geltende Auskunftsrecht hinaus die über ihn oder sein Pseudonym gespeicherten Daten unentgeltlich elektronisch einsehen kann. Dies gilt in Abweichung von den hier ergänzend anwendbaren Vorschriften des Bundesdatenschutzgesetzes, auch soweit es sich um Dateien handelt, die nur kurzfristig im Sinne von §§ 34 Abs. 4, 33 Abs. 2 Nr. 5 Bundesdatenschutzgesetz vorgehalten werden. Die Gewährleistung dieses Einsichtsrechts erübrigt sich, wenn die Inanspruchnahme von Angeboten anonym – beispielsweise mit Hilfe von vorbezahlten Wertkarten – ermöglicht wird.

Zu § 8 (Datenschutzkontrolle)

Für die Überwachung der Verarbeitung personenbezogener Daten im nicht-öffentlichen Bereich ist nach § 38 Bundesdatenschutzgesetz die Aufsichtsbehörde zuständig. Von dieser Regelung im Bundesdatenschutzgesetz soll nicht abgewichen werden. Die Aufsichtsbehörde soll jedoch auch ohne Anlaß tätig werden.

Zu Artikel 3 (Gesetz zur digitalen Signatur)

Allgemeines

I. Die Funktionsweise der digitalen Signatur

Eine digitale Signatur ist eine Art von Siegel zu digitalen Daten. Es wird unter Einsatz mathematischer Verfahren mit Hilfe eines privaten kryptographischen Schlüssels erzeugt. Mit Hilfe eines dazugehörigen öffentlichen Schlüssels kann die Signatur jederzeit überprüft und damit der Signaturschlüssel-Inhaber und die Unverfälschtheit der Daten festgestellt werden.

Die jeweils einmaligen Schlüsselpaare (privater und öffentlicher Schlüssel) werden durch anerkannte Stellen natürlichen Personen fest zugeordnet. Die Zuordnung wird durch ein Signaturschlüssel-Zertifikat beglaubigt. Es handelt sich dabei um ein signiertes „digitales Dokument", das den jeweiligen öffentlichen Schlüssel sowie den Namen der Person, der er zugeordnet ist, oder ein Pseudonym enthält. Das Zertifikat erhält der Signaturschlüssel-Inhaber, so daß er es signierten Daten für deren Überprüfung beifügen kann. Darüber hinaus ist es über öffentlich erreichbare Telekommunikationsverbindungen jederzeit für jedermann nachprüfbar.

Der praktische Ablauf bei Erzeugung einer digitalen Signatur ist dem Ablauf an Bankautomaten vergleichbar. Der private Schlüssel sowie die Signiertechnik ist in der Regel auf einer Chipkarte gespeichert, die erst in Verbindung mit einer Personenidentifikationsnummer (PIN) eingesetzt werden kann. Die Karte wird z. B. über einen PC mit Chipkartenleser zur Anwendung gebracht. Nachdem der Nutzer das zu signierende Dokument ausgewählt und den Steuerungsbefehl „Signieren" erteilt hat, wird die Signatur erzeugt. Die Signaturerzeugung erfolgt ohne feststellbaren Zeitverzug.

Der breite Einsatz von digitalen Signaturverfahren erfordert eine zuverlässige und effektive Sicherheitsinfrastruktur für die Zuordnung der Signaturschlüssel durch Zertifikate (Zertifizierungsstellen) sowie sichere technische Komponenten. Weiter müssen die Signaturschlüssel-Inhaber darüber unterrichtet sein, welche Maßnahmen sie in ihrem eigenen Interesse für sichere digitale Signaturen zu treffen haben.

Da die genannte Sicherheitsinfrastruktur bisher fehlt, sind digitale Signaturverfahren zur Zeit nur innerhalb geschlossener Benutzergruppen im Einsatz. Der Sicherheitswert der auf dem Markt verfügbaren technischen Komponenten ist unterschiedlich und ohne eingehende Prüfung der Komponenten nicht hinreichend zu beurteilen.

II. Bedeutung der digitalen Signatur im weltweiten Verbund moderner Informations- und Kommunikationstechnik

Die Entwicklung der Informations- und Kommunikationstechnik eröffnet neue Möglichkeiten des Informationsaustausches und der wirtschaftlichen Betätigung. Warenbestellungen, Zahlungsanweisungen an Banken, Anträge oder Einsprüche bei Behörden, die

Übermittlung sensitiver Daten im medizinischen Bereich und viele andere rechtlich relevante Vorgänge, die in der Vergangenheit über Papier abgewickelt wurden, erfolgen bereits zu einem großen Teil auf elektronischem Wege. Dies gilt auch für die Dokumentation von Daten, z. B. im Hinblick auf die Produkthaftung oder im Medizinbereich. Neu hinzu kommen multimediale Anwendungen.

Elektronisch übertragene oder gespeicherte Daten können jedoch verändert werden, ohne daß dies Spuren hinterläßt und nachgewiesen werden kann.

Da sich die Dokumentenerstellung, Kommunikation und Archivierung auf der Basis digitaler Daten etabliert hat und expandiert, ergibt sich der dringende Bedarf nach einer digitalen Lösung, die den Anforderungen einer offenen Kommunikation (in der sich die Teilnehmer nicht kennen müssen) gerecht wird, bei der zuverlässig auf den Urheber geschlossen werden kann und die Daten vor unbemerkter Veränderung geschützt sind. Diese Forderungen erfüllt die gesetzliche digitale Signatur.

Schließlich wird durch digitale Signaturen allgemein eine höhere Datensicherheit erreicht (Schutz von Software und Nutzdaten vor unbemerkter Veränderung).

III. Ziel des Gesetzes

Es soll ein administrativer Rahmen vorgegeben werden, bei dessen Einhaltung digitale Signaturen möglichst eindeutig einer bestimmten Person zuzuordnen sind und die Signaturen als sicher vor Fälschung sowie signierte Daten als sicher vor Verfälschung gelten können. Er umfaßt eine bundesweite Infrastruktur für die Zuordnung der Signaturschlüssel zu natürlichen Personen, den Einsatz geeigneter technischer Komponenten und die Unterrichtung der Signaturschlüssel-Inhaber über die von ihnen in ihrem eigenen Interesse zu treffenden Maßnahmen. Der Aufbau und Betrieb der Infrastruktur soll privatwirtschaftlich im freien Wettbewerb, jedoch unter behördlicher Kontrolle erfolgen.

Die gesetzliche Regelung soll eine hohe Gesamtsicherheit, von der Erzeugung der Signaturschlüssel über deren Zuordnung durch zuverlässige Zertifizierungsstellen bis zur Darstellung der zu signierenden Daten, gewährleisten. Die Nutzung anderer Verfahren bleibt, soweit nicht in anderen Rechtsvorschriften ausdrücklich eine digitale Signatur nach dem Signaturgesetz verlangt wird, unberührt.

Die Beweisfunktion signierter digitaler Daten soll über die faktische Sicherheit gesetzlicher digitaler Signaturen erreicht werden, da davon ausgegangen werden kann, daß die Gerichte diese im Rahmen der freien Beweiswürdigung honorieren werden. In einem weiteren (gesonderten) Schritt wird geprüft, ob Änderungen im Beweisrecht geboten sind.

Soweit durch Rechtsvorschrift die Schriftform vorgegeben ist, wird geprüft, ob und in welchen Fällen es zweckmäßig erscheint, neben der Schriftform auch die „digitale Form" mit digitaler Signatur zuzulassen.

IV. Notwendigkeit gesetzlicher Regelungen

Nur durch eine gesetzliche Regelung kann ein Rahmen geschaffen werden, der zu allgemein anerkannten digitalen Signaturen führt, wie sie benötigt werden (vgl. zu II).

Nur die nachweisliche Sicherheit gesetzlicher digitaler Signaturen wird es bei verschiedenen Rechtsvorschriften erlauben, neben der papiergebundenen Schriftform auch die digitale Form zuzulassen.

Außerdem beugen die gesetzlichen Regelungen einem Wildwuchs unterschiedlicher Verfahren mit einer Vielzahl gutachterlicher Untersuchungen in Gerichtsprozessen und einer damit verbundenen Belastung der Gerichte vor.

V. Wichtige Einzelaspekte

Hohe Fälschungssicherheit

Unter den gesetzlichen Voraussetzungen weisen digitale Signaturen eine hohe Sicherheit auf (vgl. auch Begründung zu § 14).

Während die Sicherheit der Signierverfahren in hohem Maße gewährleistet werden kann, können jedoch insbesondere unter folgenden Aspekten Restrisiken verbleiben:

- Infolge eines gefälschten Ausweises oder einer sonstigen fehlerhaften Identifikation kann ein Signaturschlüssel-Zertifikat auf einen falschen Namen ausgestellt und dieses für Betrugszwecke genutzt werden.
- Ungetreue Mitarbeiter einer Zertifizierungsstelle können gefälschte Zertifikate (auf existente oder fiktive Personen) ausstellen, und diese können für Betrugszwecke genutzt werden.
- Wenn Signaturschlüssel-Inhaber die in ihrem eigenen Interesse erforderlichen Maßnahmen nicht treffen, können Signaturschlüssel z. B. für Betrugszwecke mißbraucht werden.
- Infolge technischer Manipulationen oder technischer Fehler können ungewollt Daten signiert oder andere Daten signiert werden, als angezeigt werden.

Das erste Restrisiko läßt sich im Hinblick auf das zu erwartende Massengeschäft nicht ausschließen. Durch verfahrenstechnische Maßnahmen (z. B. Abgleich von Ausweismerkmalen) kann es jedoch hinreichend minimiert werden. Das zweite Restrisiko wird durch die für Zertifizierungsstellen vorgeschriebenen Sicherheitsmaßnahmen weitgehend minimiert. In beiden Fällen ist eine Fälschung über die vorgeschriebene Dokumentation bei der Zertifizierungsstelle jederzeit nachweisbar. Das dritte Restrisiko dürfte durch die Unterrichtung der Signaturschlüssel-Inhaber über die ihrerseits erforderlichen Maßnahmen hinreichend minimiert sein. Dies gilt auch für das vierte Restrisiko, wenn geeignete technische Komponenten eingesetzt werden.

Die Vorteile einer breiten Nutzung der digitalen Signatur überwiegen die verbleibenden Risiken bei weitem.

Die eigenhändige Unterschrift und die digitale Signatur im Vergleich

Der relativ hohe Sicherheitswert der eigenhändigen Unterschrift in der Vergangenheit ist infolge der technischen Entwicklung nur noch bedingt gegeben. Unterschriften und handgeschriebene Texte können, ebenso wie gedruckte Texte oder Bilder, über Scanner erfaßt und elektronisch gespeichert werden. Danach kann damit z. B. ein (relativ leicht verfügbarer) kleiner Roboter gesteuert werden, der mit einem Füllfederhalter die Unterschrift originalgetreu nachmacht. Eine solche Fälschung ist gegebenenfalls auch kriminaltechnisch kaum mehr nachzuweisen.

Im Gegensatz dazu ist eine unbemerkte Fälschung einer digitalen Signatur oder eine unbemerkte Verfälschung signierter Daten praktisch ausgeschlossen. Möglich ist eine unbefugte Nutzung des Signaturschlüssels, wenn der Signaturschlüssel-Inhaber diesen und die zu dessen Nutzung erforderlichen Identifikationsdaten nicht ausreichend schützt, sowie – bei hoher technischer Raffinesse – ein „Unterschieben" von falschen Daten zur Signatur. In einem solchen Falle ist wie bei einer gefälschten Unterschrift ein kriminaltechnischer Beweis kaum zu führen.

Im Streit-/Verdachtsfall müssen deshalb in beiden Fällen die Gesamtumstände des Einzelfalls beurteilt werden.

Durch die künftig mögliche Nutzung biometrischer Merkmale zur Identifikation des Signaturschlüssel-Inhabers gegenüber dem Signaturschlüssel (zusätzlich zu Besitz und Wissen) und die Verwendung geeigneter technischer Komponenten zur Aufbereitung zu signierender Daten können die verbleibenden Risiken bei digitalen Signaturen weitgehend minimiert werden.

Der Faktor Zeit

Die der gesetzlichen digitalen Signatur zugrundeliegenden mathematischen Verfahren können, da sie entsprechend geprüft und ausgewählt sind, für einen langen Zeitraum als sicher angesehen werden. Infolge schnellerer Rechner und neuer wissenschaftlicher Erkenntnisse können diese jedoch an Sicherheitswert verlieren.

Bei signierten Daten, die längerfristig benötigt werden, ist deshalb in regelmäßigem Zeitabstand eine neue Signatur (mit technischen Komponenten, die dem jeweiligen Stand der Technik entsprechen) erforderlich. Regelungen dazu enthält die ergänzende Rechtsverordnung. Vorhandene Signaturen können von der neuen Signatur eingeschlossen und damit „konserviert" werden. Wer die neue Signatur anbringt, ist unerheblich. Sie kann z. B. durch einen Archivar erfolgen.

Außerdem muß bei der Archivierung digitaler Daten – unabhängig von der Signatur – sichergestellt werden, daß sie „lesbar" bleiben (z. B. durch erneute Datenaufbereitung in bestimmten Zeitabständen, um ein „Verblassen" der Daten zu verhindern, und durch Bereithalten geeigneter Hard- und Software).

Aktuelle Verläßlichkeit digitaler Signaturen

Eine digitale Signatur kann als verläßlich gelten, wenn für den öffentlichen Signaturschlüssel, mit dem sie von jedermann überprüft werden kann, zum Zeitpunkt ihrer Erzeugung ein gültiges Zertifikat einer lizenzierten Zertifizierungsstelle bestand und wenn sie zum Zeitpunkt der Prüfung eine bestimmte Zeitdauer nicht überschritten hat oder andernfalls durch eine neue Signatur rechtzeitig „konserviert" wurde. Soweit das Datum, zu dem die Daten bzw. die digitale Signatur erzeugt wurden, beweiserheblich ist, bringt ein „Zeitstempel" (Bescheinigung einer Zertifizierungsstelle in digitaler Form mit digitaler Signatur) die erforderliche Sicherheit.

Sollte sich im Einzelfall ein begründeter Verdacht ergeben, daß Zertifikate gefälscht oder nicht fälschungssicher oder für digitale Signaturen eingesetzte technische Komponenten nicht sicher sind, so kann die zuständige Behörde eine Sperrung der relevanten Zertifikate anordnen. Alle Zertifikate sind (für einen bestimmten Zeitraum) jederzeit durch jedermann öffentlich nachprüfbar.

Eine Fälschung von Zertifikaten ist über die Dokumentation der Zertifizierungsstellen jederzeit nachweisbar. Eine Fälschung von digitalen Signaturen oder eine Verfälschung signierter Daten ist bei Einhaltung der gesetzlichen Bestimmungen praktisch ausgeschlossen.

Haftungsfragen

Mögliche Haftungsfragen sind aus den jeweiligen Verantwortlichkeiten und dem allgemeinen Haftungsrecht zu beantworten (jeder haftet für sein schuldhaftes Handeln oder Unterlassen).

Anwendung der digitalen Signatur durch juristische Personen

Die Vertretungsmacht für juristische Personen ist an natürliche Personen gebunden. Ebenso werden Signaturschlüssel (und damit digitale Signaturen) an natürliche Personen gebunden.

Die Vertretungsmacht für eine juristische Person kann im Signaturschlüssel-Zertifikat oder einem Attribut-Zertifikat ausgewiesen werden. Dies gilt auch für berufsrechtliche und sonstige Zulassungen (z. B. für Ärzte oder Rechtsanwälte).

Anwendung der digitalen Signatur bei automatischem Datenaustausch

Soweit bei automatischem Datenaustausch digitale Signaturen nach dem Signaturgesetz erzeugt werden sollen, können dafür personenbezogene Signaturschlüssel eingesetzt werden (ein Signaturschlüssel-Inhaber kann bei Bedarf über mehrere unterschiedliche Signaturschlüssel verfügen).

Da letztlich immer eine natürliche Person über den Einsatz von Rechnern und die Verarbeitung von Daten sowie die jeweiligen Anwendungsprogramme

entscheidet, können auch automatisch erstellte Signaturen auf eine menschliche Handlung zurückgeführt werden.

Raum für Innovation und vielfältige technische Lösungen

Der Gesetzentwurf enthält nur allgemeine Rahmenbedingungen. Er läßt Raum für unterschiedliche, innovative technische Lösungen, soweit sie das vorgegebene Sicherheitsniveau erfüllen. Es bleibt dem Markt überlassen, welche technischen Lösungen sich durchsetzen.

Die geringe Anzahl verfügbarer geeigneter mathematischer Verfahren schafft jedoch zwangsläufig eine Begrenzung der technischen Lösungen. Im übrigen können die Hauptanwendergruppen sich auf bestimmte Standardlösungen einigen, um interoperabel zu sein.

Da die mathematischen Verfahren gegenseitig nicht kompatibel sind, benötigen Nutzer, die mit mehreren Verfahren arbeiten, mehrere Chipkarten oder eine multifunktionale Chipkarte oder sie müssen für die Signaturüberprüfung im Einzelfall einen Dritten (z. B. eine Zertifizierungsstelle) in Anspruch nehmen.

Zentrale Sicherheitsfaktoren

Folgende zentrale Sicherheitsfaktoren bewirken im Verbund sichere digitale Signaturen:

- Lizenzierte Zertifizierungsstellen,
- durch die Zertifizierungsstellen unterrichtete Signaturschlüssel-Inhaber,
- sicherheitsgeprüfte geeignete technische Komponenten, insbesondere
  - Signaturschlüsselgeneratoren,
  - Signierkomponenten (z. B. in Form von Chipkarten),
  - Sicherheitskomponenten für die kontrollierte Aufbereitung zu signierender Daten (z. B. PC-Zusatzkomponente),
- Aufsicht durch die zuständige Behörde.

Wichtige Nebeneffekte der digitalen Signatur

Digitaler Ausweis

Mit Hilfe der Signaturschlüssel ist zugleich weltweit eine sichere Identifikation und Authentisierung beim Austausch von digitalen Daten möglich, indem z. B. automatisch übermittelte Zufallsdaten automatisch signiert und zur Prüfung zurückgesandt werden. So kann der Zugriff auf Rechner und Daten davon abhängig gemacht werden, daß die betreffende Person sich entsprechend ausweist („digitaler Ausweis") und autorisiert ist. Die Annahme elektronischer Post kann davon abhängig gemacht werden, daß der Absender sich entsprechend ausweist; sie kann absenderabhängig automatisch verweigert bzw. auf bestimmte Absender beschränkt werden.

Die automatische Feststellung der Urheberschaft elektronischer Post (über die Signatur) ermöglicht jeder natürlichen und juristischen Person einen wirksamen Selbstschutz vor unerwünschten Sendungen. Damit und durch sichere Identifikation/Authentisierung im weltweiten Verbund der Informations- und Kommunikationstechnik kann auch partiell ein praktischer Jugendschutz beim Austausch digitaler Daten erreicht werden (z. B. durch Zugangsbeschränkung bei bestimmten Informationsdienstleistungen/Datenzugängen auf Erwachsene und Beschränkung der Annahme oder Weiterleitung elektronischer Post auf signierte Sendungen).

Wirksamer Informationsschutz

Die Information hat sich zu einer entscheidenden Ressource für Unternehmen und Volkswirtschaften entwickelt. Deshalb ist – bei einem weltweiten Verbund der Informations- und Kommunikationstechnik – ein wirksamer technischer Schutz vertraulicher Informationen vor Wirtschafts-/Konkurrenzspionage Voraussetzung für die Wettbewerbsfähigkeit von Unternehmen und Volkswirtschaften.

Durch die Kombination der Sicherheitsfunktionen digitale Signatur, „digitaler Ausweis"/Zugriffskontrolle und Verschlüsselung wird ein hoher Schutz von Informationen im weltweiten Verbund moderner Informations- und Kommunikationstechnik möglich. Die genannten Sicherheitsfunktionen können z. B. über eine Chipkarte und eine PC-Zusatzkomponente kostengünstig realisiert werden.

Ob unabhängig davon unter besonderen Aspekten spezielle „Kryptoregelungen" erforderlich sind, ist nicht Gegenstand des Gesetzentwurfs. Die Funktionen Signatur und Verschlüsselung sind technisch wie rechtlich völlig eigenständig zu betrachten.

VI. Gesetzgebungs- und Verwaltungskompetenz des Bundes

Die Gesetzgebungskompetenz folgt aus Artikel 74 Abs. 1 Nr. 11 Grundgesetz. Die Verwaltungskompetenz ist auf Artikel 87 Abs. 3 Satz 1 Grundgesetz gegründet.

Im Hinblick auf die konkurrierende Kompetenz aus Artikel 74 Abs. 1 Nr. 11 Grundgesetz liegen die Voraussetzungen des Artikels 72 Abs. 2 für die Gesetzgebungskompetenz des Bundes (Wahrung der Rechtseinheit und Wirtschaftseinheit) vor. Damit die gesetzliche digitale Signatur bundesweit das erforderliche einheitliche Sicherheitsniveau aufweist, bedarf es einer gesetzlichen Regelung durch den Bund. Es ist ein bundeseinheitlicher Rahmen für die Wirtschaftsunternehmen erforderlich, die die notwendige Infrastruktur und die benötigten technischen Komponenten bereitstellen.

Die gesetzlichen Bestimmungen im einzelnen

Zu § 1 (Zweck und Anwendungsbereich)

Zu Absatz 1

Die Bestimmung beschreibt das zentrale Ziel des Gesetzes. Mit der gesetzlichen Regelung ist nicht ge-

sagt, daß nicht auch unter anderen Rahmenbedingungen sichere digitale Signaturen erzeugt werden können.

Unter Verfälschung fällt jede Art von Veränderung, auch infolge technischer Fehler. Soweit Fälschungen oder Verfälschungen vorkommen, müssen diese zuverlässig feststellbar sein.

Zu Absatz 2

Die Bestimmung macht deutlich, daß die Anwendung von digitalen Signaturen nach dem Signaturgesetz durch dieses selbst nicht vorgeschrieben wird. Regelungen darüber, wann digitale Signaturen nach dem Signaturgesetz anzuwenden sind, bleiben den speziellen Rechtsvorschriften vorbehalten, die nach Bedarf angepaßt werden sollen.

Die Anwendung anderer Verfahren für digitale Signaturen, die nicht den Rahmenbedingungen des Gesetzes entsprechen, ist freigestellt.

Zu § 2 (Begriffsbestimmungen)

Die definierten informationstechnischen Begriffe werden erstmals in Rechtsvorschriften übernommen. Eine gesetzliche Definition ist deshalb im Interesse der Rechtssicherheit erforderlich.

Zu Absatz 1

Der Begriff „digitale Signatur" ist dem internationalen Sprachgebrauch entnommen. Er bringt den technischen Kontext des Vorgangs, der sich von der eigenhändigen Unterschrift unterscheidet, zum Ausdruck.

Das technische Verfahren zur digitalen Signatur besteht aus

- einem Verfahren zur Erzeugung von Schlüsselpaaren, bestehend aus je einem privaten Schlüssel und dem dazugehörigen öffentlichen Schlüssel,
- einem sogenannten Hash-Algorithmus, d. h. einem Verfahren zur Berechnung eines „digitalen Fingerabdrucks" von digitalen Daten, der ein bestimmtes festes Format hat und diese Daten repräsentiert. Bei der digitalen Signatur werden im allgemeinen nicht die digitalen Daten selbst, sondern ihr „digitaler Fingerabdruck" signiert,
- einem Verfahren zur Berechnung der digitalen Signatur mit Hilfe eines privaten Schlüssels, über den nur die signierende Person verfügt,
- einem Verfahren zur Überprüfung der digitalen Signatur mit Hilfe eines öffentlichen Schlüssels.

Das Verfahren zur digitalen Signatur muß so beschaffen sein, daß die Authentizität und die Integrität der signierten Daten gesichert ist. Dies bedeutet im einzelnen:

- Die Zuordnung der Schlüsselpaare zu Personen muß von einer vertrauenswürdigen Institution (Zertifizierungsstelle) vorgenommen werden,
- es muß praktisch unmöglich sein, daß ein Schlüsselpaar (versehentlich oder absichtlich) doppelt erzeugt werden kann,
- eine mit einem öffentlichen Schlüssel eines Schlüsselpaares prüfbare Signatur kann nur unter Einsatz des privaten Schlüssels erzeugt worden sein; insbesondere muß es praktisch unmöglich sein, den privaten aus dem öffentlichen Schlüssel zu berechnen, und
- es muß praktisch unmöglich sein, verschiedene digitale Daten mit demselben „digitalen Fingerabdruck" oder digitale Daten zu einem vorgegebenen „digitalen Fingerabdruck" zu finden.

Eine digitale Signatur im Sinne des Gesetzes ist an die Voraussetzung gebunden, daß sie mit einem Signaturschlüssel erzeugt wurde, der durch eine Zertifizierungsstelle einer natürlichen Person zugeordnet ist. Nur bei einer Zertifizierungsstelle nach dem Gesetz ist gesetzlich sichergestellt, daß die vorgeschriebenen Sicherheitsmaßnahmen eingehalten und die Signaturschlüssel-Inhaber über die von ihnen in ihrem eigenen Interesse zu veranlassenden Maßnahmen unterrichtet sind.

Aufgrund der mit den gesetzlichen Bestimmungen vorgegebenen Kombination von Maßnahmen – Personenidentifikation, zuverlässige Schlüsselzuordnung durch ein Zertifikat, Bindung des privaten Schlüssels durch Besitz (z. B. Chipkarte) und Wissen (z. B. PIN oder Paßwort) an die Person, sichere technische Komponenten – ermöglicht die digitale Signatur einen zuverlässigen Rückschluß auf die Person, die sie erzeugte.

Damit eine digitale Signatur den Inhaber eines Signaturschlüssels erkennen läßt, muß das Signaturschlüssel-Zertifikat vorliegen. Soweit es dem Empfänger signierter Daten nicht bereits vorliegt, muß es den signierten Daten beigefügt oder andernfalls vom Empfänger angefordert werden.

Zu Absatz 2

Der Begriff „Zertifizierungsstelle" folgt weitgehend dem internationalen Sprachgebrauch (Zertifizierungsinstanz).

Der im Zusammenhang damit stehende Begriff „vertrauenswürdiger Dritter" wurde nicht in die Definition übernommen, da z. B. auch eine Bank für ihre Kunden Schlüssel zertifizieren können soll (wie schon bisher), ohne „Dritter" zu sein. Entscheidend ist die Zuverlässigkeit und Fachkunde (vgl. § 3 Abs. 1).

Die Zuordnung des Signaturschlüssels und die Bescheinigung darüber schließt alle damit zusammenhängenden Tätigkeiten (z. B. das Führen eines öffentlichen Schlüssel-Verzeichnisses) ein. Zertifizierungsstelle im Sinne des Gesetzes kann nur sein, wer eine Lizenz gemäß § 4 besitzt.

Zu Absatz 3

Mit der Zuordnung des öffentlichen Schlüssels zu einer Person ist zwangsläufig das gesamte Paar, also auch der private Signaturschlüssel, zugeordnet.

Die Zuordnung von Signaturschlüsseln soll auf natürliche Personen beschränkt werden, da auch die Ver-

tretungsmacht für juristische Personen an natürliche Personen gebunden ist.

In Attribut-Zertifikate können z. B. Angaben über die Vertretungsmacht für eine dritte Person (vgl. § 5 Abs. 2 und § 7 Abs. 2) aufgenommen werden. Die Bezugnahme auf das Signaturschlüssel-Zertifikat kann über die Zertifikatnummer (vgl. § 7 Abs. 1 Nr. 4) erfolgen. Attribut-Zertifikate gehören zum Signaturschlüssel-Zertifikat und sind wie dieses zu behandeln.

Zu Absatz 4

Zeitstempel verhindern ein Vor- oder Rückdatieren von „digitalen Dokumenten". Dazu genügt es, bei signierten Daten die digitale Signatur mit einem Zeitstempel zu versehen, da diese einen „digitalen Fingerabdruck" der signierten Daten enthält.

Die Nutzung anderer Verfahren für Zeitstempel bleibt unberührt; § 1 Abs. 2 gilt auch hierfür. So kann z. B. eine digitalisierte Röntgenaufnahme mit einem Zeitstempel durch eine autorisierte Stelle des Krankenhauses versehen werden.

Zu § 3 (Zuständige Behörde)

Die Verwaltungskompetenz des Bundes stützt sich auf Artikel 87 Abs. 3 Satz 1 Grundgesetz (vgl. Begründung allgemeiner Teil, Abschnitt VI.). Um das erforderliche einheitliche Sicherheitsniveau zu gewährleisten und wegen der Funktion einer „Wurzelinstanz" bei der Vergabe von Signaturschlüssel-Zertifikaten (vgl. Begründung zu § 4 Abs. 5) ist es erforderlich, die Aufgaben einer Bundesbehörde zu übertragen.

Die Regulierungsbehörde nach § 66 Telekommunikationsgesetz ist bereits nach dem Telekommunikationsgesetz mit der Erteilung von Lizenzen beauftragt und verfügt über die erforderlichen Voraussetzungen für die Wahrnehmung der genannten Aufgaben oder kann diese ohne großen Aufwand schaffen.

Bis zum Inkrafttreten des § 66 Telekommunikationsgesetz am 1. Januar 1998 werden die Aufgaben der Regulierungsbehörde vom Bundesministerium für Post- und Telekommunikation wahrgenommen (vgl. § 98 Telekommunikationsgesetz).

Zu § 4 (Lizenzerteilung für Zertifizierungsstellen)

Die Dienstleistung der Zertifizierung soll im freien Wettbewerb durch private Unternehmen unter behördlicher Aufsicht erbracht werden, ohne damit eine Zertifizierung durch Behörden für behördeneigene Zwecke auszuschließen. Die Regelungen sind weitgehend kongruent mit den diesbezüglichen Regelungen im Telekommunikationsgesetz zum Betrieb von Telekommunikationsanlagen (vgl. § 71 und § 91 Telekommunikationsgesetz).

Zu den Absätzen 1 bis 4

Die Ausstellung von Zertifikaten für Signaturschlüssel ist einerseits eine private Aufgabe. Andererseits ist sie von allgemeiner Bedeutung für die Sicherheit bei Anwendung von Informations- und Kommunikationstechnik (der Signaturschlüssel kann außer für die Erzeugung von Signaturen auch als „digitaler Ausweis" im Rahmen der Zugriffskontrolle zu Rechnern und Daten eingesetzt werden). Sie soll daher einer staatlichen Lizenz bedürfen, deren Vergabe und Aufrechterhaltung an die Erfüllung der in Absatz 2 genannten Voraussetzungen geknüpft sind.

Die Vorschrift ist Anspruchsgrundlage für die Erteilung einer Lizenz. Die Lizenzvergabe soll nach einem dem Telekommunikationsgesetz vergleichbaren Verfahren erfolgen, das durch Rechtsverordnung (vgl. § 16 Nr. 1) näher geregelt wird. Im übrigen findet das Verwaltungsverfahrensgesetz Anwendung. Die Lizenz ist an den Lizenznehmer gebunden. Eine Übertragung, Überlassung oder ein anderweitiger Übergang der Lizenz auf eine andere Person ist nicht vorgesehen. In diesem Falle ist rechtzeitig eine neue Lizenz zu beantragen. Im Falle von Zeitverzug kann im Rahmen von Absatz 4 auch eine vorläufige Lizenz erteilt werden.

Der geforderten Zuverlässigkeit der Zertifizierungsstellen kommt hohe Bedeutung zu, um z. B. eine Ausstellung gefälschter Zertifikate auszuschließen.

Die geforderte Fachkunde erstreckt sich auf den juristischen sowie den technisch-administrativen Bereich und soll eine vollständige und wirksame Umsetzung der gesetzlichen Vorgaben gewährleisten.

Das Vorliegen der übrigen Voraussetzungen soll durch ein Sicherheitskonzept sowie eine Prüfung durch eine unabhängige Prüfstelle nachgewiesen werden. Die Anerkennung von Prüfstellen setzt den Nachweis der erforderlichen Fachkunde und Erfahrungen voraus und kann mit Auflagen für die Durchführung der Prüfungen verbunden werden. Bei der Anerkennung der Prüfstellen kann die zuständige Behörde auf den Sachverstand und die praktischen Erfahrungen des Bundesamtes für Sicherheit in der Informationstechnik (BSI) zurückgreifen, das bereits verschiedene Prüfstellen akkreditiert hat. Die routinemäßigen Prüfungen der Zertifizierungsstellen sollen durch private Stellen erfolgen. Daneben kann die zuständige Behörde stichprobenartig oder aus gegebenem Anlaß selbst Kontrollen durchführen (vgl. § 13 und ergänzende Rechtsverordnung nach § 16 Nr. 5).

Durch Nebenbestimmungen nach Absatz 4 kann z. B. festgelegt werden, daß die Zertifizierungsstelle den Betrieb erst nach Zustimmung durch die zuständige Behörde, nachdem diese das Sicherheitskonzept und den Prüfbericht geprüft hat, aufnehmen darf.

Zu Absatz 5

Die zuständige Behörde soll auch die oberste nationale Zertifizierungsstelle („Wurzelinstanz") bilden, die die Zertifikate für Signaturschlüssel, die zum Signieren von Zertifikaten eingesetzt werden, ausstellt. Das Zertifikat für ihren eigenen Schlüssel stellt sie selbst aus. Die Rechtsverordnung sieht vor, daß sie ihre Telekommunikationsanschlüsse, über die von ihr ausgestellte Zertifikate abgefragt werden können, im Bundesanzeiger bekannt gibt.

Die von der zuständigen Behörde ausgestellten Zertifikate können außer bei der zuständigen Behörde insbesondere auch bei den Zertifizierungsstellen abrufbar gehalten werden (als freiwillige Serviceleistung). Das „Wurzelzertifikat" kann dem jeweiligen Signaturschlüsselinhaber von der Zertifizierungsstelle zusammen mit seinem eigenen Zertifikat authentisch mitübergeben werden (Speicherung auf dem Datenträger mit dem Signaturschlüssel).

Die Zertifizierungsstellen können ihre Signaturschlüssel selbst erzeugen; die zuständige Behörde stellt nur die Zertifikate aus.

Die von der zuständigen Behörde zertifizierten Signaturschlüssel sind ausschließlich zum Signieren von Zertifikaten sowie bei Bedarf von Zeitstempeln bestimmt. Für Zeitstempel können auch andere zertifizierte Signaturschlüssel eingesetzt werden.

Die zuständige Behörde hat nach Satz 2 für ihre Zertifizierung die gleiche Sicherheit zu gewährleisten, wie sie für die lizenzierten Zertifizierungsstellen vorgeschrieben ist, und diese gemäß der ergänzenden Rechtsverordnung ebenfalls durch eine externe Stelle prüfen zu lassen.

Die flache Zertifizierungshierarchie (1 = zuständige Behörde, 2 = Zertifizierungsstellen) schafft Transparenz und genügt den praktischen Erfordernissen, da

- eine beliebige Anzahl von Zertifizierungsstellen mit staatlicher Lizenz errichtet werden kann und
- bei Zertifizierungsstellen zu differenzieren ist zwischen
  - dem „Trust-Center" (in dem die Signaturschlüssel Personendaten zugeordnet und die Zertifikate erstellt werden), das in der Regel pro Zertifizierungsstelle nur einmal vorhanden ist, und
  - einer beliebigen Anzahl von Kundenbetreuungsstellen (bei denen die Anträge auf Zertifikate entgegengenommen, die Antragsteller identifiziert und nach § 6 unterrichtet sowie die Zertifikate gegebenenfalls auch ausgehändigt werden); sie können auch über Kooperationsverträge angeschlossen sein.

Zu Absatz 6

Hiermit soll die Anspruchsgrundlage für die Kostenhebung durch die zuständige Behörde geschaffen werden. Das Nähere wird durch Rechtsverordnung (vgl. § 16 Nr. 2) geregelt. Für vorgesehene private Leistungen (z. B. durch Stellen nach § 4 Abs. 3 oder § 14 Abs. 4), die nicht durch die zuständige Behörde veranlaßt werden, trägt der jeweilige Veranlasser (z. B. die Zertifizierungsstelle oder der Produkthersteller) die Kosten unmittelbar.

Zu § 5 (Vergabe von Zertifikaten)

Zu Absatz 1

Das Erbringen und die Inanspruchnahme der genannten Dienstleistungen bleibt vertraglichen Vereinbarungen zwischen den Beteiligten vorbehalten. Ist ein Antragsteller nicht unbeschränkt geschäftsfähig, so richtet sich die Möglichkeit des Erwerbs und der Nutzung des Signaturschlüssels nach den Bestimmungen des BGB zur Geschäftsfähigkeit. Zur Erschwerung des Zugangs zu jugendgefährdenden Publikationen kann bei Minderjährigen auch das Geburtsdatum aufgenommen werden.

Ein Kontrahierungszwang ist nicht vorgesehen, da davon ausgegangen werden kann, daß der Markt jedem Interessenten die Möglichkeit eröffnen wird, bei einer Zertifizierungsstelle einen Signaturschlüssel zu erwerben.

Die zuverlässige Identifikation des Signaturschlüssel-Inhabers (z. B. anhand des Personalausweises) ist Voraussetzung dafür, daß zuverlässig auf den Urheber einer digitalen Signatur rückgeschlossen werden kann.

Satz 2 schafft die Voraussetzungen dafür, daß ein vorliegendes Zertifikat jederzeit (das heißt innerhalb der nach der Rechtsverordnung vorgegebenen Frist) auf seine Echtheit und Gültigkeit überprüft werden kann. Eine Veröffentlichung des Zertifikates soll jedoch nur mit ausdrücklicher Zustimmung des Signaturschlüssel-Inhabers erfolgen. Auch für den Fall, daß keine Veröffentlichung erfolgt, kann das Zertifikat signierten Daten beigefügt werden, um dem Empfänger eine Überprüfung der Signatur zu ermöglichen.

Inwieweit darüber hinaus übergreifende Service-Dienste (z. B. mit allen Zertifikaten und Sperrlisten der lizenzierten Zertifizierungsstellen sowie der zuständigen Behörde) angeboten werden, bleibt dem Markt überlassen.

Zu Absatz 2

Die Regelung soll die Möglichkeit eröffnen, die Vertretungsmacht für eine dritte Person sowie berufsrechtliche oder sonstige Zulassungen im Signaturschlüssel-Zertifikat oder einem Attribut-Zertifikat auszuweisen. Damit sollen die üblichen schriftlichen Vertretungsermächtigungen und Zulassungen auch digital dargestellt werden können. Soweit dafür jeweils gesonderte Attribut-Zertifikate erstellt werden, bleibt der Signaturschlüssel-Inhaber im Falle von deren Sperrung nach § 8 Abs. 3 in seiner Handlungsfähigkeit als Privatperson unberührt, da das Signaturschlüssel-Zertifikat selbst nicht der Verfügungsgewalt Dritter unterliegt. Im übrigen bleibt die Aufnahme entsprechender Angaben in ein Zertifikat, das er beantragen muß, seiner Entscheidung überlassen.

Zu Absatz 3

Signierte Daten in Dateien und Netzen können das Erstellen von Persönlichkeitsprofilen (z. B. bezüglich des Kaufverhaltens von Personen) erleichtern. Durch die Verwendung von Pseudonymen wird die Zuordnung signierter Daten zu einer Person verhindert oder zumindest erschwert (bei Online-Diensten ist jedoch gegebenenfalls über den Telekommunikationsanschluß eine Zuordnung möglich). Darüber hinaus können Anonymisierungsdienste (z. B. Server eines vertrauenswürdigen Dritten) genutzt werden, um gegenüber Kommunikationspartnern anonym zu bleiben.

Pseudonyme sind gemäß § 7 Abs. 1 Nr. 1 als solche kenntlich zu machen, damit Kommunikationspartner sich bei Rechtsgeschäften darauf einstellen können, daß eine Offenbarung der Identität des Signaturschlüssel-Inhabers nur in dem engen Rahmen des § 12 Abs. 2 erreicht werden kann und ein Pseudonym bei Rechtsgeschäften nur unter bestimmten Voraussetzungen (z. B. allgemein bekannter Künstlername) anerkannt wird. Im übrigen kann der Träger eines Pseudonyms in einem (gegebenenfalls verschlüsselten) „digitalen Dokument" nach eigenem Ermessen seine Identität angeben.

Zu Absatz 4

Satz 1 soll die Integrität der Signaturschlüssel und der zugeordneten Personendaten sicherstellen. Dies erfordert vor allem wiederholte interne Kontrollen (z. B. stichprobenartiger Vergleich von Zertifikaten und Zertifizierungsanträgen). Da speziell technisch bedingte Verfälschungen von Daten nicht ausgeschlossen werden können, müssen diese zumindest zwangsläufig bemerkt werden (z. B. durch Anwendung digitaler Signaturen bei der Datenspeicherung/-übermittlung). Vergleiche auch Absatz 3 der Begründung zu § 14.

Die in Satz 2 geforderte Geheimhaltung des Signaturschlüssels ist absolut. Es soll keine Person (auch nicht der Signaturschlüssel-Inhaber) Kenntnis vom privaten Signaturschlüssel erhalten, da andernfalls ein Mißbrauch des Signaturschlüssels nicht hinreichend auszuschließen ist. Die Vorkehrungen der Zertifizierungsstelle bestehen darin, daß sie, soweit die Schlüssel durch sie bereitgestellt werden, durch technische und organisatorische Maßnahmen eine Preisgabe oder Speicherung in ihrem Bereich (Satz 3) ausschließt. Soweit der Signaturschlüssel-Inhaber die Schlüssel selbst erzeugt, hat sie sich zu überzeugen, daß er ein geeignetes Verfahren benutzt, bei dem eine Schlüsselpreisgabe hinreichend ausgeschlossen ist (z. B. durch einen Schlüsselgenerator auf der Chipkarte, die den Schlüssel tragen soll, so daß der private Schlüssel diese nie verläßt).

Die Forderung in Satz 3 trägt dazu bei, daß der Signaturschlüssel nur einmal (beim Signaturschlüssel-Inhaber) vorhanden ist. Technisch unvermeidbare temporäre Zwischenspeicherungen beim gesicherten Ladevorgang sind damit nicht ausgeschlossen. Die nähere Ausgestaltung der Pflichten der Zertifizierungsstellen wird nach § 16 Nr. 3 in der ergänzenden Rechtsverordnung bestimmt.

Zu Absatz 5

Zuverlässiges Personal und sichere technische Komponenten sind Voraussetzung für sichere digitale Signaturen. Während Privatpersonen nur über das Erfordernis geeigneter technischer Komponenten nach § 14 unterrichtet werden, wird Zertifizierungsstellen deren Verwendung vorgeschrieben.

Zu § 6 (Unterrichtungspflicht)

Um zu sicheren digitalen Signaturen zu gelangen, müssen Signaturschlüssel-Inhaber über die von ihnen in ihrem eigenen Interesse zu veranlassenden Maßnahmen sowie über geeignete technische Komponenten unterrichtet sein. Die ergänzende Rechtsverordnung sieht vor, daß die zuständige Behörde die geeigneten technischen Komponenten öffentlich bekanntgibt. Die Zertifizierungsstelle braucht nur eine aktuelle Liste der technischen Komponenten auszuhändigen und kann damit ein Beratungsgespräch verbinden.

Darüber hinaus sollen die Signaturschlüssel-Inhaber auch darüber unterrichtet werden, daß ihnen mit ihrem Signaturschlüssel erzeugte Signaturen aufgrund der gesetzlich vorgegebenen Kombination von Maßnahmen (vgl. Begründung zu § 2 Abs. 1) zugerechnet werden können; es sei denn, das Signaturschlüssel-Zertifikat war zum Zeitpunkt der Signaturerzeugung gesperrt oder die Frist, nach der eine neue Signatur geboten ist (das Nähere regelt die Rechtsverordnung nach § 16 Nr. 7), ist in sicherheitsrelevantem Maße überschritten oder andere Fakten stehen entgegen. Ist die Nutzung des Signaturschlüssels laut Signaturschlüssel-Zertifikat gemäß § 7 Abs. 1 Nr. 7 auf bestimmte Anwendungen nach Art und Umfang beschränkt, so erstreckt sich die Zurechnung nur auf den vorgegebenen Rahmen.

Die Rechtsverordnung bestimmt den Zeitraum sowie das Verfahren, nach dem eine neue digitale Signatur angebracht werden sollte.

Zu § 7 (Inhalt von Zertifikaten)

Zu Absatz 1

Die für ein Signaturschlüssel-Zertifikat geforderten Mindestangaben nach den Nummern 1 bis 6 werden benötigt, um den Urheber einer digitalen Signatur feststellen und die digitale Signatur prüfen zu können. Sie entsprechen internationalen Normen.

Die Regelung in Nummer 1 soll gewährleisten, daß jeder Signaturschlüssel-Inhaber im Verzeichnis einer Zertifizierungsstelle einen einmaligen Namen trägt. Soweit neben dem Namen die Adresse angegeben wird, ist ein weiterer Zusatz (z. B. Ziffer) nur in Ausnahmefällen erforderlich. Bezüglich der Verwendung von Pseudonymen vgl. Begründung zu § 5 Abs. 3.

Durch die Regelung in Nummer 7 soll erreicht werden, daß im Interesse des Signaturschlüssel-Inhabers im Signaturschlüssel-Zertifikat eine Aussage darüber erfolgt, ob die mit seinem Signaturschlüssel erzeugten digitalen Signaturen unbeschränkt oder z. B. nur für bestimmte Rechtsgeschäfte oder nur bis zu einem bestimmten Wert gelten. Ob eine Beschränkung besteht, muß ausdrücklich im Signaturschlüssel-Zertifikat selbst ausgesagt sein. Nähere Aussagen über die Beschränkungen können auch in einem Attribut-Zertifikat erfolgen.

Zu Absatz 2

Die Regelung trägt in Ergänzung zu § 5 Absatz 2 der Bedeutung, die der Darstellung der Vertretungsmacht für juristische Personen sowie von berufsrechtlichen oder sonstigen Zulassungen bei Anwendung digitaler Signaturen zukommt, Rechnung. In den Zertifikaten kann grundsätzlich jede Vertretungs-

macht und Zulassung in digitaler Form wiedergegeben werden, so daß die betreffende Person sich über die Kommunikationsnetze weltweit entsprechend ausweisen kann.

Es kann wahlweise ein eigenständiges Zertifikat oder ein Attribut-Zertifikat mit entsprechenden Angaben einer dritten Person erteilt werden. Es können für denselben Signaturschlüssel auch mehrere Signaturschlüssel-Zertifikate und Attribut-Zertifikate durch unterschiedliche Zertifizierungsstellen ausgestellt werden. Der Aufnahme weitergehender Angaben in ein Zertifikat (z. B. bei Minderjährigen das Geburtsdatum) im Rahmen vertraglicher Vereinbarungen steht nichts entgegen.

Zu § 8 (Sperrung von Zertifikaten)

Mit der Sperrung eines Signaturschlüssel-Zertifikates sind auch alle zugehörigen Attribut-Zertifikate gesperrt. Attribut-Zertifikate können gesondert gesperrt werden. Vergleiche auch Begründung zu § 5 Absatz 2.

Die Gültigkeit der digitalen Signaturen, die vor dem Zeitpunkt der Sperrung erzeugt wurden, wird durch die Sperrung nicht tangiert. Sicherheit darüber, ob eine Signatur vor oder nach der Sperrung erzeugt wurde, gibt im Zweifelsfalle ein Zeitstempel (vgl. § 9).

Zu Absatz 1

Die Regelung ist notwendig, um bei Verlust eines Signaturschlüssels einen möglichen Mißbrauch zu verhindern. Außerdem sollen sich Signaturschlüssel-Inhaber durch Sperrung des Zertifikates nach eigenem Ermessen jederzeit aus dem „elektronischen Rechtsverkehr" zurückziehen können. Weitergehende vertragliche Vereinbarungen, nach denen auch andere Personen eine Sperrung veranlassen können, bleiben unbenommen.

Soweit ein Signaturschlüssel im Zusammenhang mit Straftaten eingesetzt wird, kann nach § 74 ff Strafgesetzbuch eine Sperrung verfügt werden.

Der Zeitpunkt der Sperrung umfaßt das Datum und die Uhrzeit. Das Verbot einer rückwirkenden Sperrung nach Satz 3 schließt die Fälle nach Absatz 2 und 3 sowie nach § 13 Abs. 5 ein.

Durch die Sperrung kann nicht verhindert werden, daß danach noch digitale Signaturen für rückdatierte Daten erzeugt werden. Dies verhindert ein Zeitstempel. Die Rechtsverordnung sieht eine Unterrichtung der Signaturschlüssel-Inhaber darüber vor, wann ein Zeitstempel geboten ist. Die signierten Signaturschlüssel-Zertifikate selbst enthalten Angaben über Beginn und Ende ihrer Gültigkeit (vgl. § 7 Abs. 1 Nr. 5). Außerdem sieht die ergänzende Rechtsverordnung vor, daß der Zeitpunkt der Ausstellung und Übergabe der Zertifikate durch die Zertifizierungsstelle zu dokumentieren ist.

Zu Absatz 2

Ein Signaturschlüssel-Zertifikat oder ein Attribut-Zertifikat kann nach § 5 Abs. 2 in Verbindung mit § 7 Abs. 2 auch Angaben einer dritten Person enthalten. Falls sich bezüglich dieser Angaben Änderungen ergeben (z. B. eine Zulassung entzogen wird), muß auch die dritte Person eine Sperrung des jeweiligen Zertifikates veranlassen können.

Zu Absatz 3

Nach § 4 Abs. 5 Satz 2 gelten die Regelungen in Absatz 1 für die Sperrung der von der zuständigen Behörde ausgestellten Zertifikate entsprechend. Darüber hinaus hat sie in den in Absatz 3 genannten Fällen eine Sperrung vorzunehmen.

Zu § 9 (Zeitstempel)

Die Vergabe von Zeitstempeln (vgl. § 2 Abs. 4) soll als Pflichtdienstleistung für Zertifizierungsstellen vorgegeben werden, da Zeitstempel bei Anwendung digitaler Signaturen zwingend benötigt werden, soweit beweiserheblich werden kann, ob Daten zu einem bestimmten Zeitpunkt vorgelegen haben. Einen Zeitstempel kann jedermann verlangen, der Daten erzeugt oder dem fremde Daten vorliegen, bei denen er aus Beweisgründen ein Interesse daran hat. Bei signierten Daten genügt es, für die digitale Signatur einen Zeitstempel einzuholen, da diese die gesamten signierten Daten repräsentiert.

Durch die Regelung in Satz 2 soll für das Erstellen von Zeitstempeln die gleiche personelle und technische Sicherheit vorgegeben werden, wie für das Erstellen von Zertifikaten.

Zu § 10 (Dokumentation)

Die Dokumentation der Sicherheitsmaßnahmen soll vor allem dazu beitragen, daß wirksame Kontrollen durchgeführt und mögliche (gegebenenfalls auch haftungsrelevante) Pflichtverletzungen festgestellt werden können. Die Dokumentation der Zertifikate ist erforderlich, um digitale Signaturen jederzeit zuverlässig überprüfen zu können. Die Aufbewahrungsdauer wird nach § 16 Nr. 3 in der ergänzenden Rechtsverordnung bestimmt.

Zu § 11 (Einstellung der Tätigkeit)

Die Regelungen soll der Wahrung der Interessen der Signaturschlüssel-Inhaber dienen. Es soll in Verbindung mit § 13 Abs. 4 sichergestellt werden, daß bereits erzeugte digitale Signaturen auch nach Beendigung der Tätigkeit einer Zertifizierungsstelle zuverlässig überprüft werden können.

Zu § 12 (Datenschutz)

Zu Absatz 1

Die Regelung soll die Erhebung personenbezogener Daten für Zwecke der digitalen Signatur auf das Notwendige begrenzen. Sie soll grundsätzlich beim Betroffenen erfolgen und bei Dritten nur mit seiner Einwilligung zulässig sein. Die Verwendung der erhobenen personenbezogenen Daten unterliegt einer engen Zweckbindung.

Zu Absatz 2

Aufgrund der engen Zweckbindung nach Absatz 1 ist eine Regelung für den Fall erforderlich, daß die genannten Stellen in den genannten Fällen die Identität eines Signaturschlüssel-Inhabers benötigen. Die Regelung ist in den Formulierungen weitgehend kongruent mit § 89 Abs. 6 Telekommunikationsgesetz, jedoch beschränkt auf die Übermittlung von Daten zur Feststellung der Identität einer Person bei Verwendung eines Pseudonyms. Andernfalls ist die Identität bereits aus dem Signaturschlüssel-Zertifikat ersichtlich. Die Dokumentation der Auskünfte soll Kontrollen im Rahmen des Datenschutzes erleichtern.

Zu Absatz 3

Die Regelung soll ermöglichen, daß die für den Datenschutz zuständigen Aufsichtsbehörden auch ohne konkreten Anlaß kontrollieren können. Zugleich soll klargestellt werden, daß die datenschutzrechtlichen Kontrollen nicht der Behörde nach § 3, sondern den für den Datenschutz zuständigen Aufsichtsbehörden obliegt.

Zu § 13 (Kontrolle und Durchsetzung von Verpflichtungen)

Die Vorschrift regelt die Kontroll- und Anordnungsbefugnisse der zuständigen Behörde zur Durchsetzung der Verpflichtungen, die Zertifizierungsstellen nach dem Gesetz und der ergänzenden Rechtsverordnung obliegen. Damit erhält die zuständige Behörde die Möglichkeit, angemessen zu reagieren. Die Regelungen sind weitgehend kongruent mit den Regelungen in § 91 Abs. 1 und 3 Telekommunikationsgesetz.

Zu Absatz 1

Hier wird die zuständige Behörde in allgemeiner Form ermächtigt, alle geeigneten Maßnahmen und Anordnungen zu treffen, um die Einhaltung der Rechtsvorschriften durch die Zertifizierungsstellen sicherzustellen. Die Untersagungsverfügung nach Satz 2 gibt die Möglichkeit, ein rechtswidriges Verhalten abzustellen oder zu verhindern. Sie ist für eine befristete Zeit bis zur Beseitigung des rechtswidrigen Verhaltens bestimmt. Die Untersagung der Tätigkeit nach Satz 2 oder 3 bildet die ultima ratio, wenn andere Maßnahmen (z. B. Untersagung unlauterer Werbemethoden in Fällen nach Satz 3) nicht greifen. Eine teilweise Untersagung der Tätigkeit kann z. B. darin bestehen, daß zunächst keine weiteren Zertifikate ausgestellt werden dürfen.

Zu Absatz 2

Hier werden der zuständigen Behörde die zur Überwachung nach Absatz 1 notwendigen prozessualen Eingriffsbefugnisse (Auskunfts-, Betretungs- und Besichtigungsrechte) verliehen.

Zu Absatz 3

Wird ein rechtswidriges Verhalten nicht beseitigt oder ist damit nicht zu rechnen, ist der Entzug der Lizenz vorgesehen, der – anders als beim Telekommunikationsgesetz – nur vollständig möglich ist.

Zu Absatz 4

Im Hinblick auf die Bedeutung der kontinuierlichen Überprüfbarkeit digitaler Signaturen soll für die genannten Fälle die Pflicht der zuständigen Behörde konstituiert werden, eine Übernahme der Tätigkeit durch eine andere Zertifizierungsstelle oder eine sonstige Abwicklung sicherzustellen. Zunächst ist allerdings die betreffende Zertifizierungsstelle in der Pflicht (vgl. § 11). Die zuständige Behörde greift nur ein, falls die Zertifizierungsstelle ihren Pflichten nicht nachkommt. In diesem Falle kann die Behörde im Rahmen ihrer Befugnisse nach Absatz 1 und 4 z. B. die nach § 10 Abs. 1 vorgesehene Sperrung von Signaturschlüssel-Zertifikaten anordnen.

Zu Absatz 5

Die Regelung in Satz 1 dient der Klarstellung. Satz 2 stellt die Entscheidung, ob in den dort genannten Fällen eine Sperrung von Zertifikaten geboten ist, in das pflichtgemäße Ermessen der zuständigen Behörde.

Zu § 14 (Technische Komponenten)

Die Regelung enthält die Zielvorgaben, die durch die technischen Komponenten erreicht werden müssen. Näheres regelt die ergänzende Rechtsverordnung (vgl. § 16 Nr. 6).

Zertifizierungsstellen sind verpflichtet, geeignete technische Komponenten (vgl. § 5 Abs. 5 Satz 2 und 3 und § 9) einzusetzen.

Signaturschlüssel-Inhaber werden über das Erfordernis, geeignete technische Komponenten einzusetzen, sowie über infrage kommende technische Komponenten unterrichtet. Bezüglich des Signaturschlüssels und der damit verbundenen Signierkomponente (beides kann sich z. B. zusammen auf einer Chipkarte befinden) übernimmt die Zertifizierungsstelle im Rahmen von § 5 Abs. 4 Satz 2 eine Garantenfunktion, daß nur geeignete technische Komponenten eingesetzt werden, und erteilt andernfalls kein Zertifikat.

Bei der Aufbereitung zu signierender oder zu prüfender signierter Daten liegt es nach Unterrichtung durch die Zerfitizierungsstelle allein beim Signaturschlüssel-Inhaber, geeignete technische Komponenten einzusetzen, um möglichen technischen Fehlern und Manipulationen vorzubeugen.

Zu Absatz 1

Damit eine digitale Signatur nicht unbemerkt gefälscht und signierte Daten nicht unbemerkt verfälscht werden können, sind geeignete technische Komponenten (Hardware, Software und mathematische Verfahren) erforderlich. Werden für die Erzeugung einer digitalen Signatur geeignete technische Komponenten eingesetzt und werden der private Signaturschlüssel und die zu seiner Anwendung benötigten Identifikationsdaten (Personenidentifikationsnummer [PIN] oder Paßwort) vor Unbefugten ge-

schützt, sind die signierten Daten mit an Sicherheit grenzender Wahrscheinlichkeit sicher vor Fälschung und Verfälschung.

Die Regelung in Satz 1 erfordert die Einmaligkeit eines jeden durch eine Zertifizierungsstelle zugeordneten Signaturschlüssels. Dies kann mathematisch/technisch gewährleistet werden. Es stehen Schlüsselgenerierungs-Algorithmen zur Verfügung, die eine nahezu unbegrenzte Anzahl unterschiedlicher Signaturschlüssel erzeugen, so daß selbst bei Milliarden von Schlüsseln die Erzeugung von zwei gleichen Schlüsselpaaren praktisch ausgeschlossen ist.

Der private (geheime) Signaturschlüssel kann z. B. auf einer Chipkarte so gespeichert werden, daß er nicht ausgelesen werden kann (allenfalls mit äußerst aufwendigen Analyseverfahren bei Zerstörung der Karte). Die Erzeugung des Schlüsselpaares kann auf der Karte selbst so erfolgen, daß der private Schlüssel diese niemals verläßt. Erfolgt die Schlüsselerzeugung außerhalb, so kann das Laden der Chipkarte mit dem privaten Schlüssel technisch und organisatorisch (Vieraugenprinzip) so gestaltet werden, daß auch hier die Einmaligkeit und Geheimhaltung des privaten Signaturschlüssels zuverlässig gewahrt ist.

Die zum Signieren benötigten mathematischen Verfahren (Hash-Algorithmen und Signier-Algorithmen) sind fortwährend Gegenstand einer weltweiten wissenschaftlichen Diskussion und werden bei geeigneter Dimensionierung der weiteren Parameter (z. B. Länge der Signaturschlüssel) von den Experten nach dem Stand der Technik als „nicht brechbar" beurteilt. Die technische Implementierung der mathematischen Verfahren kann nach dem Stand der Technik ebenfalls auf eine Weise erfolgen und geprüft werden, bei der sicherheitsrelevante Fehler oder Manipulationen hinreichend ausgeschlossen sind. Die Signaturkomponenten, wie sie z. B. auf Chipkarten realisiert werden, können deshalb als sehr sicher bezeichnet werden.

Um eine mißbräuchliche Verwendung von Signierkomponenten mit dem privaten Signaturschlüssel auszuschließen, muß eine zuverlässige Zuordnung des jeweiligen Signaturschlüsselpaares zu einer Person (durch ein fälschungssicheres Signaturschlüssel-Zertifikat) und eine sichere Identifikation des Signaturschlüssel-Inhabers durch die Signierkomponente vor Benutzung des Signaturschlüssels durch Besitz (Signaturschlüssel) und Wissen (z. B. persönliche Identifikationsnummer [PIN]) erfolgen.

Zu Absatz 2

Die Aufbereitung von Daten für Zwecke der digitalen Signatur muß so erfolgen, daß der Nutzer hinreichend sicher sein kann, daß die z. B. auf dem Bildschirm angezeigten Daten mit den signierten Daten übereinstimmen. Dies erfordert Zusatzkomponenten zur handelsüblichen Informationstechnik oder spezielle technische Komponenten.

Bei der (automatischen) Prüfung einer digitalen Signatur muß neben einer korrekten Darstellung der signierten Daten gewährleistet sein, daß keine unzutreffende Korrektheitsbestätigung der digitalen Signatur erfolgt. Sowohl bei einer Fälschung der Signatur als auch bei einer Verfälschung des signierten Dokumentes darf keine Korrektheitsbestätigung erfolgen. Außerdem muß (mittelbar über den zertifizierten öffentlichen Schlüssel) der Inhaber des Signaturschlüssels, mit dem die Signatur erfolgte, erkennbar werden.

Soweit eine Person für die Aufbereitung zu signierender Daten oder die Prüfung signierter Daten technische Komponenten ohne entsprechende ‚Sicherheitsvorkehrungen einsetzt, trägt sie das Risiko falscher Ergebnisse. Die Zertifizierungsstellen sind nach § 5 Abs. 5 Satz 2 und § 9 verpflichtet, für das Erstellen von Signaturschlüssel-Zertifikaten und Zeitstempeln entsprechende technische Komponenten einzusetzen und unterliegen auch diesbezüglich der behördlichen Kontrolle nach § 13.

Zu Absatz 3

Die Zertifikatverzeichnisse müssen vor allem vor unbefugter Sperrung von Zertifikaten sowie vor Beseitigung von Sperrungen geschützt sein. Soweit der Signaturschlüssel-Inhaber der Abrufbarkeit seines Zertifikates über öffentliche Netze nicht zugestimmt hat (vgl. § 5 Abs. 1), muß es auch vor unbefugtem Abruf geschützt sein (ein befugter Abruf für interne Zwekke der Zertifizierungsstelle bleibt unberührt).

Zu Absatz 4

Für die Bestätigung der Sicherheit technischer Komponenten steht zunächst das Bundesamt für Sicherheit in der Informationstechnik (BSI) zur Verfügung. Dessen Anerkennung ist aufgrund seiner Sachkunde infolge der Aufgabenstellung nach dem BSI-Einrichtungsgesetz (vgl. BGBl. 1990 I S. 2834 ff.) selbstverständlich. Es hat nach dem BSI-Errichtungsgesetz den Auftrag, informationstechnische Komponenten auf ihre Sicherheit zu prüfen und Sicherheitszertifikate zu vergeben. Näheres regeln die BSI-Zertifizierungsverordnung sowie die BSI-Kostenverordnung. Das BSI verfügt über die aktuellen Erkenntnisse der Sicherheitsbehörden zu relevanten kriminellen Aktivitäten (z. B. spezielle technische Angriffe) sowie über relevante Erkenntnisse von Partnerbehörden im Ausland.

Dem BSI wird jedoch keine Monopolstellung eingeräumt. Neben dem BSI kann die zuständige Behörde auch andere Stellen anerkennen, soweit die von diesen erteilten Sicherheitszertifikate (oder Bestätigungen anderer Art) die erforderliche Sicherheit ausweisen.

Das Nähere zur Prüfung der technischen Komponenten regelt die ergänzende Rechtsverordnung (vgl. § 16 Nr. 6).

Zu Absatz 5

Produkte sowie anerkannte Produktbewertungen im Sinne von Absatz 4 aus den genannten europäischen Staaten werden hiermit gleichgestellt.

Zu § 15 (Ausländische Zertifikate)

Zu Absatz 1

Mit der Regelung werden – in Ergänzung zu § 14 Abs. 5 – digitale Signaturen aus den genannten europäischen Staaten gleichgestellt, soweit sie eine vergleichbare Sicherheit aufweisen.

Zu Absatz 2

Da digitale Signaturen international Anwendung finden, dürfte es weltweit zu einer überstaatlichen oder zwischenstaatlichen Anerkennung digitaler Signaturen kommen. Die Regelung soll dafür die nationale Grundlage bilden. Es können für einen öffentlichen Signaturschlüssel auch mehrere Zertifikate bei verschiedenen Zertifizierungsstellen in verschiedenen Staaten beantragt und ausgestellt werden.

Zu § 16 (Rechtsverordnung)

Die Rechtsverordnung, für die hier die Ermächtigungsgrundlage geschaffen werden soll, ist erforderlich, um das Gesetz von Details weitgehend freizuhalten und auf technische Veränderungen unverzüglich reagieren zu können.

Zu Artikel 4 (Änderung des Strafgesetzbuchs)

Zu Nummer 1

§ 11 Abs. 3 Strafgesetzbuch stellt bislang den Schriften Ton- und Bildträger, Abbildungen und andere Darstellungen gleich. Überall dort, wo auf § 11 Abs. 3 Strafgesetzbuch verwiesen wird, wird der Begriff der Schriften stellvertretend für alle oben genannten Gegenstände benutzt, wobei überwiegend Darstellung als der eigentliche Oberbegriff angesehen wird.

Darstellung ist jedes körperliche Gebilde von gewisser Dauer, das, sinnlich wahrnehmbar, eine Vorstellung oder einen Gedanken ausdrückt (Walter, NStZ 1990, 523, m.w.N.; Dreher/Tröndle, Strafgesetzbuch, 47. Aufl. München 1995, § 11, Rn. 44; Schönke/Schröder-Eser, Strafgesetzbuch, 24. Aufl. München 1991, § 11, Rn. 78; Sieber, JZ 1996, 429 ff., 494 ff., 495). In der Rechtsprechung wurde entschieden, daß im Btx-Verfahren verwendete Datenträger Bildträger i. S. d. o. g. Vorschrift sind (OLG Stuttgart, NStZ 1992, 38).

Angesichts der bezüglich moderner Datentechnik spärlichen Rechtsprechung (vgl. OLG Stuttgart a. a. O.) und im Hinblick auf die Auffassung, Darstellungen seien nur körperliche Gebilde von gewisser Dauer, ist klarzustellen, daß auch elektronische, elektromagnetische, optische, chemische oder sonstige Datenspeicher, die gedankliche Inhalte verkörpern, die nur unter Zuhilfenahme technischer Geräte wahrnehmbar werden, den Schriften gleichstehen. Sie können in vergleichbarer Weise zur Wiedergabe rechtswidriger Inhalte verwendet werden und sind daher in das strafrechtliche System einzubeziehen. Gleichgültig ist dabei, welcher Art das zur Wahrnehmbarmachung eingesetzte Gerät ist; in Betracht kommt insbesondere die Anzeige auf einem Bildschirm.

Die Klarstellung erfaßt damit sowohl Inhalte in Datenträgern (Magnetbänder, Festplatten, CD-ROMs u. a.) als auch in elektronischen Arbeitsspeichern, welche die Inhalte nur vorübergehend bereithalten. Es wird zugleich daran festgehalten, daß diejenigen Inhalte nicht erfaßt werden, die unmittelbar in Echtzeit oder Echtzeit-entsprechend übermittelt werden (z. B. Fernsehübertragung in Echtzeit; paketweise Datenübermittlung in Echtzeit). Kurzfristige Zwischenspeicherungen z. B. im Telekommunikationsnetz zum Zwecke der Echtzeitübermittlung fallen danach nicht unter den Begriff des Datenspeichers.

Zu Nummer 2

Zu Buchstabe a

Die Verweisung auf § 11 Abs. 3 fehlt in Absatz 3, obwohl der systematische Zusammenhang mit Absatz 1 offenbar eine Übereinstimmung voraussetzt. Das vorliegende Gesetz gibt Gelegenheit zur Berichtigung.

Zu Buchstabe b

Die Änderung folgt der Klarstellung des Schriftenbegriffes in § 11 Abs. 3. Sie stellt sicher, daß auch Datenspeicher mit in § 74 d Abs. 1 bezeichnetem Inhalt der Einziehung unterliegen. Gegebenenfalls kann bei Vorliegen der Voraussetzungen des § 74 b Abs. 2 die Löschung oder sonstige Unbrauchbarmachung solcher Inhalte herbeigeführt werden.

Zu Nummer 3

Die Erweiterung des § 86 Abs. 1 Strafgesetzbuch gewährleistet, daß nicht durch Einspeisung der in § 86 genannten Propagandamittel in Datenspeicher eine Strafbarkeitslücke genutzt werden kann. Eine solche könnte sich ergeben, weil die bisherige Textfassung überwiegend so ausgelegt wird, daß sie nur die körperliche Verbreitung von Schriften, nicht aber sonstige Übermittlungsformen erfaßt. Nunmehr wird sichergestellt, daß auch Propagandatexte und -abbildungen bzw. entsprechende Multimediadarstellungen, die z. B. per elektronischer Post Anderen zur Kenntnis gebracht oder angeboten werden, die Strafbarkeit begründen, wenn einem nach Art und Zahl unbestimmten Personenkreis die Möglichkeit zur Kenntnisnahme dieser rechtswidrigen Inhalte gegeben wird.

Zu Artikel 5 (Änderung des Gesetzes über Ordnungswidrigkeiten)

Zu Nummer 1

Die Änderungen der §§ 116 Abs. 1, 120 Abs. 1 Nr. 2 und 123 Abs. 2 Satz 1 tragen der erweiterten Fassung des § 11 Abs. 3 Strafgesetzbuch Rechnung und gewährleisten, daß – wie auch bisher – der Schriftenbegriff im Strafrecht und im Ordnungswidrigkeitenrecht übereinstimmt. Zur Ergänzung des Schriftenbegriffes vgl. die Begründung zu Artikel 4 Nr. 1.

§ 116 sanktioniert die Aufforderung zu mit Geldbuße bedrohten Handlungen in drei Fallgestaltungen (öffentlich, in einer Versammlung, durch Verbreiten von

Schriften pp.). Einer Ergänzung bedarf lediglich die Fallgestaltung der (auch nichtöffentlich bußgeldbewehrten) körperlichen Verbreitung von Schriften pp. durch den Begriff des Datenspeichers. Diese Fälle dürften zwar gegenüber dem Abruf von gespeicherten Inhalten mithilfe von Datenübermittlungsvorrichtungen nur eine eher untergeordnete Rolle spielen; sie haben jedoch aufgrund fortschreitender Miniaturisierung und sinkender Herstellungskosten eine eigenständige Bedeutung, z. B. bei Miniaturcomputern (Spielecomputern). Auch diese können für Aufforderungen zu mit Geldbuße bedrohten Handlungen benutzt werden. Dagegen wird davon ausgegangen, daß bereits nach geltendem Recht auch derjenige im Sinne des § 116 Abs. 1 öffentlich auffordert, der zu diesem Zwecke eine solche Aufforderung in einem Datenspeicher öffentlich zugänglich macht (vgl. dazu die parallele Fallgestaltung in § 111 Strafgesetzbuch).

Unter das sonstige öffentliche Zugänglichmachen eines Datenspeichers (§ 120 Abs. 1 Nr. 2) fällt auch die Bekanntgabe seines gedanklichen Inhalts durch unkörperliches Zugänglichmachen (vgl. hierzu Laufhütte, Leipziger Kommentar zum Strafgesetzbuch, § 184, Rn. 21).

Die Ergänzung des § 123 Abs. 2 Satz 1 stellt sicher, daß auch Datenspeicher aufgrund ihres rechtswidrigen Inhalts eingezogen werden können. Gemäß § 24 Abs. 2 unterliegt dies einer Verhältnismäßigkeitsprüfung, die insbesondere dazu führen kann, daß an Stelle einer Einziehung die Löschung bestimmter Inhalte erzwungen wird, wenn der mit ihrer Einziehung verfolgte Zweck bereits dadurch erreicht wird.

Zu Nummer 2

Zu Buchstabe a

§ 119 Abs. 1 Nr. 2 erfaßt bislang nur die Fälle, in denen Gelegenheiten zu sexuellen Handlungen in grob anstößiger Weise durch Verbreiten von Schriften in ihrer Substanz – nicht bloß ihres Inhalts – angeboten (etc.) werden. Derartige Angebote können aber auch in Datenspeichern abgelegt und z. B. über Daten(fern)leitungen einem nach Art und Zahl unbestimmten Personenkreis zugänglich gemacht werden. Eine solche unkörperliche Übermittlung erscheint nicht weniger sanktionswürdig als die körperliche Verbreitung von Schriften, da sie in vergleichbarer Weise grob anstößig sein kann. Die vorliegende Änderung reagiert auf diese sich weiterentwickelnden technischen Möglichkeiten.

Zu Buchstabe b

Die Änderung dient dem schon oben zu Nummer 1. genannten Ziel, die Parallelität der Bestimmungen im Straf- und Ordnungswidrigkeitenrecht zu wahren. Die bereits vorhandene Formulierung „oder sonst öffentlich zugänglich macht" erfaßt bereits die unkörperliche Vermittlung des Inhalts, so daß mit Hinzufügen des Wortes „Datenspeicher" sichergestellt wird, daß das öffentliche Zugänglichmachen eines am jeweiligen Ort grob anstößig wirkenden sexuellen Inhalts eines Datenspeichers auch dann erfaßt wird, wenn dieser z. B. auf einem Computer in einem Cybercafe (eine Gaststätte, in der den Besuchern Computer mit Dialogmöglichkeiten nach außen, vielfach über das Internet, angeboten werden) dargestellt und dabei nur der Arbeitsspeicher in Anspruch genommen wird (vgl. die Begründung zu Artikel 4 Nr. 1).

Zu Artikel 6 (Änderung des Gesetzes über die Verbreitung jugendgefährdender Schriften)

Zu Nummer 1

Durch die Änderung der Bezeichnung des Gesetzes wird dem erweiterten Geltungsbereich Rechnung getragen.

Zu Nummer 2

Der in § 1 Abs. 3 des Gesetzes über die Verbreitung jugendgefährdender Schriften (GjS) und in § 11 Abs. 3 des Strafgesetzbuches jetzt inhaltsgleich definierte Schriftenbegriff hat auch die gleiche gegenständliche Reichweite. Der neu in den Gesetzestext aufgenommene Begriff „Datenspeicher" dient der Klarstellung, daß auf Datenspeichern bereitgehaltene Darstellungen gegenüber solchen in Druckschriften sowie auf Ton- und Bildträgern nicht privilegiert sind, sondern ebenfalls der Listenaufnahme gem. § 1 Abs. 1 Satz 1 des Gesetzes über die Verbreitung jugendgefährdender Schriften unterliegen. Entscheidend ist dabei eine Fixierung für eine gewisse Dauer, unabhängig davon, ob die Schrift mit oder ohne technische Hilfsmittel wahrgenommen werden kann. Ebenfalls unerheblich ist, welcher Art das zur Wahrnehmbarmachung eingesetzte Gerät ist; in Betracht kommt insbesondere die Anzeige auf einem Bildschirm.

Diese Klarstellung ist erforderlich geworden durch die unterschiedliche Auslegung des Schriftenbegriffs in der strafgerichtlichen (Beschluß des OLG Stuttgart vom 27. August 1991; NStZ 1992 S. 38) und der verwaltungsgerichtlichen (Urteil des VG Köln vom 19. Februar 1991; NJW 1991 S. 1773 sowie Beschluß des OVG Münster vom 22. September 1992; NJW 1993 S. 1494) Rechtsprechung. Das Gesetz über die Verbreitung jugendgefährdender Schriften ist in seiner Anwendbarkeit durch die Rechtsprechung der Verwaltungsgerichte im wesentlichen auf Druckwerke und andere verkörperte Darstellungsformen beschränkt worden. Deshalb ist eine Regelung notwendig, die die Gewährleistung des gesetzlichen Jugendschutzes auch im Bereich der neuen Informations- und Kommunikationsdienste sicherstellt, wenn durch diese jugendgefährdende Inhalte verbreitet werden.

Hinsichtlich der Einzelheiten wird auf die vorstehenden Ausführungen zu Artikel 4 Bezug genommen.

Zu Nummer 3

Die vorgesehene Ergänzung hat, soweit sie die Verbreitungsverbote auch auf die Informations- und Kommunikationsdienste erstreckt, lediglich klarstel-

lenden Charakter. Schon die Verbreitungsverbote in der bisherigen Fassung des § 3 Abs. 1 Nr. 1 (in der Form des Zugänglichmachens) und Nr. 2 (in der Form des Vorführens oder sonstigen Zugänglichmachens an einem Ort, der Kindern oder Jugendlichen zugänglich oder einsehbar ist) des Gesetzes über die Verbreitung jugendgefährdender Schriften erfassen ohne weiteres das Vorführen oder sonstige Zugänglichmachen durch Darstellungen bzw. schlichtes Sichtbarmachen auf einem Bildschirm.

Eine ausdrückliche Regelung der die Informations- und Kommunikationsdienste betreffenden Verbreitungsverbote in § 3 Abs. 1 Nr. 4 ist notwendig, um eine unter Gesichtspunkten von Artikel 5 des Grundgesetzes zu würdigende Einengung des Zugangs zu Angeboten von Informations- und Kommunikationsdiensten für Erwachsene zu vermeiden. Dem Anbieter indizierter Inhalte wird die Möglichkeit eröffnet, durch technische Vorkehrungen Vorsorge zu treffen, daß – auch im Zusammenwirken mit den Personensorgeberechtigten – das Angebot oder die Verbreitung im Inland auf volljährige Benutzer beschränkt werden kann. Es bleibt dem Anbieter überlassen, ob er von dieser Möglichkeit Gebrauch macht oder aber auf die Verbreitung verzichtet. Hinsichtlich der Art der technischen Vorkehrungen nimmt das Gesetz keine Festlegungen vor und bleibt damit für neue technische Entwicklungen offen. Die Zugangsbeschränkung kann z. B. im Wege einer Verschlüsselung, Chiffrierung oder Schaffung geschlossener Benutzergruppen (jeweils mit Kontrolle des Alters der berechtigten Anschlußinhaber) umgesetzt werden. Durch die Anordnung von Zeitgrenzen für die Übertragung kann ein zuverlässiger Ausschluß von Kindern oder Jugendlichen von der Nutzung nicht erreicht werden.

Im Ergebnis kommt es darauf an, daß die technischen Vorkehrungen, die die Informationsmöglichkeiten für Erwachsene sichern sollen, in der Praxis zuverlässig umsetzbar sind und keine unzumutbaren Anforderungen an den Anbieter stellen.

Zur Frage der Verantwortlichkeiten verbleibt es bei den in Artikel 1 § 5 Informations- und Kommunikationsdienste-Gesetz aufgeführten Regelungen.

Zu Nummer 4

Die vorgesehene Neufassung des § 5 Abs. 3 folgt der Systematik der mit einer Indizierung verbundenen Rechtsfolgen, hier der Werbebeschränkungen. Es ist sachgerecht, den Anwendungsbereich des Absatzes 2 auch für die Fälle zu beschränken, in denen durch technische Vorkehrungen eine Übermittlung an Kinder oder Jugendliche ausgeschlossen ist.

Da es sich bei den in § 5 des Gesetzes über die Verbreitung jugendgefährdender Schriften geregelten Werbeverboten um absolute Verbote handelt, die keine Privilegierung Erwachsener vorsehen, müssen auch die technischen Vorkehrungen im Sinne des § 5 Abs. 3 Nr. 2 so ausgestaltet sein, daß eine Übermittlung an Kinder und Jugendliche ausgeschlossen ist.

Zu Nummer 5

Der Jugendschutz hat sich im Bereich der neuen Dienste zu einem wichtigen Schwerpunkt entwickelt. Ein Kernpunkt der vom Bund vorgeschlagenen Weiterentwicklung des Jugendschutzrechtes ist die Verpflichtung zur Bestellung von Jugendschutzbeauftragten bei den Diensteanbietern als Ansprechpartner für Nutzer und als interner Berater der Diensteanbieter.

Damit wird durch organisatorische Maßnahmen im Bereich der Diensteanbieter sichergestellt, daß jugendgefährdende Inhalte von Kindern und Jugendlichen weitgehend ferngehalten werden können. Durch die Möglichkeit, die Wahrnehmung der Aufgaben des Jugendschutzbeauftragten auf Einrichtungen der freiwilligen Selbstkontrolle zu delegieren, wird für die betroffenen Diensteanbieter ein gesetzlicher Anreiz zum Zusammenschluß in freiwilligen Selbstkontrolleinrichtungen geschaffen, ein Instrument, daß seit langem in der Bundesrepublik eingeführt ist und sich im Bereich der Medien bisher bewährt hat. Durch die Delegationsmöglichkeit können insbesondere kleine und mittlere Betriebe von den mit der Bestellung verbundenen Kosten entlastet werden.

Adressat der Vorschrift sind Diensteanbieter, die ihre Dienste gewerbsmäßig anbieten, wenn diese Angebote jugendgefährdende Inhalte enthalten können. Ausgenommen sind geschlossene Benutzergruppen, behörden- oder firmeninterne Informations- und Kommunikationsdienste sowie private Gelegenheitsanbieter.

Der Jugendschutzbeauftragte des Diensteanbieters soll nach innen und außen tätig werden. Das Gesetz nennt aus der Vielzahl der Möglichkeiten einer internen Beteiligung drei besonders wichtige Maßnahmen: Bei der Beteiligung an der Angebotsplanung und bei der Gestaltung der allgemeinen Geschäftsbedingungen für die Verträge, die der Diensteanbieter mit den Inhaltszulieferern schließt, besteht in besonderem Maße die Möglichkeit, von vornherein auf eine jugendfreundliche Gestaltung der Angebote oder einer frühzeitigen Einplanung von Maßnahmen, die den Zugang auf Volljährige beschränken, Einfluß nehmen zu können. Eine ebenfalls wichtige Maßnahme ist die Beratung im Hinblick auf eine Beschränkung von Angeboten durch den Diensteanbieter in Form einer Sperrung beziehungsweise Altersbegrenzung.

Als Ansprechpartner für Nutzer, insbesondere für Erziehungsberechtigte, soll der Jugendschutzbeauftragte über technische Sicherungsmöglichkeiten beraten. Daneben kann er Hinweise auf jugendgefährdende Inhalte in Angeboten aufnehmen und diese an den Diensteanbieter, die Jugendbehörden und die Strafverfolgungsbehörden weiterleiten.

Die bisherigen Erfahrungen haben gezeigt, daß den Gefahren eines quasi-anarchischen Systems wie dem Internet nicht mit hierarchisch gegliederten, starren Ge- oder Verboten begegnet werden kann. Hier sind vielmehr schon von ihrer Struktur her flexibel angelegte Reaktionsmechanismen erforderlich. Der Ju-

gendschutzbeauftragte besitzt die Fähigkeit, flexibel und von Fall zu Fall angepaßt auf unterschiedliche Gefährdungspotentiale einzugehen und je nach Fall die richtige Hilfestellung zu geben. Die Beauftragten können dabei mit generellen Hinweisen, aber auch im Einzelfall arbeiten.

Zu Nummer 6

Die vorgesehene Ergänzung enthält die notwendige Strafbewehrung eines Verstoßes gegen § 3 Abs. 1 Nr. 4. Zur Frage der Verantwortlichkeiten verbleibt es bei den in Artikel 1 § 5 Informations- und Kommunikationsdienste-Gesetz aufgeführten Regelungen.

Zu Artikel 7 (Änderung des Urheberrechtsgesetzes)

Allgemeines

1. Europäische Harmonisierung des Immaterialgüterschutzes für Datenbanken

Die neuen Informations- und Kommunikationstechnologien, insbesondere die digitale Technologie und ihre schnell fortschreitende Anwendung in globalen Kommunikationsnetzwerken, machen auch Anpassungen des nationalen Urheberrechts und der internationalen Urheberrechtsabkommen notwendig. Der Meinungsbildungsprozeß über das Ausmaß der erforderlichen Anpassungen des nationalen Urheberrechts ist in Deutschland, wie auch in den meisten anderen Industriestaaten, noch nicht abgeschlossen. Auf internationaler Ebene ist für Ende 1996 eine diplomatische Konferenz zu wichtigen Übereinkommen im Rahmen der Weltorganisation für Geistiges Eigentum (WIPO), Genf, vorgesehenen. Innerhalb der EU wurde 1995 die Prüfung des Bedarfs für die gemeinschaftsweite Harmonisierung des Urheberrechts durch das Grünbuch der EG-Kommission über das Urheberrecht und die verwandten Schutzrechte in der Informationsgesellschaft – Dokument KOM (95) 382 endg. vom 19. Juli 1995 – eingeleitet und dauert an. Abgeschlossen werden konnte hingegen bereits die europäische Harmonisierung des Rechtsschutzes der Anbieter in einem weitreichenden Teilgebiet der neuen Informations- und Kommunikationsdienste, welches die Datenbanken bilden.

Die Richtlinie 96/9/EG vom 11. März 1996 über den rechtlichen Schutz von Datenbanken harmonisiert bzw. begründet erstmals in den Mitgliedstaaten einen zweistufigen Rechtsschutz für Datenbanken:

- in Kapitel II einen urheberrechtlichen Schutz für eine nach „Auswahl oder Anordnung" des gesammelten Stoffes schöpferisch gestaltete Datenbank, der ein Auswertungsrecht in bezug auf diese Gestaltung, aber nicht auch in bezug auf den gesammelten Inhalt verleiht, sowie
- in Kapitel III ein Schutzrecht „sui generis", durch welches der unternehmerisch verantwortliche Hersteller einer Datenbank für die bei der Anlage der Datensammlung getätigte wesentliche Investition mit einem beschränkten Auswertungsmonopol in bezug auf den zusammengetragenen Inhalt belohnt wird.

Wegen der unterschiedlichen Schutzvoraussetzungen können im Einzelfall an ein und derselben Datenbank beide Schutzrechte oder nur eines von beiden bestehen. Hinsichtlich der Tragweite des gewährten Schutzes ergänzen sich die beiden Schutzrechte.

Die Richtlinie ist nach ihrem Artikel 16 Abs. 1 bis zum 1. Januar 1998 in das innerstaatliche Recht der Mitgliedstaaten umzusetzen. In Deutschland ist dafür Gesetzgebung erforderlich; zur Verfügung steht die ausschließliche Kompetenz des Bundes für den gewerblichen Rechtsschutz und das Urheberrecht (Artikel 73 Nr. 9 des Grundgesetzes).

Die in Artikel 7 vorgeschlagene Änderung des Urheberrechtsgesetzes erschöpft den durch die Richtlinie entstehenden Umsetzungsbedarf. Der Regelungsvorschlag beruht im wesentlichen auf einer Zweiteilung der Regelungsstandorte im Urheberrechtsgesetz, entsprechend der Zweistufigkeit des in der Richtlinie vorgesehenen Rechtsschutzes.

2. Zum urheberrechtlichen Schutz von Datenbanken nach der Richtlinie 96/9/EG und nach geltendem Recht

Die Richtlinie lehnt sich in ihrem Kapitel II über den urheberrechtlichen Schutz von Datenbanken an Rechtstraditionen der Mitgliedstaaten an, die sämtlich Vertragsparteien der Revidierten Berner Übereinkunft zum Schutz von Werken der Literatur und Kunst (RBÜ) sind. Nach deren Artikel 2 Abs. 5 sind „Sammlungen von Werken", die wegen der Auswahl und der Anordnung des Stoffes geistige Schöpfungen darstellen, als solche urheberrechtlich geschützt. § 4 Urheberrechtsgesetz verleiht Sammlungen von Werken „und anderen Beiträgen" ebenfalls unter der Voraussetzung, daß die Sammlung wegen der Auswahl oder der Anordnung eine geistige Schöpfung darstellt, urheberrechtlichen Schutz. Artikel 10 Abs. 2 des Übereinkommens über handelsbezogene Aspekte der Rechte des geistigen Eigentums (BGBl. 1994 II S. 1730) erstreckt den urheberrechtlichen Schutz auf Zusammenstellungen von Daten oder sonstigem Material, gleichviel, ob in maschinenlesbarer oder anderer Form, die aufgrund der Auswahl und Anordnung ihres Inhalts geistige Schöpfungen bilden. Die letztere Regelung, die ebenfalls für alle Mitgliedstaaten, aber auch für die Europäische Gemeinschaft als solche verbindlich ist, bezieht klarer und eindeutiger als die vorgenannten, in länger zurückliegender Zeit getroffenen Regelungen moderne Datenbanken, insbesondere solche überwiegend oder rein informationellen Inhalts, in ihren Geltungsbereich mit ein. In der Europäischen Gemeinschaft bedeutet daher die Umsetzung des Kapitels II der Richtlinie, betreffend das Urheberrecht an Datenbanken, in bezug auf das grundsätzliche Bestehen dieses Rechtsschutzes keine Neuerung, sondern bringt lediglich eine Reihe von Präzisierungen in Einzelfragen mit sich, die überwiegend klarstellenden Charakter haben.

Es wird vorgeschlagen, dem Ersten Teil des Urheberrechtsgesetzes, der dem Urheberrecht im engeren Sinne (Recht des Urhebers) gewidmet ist, einen

Neunten Abschnitt mit Besonderen Bestimmungen für Datenbanken anzufügen (Artikel 7 Nr. 1). Damit folgt der Entwurf derselben Regelungstechnik wie das Zweite Gesetz zur Änderung des Urheberrechtsgesetzes, durch welches im Jahr 1993 die Richtlinie 91/250/EWG über den Rechtsschutz von Computerprogrammen umgesetzt wurde.

3. Das neue Schutzrecht sui generis

a) Einleitung

Neben der Harmonisierung des Urheberrechtsschutzes für Datenbanken verpflichtet die Richtlinie in ihrem Kapitel III die Mitgliedstaaten zur Einführung eines neuen Datenbankschutzrechtes eigener Art. Die Richtlinie bezeichnet es als „Schutzrecht sui generis". Es ist darauf gerichtet, die bei der Beschaffung, Überprüfung und Darstellung des Inhalts einer Datenbank vorgenommene Investition zu schützen (Erwägungsgrund 40), soweit diese qualitativ oder quantitativ als wesentlich bezeichnet werden kann.

Ein besonderer Investitionsschutz für Datenbankhersteller erweist sich angesichts der neuen digitalen Speicher- und Kommunikationstechnologien als erforderlich (vgl. Erwägungsgründe 7 bis 12, 38). Der Aufbau von Datenbanken kann mit erheblichen Investitionen verbunden sein, während die Daten für einen Bruchteil der Investitionskosten abgefragt und kopiert werden können. Die unerlaubte Nutzung des Inhalts einer Datenbank beeinträchtigt die wirtschaftliche Entwicklung des Datenbankgeschäfts und kann damit auch die technische Entwicklung negativ beeinflussen. Die für den wachsenden Informationsmarkt erforderlichen Investitionen in moderne Datenspeicher- und Datenverarbeitungssysteme können vereitelt oder behindert werden. Die Einführung des neuen Schutzrechtes soll dem entgegenwirken.

Der zu gewährende Schutz gegenüber unerlaubter Entnahme und Weiterverwendung des Inhalts von Datenbanken zielt besonders auf Wettbewerbsverhältnisse (Erwägungsgrund 6). Über den Schutz gegenüber der Herstellung „parasitärer Konkurrenzprodukte" hinaus sollen jedoch auch alle sonstigen investitionsschädigenden Nutzungen unterbunden werden (Erwägungsgrund 42).

b) Zur Bedeutung des neuen Schutzrechts in der Rechtsordnung

Die Bedeutung des neuen Rechts, das anderweitigen rechtlichen Schutz nicht verdrängt, sondern neben diesen tritt (Artikel 7 Abs. 4, Artikel 13 der Richtlinie), liegt in dem Schutz vor dem unerlaubten Zugriff auf den Inhalt von Datenbanken, der weder selbst noch über den Strukturschutz der Datenbank vom Urheberrecht geschützt wird. Das wird nicht selten der Fall sein. Sammlungen von Informationen über Fakten, etwa Adressen, Telefonnummern oder meteorologische Meßergebnisse, sind in der Regel mangels geistiger Schöpfung urheberrechtlich nicht schutzfähig. Als „Datenbank" erfahren sie urheberrechtlichen Schutz lediglich dann, wenn die Auswahl oder Anordnung eine individuelle schöpferische Leistung darstellt. Insbesondere bei Datenbanken, die auf eine vollständige Erfassung von Fakten gerichtet sind oder bei denen die Anordnung nach allgemein bekannten und gängigen Prinzipien erfolgt (Alphabet, Wohnort), kann es hieran fehlen. Soweit in diesen Fällen der nach der Richtlinie erforderliche Investitionsumfang erreicht wird, soll künftig der Datenbankhersteller besonders geschützt werden.

Der zu schaffende Schutz geht über den – weiterhin bestehenbleibenden – wettbewerbsrechtlichen Leistungsschutz hinaus. Nach geltendem Recht sichert § 1 des Gesetzes gegen den unlauteren Wettbewerb (UWG) gegenüber der unlauteren Übernahme fremder Leistungsergebnisse. Die in einer Datenbank gesammelten Informationen können solchermaßen gegen Ausbeutung geschützt sein. Doch wirkt dieser Schutz nur in Wettbewerbsverhältnissen, nicht hingegen im Verhältnis zum privaten Endverbraucher. Außerdem besteht ein Verbotsrecht nicht bereits bei Übernahme eines fremden Leistungsergebnisses, sondern erst bei Hinzutreten besonderer die Unlauterkeit begründender Umstände. Welche Umstände das sein können, kann nur durch eine die unterschiedlichen Interessen berücksichtigende, abwägende Entscheidung im Einzelfall festgestellt werden. Mit der rechtlichen Unsicherheit gehen Schwierigkeiten einher, die sich daraus ergeben, daß der Schutzsuchende die die Unlauterkeit begründenden Tatsachen beweisen muß. Auch aus Beweisgründen wird sich daher der Rechtsschutz für Datenbankhersteller mit Einführung des neuen Datenbankschutzrechts verbessern.

Das neue Schutzrecht sichert die Befugnis des Herstellers, über die Verwendung des gesamten Inhalts oder wesentlicher Teile des Inhalts der Datenbank zu befinden. Unwesentliche Inhaltsteile werden von dem Schutzrecht dagegen nicht erfaßt. Der beabsichtigte Investitionsschutz erfordert deren Einbeziehung nicht. Die begrenzte Reichweite des Schutzes dient zudem dazu, den erforderlichen Investitionsschutz mit dem Interesse an einem möglichst freien Informationsfluß in Einklang zu bringen. Der Sicherung der Informationsfreiheit und der Ausgewogenheit der Gesamtregelung dient es auch, daß die Richtlinie klar definierte Benutzerrechte verbindlich festlegt (Artikel 8, 15). Dem rechtmäßigen Benutzer einer Datenbank kann daher nicht untersagt werden, unwesentliche Teile des Inhalts der Datenbank zu entnehmen oder weiterzuverwenden.

Der Wettbewerb zwischen verschiedenen Anbietern von Datenbanken soll durch das neue Schutzrecht nicht beeinträchtigt werden. Europäisches und nationales Kartellrecht bleiben von der Neuregelung unberührt (Erwägungsgrund 47). Das ermöglicht es, die unangemessene Ausnutzung von Informationsmonopolen zu verhindern. Die Ausübung des neuen Schutzrechts durch den Datenbankhersteller darf nicht dazu führen, daß der Zugang zu Informationen mißbräuchlich beschränkt wird.

Mit der Einführung eines besonderen Datenbankschutzrechtes hat sich die Europäische Union weltweit an die Spitze bei der Schutzgewährung in diesem Bereich gestellt. Der wünschenswerten globalen

Ausweitung des Rechtsschutzes dient es, daß der neue Schutz (zunächst) nur Herstellern aus dem Europäischen Wirtschaftsraum gewährt wird und eine Erstreckung auf sonstige ausländische Personen und Unternehmen nur unter der Voraussetzung der Gegenseitigkeit (Reziprozität), also einer entsprechenden Schutzgewährung für Datenbanken in Drittstaaten (Erwägungsgrund 56), erfolgt.

c) Umsetzung der Richtlinie durch Einführung eines neuen Leistungsschutzrechtes

Es wird vorgeschlagen, das Schutzrecht des Datenbankherstellers als Leistungsschutzrecht in den Zweiten Teil des Urheberrechtsgesetzes einzustellen.

Die Datenbankenrichtlinie enthält keine Vorgaben über die Art und Weise ihrer Umsetzung. Möglich wäre es auch, diese, ähnlich wie beim Halbleiterschutzgesetz (BGBl. 1987 I S. 2294), in einem gesonderten Gesetz vorzunehmen. Die bewußte, auch vom Wortlaut der Richtlinie dokumentierte Distanz des „Schutzrechts sui generis" zu den Leistungsschutzrechten könnte zugunsten einer solchen Normierung in einem speziellen Gesetz angeführt werden.

Es sprechen jedoch eine Reihe von Gründen dafür, die Umsetzungsregelung im Urheberrechtsgesetz vorzunehmen. Das neue Schutzrecht ist mehr als bloßer Wettbewerbsschutz. Es gewährt nicht allein ein Verbotsrecht, sondern ist als übertragbares Ausschließlichkeitsrecht mit einer festen Schutzfrist ausgestaltet. Es kann daher als eigenständiges Immaterialgüterrecht an die Seite der im Zweiten Teil des Urheberrechtsgesetzes geregelten „verwandten Schutzrechte" gestellt werden. Auch bei den bereits bisher dort erfaßten Rechten besteht zum Teil nur eine lose Verbindung zum Urheberrecht und zur Werkvermittlung. Der Schutz des Sendeunternehmens (§ 87 UrhG) etwa besteht nicht nur bei Sendung urheberrechtsschutzfähiger Werke oder Darbietungen, sondern für Funksendungen jeden Inhalts und Charakters. Vergleichbar ist nunmehr der Hersteller von Datenbanken zu schützen, auch wenn eine Datenbank lediglich Daten enthält, die selbst nicht urheberrechtsschutzfähig sind. Auch wegen der sachlichen Nähe beider nach der Richtlinie zu gewährenden Schutzinstrumente zueinander erscheint es zweckmäßig, den neuen Datenbankschutz neben dem urheberrechtlichen Schutz von Datenbanken in demselben Gesetzeswerk zu regeln.

d) Grundzüge der Richtlinie und Überblick über die Umsetzung

Kapitel III der Richtlinie 96/9/EG über den rechtlichen Schutz von Datenbanken verpflichtet die Mitgliedstaaten, ein neues „Schutzrecht sui generis" einzuführen. Sein Ziel ist es, „wesentliche Investitionen" in Datenbanken zu schützen. Es handelt sich hierbei um ein neuartiges Schutzrecht, das weder in Deutschland noch in der Europäischen Union oder im sonstigen Ausland ein Vorbild hat.

Artikel 7 der Richtlinie enthält die grundlegenden Bestimmungen über den Schutzgegenstand des einzuführenden Schutzrechtes. Dem Hersteller einer Datenbank, der in diese wesentlich investiert hat, muß das Recht eingeräumt werden, die Entnahme oder Weiterverwendung ihres Inhalts oder wesentlicher Teile ihres Inhalts zu untersagen. Neben den Grundlagen des Schutzes werden die Übertragbarkeit des Rechts (Abs. 3) und die Konkurrenz zu anderen datenbankschützenden Bestimmungen (Abs. 4) geregelt. Die Umsetzung nimmt der Entwurf in § 87a des Urheberrechtsgesetzes vor.

Artikel 8 der Richtlinie macht Vorgaben für die Rechte und Pflichten des rechtmäßigen Benutzers einer Datenbank. Die Vorschrift steht in Zusammenhang mit Artikel 15 der Richtlinie, wonach Artikel 8 zuwiderlaufende vertragliche Vereinbarungen nichtig sind. Für die Umsetzung von Artikel 8 Abs. 1 und 2 der Richtlinie wird die Regelung in § 87d des Urheberrechtsgesetzes vorgeschlagen. Da es sich um vertragsrechtliche Bestimmungen handelt, sieht der Entwurf abweichend von der Systematik der Richtlinie vor, daß die Umsetzung erst im Anschluß an die weiteren das Schutzrecht selbst betreffenden neuen Vorschriften des Urheberrechtsgesetzes erfolgt. Eine besondere Umsetzung des Artikels 8 Abs. 3 der Richtlinie erscheint entbehrlich. Das dem rechtmäßigen Benutzer obliegende Schädigungsverbot gegenüber Rechtsinhabern an in der Datenbank enthaltenen Werken und Leistungen folgt bereits aus den allgemeinen Vorschriften des Urheberrechtsgesetzes (insbesondere § 97 Urheberrechtsgesetz – Anspruch auf Unterlassung und Schadensersatz).

Artikel 9 der Richtlinie gibt den Mitgliedstaaten die Möglichkeit, über „Ausnahmen vom Recht sui generis" die Reichweite des neuen Schutzrechts einzuschränken. Da es sich bei dem Recht sui generis um eine juristische Neuerung handelt, eröffnet die Richtlinie – anders als Artikel 6 Abs. 2 für den Urheberrechtsschutz für Datenbanken – nicht die Möglichkeit, Ausnahmen entsprechend traditionellem nationalen Recht vorzusehen. Das führt dazu, daß Datenbankhersteller im Einzelfall stärker geschützt sein können als Urheber von Datenbanken, da die Urheber weitergehenden Schranken unterliegen, als sie für Datenbankhersteller nach der Richtlinie vorgesehen werden können. Für die Umsetzung wird die Schrankenregelung in § 87b des Urheberrechtsgesetzes vorgeschlagen.

Die Schutzdauer des sui-generis-Rechts beträgt gemäß Artikel 10 der Richtlinie fünfzehn Jahre, wobei jede wesentliche Neuinvestition in die Datenbank eine neue, eigene Schutzdauer beginnen läßt. Fortlaufend aktualisierte Datenbanken können daher in den Genuß eines zeitlich unbegrenzten Schutzes gelangen. Die Umsetzung von Artikel 10 der Richtlinie ist in § 87c des Entwurfs zum Urheberrechtsgesetz enthalten.

Artikel 11 der Richtlinie enthält die fremdenrechtlichen Vorschriften über den Anwendungsbereich des neuen Schutzrechts. Wie bereits ausgeführt, wird die Bestimmung von dem Gedanken getragen, daß ein Schutz nur solchen Personen gewährt werden soll, deren Heimatrecht einen vergleichbaren Schutz für Hersteller von Datenbanken aus der Europäischen Union bietet (Erwägungsgrund 56). Der Schutz beschränkt sich demnach bis zum Abschluß von Verein-

barungen durch die Europäische Union mit Drittländern (Artikel 11 Abs. 3 der Richtlinie) auf Hersteller, die Unionsangehörige sind oder dort ihren gewöhnlichen Aufenthalt haben; für Unternehmen wird die Regelung aus Artikel 58 des EG-Vertrages übernommen. Für die Umsetzung wird der neue § 127a des Urheberrechtsgesetzes vorgeschlagen, der im Fünften Teil des Urheberrechtsgesetzes bei den Vorschriften zu dessen Anwendungsbereich einzufügen ist.

Die Mitgliedstaaten sind nach Artikel 12 der Richtlinie verpflichtet, zur Absicherung des einzuräumenden Schutzrechtes geeignete Sanktionen vorzusehen. Hier erscheinen nur wenige Ergänzungen des Urheberrechtsgesetzes erforderlich, die unter Artikel 7 Nr. 3 bis 5 des Entwurfs für das Verwertungsverbot gemäß § 96 Urheberrechtsgesetz, die Strafvorschrift des § 108 Urheberrechtsgesetz und die Zwangsvollstreckungsregelung des § 119 Urheberrechtsgesetz vorgeschlagenen werden. Im übrigen erfassen die zivilrechtlichen Vorschriften über Rechtsverletzungen in §§ 97 ff. Urheberrechtsgesetz alle Fälle, in denen vom Urheberrechtsgesetz gewährte ausschließliche Rechte verletzt werden. Die Vorschriften gewähren daher auch dem Datenbankhersteller einen umfassenden Schutz gegenüber der Verletzung seiner Rechte.

Artikel 14 Abs. 3 und 5 der Richtlinie betreffen den Schutz solcher Datenbanken, die vor dem 1. Januar 1998 hergestellt worden sind. Für diese Übergangsregelung sieht der Entwurf die Umsetzung durch Artikel 7 Nr. 7 in § 137h Abs. 2 des Urheberrechtsgesetzes vor.

Zu den Vorschriften im einzelnen

Zu Artikel 7 Nr. 1 (Einfügung eines Neunten Abschnitts – Besondere Bestimmungen für Datenbanken)

Zu § 69h (Definition der Datenbank)

Eingeleitet wird der Neunte Abschnitt, der dem in Kapitel II der Richtlinie geregelten urheberrechtlichen Schutz für Datenbanken gewidmet ist, durch eine Definition des Begriffs der Datenbank. Zugleich wird damit der Geltungsbereich sämtlicher Vorschriften des neuen Neunten Abschnitts eingegrenzt. Die Definition der Datenbank im neuen § 69h des Urheberrechtsgesetzes folgt wörtlich der Definition in Artikel 1 Abs. 2 der Richtlinie, die sowohl für den urheberrechtlichen Teil der Richtlinie als auch für das neue Schutzrecht sui generis gilt. Durch diesen begrifflichen Gleichklang soll gewährleistet werden, daß bezüglich des Geltungsbereichs der Umsetzungsregeln der größtmögliche Harmonisierungseffekt eintritt.

Neben der operativen Bestimmung des Artikels 1 Abs. 2 der Richtlinie befassen sich mit dem Begriff der Datenbank auch die Erwägungsgründe 14, 17, 19, 21, 22 und 23. Darin werden, teilweise erklärlich aus der Entstehungsgeschichte der Richtlinie, verschiedene Einzelfragen der Definition angesprochen. Die Sachentscheidungen über den Geltungsbereich der Richtlinie können aber zutreffend bereits aus der operativen Bestimmung des Artikels 1 Abs. 2 abgeleitet werden. Aus dieser ergibt sich u. a., daß sowohl elektronische als auch nichtelektronische Datenbanken umfaßt sind, ferner Datenbanken, die in Form von CD-ROM vertrieben werden, ebenso wie Online-Datenbanken (s. Erwägungsgründe 14 und 22). Bei einer elektronischen Datenbank werden die Elemente der Sammlung in der Regel mit Hilfe eines Computerprogramms einzeln zugänglich sein. Gleichwohl ist ein solches Computerprogramm ebensowenig wie sonstige für den Betrieb einer elektronischen Datenbank etwa verwendete Computerprogramme vom Geltungsbereich der Richtlinie erfaßt. Vielmehr gelten für den Rechtsschutz an diesen Programmen allein die in der Gemeinschaft harmonisierten Regeln über den Rechtsschutz von Computerprogrammen, d. h. die §§ 69a ff. Urheberrechtsgesetz. Artikel 1 Abs. 3 der Richtlinie, der dies klarstellt, bedarf keiner Umsetzung.

Nach dem Erwägungsgrund 20 kann sich der in der Richtlinie vorgesehene Schutz auch auf Elemente erstrecken, die für den Betrieb oder die Abfrage bestimmter Datenbanken erforderlich sind, beispielsweise auf den Thesaurus oder die Indexierungssysteme. Dieser Erwägungsgrund ist ein Überbleibsel aus der Datenbankdefinition in Artikel 1 Abs. 1 des Geänderten Vorschlags der Kommission – Dokument KOM (93) 464 endg. – SYN 393 –, wonach zur Datenbank auch gehört das „Material, das für den Betrieb der Datenbank erforderlich ist, wie ihr Thesaurus, Index oder Abfragesystem". Die Richtlinie in ihrer endgültigen Fassung läßt offen, ob und ggf. unter welchen Voraussetzungen dieses Material geschützt ist. Der Erwägungsgrund 20 dürfte dahin zu verstehen sein, daß je nach Lage des Einzelfalles dieses besondere „Material" die Kriterien des urheberrechtlichen Schutzes erfüllen kann („Auswahl oder Anordnung" im Sinne des Artikels 3 Abs. 1 der Richtlinie).

Zu § 69i (Voraussetzung und Gegenstand des urheberrechtlichen Schutzes)

Der vorgeschlagene § 69i Urheberrechtsgesetz ist die grundlegende Bestimmung für den urheberrechtlichen Schutz von Datenbanken. Das Kriterium für die Urheberrechtsfähigkeit in Absatz 1 ist dem Artikel 3 Abs. 1 Satz 1 der Richtlinie wörtlich entnommen. Es stimmt mit dem in § 4 Urheberrechtsgesetz festgelegten Kriterium für die Urheberrechtsfähigkeit von Sammelwerken ebenso überein wie mit den entsprechenden Formulierungen des Artikels 2 Abs. 5 der Revidierten Berner Übereinkunft zum Schutz von Werken der Literatur und Kunst und des Artikels 10 Abs. 2 des Übereinkommens über handelsbezogene Aspekte der Rechte des geistigen Eigentums. Mit der Rechtsfolgeanordnung, daß die so qualifizierten Datenbanken als Werke geschützt werden, wird insbesondere bewirkt, daß die für Werke geltenden Vorschriften des Ersten Teils gelten, soweit nicht nachfolgend abweichende Regeln getroffen werden.

§ 4 Urheberrechtsgesetz bleibt unangetastet; die Vorschrift hat nach wie vor für Sammelwerke Bedeutung, die in bezug auf Anordnung des Stoffes und

Zugänglichkeit dem § 69h Urheberrechtsgesetz nicht (voll) entsprechen.

Keine Sonderregelung der urheberrechtsfähigen Gestaltungshöhe

Der Entwurf verzichtet darauf, den Artikel 3 Abs. 1 Satz 2 der Richtlinie („Bei der Bestimmung, ob sie für diesen Schutz in Betracht kommen, sind keine anderen Kriterien anzuwenden.") durch eine ausdrückliche Bestimmung umzusetzen. Darin folgt der Entwurf der Methode bei der Umsetzung des Artikels 6 der Richtlinie 93/98/EWG zur Harmonisierung der Schutzdauer des Urheberrechts und bestimmter verwandter Schutzrechte, welcher den urheberrechtlichen Schutz fotografischer Werke zum Gegenstand hat, durch das Dritte Gesetz zur Änderung des Urheberrechtsgesetzes vom 23. Juni 1995 (BGBl. I S. 842). Anders war noch verfahren worden bei der Umsetzung der Richtlinie über den Rechtsschutz von Computerprogrammen, s. § 69a Abs. 3 Satz 2 Urheberrechtsgesetz. Bei der letztgenannten Richtlinie bestand aber ein besonderes Harmonisierungsziel darin, die in Deutschland vor Verabschiedung der Richtlinie von der Rechtsprechung aufgestellten erhöhten Anforderungen an die urheberrechtliche Gestaltungshöhe (§ 2 Abs. 2 UrhG) von Computerprogrammen abzusenken. Dem war bei der Umsetzung seinerzeit Rechnung zu tragen. In bezug auf den urheberrechtlichen Schutz von Datenbanken oder Sammelwerken allgemein (§ 4 UrhG) besteht eine solche Problemlage in Deutschland nicht. Insbesondere stellt der Bundesgerichtshof in jüngeren Entscheidungen zur urheberrechtlichen Gestaltungshöhe von Sammlungen im Sinne des § 4 Urheberrechtsgesetz keine verschärften Anforderungen an die erforderliche Qualität von Auslese oder Anordnung des gesammelten Stoffs (siehe u.a. BGH GRUR 1992, 382-386 – Leitsätze).

§ 69i Abs. 2 des Entwurfs übernimmt den Gehalt von Artikel 3 Abs. 2 der Richtlinie sowie ein Regelungselement des einleitenden Satzteils von Artikel 5 der Richtlinie. Auch auf Artikel 10 Abs. 2 Satz 2 des Übereinkommens über handelsbezogene Aspekte der Rechte des geistigen Eigentums ist hinzuweisen. Der Regelungsgehalt dieses Absatzes steht in Einklang mit der deutschen Lehre und Rechtsprechung zu § 4 Urheberrechtsgesetz in bezug auf Sammelwerke und hat deshalb klarstellenden Charakter.

Keine Sonderregelung über Rechtsübergang im Arbeitsverhältnis

Die Richtlinie trifft in ihrem urheberrechtlichen Teil keine Regelung darüber, wem die Verwertungsbefugnisse zustehen, wenn der Urheber die Datenbank im Rahmen einer unselbständigen Tätigkeit, also insbesondere im Arbeitsverhältnis, geschaffen hat. Erwägungsgrund 29 stellt klar, daß diese Frage durch vertragliche Regelungen des Arbeitsverhältnisses geklärt werden kann und daß die Mitgliedstaaten befugt bleiben, darüber Auslegungsregeln vorzusehen. Eine Sonderregelung in dieser Hinsicht wird nicht für erforderlich gehalten. § 43 Urheberrechtsgesetz ist daher anwendbar, soweit keine autonome Regelung zwischen den Beteiligten getroffen worden ist.

Keine Sonderregelung der Verwertungsrechte

Die Harmonisierung des Urheberrechts in der Europäischen Union ist noch nicht so weit fortgeschritten, daß die Verwertungsbefugnisse des Urhebers von Werken im allgemeinen, seine sog. ausschließlichen Rechte, die ihm die Befugnis verleihen, in ihrem jeweiligen Bereich die Werkverwertung durch andere zu verbieten bzw. zu gestatten, bereits harmonisiert wären. (Einen Ausnahmefall stellt bisher nur das Vermietrecht dar, vgl. die Richtlinie 92/100/EWG.) Deshalb mußte die vorliegende Richtlinie in Artikel 5 für eine abgerundete Harmonisierung des urheberrechtlichen Schutzes von Datenbanken auch die ausschließlichen Verwertungsrechte des Urhebers („zustimmungsbedürftige Handlungen") bestimmen. Die Verwertungsbefugnisse sind in den Buchstaben a bis e aufgeführt. Für das Verständnis der Bestimmungen sind die wichtigen Erwägungsgründe 30 bis 33 heranzuziehen. Aus Erwägungsgrund 32 geht insbesondere hervor, daß die Mitgliedstaaten nicht gehalten sind, eine bestimmte Systematik der Verwertungsrechte einzuführen, wenn sie nur die materielle Dekkungsgleichheit mit den Regeln der Richtlinie gewährleisten.

Der Entwurf geht, indem er für den Neunten Abschnitt keine Regeln zur Umsetzung des Artikels 5 der Richtlinie vorsieht, davon aus, daß die allgemeinen Regeln über die Verwertungsrechte des Urhebers im Vierten Abschnitt des Ersten Teils (§§ 15ff. UrhG) die dem Urheber einer Datenbank durch Artikel 5 der Richtlinie vorbehaltenen Handlungen hinreichend abdecken. Für das Vervielfältigungsrecht (§ 16 UrhG), das Recht zu Bearbeitungen oder anderen Umgestaltungen (§ 23 UrhG) und das Verbreitungsrecht im Sinne einer Verbreitung von Vervielfältigungsstücken der Datenbank in körperlicher Form, z. B. als CD-ROM, „off-line", (§ 17 UrhG) erscheint dies ohne weiteres einleuchtend. Zugleich wird mit dem Festhalten am herkömmlichen Verbreitungsbegriff (Beschränkung auf die Verbreitung von Vervielfältigungsstücken in körperlicher Form) auch sichergestellt, daß das Erschöpfungsprinzip – in Artikel 5 Buchstabe c Satz 2 der Richtlinie dekkungsgleich mit § 17 Abs. 2 Urheberrechtsgesetz als Grundsatz der nationalen bzw. gemeinschaftsweiten Erschöpfung festgelegt – nicht auch gilt für unkörperliche Formen der Vermarktung; in der Richtlinie wird dies durch den Erwägungsgrund 33 ausdrücklich klargestellt. Auch das Recht der öffentlichen Wiedergabe (§ 15 Abs. 2 UrhG) mit seinen Unterarten dient der Abdeckung der in Artikel 5 der Richtlinie genannten Handlungen.

Von wesentlicher Bedeutung für die Tragweite der Verwertungsrechte des Artikels 5 der Richtlinie sind die Erwägungsgründe 30 und 31 der Richtlinie, wonach der Urheber das Recht haben soll zu bestimmen, in welcher Weise und durch wen das Werk genutzt wird, einschließlich der „Zurverfügungstellung von Datenbanken in einer anderen Weise als durch die Verbreitung von Vervielfältigungsstücken". Da-

mit ist ausdrücklich die Verwertung der Datenbanken durch Bereitstellung eines elektronischen, interaktiven Zugangs im Rahmen der Netzkommunikation, also die Online-Verwertung, angesprochen. Die Richtlinie ordnet diese wirtschaftlich außerordentlich wichtige Verwertungsform nicht ausdrücklich einer bestimmten Untergliederung der in Artikel 5 vorbehaltenen Handlungen zu. Die Mitgliedstaaten sollen zwar ein ausschließliches Recht in diesem Bereich gewähren, aber in der systematischen Zuordnung frei bleiben.

Für die Beurteilung nach dem geltenden deutschen Urheberrecht ist von wesentlicher Bedeutung, daß der Aufzählung der Verwertungsrechte des Urhebers in § 15 Urheberrechtsgesetz ebenfalls der im Erwägungsgrund 30 der Richtlinie hervorgehobene Grundsatz zu entnehmen ist, daß dem Urheber allgemein das ausschließliche Recht zugeordnet ist, über die Verwertung seines Werkes zu entscheiden. In der Begründung des Regierungsentwurfs des Urheberrechtsgesetzes heißt es zu § 15 Urheberrechtsgesetz: „... verzichtet der Entwurf auf eine erschöpfende Aufzählung der Verwertungsrechte und gibt dem Urheber statt dessen ganz allgemein das Recht, sein Werk zu verwerten, wobei die einzelnen zur Zeit bekannten, im Geschäftsverkehr entwickelten Verwertungsformen ... nur als Beispiele angeführt werden. Dadurch wird klargestellt, daß auch etwaige künftige Verwertungsformen, die heute noch nicht bekannt sind, dem Urheber vorbehalten sein sollen (BT-Drs. IV/270)." Es kann daher als bereits durch den gegenwärtigen Rechtszustand gesichert gelten, daß die Verwertung einer Datenbank in der Form der Online-Zurverfügungstellung für den individuellen Abruf durch die eine Öffentlichkeit darstellenden Benutzer dem Urheber als ausschließliches Recht vorbehalten ist. Damit ist die Umsetzung der durch Artikel 5 der Richtlinie festgelegten ausschließlichen Rechte in der Substanz bereits sichergestellt. Zur systematischen Einordnung der interaktiven Netzkommunikation zeichnet sich als vorherrschend diejenige Lehrmeinung ab, die diesen Vorgang dem alle unkörperlichen Verwertungsarten übergreifenden Recht der öffentlichen Wiedergabe (§ 15 Abs. 2 UrhG) zuordnet. Eine Klärung dieser rechtssystematischen Frage speziell für das Recht der Urheber von Datenbanken stellt der Entwurf zurück. Aus dem oben im allgemeinen Abschnitt unter 1. dargestellten aktuellen rechtspolitischen Kontext geht hervor, daß diese Frage ohnehin in absehbarer Zeit in allgemeinerer Weise zur gesetzgeberischen Klärung anstehen wird.

Zu den Schranken der Rechte des Urhebers

Die Richtlinie sieht in Artikel 6 unter der Überschrift „Ausnahmen von den zustimmungsbedürftigen Handlungen" Regelungen unterschiedlichen Charakters vor: Zum einen enthält Absatz 1 Regeln über die Mindestbefugnisse des rechtmäßigen Benutzers einer Datenbank. Zum anderen befaßt sich Absatz 2 mit Ausnahmen und Beschränkungen, denen die dem Urheber in bezug auf die urheberrechtsfähige Ausdrucksform der Datenbank zustehenden ausschließlichen Rechte durch die Rechtsordnung der Mitgliedstaaten unterworfen werden können. Artikel 6 Abs. 1 der Richtlinie wird durch den vorgeschlagenen § 69k Urheberrechtsgesetz, Artikel 6 Abs. 2 der Richtlinie durch § 691 Urheberrechtsgesetz umgesetzt.

Die in Artikel 6 Abs. 3 der Richtlinie enthaltene Auslegungsrichtlinie ist sicher für die Auslegung der Umsetzungsregeln zu den vorausgehenden Absätzen von Bedeutung, bedarf aber keiner gesonderten Umsetzung. Im übrigen ist eine solche Auslegungshilfe bereits mit einem weitumfassenden urheberrechtlichen Geltungsbereich durch Artikel 13 des Übereinkommens über handelsbezogene Aspekte der Rechte des geistigen Eigentums im deutschen Recht verankert worden.

Zu § 69k (Mindestbefugnisse des rechtmäßigen Benutzers)

Der vorgeschlagene § 69k Urheberrechtsgesetz setzt den Artikel 6 Abs. 1 der Richtlinie um, der durch Artikel 15 der Richtlinie den Charakter zwingenden Vertragsrechts im Sinne eines Mindestschutzes des vertraglich berechtigten Benutzers im Verhältnis zu dem Inhaber der urheberrechtlichen Verwertungsrechte erhält.

Die Regelung steht systematisch in Beziehung zu den Vorschriften im Fünften Abschnitt des Ersten Teils über den Rechtsverkehr im Urheberrecht

Zu § 691 (Vervielfältigung zum privaten Gebrauch)

§ 691 Urheberrechtsgesetz enthält eine wichtige Spezialregelung im Verhältnis zu den Vorschriften des Sechsten Abschnitts über die Schranken des Urheberrechts. Diese trägt dem Artikel 6 Abs. 2 Buchstabe a der Richtlinie Rechnung, durch den im Umkehrschluß erkennbar wird, daß es den Mitgliedstaaten nicht erlaubt ist, eine Ausnahme vom Vervielfältigungsrecht des Urhebers einer elektronischen Datenbank für den Bereich des privaten Gebrauchs vorzusehen. Zu berücksichtigen ist allerdings, daß das Urheberrecht an der Datenbank überhaupt nur berührt wird durch solche Vervielfältigungen, aus denen die den urheberrechtlichen Schutz begründende spezifische Auswahl oder Anordnung des in der Datenbank gesammelten Inhalts ersichtlich wird.

Die übrigen im Ersten Teil des Urheberrechtsgesetzes enthaltenen Ausnahmen und Schranken sind auch im Rahmen des urheberrechtlichen Schutzes für Datenbanken anwendbar; sie sind im wesentlichen durch die Regelungsfreiräume abgedeckt, die Artikel 6 Abs. 2 Buchstaben b bis d der Richtlinie gewähren. Dabei ist wiederum in Rechnung zu stellen, daß einzelne Regelungen des Urheberrechtsgesetzes schon deswegen praktisch nicht relevant werden, weil die Verwertungsbefugnisse des Urhebers der Datenbank überhaupt nur berührt sind, soweit die urheberrechtlich schutzfähige Ausdrucksform („Auswahl oder Anordnung des Stoffes") durch die Benutzungshandlung betroffen wird.

Zu Artikel 7 Nr. 2 (Einfügung eines Sechsten Abschnitts – Schutz der Hersteller von Datenbanken)

Zu § 87a (Gegenstand des Schutzes und Verwertungsrechte)

Zu Absätzen 1 und 2

§ 87a Abs. 1, 2 Urheberrechtsgesetz setzt Artikel 7 Abs. 1, 5 der Richtlinie um.

Absatz 1 umschreibt den Schutzgegenstand, die wesentliche Investition des Datenbankherstellers. Der Begriff der Datenbank ist derselbe, der für den urheberrechtlichen Schutz einer Datenbank gilt, so daß insofern auf § 69h Urheberrechtsgesetz verwiesen werden kann. Für den Herstellerbegriff, der nicht näher definiert werden soll, ist auf Erwägungsgrund 41 hinzuweisen. Danach ist Hersteller einer Datenbank diejenige Person, die die unternehmerische Initiative zur Herstellung ergreift und das Investitionsrisiko trägt.

Schutzvoraussetzung ist, daß für die Beschaffung, die Überprüfung oder die Darstellung des Inhalts der Datenbank eine in qualitativer oder quantitativer Hinsicht wesentliche Investition getätigt worden ist. Die für die Umsetzungsregelung gewählte nähere Umschreibung lehnt sich eng an den Richtlinienwortlaut an. Aus Erwägungsgrund 40 folgt, daß die erforderliche Investition sowohl in der Bereitstellung finanzieller Mittel als auch im Einsatz von Zeit, Arbeit und Energie bestehen kann. Ob eine qualitativ oder quantitativ wesentliche Investition im Einzelfall gegeben ist, wird anhand einer wertenden Beurteilung der Schutzwürdigkeit der Investition festzustellen sein. Sowohl die Richtlinie als auch der Umsetzungsentwurf verzichten darauf, den Wesentlichkeitsbegriff zu definieren. Eine aussagekräftige abstrakte Definition erscheint nicht möglich. Es wird daher Aufgabe der Rechtsprechung sein, die unbestimmten Rechtsbegriffe auszufüllen.

Absatz 2 Satz 1 behält dem Datenbankhersteller das ausschließliche Recht der Entnahme oder Weiterverwendung wesentlicher Teile des Inhalts der Datenbank vor. Auch hier folgt der Entwurf weitgehend dem Wortlaut der Richtlinie.

Es wird darauf verzichtet, an Stelle der in der Richtlinie gewählten Begriffe der Entnahme und Weiterverwendung bei der Umsetzung auf die bekannten urheberrechtlichen Verwertungsbegriffe der Vervielfältigung, der Verbreitung und der öffentlichen Wiedergabe zurückzugreifen. Ein solcher Rückgriff hätte zwar den Vorteil, daß die Legaldefinitionen für „Entnahme" und „Weiterverwendung" (Absatz 3) und wegen § 17 Abs. 2 Urheberrechtsgesetz wohl auch die gesonderte Umsetzung der Regel über die Erschöpfung des Verbreitungsrechts (Absatz 4) entbehrlich wären. Mehrere Gründe sprechen jedoch dagegen, von der Begriffsbildung der Richtlinie abzuweichen. Der Richtliniengeber hat das – neuartige – Recht sui generis auch durch die Wahl des Wortlauts der Normen bewußt gegenüber dem Urheberrecht abgegrenzt. Die Verwendung der Richtlinienbegriffe auch im deutschen Umsetzungsgesetz fördert eine möglichst EG-weite einheitliche Auslegung der Bestimmungen zum Rechtsschutz für Datenbankhersteller. Es steht zu erwarten, daß auch in künftigen internationalen Abkommen die neuen Begriffe Entnahme und Weiterverwendung zur Anwendung gelangen werden. Und schließlich wäre eine Verwendung der urheberrechtlichen Begriffe mit der derzeit noch unentschiedenen Frage der rechtsdogmatischen Einordnung der digitalen Übermittlung in die urheberrechtlichen Verwertungsrechte (siehe dazu Begründung zu § 69i UrhG) belastet.

Das Ausschließlichkeitsrecht des Herstellers ist entsprechend den Richtlinienvorgaben darauf begrenzt, daß nur die Entnahme oder Weiterverwendung wesentlicher Teile des Inhalts der Datenbank seiner Einwilligung bedarf und von ihm untersagt werden kann. Die Nutzung unwesentlicher Teile des Inhalts unterfällt daher nicht dem Schutzrecht. Der Wesentlichkeitsbegriff ist von dem für den Schutzgegenstand maßgeblichen Terminus der wesentlichen Investition zu unterscheiden. Nach Erwägungsgrund 42 ist bei der Grenzziehung zwischen der Nutzung unwesentlicher und derjenigen wesentlicher Teile zu berücksichtigen, ob der Benutzer einen – qualitativ oder quantitativ – erheblichen Schaden für die Investition verursacht. Auch die Ausfüllung dieses Wesentlichkeitsbegriffs wird letztlich den Gerichten obliegen.

Absatz 2 Satz 2 dient der Umsetzung von Artikel 7 Abs. 5 der Richtlinie. Es wird klargestellt, daß die wiederholte und systematische Nutzung unwesentlicher Teile des Inhalts der Datenbank dem Ausschließlichkeitsrecht unterfällt. Die Norm dient dem Umgehungsschutz. In dem Umsetzungsvorschlag wird die Wortwahl der Richtlinie, „die einer normalen Nutzung der Datenbank entgegenstehen", in Anlehnung an den Text der amtlichen deutschen Übersetzung von Artikel 9 Abs. 2 der Revidierten Berner Übereinkunft zum Schutz von Werken der Literatur und Kunst modifiziert. Das steht im Einklang mit der englischen und der französischen Fassung der Datenbankenrichtlinie und entspricht § 69e Abs. 3 Urheberrechtsgesetz.

Zu Absatz 3

Absatz 3 übernimmt weitgehend wörtlich, aber Wiederholungen des Richtlinienwortlauts weglassend, die Legaldefinitionen für Entnahme und Weiterverwendung in Artikel 7 Abs. 2 der Richtlinie.

Das Entnahmerecht entspricht dem Vervielfältigungsrecht. Wird der Inhalt einer Datenbank auf dem Bildschirm sichtbar gemacht, stellt dies eine Entnahmehandlung dar, wenn die wenigstens vorübergehende Übertragung auf einen anderen Datenträger erforderlich ist (Erwägungsgrund 44). Das entspricht § 69c Nr. 1 Satz 2 Urheberrechtsgesetz.

Der Begriff der Weiterverwendung zielt vor allem auf kommerzielle Nutzungen des Inhalts einer Datenbank, erfaßt darüber hinaus aber auch alle sonstigen Fälle der öffentlichen Verfügbarmachung einer Datenbank. Der Terminus „öffentlich" dient dazu, die Kommunikation zwischen Privaten aus dem Weiterverwendungsbegriff auszuscheiden. Durch die Un-

abhängigkeit der Nutzung von Mittel und Form werden auch künftige, heute noch unbekannte Formen der Entnahme und Weiterverwendung erfaßt.

Zu Absatz 4

Durch Absatz 4 Satz 1 wird Artikel 7 Abs. 2 Buchstabe b Satz 2 der Richtlinie umgesetzt. Der Wortlaut des Entwurfs folgt den parallelen Regelungen in §§ 17 Abs. 2, 69c Nr. 3 Urheberrechtsgesetz. Die Erschöpfung, also der Verbrauch des ausschließlichen Verbreitungsrechts, gilt nur bei Veräußerung von Vervielfältigungsstücken. Sie gilt nicht im Fall der Online-Übermittlung. Erwägungsgrund 43 stellt das klar. Dann erschöpft sich das Recht, die Weiterverwendung zu untersagen, auch nicht im Hinblick auf ein vom Empfänger der Online-Übermittlung mit Zustimmung des Rechtsinhabers angefertigtes physisches Vervielfältigungsstück. Der Rechtsinhaber kann in diesem Fall die Weiterverbreitung des Vervielfältigungsstückes also dinglich kontrollieren.

Artikel 7 Abs. 2 Satz 3 der Richtlinie bestimmt, daß der öffentliche Verleih weder Entnahme noch Weiterverwendung ist. Damit soll klargestellt werden, daß die Rechtsstellung des Datenbankherstellers hinsichtlich des öffentlichen Verleihs, also der Gebrauchsüberlassung von Vervielfältigungsstücken einer Datenbank durch der Öffentlichkeit zugängliche Einrichtungen (vgl. § 27 Abs. 2 Satz 2 UrhG), nicht harmonisiert ist. Zumindest sind die Mitgliedstaaten frei darin zu entscheiden, ob dem Datenbankhersteller eine Vergütung für den öffentlichen Verleih zusteht.

Der Entwurf entscheidet sich in Absatz 4 Satz 2 für eine Regelung, die derjenigen für die Leistungsschutzrechte der Tonträgerhersteller (§ 85 Abs. 3 UrhG) und der Filmhersteller (§ 94 Abs. 4 UrhG) entspricht. Für den Verleih von Vervielfältigungsstücken einer Datenbank, deren Weiterverbreitung gemäß § 87a Abs. 4 Satz 1 Urheberrechtsgesetz zulässig ist, ist danach dem Hersteller eine angemessene Vergütung zu zahlen. Solange dagegen das Verbreitungsrecht mangels Erschöpfung noch besteht, soll es dabei verbleiben, daß auch der öffentliche Verleih von Datenbanken dem Ausschließlichkeitsrecht des Herstellers unterfällt.

Zu Absatz 5

Die Regelung stellt in Umsetzung von Artikel 7 Abs. 3 der Richtlinie klar, daß das Schutzrecht des Datenbankherstellers übertragen werden kann.

Zu Absatz 6

Diese Unberührtheitsklausel stellt, Artikel 7 Abs. 4 der Richtlinie folgend klar, daß das neue Schutzrecht kumulativ neben anderweitige Schutzinstrumente tritt. Hinzuweisen ist in diesem Zusammenhang auch auf Artikel 13 der Richtlinie, der ausdrücklich festlegt, daß anderweitige nationale Rechtsvorschriften, die (auch) Datenbanken betreffen, weiterhin anwendbar bleiben. Einer besonderen Umsetzung bedarf diese Regelung, die allgemeinen Rechtsgrundsätzen entspricht, nicht.

Zu § 87b (Schranken des Schutzes des Herstellers)

Artikel 9 der Richtlinie räumt den Mitgliedstaaten die Möglichkeit ein, die Befugnisse des Datenbankherstellers aus dem ihm gewährten Schutzrecht zugunsten bestimmter einzelner privater und allgemeiner Interessen einzuschränken. Da anders als nach Artikel 6 Abs. 2 Buchstabe d der Richtlinie Ausnahmen entsprechend traditionellem nationalem Recht nicht möglich sind, reichen die von der Richtlinie im Bereich des Rechts sui generis zugelassenen Schranken nicht so weit wie diejenigen, die das Urheberrecht zuläßt (siehe schon oben Allgemeines 3.d). Der Schrankenregelung für das Recht sui generis liegt insbesondere auch der Gedanke zugrunde, Ausnahmen zugunsten von Nutzungen im Rahmen kommerzieller Zwecke in keinem Fall zu ermöglichen (Erwägungsgrund 50).

Der Entwurf schöpft die von der Richtlinie eröffneten Möglichkeiten aus, Ausnahmen vom neuen Datenbankschutzrecht festzuschreiben, soweit entsprechende Schranken für das Urheberrecht bestehen. Das dient dem Gleichklang zwischen Urheber- und neuem Leistungsschutzrecht und ist gerechtfertigt, weil die die Schranken des Urheberrechts begründenden Interessenwertungen, die den Schutz der Urheber von Datenbanken mit demjenigen der Datenbankbenutzer ausbalancieren, in gleicher Weise im Verhältnis zwischen Datenbankhersteller und Datenbankbenutzer gelten.

Die intendierte Parallelität der Schrankenregelungen führt zu dem Vorschlag, von der durch Artikel 9 Buchstabe b der Richtlinie gegebenen Option, das Schutzrecht zugunsten der Veranschaulichung des Unterrichts einzuschränken, keinen Gebrauch zu machen. Die geltende entsprechende Regelung in § 53 Abs. 3 Nr. 1 Urheberrechtsgesetz, die nach dem Entwurf auch für den urheberrechtlichen Schutz von Datenbanken gilt (vgl. § 69i Abs. 1 UrhG), läßt Vervielfältigungen für den Schulgebrauch nur zu, soweit es um kleine Teile eines Druckwerkes oder um einzelne Beiträge aus Zeitungen oder Zeitschriften geht. Die Vervielfältigung größerer Teile oder mehrerer Beiträge ist dagegen nur mit Zustimmung des Rechtsinhabers erlaubt. Für die dem entsprechende Entnahme wesentlicher Teile des Inhalts einer Datenbank soll dasselbe gelten. Die Entnahme unwesentlicher Teile des Inhalts einer Datenbank ist – auch für den Schulgebrauch – im Rahmen des 87d Abs. 1 Urheberrechtsgesetz zulässig.

Zu Absatz 1

Nach Absatz 1 Nr. 1, mit der Artikel 9 Buchstabe a der Richtlinie umgesetzt wird, wird die Entnahme zu privaten Zwecken privilegiert. Das gilt allerdings, den Vorgaben der Richtlinie folgend, nur für die Nutzung nichtelektronischer Datenbanken. Die Norm entspricht § 69l Urheberrechtsgesetz.

Absatz 1 Nr. 2 setzt Artikel 9 Buchstabe b, 2. Alternative der Richtlinie um. Zulässig ist danach die Entnahme wesentlicher Teile des Inhalts einer Datenbank zu Zwecken der wissenschaftlichen Forschung (vgl. Erwägungsgründe 36 und 50). Die Schranke entspricht § 53 Abs. 2 Nr. 1 Urheberrechtsgesetz, wo-

bei aber stets eine Quellenangabe erforderlich ist. Diese Abweichung gegenüber § 63 Urheberrechtsgesetz ist durch die Richtlinie bedingt.

Absatz 1 Nr. 3 setzt Artikel 9 Buchstabe c der Richtlinie um und entspricht der Schranke zugunsten Rechtspflege und öffentlicher Sicherheit gemäß § 45 Urheberrechtsgesetz.

Sämtliche Ausnahmen gelten nur im Verhältnis zum rechtmäßigen Benutzer einer, so der Richtlinienwortlaut, der Öffentlichkeit – in welcher Weise auch immer – zur Verfügung gestellten Datenbank. Diese Begriffsbildung dürfte im wesentlichen mit der Legaldefinition des § 6 Abs. 1 Urheberrechtsgesetz für den urheberrechtlichen Veröffentlichungsbegriff in Einklang stehen. Deshalb lehnt sich der Gesetzentwurf an den Sprachgebrauch des § 6 Urheberrechtsgesetz an.

Zu Absatz 2

Absatz 2 enthält durch die Verweisung auf §§ 54 ff. Urheberrechtsgesetz eine Vergütungsregelung für Fälle gesetzlich erlaubter Vervielfältigung/Entnahme, wie sie auch für andere Leistungsschutzberechtigte, nämlich den Tonträgerhersteller (§ 85 Abs. 3 UrhG) und den Filmhersteller (§ 94 Abs. 4 UrhG), gilt. Danach partizipieren die Datenbankhersteller an der Geräte-, Leerkassetten-, Ablichtungs- und Betreibervergütung und erhalten dadurch einen Ausgleich für die finanziellen Nachteile, die ihnen durch die erlaubte Entnahme zum privaten Gebrauch und zum eigenen wissenschaftlichen Gebrauch gemäß § 87b Abs. 1 Nr. 1 und 2 Urheberrechtsgesetz erwachsen.

Die Datenbankenrichtlinie steht einer solchen Vergütungsregelung nicht entgegen. Es steht den Mitgliedstaaten frei, darüber zu entscheiden, in welchem Umfang sie von den von der Richtlinie eröffneten Möglichkeiten Gebrauch machen wollen, das Schutzrecht des Datenbankherstellers zu beschränken. Die Richtlinie ließe eine Beschränkung des Herstellerrechts auch ohne Vergütungsregelung zu. Als im Vergleich hiermit weniger weitgehende Regelung ist eine Beschränkung gegen Vergütung von Artikel 9 der Richtlinie gedeckt.

Die privaten und wissenschaftlichen Interessen, die die freie Entnahmemöglichkeit und die damit verbundene Einschränkung der Herstellerrechte rechtfertigen, erfordern es nicht, eine unentgeltliche Nutzung von Datenbanken zu erlauben. Die infolge der Weitergabe über den Preis wirtschaftlich letztlich den Benutzer belastende Geräte-, Leerkassetten-, Ablichtungs- und Betreibervergütung führt zu einem angemessenen Ausgleich zwischen dem besonders geschützten Nutzungsinteresse beim privaten und sonstigen eigenen Gebrauch und den berechtigten finanziellen Interessen des investierenden Datenbankherstellers, der in seinem Vergütungsinteresse durch Artikel 14 des Grundgesetzes geschützt wird. Wie Urheber und Leistungsschutzberechtigte sollen daher auch Datenbankhersteller einen finanziellen Ausgleich dafür erhalten, daß ihr Ausschließlichkeitsrecht in den Fällen des § 87b Abs. 1 Nr. 1, 2 Urheberrechtsgesetz zugunsten anderer Interessen eingeschränkt wird.

Zu § 87c (Schutzdauer)

Absatz 1 setzt die Richtlinienregelung des Artikels 10 über die fünfzehnjährige Schutzdauer für das neue Datenbankschutzrecht um. Dem Ziel des Investitionsschutzes entsprechend orientiert sich die Frist am angenommenen regelmäßigen Amortisationszeitraum. Der Lauf der Schutzfrist beginnt mit dem Abschluß der Herstellung. Wird die Datenbank während der Fünfzehnjahresfrist, die auf den Zeitpunkt des Herstellungsabschlusses folgt, erstmals der Öffentlichkeit zur Verfügung gestellt (siehe dazu Begründung zu § 87b UrhG), verlängert sich die Schutzdauer. Der Schutz endet dann erst fünfzehn Jahre nach dem Zeitpunkt, in dem die Datenbank erstmals der Öffentlichkeit zugänglich gemacht worden ist.

Von großer praktischer Bedeutung ist es, daß jede wesentliche Änderung des Inhalts der Datenbank, die eine wesentliche Neuinvestition darstellt, eine eigene fünfzehnjährige Schutzdauer begründet. Das regelt Absatz 2 des Entwurfs, mit dem Artikel 10 Abs. 3 der Richtlinie umgesetzt wird. Eine wesentliche Neuinvestition, deren Voraussetzungen der Hersteller zu beweisen hat, kann allein schon in einer eingehenden Überprüfung des Inhalts einer Datenbank liegen (Erwägungsgründe 54, 55). Fortlaufend aktualisierte Datenbanken, also insbesondere informationelle Online-Datenbanken, können damit für ihre jeweils neueste Fassung einen nicht endenden Schutz erlangen.

Zu § 87d (Rechte und Pflichten des rechtmäßigen Benutzers)

Zu Absatz 1

Die Vorschrift setzt Artikel 8 Abs. 1 in Verbindung mit Artikel 15 der Richtlinie um.

Die Richtlinie verpflichtet dazu, einen Mindestschutz für den rechtmäßigen Benutzer einer der Öffentlichkeit zur Verfügung gestellten (siehe Begründung zu § 87b UrhG) Datenbank vorzusehen, der als zwingendes Recht auszugestalten ist und daher auch durch vertraglich vom Rechtsinhaber auferlegte Nutzungsbedingungen nicht unterlaufen werden kann. Die garantierten Endbenutzerrechte sind im Interesse der Zugangsmöglichkeit zu Informationen weitreichend. Der rechtmäßige Benutzer muß in jedem Fall unwesentliche Teile des Inhalts der Datenbank zu beliebigen Zwecken entnehmen und weiterverwenden können.

Der zwingende Schutz des rechtmäßigen Benutzers einer Datenbank bildet ein Gegengewicht zu der durch das neue Schutzrecht gestärkten Position des Datenbankherstellers, dessen Befugnisse gegenüber dem rechtmäßigen Benutzer darauf beschränkt bleiben sollen, die Nutzung wesentlicher Teile des Inhalts der Datenbank zu untersagen.

Der Umsetzungsvorschlag verdeutlicht, daß es bei den zu regelnden Rechten des rechtmäßigen Benut-

zers nicht um den Inhalt des dem Hersteller zustehenden dinglichen Ausschließlichkeitsrechts geht, sondern um die jenseits dieses Rechts bestehenden Grenzen für vertragliche Vereinbarungen zwischen Datenbankhersteller und -benutzer im Interesse des Schutzes der Benutzer.

Eine ausdrückliche Umsetzung von Artikel 8 Abs. 1 Satz 2 der Richtlinie, durch den klargestellt wird, daß die Rechte des rechtmäßigen Benutzers zur Nutzung unwesentlicher Teile des Inhalts der Datenbank auf den Teil der Datenbank beschränkt sind, für den die Zugangsberechtigung besteht, erscheint nicht erforderlich. Diese Eingrenzung des Rechts ergibt sich bereits daraus, daß nur zugunsten des berechtigten Benutzers Rechte gesichert werden. Im Hinblick auf Teile der Datenbank, für die keine Zugangsberechtigung besteht, ist ein Benutzer nicht „berechtigt" und daher auch nicht befugt, unwesentliche Teile des Inhalts der Datenbank zu entnehmen oder weiterzuverwenden.

Zu Absatz 2

Die Vorschrift dient der Umsetzung von Artikel 8 Abs. 2 der Richtlinie. Zu dem dem Artikel 9 Abs. 2 der Revidierten Berner Übereinkunft zum Schutz von Werken der Literatur und Kunst entlehnten Wortlaut des Entwurfs wird auf die Begründung zu § 87a Abs. 2 Urheberrechtsgesetz verwiesen.

Zu Artikel 7 Nr. 3 (§ 96 Abs. 1 UrhG)

Die dem Schutz des Schutzrechtsinhabers für Ansprüche gegenüber Dritten dienende Vorschrift über das Verwertungsverbot soll auch für die Absicherung des neuen Schutzrechts des Datenbankherstellers gelten. Hierfür ist die Ergänzung der Norm erforderlich.

Zu Artikel 7 Nr. 4 (§ 108 Abs. 1 UrhG)

Mit der Änderung wird die Strafbestimmung ergänzt, die vorsätzliche Verletzungen der Verwertungsrechte der Inhaber der verwandten Schutzrechte mit Freiheits- bzw. Geldstrafe bedroht. Der Vorschlag geht davon aus, daß hinsichtlich des Bedarfs für eine strafrechtliche Flankierung des Rechtsschutzes das Recht des Datenbankherstellers dem eines Tonträgerherstellers oder Sendeunternehmens vergleichbar ist.

Zu Artikel 7 Nr. 5 (§ 119 Abs. 3 UrhG)

Die Änderung erstreckt die Beschränkung der Zwangsvollstreckung wegen Geldforderungen, nach der Vorrichtungen für geschützte Leistungen nur für einen nutzungsberechtigten Gläubiger gepfändet werden dürfen, auf das neue Datenbankschutzrecht.

Zu Artikel 7 Nr. 6 (Einfügung eines § 127a)

Mit der Vorschrift wird Artikel 11 der Richtlinie umgesetzt (siehe bereits oben Allgemeines 3.b und d).

Zu Absatz 1

Den Vorgaben der Richtlinie entsprechend erstreckt sich der Schutz in persönlicher Hinsicht auf Datenbanken, deren Hersteller Staatsangehöriger eines Mitgliedstaates ist oder seinen gewöhnlichen Aufenthalt im Gebiet der Europäischen Union hat. Dasselbe gilt für Personen aus den Vertragsstaaten des Abkommens über den Europäischen Wirtschaftsraum. Durch die Verweisung auf § 120 Abs. 2 Nr. 1 UrhG werden als deutsche Staatsangehörige auch Deutsche gemäß Artikel 116 Abs. 1 des Grundgesetzes geschützt.

Die Formulierung in Artikel 11 Abs. 1 der Richtlinie „oder Rechtsinhaber" ist irreführend und wird daher nicht transformiert. Wird eine in einem Drittland hergestellte Datenbank von einem Europäer erworben, besteht kein Schutz nach dem Recht sui generis für den „Rechtsinhaber". Für die in einem Drittstaat hergestellte Datenbank entsteht kein Schutz, der folglich auch nicht übertragen werden kann. Der abgeleitete Rechtserwerb als solcher begründet keinen Schutz.

Zu Absatz 2

Die Regelung, mit der Artikel 11 Abs. 2 der Richtlinie umgesetzt wird, bezieht europäische Unternehmen, die eine Datenbank hergestellt haben, in den Schutz ein. Die Schutzvoraussetzungen entsprechen denjenigen des Artikels 58 des EG-Vertrages.

Zu Absatz 3

Gemäß Artikel 11 Abs. 3 der Richtlinie kann der Rat den Rechtsschutz im Wege bilateraler oder multilateraler Vereinbarungen auf Drittstaaten ausdehnen. Absatz 3 des Entwurfs sieht daher vor, daß sich der Schutz nicht von den Absätzen 1 und 2 erfaßter Personen und Unternehmen nach dem Inhalt der Staatsverträge richtet.

Zu Artikel 7 Nr. 7 (Einfügung eines § 137h – Übergangsregelung)

Zu Absatz 1

Der Regelungsvorschlag für den zeitlichen Rechtsübergang beim Urheberrechtsschutz für Datenbanken dient der Umsetzung von Artikel 14 Abs. 1 der Richtlinie. Danach kommen auch Altdatenbanken, also solche, deren Herstellung vor dem Umsetzungsstichtag nach Artikel 16 Abs. 1 der Richtlinie (1. Januar 1998) abgeschlossen worden ist, für die Zeit von diesem Datum an in den Genuß des urheberrechtlichen Schutzes, wenn sie die neu festgelegten gesetzlichen Voraussetzungen erfüllen.

Zu Absatz 2

Die Vorschrift enthält die Übergangsregelung für das neue Schutzrecht des Datenbankherstellers. Mit ihr wird Artikel 14 Abs. 3 und 5 der Richtlinie umgesetzt. Die Regelung ergänzt § 87c Urheberrechtsgesetz über die Schutzdauer. Altdatenbanken (siehe Begründung zu Absatz 1), die den Schutzanforderun-

gen genügen, gelangen in den Schutz des neuen Rechts, wenn die Herstellung während der letzten fünfzehn Jahre vor dem Umsetzungsstichtag erfolgt ist. Artikel 14 Abs. 5 der Richtlinie folgend beginnt der Lauf der fünfzehnjährigen Schutzfrist in diesen Fällen erst am 1. Januar 1998.

Zu Artikel 8 (Änderung des Preisangabengesetzes)

Infolge des technischen Fortschritts sind neue Angebotsformen entstanden und werden noch entstehen, bei denen Angebot und fortlaufende Inanspruchnahme im engen technischen und zeitlichen Zusammenhang stehen. Auf diese Angebotsformen soll mit der Änderung eingegangen werden, um sowohl dem Verbraucherschutz zu genügen wie auch Markt- bzw. Preistransparenz in diesem neuartigen Bereich zu gewährleisten.

Zu Artikel 9 (Änderung der Preisangabenverordnung)

Der Bereich der Informations- und Kommunikationsdienste hat sich erst nach Erlaß der Preisangabenverordnung entwickelt. Aufgrund neuer Angebotsformen z. B. über Online-Dienste oder Internet ist eine Klarstellung erforderlich, die der Wahrung von Preistransparenz auch in diesem Bereich dient. Auch ein auf Bildschirm übertragenes Angebot muß mit einer Preisangabe versehen sein. Weiter zeichnet sich ab, daß fortlaufende Leistungen – sofern sie nicht durch Pauschalen als einmalige Zahlungen abgegolten werden – im Hinblick auf Verbraucherinformation nur teilweise erfaßt werden, und zwar lediglich in Form von Vorabhinweisen auf den Preis je Zeit- oder Recheneinheit. Der tatsächliche im Zuge der Inanspruchnahme der Leistung sich ergebende Preis wird jedoch nicht transparent. Diese sich aus der Weiterentwicklung der Angebotsformen ergebende Regelungslücke soll mit der Ergänzung geschlossen werden.

Da bei bestimmten Nutzungen eine Preisanzeige unter Umständen als optisch störend empfunden werden kann, soll jedoch der Verbraucher die Möglichkeit haben, auf die Anzeige zu verzichten. Um Mißverständnissen vorzubeugen, wird auf die der Systematik der Preisangabenverordnung entsprechende Unentgeltlichkeit der Preisangabe besonders hingewiesen.

Zu Artikel 10 (Rückkehr zum einheitlichen Verordnungsrang)

Um zu vermeiden, daß die im Rahmen dieses Gesetzes vorgenommenen Änderungen in der Rechtsverordnung künftig nur noch durch Gesetz, aber nicht mehr vom Verordnungsgeber späteren Erfordernissen angepaßt werden können, wird eine besondere Bestimmung vorgesehen, die dies gestattet.

Zu Artikel 11 (Inkrafttreten)

Die Inkrafttretensregel für Artikel 7 – Änderung des Urheberrechtsgesetzes – trägt dem Artikel 16 Abs. 1 der Richtlinie über den rechtlichen Schutz von Datenbanken Rechnung, wonach die Mitgliedstaaten bis zum 1. Januar 1998 die zur Umsetzung der Richtlinie erforderlichen Rechtsvorschriften zu erlassen haben.