

14.09.98**Empfehlungen
der Ausschüsse**EU - In - K - R - Wizu **Punkt** der 729. Sitzung des Bundesrates am 25. September 1998

Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über gemeinsame Rahmenbedingungen für elektronische Signaturen

KOM(98) 297 endg.; Ratsdok. 9708/98

A

Der federführende Ausschuß für Fragen der Europäischen Union (EU),
der Ausschuß für Innere Angelegenheiten (In) und
der Rechtsausschuß (R)

empfehlen dem Bundesrat, zu der Vorlage gemäß §§ 3 und 5 EUZBLG wie folgt
Stellung zu nehmen:

EU
In
R**1. Zum Richtlinienvorschlag insgesamt**

Der Bundesrat begrüßt, daß die Kommission sich mit dem Richtlinienvorschlag um eine gemeinschaftsweite Regelung der elektronischen Signatur bemüht. Angesichts weltweiter offener Netze ist es von großer Bedeutung, daß nicht innerhalb der Gemeinschaft elektronische Signaturen grundsätzlich unterschiedlich behandelt werden. Ein durchgängiges Regelungssystem ist für die wirtschaftliche Entwicklung von Bedeutung und liegt im Interesse der Verbraucher.

Im einzelnen hält der Bundesrat jedoch wesentliche Änderungen des Richtlinienvorschlags für geboten.

EU
In
R**2. Zu Artikel 2 Nummer 5**

Der Begriff des qualifizierten Zertifikats ist nicht hinreichend klar. Es ist nicht ersichtlich, durch welche Merkmale sich ein qualifiziertes von einem nicht qualifizierten Zertifikat unterscheiden soll. Im Hinblick auf die Rechtsfolgen der

Ausgeliefert am 15. SEP. 1998

Vertrieb: Bundesanzeiger Verlagsgesellschaft mbH, Postfach 1320, 53003 Bonn
Telefon: 0228/3820840, Telefax 0228/3820844
ISSN 0720-2946

— 1 —

Unterscheidung (insbesondere Artikel 5 Abs. 2 und Artikel 6) ist jedoch eine eindeutige Abgrenzung im Text der Richtlinie unabweisbar.

EU
in
R

3. Zu Artikel 3 Abs. 1 und 2

Zertifizierungsdienste werden für das Funktionieren eines fortgeschrittenen elektronischen Rechtsverkehrs von großer Bedeutung sein, insbesondere hinsichtlich der Gewährleistung der Authentizität und Integrität elektronischer Erklärungen. Dabei ist vor allem von Bedeutung, daß die Teilnehmer am Rechtsverkehr den Zertifikaten und damit den elektronischen Signaturen vertrauen können. Da die Empfänger elektronischer Signaturen die Stelle, die das zugehörige Zertifikat ausgestellt hat, nicht selbst auswählen können, sondern mit einer Leistung konfrontiert werden, die der Absender der Signatur mit der Zertifizierungsstelle vereinbart hat, fehlt den Empfängern eine eigene Grundlage, um dem Zertifikat zu vertrauen.

Angesichts dieser zwangsläufigen Konstellation begegnet es gravierenden Bedenken, wenn durch Artikel 3 Abs. 1 die vorherige Genehmigung von Zertifizierungsdiensten ausgeschlossen werden soll. Nur durch eine vorherige Genehmigung der Tätigkeit von Zertifizierungsdienste-Anbietern kann sichergestellt werden, daß diese den an sie gestellten Anforderungen gerecht werden. Da ein legitimes öffentliches Interesse daran besteht, daß nur kompetente und vertrauenswürdige Anbieter auf dem Markt tätig werden, müssen die Mitgliedstaaten in die Lage versetzt werden, im Rahmen eines Genehmigungsverfahrens und in der Folgezeit durch Aufsichtsmaßnahmen gegenüber der Öffentlichkeit zu gewährleisten, daß das in Anspruch genommene Vertrauen gerechtfertigt ist. Im Interesse des Wettbewerbs mag dabei das Prinzip des Absatzes 2 Satz 3 zugrunde gelegt werden.

Die in Absatz 2 vorgesehene Möglichkeit, "freiwillige Akkreditierungssysteme" zu schaffen, kann die gegen Absatz 1 bestehenden Bedenken nicht ausräumen, weil der Richtlinienvorschlag hierin nicht den Normalfall sieht und die Gesamtregelung der Richtlinie auf die Tätigkeit von Anbietern abstellt, die nicht der Genehmigung bedarf. Im übrigen ist auch der Inhalt der Regelung in Absatz 2 Satz 1 und 2 recht unbestimmt. Diese Vorschrift überläßt nahezu alles den Mitgliedstaaten. Dabei wäre es gerade auch für höherwertige Zertifizierungsdienste wichtig, daß sie einheitlichen Regeln unterworfen würden, die nicht an den Grenzen der Mitgliedstaaten enden.

In jedem Fall müssen die Mitgliedstaaten im Interesse der Sicherheit des Rechtsverkehrs die effektive Möglichkeit haben, Diensteanbietern, die sich in ihrer Tätigkeit als nicht hinreichend zuverlässig erwiesen haben, das weitere Tätigwerden zu unterbinden.

EU
In
R

4. Zu Artikel 3 Abs. 3

Der Bundesrat hält es nicht für vertretbar, daß die Kommission die Normen festlegen soll, die das Sicherheitsniveau für die Zertifizierung elektronischer Signaturen bestimmen. Die Existenz des Ausschusses nach Artikel 9 kann eine hinreichende Beteiligung der Mitgliedstaaten nicht bewirken, weil der Ausschuß nur beratende Funktion haben soll, weil er seine Auffassung mit einfacher Mehrheit festlegt und weil die Kommission ohne weiteres über die Stellungnahme des Ausschusses hinweggehen kann.

Nach Auffassung des Bundesrates können die Sicherheitsnormen nur in der Richtlinie selbst oder in einem Verfahren festgelegt werden, das den Mitgliedstaaten hinreichenden Einfluß auf die Entscheidung gibt.

EU
In
R

5. Zu Artikel 4

Der Bundesrat befürwortet das dem Artikel zugrunde liegende Prinzip, daß die Anbieter von Zertifizierungsdiensten in allen Mitgliedstaaten nach einheitlichen Regeln sollen tätig werden dürfen. Daß alle Anbieter nach den Regeln ihres Sitzstaates in der gesamten Gemeinschaft sollen tätig werden dürfen, ist jedoch nicht vertretbar, solange nicht durch die Richtlinie sichergestellt wird, daß in allen Mitgliedstaaten die Tätigkeit der Anbieter in ausreichendem Maße überwacht wird.

EU
In
R

6. Zu Artikel 5

Der Bundesrat geht davon aus, daß die Regelung in Absatz 1, die nicht ein qualifiziertes Zertifikat voraussetzt, lediglich für den formfreien Rechtsverkehr die Gültigkeit rechtsgeschäftlicher Erklärungen bestimmen will, die mittels einer elektronischen Signatur abgegeben werden. Gegen eine solche Regelung bestehen keine Bedenken, weil es dem Charakter formfreier Erklärungen entspricht, daß sie in jeglicher Form abgegeben werden können, auch in elektronischer Form, sei es mit, sei es ohne elektronische Signatur. Dieser Inhalt der Bestimmung sollte allerdings deutlicher zum Ausdruck gebracht werden. Weder aus dem Text der Richtlinie noch aus den Erwägungsgründen (Nummer 10) oder aus der Begründung (Abschnitt III Nr. 6 – Seite 6 –) ist sicher zu entnehmen, daß nur der formfreie Rechtsverkehr gemeint ist.

Elektronische Signaturen werden zunächst vor allem im formfreien Rechtsverkehr praktische Bedeutung erlangen. Es wird sich allerdings auch das Bedürfnis ergeben, elektronische Signaturen darüber hinaus für bestimmte Erklärungen zuzulassen, in denen das Recht der einzelnen Mitgliedstaaten bislang die handschriftliche Unterzeichnung verlangt. Zu Recht greift der Richtlinienvorschlag deshalb in Absatz 2 dieses Thema auf. Es ist auch zu begrüßen, daß der Vor-

schlag insoweit von vornherein nur elektronische Signaturen mit qualifizierten Zertifikaten in Betracht zieht. Grundsätzliche Bedenken bestehen aber dagegen, daß solche elektronischen Signaturen unterschiedslos mit der handschriftlichen Unterzeichnung gleichgestellt werden sollen. Elektronische Signaturen können nicht in jeder Hinsicht dieselbe Funktion erfüllen wie die handschriftliche Unterzeichnung. Sie können zwar – einen ausreichenden Sicherheitsstandard und die Vertrauenswürdigkeit der Zertifizierungsdienste vorausgesetzt – hinreichend gewährleisten, daß die Erklärung nicht gefälscht und nicht verändert ist; unter Umständen bieten sie insofern sogar größere Sicherheit als handschriftlich gezeichnete Dokumente. Aber schon die Authentizität ist nur mit Einschränkungen gesichert, weil die Gefahr besteht, daß eine Chipkarte mit dem geheimen Schlüssel und die zugehörige PIN-Nummer z.B. innerhalb eines Unternehmens an Mitarbeiter weitergegeben wird und daß die elektronische Signatur dann für nicht autorisierte Erklärungen benutzt wird. Im Gegensatz zur herkömmlichen Schriftform kann die elektronische Signatur eine Warnfunktion nicht übernehmen und einen Schutz vor Übereilung nicht bieten. Die Leichtigkeit, Schnelligkeit und Flüchtigkeit des Vorgangs der elektronischen Signierung kann einem sorgfältigen Überdenken der zu treffenden Entscheidung entgegenstehen. Wenn die technischen Abläufe die Aufmerksamkeit der erklärenden Person stark in Anspruch nehmen, fehlt es möglicherweise an Konzentration für den Inhalt einer Willenserklärung und für deren wirtschaftliche Bedeutung. Allgemein muß davon ausgegangen werden, daß Text, der auf dem Bildschirm erscheint, weniger intensiv wahrgenommen wird als Text, der auf Papier geschrieben ist. Wenn die Person, die eine Erklärung abzugeben hat, weniger geübt ist mit elektronischen Texten und elektronischen Signaturen, wird das die Wahrscheinlichkeit unbesonnener Erklärungen noch steigern.

Im übrigen stellt es ein Problem dar, wenn die Gleichstellung der elektronischen Signatur davon abhängen soll, daß es sich um ein qualifiziertes Zertifikat nach Anhang I der Richtlinie handelt und daß es von einem Zertifizierungsdiensteanbieter erteilt ist, der den Anforderungen in Anhang II genügt. Ob dies der Fall ist, kann der Empfänger der Signatur schwerlich erkennen; letztlich kann es im Streitfall erst von den Gerichten verbindlich entschieden werden.

Hinzu kommt, daß eine elektronische Signatur zwar möglicherweise die Beweisfunktion ebenso gut übernehmen kann wie ein handschriftlich unterzeichnetes Dokument, daß im Streitfall aber zur Handhabung des Beweises unter Umständen in erheblichem Umfang sachverständige Unterstützung notwendig ist, so daß der Beweis nur mit erheblich höherem Aufwand und nicht für jedermann augenfällig erbracht werden kann.

Angesichts solcher Unterschiede zwischen elektronischer Signatur und handschriftlicher Unterzeichnung verbietet sich eine schematische Gleichstellung. Sachgerecht ist es vielmehr, für jede einzelne Norm, die die Schriftform vorschreibt, den zugehörigen Sachverhalt sorgfältig darauf zu untersuchen, welche

Aufgabe die Formvorschrift hat und inwieweit die handschriftliche Unterzeichnung durch eine elektronische Signatur ersetzt werden kann. Da die Rechtsordnungen der einzelnen Mitgliedstaaten in unterschiedlicher Weise für bestimmte Erklärungen die handschriftliche Unterzeichnung vorsehen, kann diese Aufgabe nur jeweils gesondert von den Mitgliedstaaten geleistet werden, nicht in einer pauschalen Regelung der Gemeinschaft. Die Regelung des Absatzes 2 kann deshalb in der vorgesehenen Form keinen Bestand haben. Allenfalls kann sie durch eine Aufforderung an die Mitgliedstaaten ersetzt werden, geltende Formvorschriften darauf zu überprüfen, inwieweit die elektronische Signatur die handschriftliche Unterzeichnung ersetzen kann.

Als nicht akzeptabel sieht es der Bundesrat an, wenn in Absatz 2 außerdem gefordert werden soll, daß in Gerichtsverfahren die elektronische Signatur mit qualifiziertem Zertifikat in gleicher Weise wie handschriftliche Unterschriften als Beweismittel zugelassen wird. Es ist zwar zweifelsfrei, daß elektronische Dokumente mit elektronischer Signatur als Beweismittel in Gerichtsverfahren möglich sein müssen. Eine Gleichbehandlung mit handschriftlich unterzeichneten Urkunden verbietet sich aber angesichts der tatsächlich bestehenden Unterschiede. Wenn nach deutschem Verfahrensrecht mit einer privaten Urkunde der Beweis erbracht wird, daß der Aussteller der Urkunde die betreffende Erklärung abgegeben hat, so ist bei elektronischen Signaturen der entsprechende Schluß nicht gerechtfertigt. Mit der Tatsache, daß ein elektronisches Dokument eine digitale Signatur trägt, die einer bestimmten Person zusteht, kann nicht bewiesen werden, daß diese Person das Dokument mit der digitalen Signatur versehen hat, da es ebenso möglich ist, daß der geheime Schlüssel (die Chipkarte) im Besitz einer anderen Person war, die auch über die zugehörige PIN verfügte. Schon aus diesem Grunde wäre eine vollständige und formale Gleichbehandlung der elektronischen Signatur mit der handschriftlichen Unterschrift im Beweisrecht nicht vertretbar. Unter Berücksichtigung der bestehenden Unterschiede zur handschriftlichen Unterschrift und im Hinblick auf den für die Beurteilung erforderlichen EDV-Sachverstand können elektronisch signierte Dokumente nur Gegenstand einer freien Beweiswürdigung sein. Von der vorgesehenen formalen Gleichstellung durch die Richtlinie muß abgesehen werden.

EU
In
R

7. Zu Artikel 6

Der Bundesrat begrüßt, daß die Mitgliedstaaten durch die Richtlinie verpflichtet werden sollen, eine Haftungsregelung für qualifizierte Zertifikate einzuführen. Der Bundesrat erinnert in diesem Zusammenhang daran, daß er in seiner Entschließung vom 4. Juli 1997 zum Informations- und Kommunikationsdienstesgesetz (BR-Drucksache 420/97 (Beschluß)) die Bundesregierung unter anderem aufgefordert hat, unverzüglich auf eine Änderung des Signaturgesetzes hinzuwirken, mit der eine spezifische Haftungsregelung für Schäden eingeführt wird, die Dritten durch die Tätigkeit von Zertifizierungsstellen entstehen. Der Bundesrat ist unverändert der Auffassung, daß die Anbieter von Zertifizierungs-

diensten auch gegenüber Dritten, insbesondere den Empfängern von elektronischen Signaturen, gesetzlich haften müssen, wenn das für den elektronischen Rechtsverkehr notwendige Vertrauen entstehen soll, und daß insoweit eine spezielle Haftungsregelung geschaffen werden muß, um Zweifel an der Reichweite der Haftung zu vermeiden und um Haftungslücken gar nicht erst entstehen zu lassen. Im Hinblick darauf, daß die Diensteanbieter ihre Leistungen ungehindert in allen Mitgliedstaaten sollen erbringen dürfen (Artikel 4), erscheint es geboten, eine hinreichend konkrete gemeinschaftsrechtliche Norm zu schaffen.

Artikel 6 des Richtlinienvorschlags stellt eine grundsätzlich geeignete Vorschrift zur Festlegung des Rahmens dar, in dem die Mitgliedstaaten eine Haftung der Diensteanbieter zu schaffen haben. Die Abgrenzung des Haftungstatbestandes in Artikel 6 Abs. 1 Buchstabe a bis d ist allerdings zu eng und erfaßt nicht alle denkbaren Verhaltensweisen von Diensteanbietern, die zu Schäden führen können. So wird eine Haftung etwa für folgende Fehler von Diensteanbietern nicht vorgeschrieben:

- Der geheime Schlüssel und die PIN werden unbefugt Dritten offenbart.
- Die Chipkarte mit dem geheimen Schlüssel und die PIN werden irrtümlich statt an den Schlüsselinhaber einer dritten Person ausgehändigt.
- Das öffentliche Verzeichnis der erstellten Zertifikate wird nicht ordnungsmäßig geführt, erteilte Zertifikate oder erfolgte Sperrungen werden nicht eingetragen.

Derartige Fehlleistungen, die Schäden verursachen können, werden von Artikel 6 Abs. 1 Buchstabe b nicht erfaßt, weil die Richtlinie im Anhang II nur grundsätzliche Anforderungen an die Qualität des Zertifizierungsdienstes festlegt, nicht aber konkrete Handlungspflichten: Ein einmaliges pflichtwidriges Verhalten, das einen Schaden verursacht, kann auch einem Diensteanbieter unterlaufen, der alle Voraussetzungen des Anhangs II erfüllt.

Vorgeschrieben werden sollte also eine Haftung für die Verletzung von Pflichten, die den Diensteanbietern aufgrund der gesetzlichen Regelung oder aufgrund des Vertrages mit dem Unterzeichner obliegen.

Andererseits wird der Kreis der Begünstigten vom Richtlinienvorschlag nicht hinreichend eingegrenzt. Das Merkmal "jede Person, die vernünftigerweise auf das Zertifikat vertraut", ist zu wenig faßbar und kann auch Personen einbeziehen, die keine unmittelbare Beziehung zu dem betroffenen elektronischen Rechtsgeschäft haben. Wenn es, wie hier, um eine Haftung für reine Vermögensschäden geht, sollten nur die unmittelbar Beteiligten anspruchsberechtigt sein. Das könnten die Empfänger der elektronischen Signatur sein.

Bedenken bestehen dagegen, daß die Haftungsregelung auf qualifizierte Zertifikate beschränkt werden soll. Qualifizierte Zertifikate werden zwar in einem bedeutsamen Bereich der elektronischen Signatur angewendet werden. Auch der

sonstige Bereich der elektronischen Signatur wird aber von nicht geringer wirtschaftlicher Bedeutung sein, und auch dort werden Teilnehmer des Rechtsverkehrs darauf angewiesen sein, auf eine elektronische Signatur und das zugehörige Zertifikat zu vertrauen. Auch in diesem Tätigkeitsfeld wäre es nicht angemessen, wenn die Diensteanbieter für ihre Tätigkeit nicht haften. Da nicht davon ausgegangen werden kann, daß sich eine solche Haftung in allen Mitgliedstaaten bereits aus allgemeinen Normen ergibt, müssen alle Diensteanbieter, die Signaturdienste erbringen, in die Haftungsregelung einbezogen werden.

Aufgrund der Vorschrift des Artikels 6 Abs. 2 geht der Bundesrat davon aus, daß der Richtlinienvorschlag eine Verschuldenshaftung vorschreiben, aber dem Diensteanbieter die Beweislast für ein fehlendes Verschulden aufbürden will. Er geht weiter davon aus, daß für das Verschulden von Hilfspersonen in gleicher Weise wie bei einer vertraglichen Haftung einzustehen sein soll. Der Bundesrat hält dies für angemessen: Eine uneingeschränkte Gehilfenhaftung ist geboten, weil für den Rechtsverkehr nur so die nötige Sicherheit entsteht, und die Beweislast muß den Diensteanbieter treffen, weil Fehler sich in seinem Verantwortungsbereich ergeben. Beides sollte allerdings in Absatz 2 eindeutiger zum Ausdruck gebracht werden.

Zu begrüßen ist es, daß Diensteanbieter gemäß Absatz 3 und 4 die Möglichkeit bekommen sollen, die Wirkung ihrer Zertifikate auf bestimmte Anwendungsbereiche und bestimmte Transaktionen zu beschränken. Die Anbieter können damit ihr Risiko sachgerecht begrenzen. Das nutzt zugleich den Unterzeichnern, für die sich diese Möglichkeit im Preis günstig auswirken wird. Darüber hinaus muß aber geregelt werden, ob die Diensteanbieter die Haftung für ihre Zertifikate sollen betragsmäßig begrenzen dürfen. Eine Beschränkung der Haftung auf einen bestimmten Betrag wäre eine zusätzliche Möglichkeit, die sich nicht bereits aus der Begrenzung des Wertes der Transaktion ergibt. Auch eine solche Haftungsbeschränkung dient der angemessenen Begrenzung des Risikos für den Anbieter und wird sich zugleich preissenkend auswirken.

Es muß allerdings in der Richtlinie sichergestellt werden, daß Haftungsbeschränkungen der Höhe nach und Beschränkungen nach Artikel 6 Abs. 3 und 4 dem Publikum leicht erkennbar und zweifelsfrei mitgeteilt werden. Die Aussage hierzu im 13. Erwägungsgrund reicht nicht aus. Es ist vielmehr eine Bestimmung im operativen Teil der Richtlinie erforderlich. Dabei müßte bestimmt werden, daß derartige Beschränkungen der Haftung den Anspruchsberechtigten gegenüber nur geltend gemacht werden können, sofern sie im Zertifikat selbst enthalten sind. Wenn der Rechtsverkehr auf Zertifikate vertrauen soll, muß es den Adressaten elektronischer Signaturen möglich sein, sich aus dem Zertifikat selbst über Grenzen der Haftung zu informieren. Den Nutzern sollte nicht zugemutet werden, anderswo zusätzliche Informationen einzuholen. Die Eigenart elektronischer Zertifikate ermöglicht es ohne weiteres, daß sie derartige Informationen enthalten. Die Diensteanbieter werden damit nicht in unzumutbarer Weise belastet.

Artikel 6 muß um eine Regelung über eine ausreichende Deckungsvorsorge ergänzt werden. Der Bundesrat erinnert insoweit daran, daß er in seiner Entschlie-ßung vom 4. Juli 1997 (BR-Drucksache 420/97 (Beschluß)) für das deutsche Recht eine entsprechende Vorschrift gefordert hat. Es ist zwar zu begrüßen, daß in Anhang II Buchstabe g dieser Gesichtspunkt als Anforderung an Zertifizierungsdiensteanbieter erwähnt wird. Dies reicht jedoch nicht aus. Es muß in den Formen der Richtlinie näher festgelegt werden, welche Anforderungen an eine ausreichende Deckungsvorsorge zu stellen sind. Dies kann nicht den nationalen Rechtsvorschriften überlassen bleiben. Es wäre sonst zu befürchten, daß Diensteanbieter ihren Sitz vornehmlich in solchen Mitgliedstaaten begründen, die geringe Anforderungen an die Deckungsvorsorge stellen. Durch Festlegung in der Richtlinie kann dagegen vermieden werden, daß sich Unterschiede in der Deckungsvorsorge wettbewerbsverzerrend auswirken.

EU
In
R

8. Zu Artikel 7

Angeichts des Umstandes, daß elektronische Signaturen in weltumspannenden offenen Netzen eingesetzt werden, mißt der Bundesrat der internationalen Anerkennung elektronischer Signaturen große Bedeutung bei. Er hat allerdings Zweifel, ob dieses Ziel im Rahmen des Absatzes 1 mit dem Maßstab des Regelwerks der Gemeinschaft verwirklicht werden kann. Er geht vielmehr davon aus, daß insoweit nur internationale Vereinbarungen Entscheidendes bewirken können.

EU
In

9. Zu Artikel 8

In Artikel 8 Datenschutz werden Regelungen getroffen, die hinter dem derzeit in Deutschland geltenden Recht (Signaturgesetz) zurückbleiben. Danach ist die Offenbarung der Identität von Personen, die Pseudonyme verwenden, an Behörden grundsätzlich nur mit Zustimmung der Betroffenen vorgesehen. Ohne Zustimmung des Betroffenen ist eine Offenbarung nur zur Aufklärung von Straftaten zugelassen. Die Formulierung erweckt den Eindruck, daß die Offenbarung für Zwecke der Gefahrenabwehr, zur Verfolgung von Ordnungswidrigkeiten, sowie für gesetzlich vorgeschriebene Aufgaben der Verfassungsschutzbehörden, des Bundesnachrichtendienstes, des militärischen Abschirmdienstes und des Zollkriminalamtes, der EU sich nicht auf Fragen der öffentlichen Sicherheit erstreckt, sollten Regelungen vermieden werden, die vom Wortlaut den Eindruck erwecken, daß die Entscheidungskompetenz der nationalen Gesetzgeber eingeschränkt werden soll. Dies könnte erreicht werden, wenn Artikel 8 Nr. 4 Satz 2 wie folgt gefaßt wird:

"Wenn nach nationalem Recht aus wichtigem überwiegendem öffentlichem Interesse die Weitergabe der Daten über die Identität ohne Einwilligung der Betroffenen erforderlich ist, ist die Weitergabe zu registrieren und die betroffene Person nach Abschluß der Ermittlungen so bald wie möglich über die Weitergabe ihrer Daten zu unterrichten."

Darüber hinaus sollte, wie im Datenschutzrecht üblich und auch in diesem Fall angezeigt, von der erforderlichen Einwilligung der Betroffenen gesprochen werden, um eine nachträgliche Zustimmung (Genehmigung) begrifflich auszuschließen.

EU
In
R

10. Zu Artikel 9 und 10

Gegen den vorgesehenen Ausschuß und seine Funktion hat der Bundesrat Bedenken. Insoweit wird auf die Ausführungen zu Artikel 3 Abs. 3 Bezug genommen.

EU
In
R

11. Zu Artikel 13

Die vorgesehene Frist für die Umsetzung der Richtlinie ist zu knapp. Da damit zu rechnen ist, daß die Richtlinie keinesfalls vor Mitte des Jahres 1999 erlassen wird, bliebe für die Umsetzung allenfalls ein Zeitraum von eineinhalb Jahren, der für eine angemessene Beteiligung der Länder nicht genügend Zeit läßt. Die Frist ist so zu verlängern, daß für die Umsetzung mindestens zweieinhalb bis drei Jahre zur Verfügung stehen.

B

12. Der Ausschuß für Kulturfragen und
der Wirtschaftsausschuß

empfehlen dem Bundesrat, von der Vorlage gemäß §§ 3 und 5 EUZBLG Kenntnis zu nehmen.

17.09.98

**Empfehlungen
der Ausschüsse**EU - In - K - R - Wizu Punkt der 729. Sitzung des Bundesrates am 25. September 1998

Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über gemeinsame Rahmenbedingungen für elektronische Signaturen

KOM(98) 297 endg.; Ratsdok. 9708/98

Betr.: Änderung der Drucksache 703/1/98Ziffer 9 der **Drucksache 703/1/98** wird wie folgt gefaßt:EU
In9. Zu Artikel 8

In Artikel 8 Datenschutz werden Regelungen getroffen, die hinter dem derzeit in Deutschland geltenden Recht (Signaturgesetz) zurückbleiben. Danach ist die Offenbarung der Identität von Personen, die Pseudonyme verwenden, an Behörden grundsätzlich nur mit Zustimmung der Betroffenen vorgesehen. Ohne Zustimmung des Betroffenen ist eine Offenbarung nur zur Aufklärung von Straftaten zugelassen. Die Formulierung erweckt den Eindruck, daß die Offenbarung für Zwecke der Gefahrenabwehr, zur Verfolgung von Ordnungswidrigkeiten, sowie für gesetzlich vorgeschriebene Aufgaben der Verfassungsschutzbehörden, des Bundesnachrichtendienstes, des militärischen Abschirmdienstes und des Zollkriminalamtes nach nationalem Recht nicht mehr vorgesehen werden dürfte. Da die Regelungskompetenz der EU sich nicht auf Fragen der öffentlichen Sicherheit erstreckt, sollten Regelungen vermieden werden, die vom Wortlaut den Eindruck erwecken, daß die Entscheidungskompetenz der nationalen Gesetzgeber eingeschränkt werden soll. Dies könnte erreicht werden, wenn Artikel 8 Nr. 4 Satz 2 wie folgt gefaßt wird:

Ausgeliefert am 17. SEP. 1998

"Wenn nach nationalem Recht aus wichtigem überwiegendem öffentlichem Interesse die Weitergabe der Daten über die Identität ohne Einwilligung der Betroffenen erforderlich ist, ist die Weitergabe zu registrieren und die betroffene Person nach Abschluß der Ermittlungen so bald wie möglich über die Weitergabe ihrer Daten zu unterrichten."

Darüber hinaus sollte, wie im Datenschutzrecht üblich und auch in diesem Fall angezeigt, von der erforderlichen Einwilligung der Betroffenen gesprochen werden, um eine nachträgliche Zustimmung (Genehmigung) begrifflich auszuschließen.