

# Gliederung

<b>I. Entstehungsgeschichte</b>	1
<b>II. Ermächtigungsgrundlage</b>	3
<b>III. Interpretationsgrundsätze</b>	4
<b>IV. Gegenstand der Richtlinie</b>	5
<b>V. Anwendungsbereich</b>	6
1. Sachlicher Anwendungsbereich	6
2. Persönlicher Anwendungsbereich	7
3. Räumlicher Anwendungsbereich	7
<b>IV. Grundsätze für die Verarbeitung personenbezogener Daten</b>	8
5. Grundsatz der Zweckbindung	8
6. Grundsatz der Einwilligung und der Erforderlichkeit	8
7. Verarbeitung sensibler Daten	9
8. Medienprivileg	10
<b>IX. Rechte der Betroffenen</b>	11
10. Informationsrecht	11
11. Auskunftsrecht	11
12. Widerspruchsrecht	12
13. Ausnahmen und Einschränkungen	12
<b>XIV. Datensicherung und Kontrolle</b>	13
15. Datensicherung	13
16. Kontrollstellen und Meldepflichten	13
<b>XVII. Rechtsbehelf und Haftung</b>	14
<b>XVIII. Datenübermittlung in Drittländer</b>	15
<b>XIX. Ausblick</b>	16

## **Grundrechtsschutz und freier Datenverkehr-**

### **Die EG- Richtlinie 95/46/EG**

#### **Regelungen über die Zulässigkeit der Verarbeitung personenbezogener Daten**

##### **I. Entstehungsgeschichte**

Den ersten Appelle im Jahre 1975 des Europäischen Parlamentes, mit Hinblick auf den stetigen Zuwachs der Verarbeitung personenbezogener Daten, eine einheitliche Regelung diesbezüglich zu schaffen, wick die für die Gesetzgebung zuständige Kommission zunächst beharlich aus. Diese Situation spiegelte die unterschiedlichen Interessen der beiden Organe wieder:

Das Europäische Parlament fühlte sich berufen, die Rechte der einzelnen möglichst effektiv zu schützen. Die Harmonisierung des Datenschutzes war aus der Perspektive des Schutz der subjektiven Rechte der EU-Bürger aus mehreren Gründen notwendig. Zum einem ging es ihr darum, der Gefahr der Aushöhlung mitgliedstaatlicher Datenschutzstandarts durch grenzüberschreitenden Datenverkehr zu entgegnen. Werden beispielsweise aus einem Land mit einem hohen Datenschutzniveau Daten in ein Land mit einem anderen oder gar keinen Datenschutz übermittelt, richtet sich das anzuwendende Recht jeweils danach, wo die Daten verarbeitet werden, hier also dann nach dem Land, mit dem niedrigerem Schutzstandart. Die Folge ist, daß sich sogenannte Datenoasen bilden, d.h. Staaten mit niedrigem Datenschutz bevorzugt von datenverarbeitenden Stellen als Verarbeitungsort gewählt werden, und so die von einem Mitgliedstaat gewährten Schutzstandarts durch fehlende Regelungen in einem anderen EU-Staat ausgehöhlt werden. Als weiterer Grund, warum ein einheitlicher Datenschutz rechtlich geboten war, war die Tatsache, daß sich die Europäische Gemeinschaft verpflichtete, die Grundrechte aller Gemeinschaftsbürger zu wahren. So hatte der EuGH

ein Recht auf Datenschutz zwar bisher nicht explizit genannt, jedoch im Jahre 1994 das in Art. 8 ERMK verankerte Recht auf Achtung des Privatlebens ausdrücklich als ein von der Gemeinschaft geschütztes Grundrecht bezeichnet. Durch den Vertrag von Amsterdam fand dann das Datenschutzrecht ausdrückliche Erwähnung in Art. 286 EGV, dies geschah jedoch erst nach der Verabschiedung der Richtlinie .

Aus der Sicht der Kommission hingegen, war die Ausgangslage eine völlig andere. Sie verfolgte primär das industriepolitische Ziel, den gemeinsamen Binnemarkt auszubauen und den freien Handel zu gewährleisten. Die Erschaffung neuer Hindernisse, die ein EG-weiter Datenschutz darstellen würde, war ihr höchst unerwünscht. Vielmehr setzte sie sich permanent für die Förderung der Entwicklung und Anwendung der Datenverarbeitung ein, um die wettbewerbsfähigkeit der EG auf diesem Gebiet zu erhöhen. Sie sah in den Daten vornehmlich ein marktfähiges Gut, wobei die Fragen des Datenschutzes nur insoweit eine Rolle spielten, als sie geeignet waren, die Akzeptanz in der Bevölkerung gegenüber einer immer weitergehenden Verwendung moderner Datenverarbeitung zu erhöhen.

Die einzige Reaktion der Kommission war daher, zu empfehlen, zunächst erstmal die Datenschutzkonvention des Europarates zu ratifizieren.

Bei der Entwicklung der 1981 ins Leben gerufenen Konvention, ging der Europarat davon aus, daß sie lediglich einen allgemeinen Regelungsrahmen für die Schaffung eines Datenschutzstandarts darstellen könne. In weiten Bereichen sei aber eine spezifischere Gestaltung ,als von der Konvention vorgenommen, von Bedarf.

Der Druck auf die Kommission durch das Europäische Parlament wuchs jedoch stetig, nachdem etliche Mitgliedstaaten der Empfehlung, das Europaratsübereinkommen zu ratifizieren nicht nachgekommen waren und die Rechtsentwicklung im Bereich des Datenschutzes in den Mitgliedstaaten zunehmend fortschritt. Allen nationalen Gesetzen, so unterschiedlich sie auch ausgestaltet waren, wohnte die Überzeugung inne, daß sich in den normativen Anforderungen an die Verarbeitung personenbezogener Daten der Schutz der Handlungs- und Partizipationsfähigkeit des einzelnen artikuliert, wovon auch das Bundesverfassungsgericht in seinem Volkszählungsurteil ausging, als es das sogenannte informationelle Selbstbestimmungsrecht entwickelte

Auf Grund dieser Entwicklung reagierte dann 1988 die Kommission und legte 1990 die ersten Vorschläge für eine einheitliche Regelung vor, bis dann 1995 die „Richtlinie des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr“, verabschiedet wurde und bis zum 24.10.1998 in das Recht der Mitgliedsstaaten umzusetzen war. Bis zum heutigen Zeitpunkt geschah dies erst in 6 der 15 Mitgliedsstaaten, jedoch wird überall daran mehr oder weniger nachdrücklich gearbeitet.

## **II. Ermächtigungsgrundlage**

Die Frage, ob die EU überhaupt die Kompetenz zum Erlass einer solchen Richtlinie hatte, war von Anfang an höchst umstritten.

Da der Datenschutz selbst keinen eigenen Politikbereich bildete, kamen als Ermächtigungsgrundlage die Art. 235 (heute Art. 308); 100 (Art. 94) und 100a (Art. 95) EGV in Betracht. Die Auseinandersetzung um die Kompetenz war aber weniger ein Streit um die Sache selbst, als vielmehr das Tauziehen um die juristische Fundamentalfrage, wie weit die Kompetenzen der Union reichen. So hat die Berufung auf Art 100a und nicht auf Art.100 oder 235 EGV den strategischen Vorteil, daß Art 100a EGV lediglich eine qualifizierte Mehrheit zur Beschlußfassung erfordert, während Art. 100 und 235 EGV einen einstimmigen Beschluß voraussetzen.

In der Richtlinie selbst beziehen sich dann Rat und Parlament auch auf den Vertrag zur Gründung der EG, insbesondere auf Art. 100 a (heute Art. 95) EGV. Die Einschlägigkeit dieser Kompetenznorm ist immer dann begründet, wenn die von ihr ermächtigte Richtlinie der Verwirklichung des Binnenmarktes dient. Gem. Art 8a EWG-Vertrag wird unter Binnenmarkt ein Raum ohne Binnengrenzen verstanden, in dem der freie Verkehr von Waren, Personen und Dienstleistungen gewährleistet ist. Da dieser freie Verkehr beispielsweise in den Bereichen der Dienstleistungsunternehmen, die auf Datenverarbeitung zurückgreifen, wie Banken, Versicherungen oder die Tourismusbranche, ein angeglichenes Datenschutzniveau erfordert, kann die Berufung auf Art. 100a EGV als rechtmäßig angesehen werden. Die Erwägungsgründe der Richtlinie sprechen davon, daß ein unterschiedliches Datenschutzniveau in den Mitgliedstaaten ein Hemmnis für die Ausübung einer Reihe von Wirtschaftstätigkeiten darstellen und damit den Wettbewerb verfälschen und auch die Behördentätigkeit

behindern kann (Erwägungsgrund 7). Zur Beseitigung dieser Hemmnisse soll daher ein gleichwertiges Schutzniveau hinsichtlich der Rechte und Freiheiten der Personen bei der Verarbeitung dieser Daten in allen Mitgliedstaaten hergestellt werden (Erwägungsgrund 8).

Noch nicht beantwortet ist allerdings die Frage, ob bereichsspezifische Verarbeitungsregeln ebenfalls auf Art. 100a bzw. 95 EGV gestützt werden können. Zweifelhaft erscheint dies z.B. bei Datenschutzregeln, die sich auf den Persönlichkeitsschutz von Arbeitnehmern bei der Datenverarbeitung durch den Arbeitgeber. Würde man diese Bestimmungen als arbeitsrechtliche Vorschriften bewerten, wäre Art. 95 EGV nicht mehr einschlägig, gem. Art 95 Abs. II EGV gilt er nämlich nicht für Bestimmungen über die Rechte und Interessen der Arbeitnehmer. Teilweise wird daher vorgeschlagen, anstelle von Art 95 den Art. 94 (ex Art.100) EGV heranzuziehen. Andere Stimmen hingegen fordern, den Arbeitnehmerdatenschutz dem Datenschutz zuzurechnen, womit der Weg über Art. 95 EGV offen bliebe.

### **III. Interpretationsgrundsätze**

Zum Zeitpunkt des Erlasses der Richtlinie waren bereits viele nationale Datenschutzregeln entstanden. Eine wirklich neue Regelung zu erschaffen wäre äußerst kompliziert geworden. Ein völlig neuer Ansatzpunkt hätte entwickelt werden müssen, dazu käme, daß sie auch sehr schwer gegen die nationalen Interessen der Mitgliedsstaaten durchzusetzen gewesen wäre.

Deswegen ging die Kommission bei der Schaffung der Richtlinie von einer konsistenten Kombination und nicht von einer effektiven Kombination aus, und verband die wichtigsten Elemente der verschiedenen Datenschutzregelungen. Der Vorteil dieses Ansatzes ist sicherlich darin zu sehen, daß auf die zurückliegenden Erfahrungen der Mitgliedsstaaten in der Anwendung der Regeln zurückgegriffen werden kann. Genau darin liegt aber auch die Gefahr: Wird bei der Interpretation der Richtlinie von jedem Mitgliedsstaat auf die eigenen entwickelten nationalen Interpretationsgrundsätze zurückgegriffen, zerfällt die supranationale Regelung in ihre nationalen Bestandteile. Ein Ausweg aus diesem Dilemma kann darin gesehen werden, sich bei der Interpretation an die in der Richtlinie genannten Erwägungsgründe zu orientieren, wie beispielsweise an Erwägungsgrund Nr. 10, in dem von einem hohen Datenschutzniveau ausgegangen

wird. Weiter besteht die Möglichkeit, auf die Beratungsprotokolle zurückzugreifen, um zu klären, wie die einzelne Vorschrift zu verstehen ist. Dies jedoch nur als letztes Mittel, sind die Beratungsprotokolle doch meistens nicht veröffentlicht und haben auch keine bindende Wirkung.

#### **IV. Gegenstand der Richtlinie**

Aus der Überschrift der Richtlinie „Richtlinie zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr“, läßt vermuten, daß hier eine Regelung geschaffen wurde, die den Zweck hat, die Balance zwischen Datenschutz und Datenverkehr festzuschreiben. Auch aus den in der Richtlinie genannten Erwägungsgründen ergibt sich eine zweifache Zielsetzung: Zum einen sollen die Grundrechte auf Schutz der Privatsphäre und freie Meinungsäußerung gem. Art 8 und 10 ERMK des europäischen Bürgers geschützt werden, zum anderen geht es darum, den freien Datenverkehr im Binnenmarkt herzustellen.

Den Eindruck, (den auch schon die Entstehungsgeschichte impliziert,) daß nämlich der freie Datenverkehr im Vordergrund steht und der Schutz der Daten eine eher untergeordnete Rolle spielt, beziehungsweise lediglich toleriert wird, verstärkt Art. 1 II der Richtlinie. Er besagt, daß der freie Verkehr personenbezogener Daten zwischen den Mitgliedsstaaten nicht aus Gründen des Datenschutzes beschränkt werden dürfe. Jedoch läßt sich aus Erwägungsgrund 10 der Richtlinie ersehen, daß ein möglichst hohes Schutzniveau erreicht werden soll. Erwägungsgrund 9 räumt den Mitgliedsstaaten das Recht ein, sich stetig um eine Verbesserung des Datenschutzes zu bemühen, auch wenn dadurch Unterschiede bei der Durchführung der Richtlinie auftreten, die sich auf den freien Informationsfluß auswirken. Damit ist klar, daß die Vereinfachung des Datenaustausches nicht um den Preis eines verminderten Datenschutzes erfolgen soll. Die Formulierung des Art 1 der Richtlinie ist also dahingehend zu interpretieren, daß die Mitgliedsstaaten, wenn sie den Schutz der Bürgerrechte im Sinne der Richtlinie gewährleisten, den freien Datenverkehr nicht behindern dürfen.

#### **V. Anwendungsbereich**

##### **1. Sachlicher Anwendungsbereich**

Der sachliche Anwendungsbereich der Richtlinie wird in Art. 3 definiert und ist eröffnet, wenn personenbezogene Daten verarbeitet werden.. Wann personenbezogene Daten verarbeitet werden, ergibt sich aus Art. 2, welcher die Begriffe bestimmt.

Der Begriff der Verarbeitung umfaßt demnach sämtliche Handlungen von der Erhebung über die Weitergabe bis zur Löschung, um den Anwendungsbereich der Richtlinie möglichst weit zu halten.

Die Unterscheidung ob die Verarbeitung von öffentlichen oder nicht-öffentlichen Stellen vorgenommen wird, wie sie aus dem BDSG bekannt ist und auch im ersten Entwurf der Richtlinie von 1990 vorgesehen war, wurde nicht übernommen. Der Grund dafür mag in der Einsicht liegen, daß der Zuwachs bei der Verarbeitung personenbezogener Daten im nicht-öffentlichen Bereich die Privatsphäre mindestens genauso gefährdet wie die Verarbeitung im öffentlichen Bereich. Hinzu kommt die Privatisierung vieler traditionell öffentlicher Aufgaben, die dazu führt, daß viele Daten die früher von öffentlichen Stellen erhoben wurden, nun von privater Seite verarbeitet werden.

Außerdem würde eine solche Unterscheidung zu erheblichen Schwierigkeiten bei der genauen Bestimmung führen, werden doch die Begriffe „öffentlich,, und „privat,, in den Mitgliedsstaaten höchst unterschiedlich verwendet.

Dieser weite sachliche Anwendungsbereich wird in zweifacher Hinsicht eingeschränkt: Zum einen ist die Richtlinie bei manueller Verarbeitung nur einschlägig wenn die Daten in „Dateien,, gespeichert werden (Art 3 I), wobei jedoch bei der Begriffsbestimmung der Datei wiederum eine weite Definition zugrunde gelegt wird, der jede „strukturierte Sammlung,, personenbezogener Daten umfaßt (Art. 2 c). Anders als das BDSG erstreckt sich die Richtlinie somit auch auf Akten, beziehungsweise Aktenvorgänge, sofern sie als Dateien begriffen werden müssen.

Die zweite Einschränkung ergibt sich aus Art. 3 II der Richtlinie. Danach findet diese keine Anwendung, wenn es um die Datenverarbeitung im Zusammenhang mit Tätigkeiten, die nicht in den Anwendungsbereich des Gemeinschaftsrechts fallen. Hierzu gehören die Tätigkeiten, die in den Titeln V und VI des Vertrages über die Europäische Union genannt sind. Diese, die Gemeinsame Außen- und Sicherheitspolitik (GASP) sowie die Zusammenarbeit der Mitgliedsstaaten in den Bereichen Justiz und Inneres betreffenden Titel gehören nicht zum Gemeinschaftsrecht, sondern zum

Unionsrecht. Außerdem findet die Richtlinie keine Anwendung auf Verarbeitungen, die die öffentliche Sicherheit, die Landesverteidigung, die Sicherheit des Staates oder das Strafrecht betreffen.

Ebenso sind solche Verarbeitungen von Daten von der Richtlinie ausgenommen, die rein persönlichen oder familiären Zwecken dienen, wie Adreßbücher o.ä. .

## 2. Persönlicher Anwendungsbereich

Wie sich aus der Überschrift der Richtlinie ergibt, fallen nur natürliche Personen unter den Schutzbereich der Richtlinie.

## 3. Räumlicher Anwendungsbereich

Nach Maßgabe von Art. 4 a lit. 1 der Richtlinie bestimmt sich die örtliche Anwendbarkeit einzelstaatlichen Rechts danach, in welchem Mitgliedsstaat der Verantwortliche der Verarbeitung ansässig ist. Nach der Definition in Artikel 2 Buchstabe d der Richtlinie ist der Verantwortliche der Verarbeitung die natürliche oder juristische Person, Behörde, Einrichtung oder jede sonstige Stelle, die über Zwecke und Mittel der Verarbeitung personenbezogener Daten entscheidet.

Will jemand aus einem Land, welches nicht in der EU liegt, auf Daten aus einem Mitgliedsstaat zugreifen, um diese zu verarbeiten, muß er einen Vertreter für diesen Mitgliedsstaat benennen, demgegenüber die in der Richtlinie genannten Aufsichtsbefugnisse durch die entsprechenden Stellen dann geltend gemacht werden können.

## **VI. Grundsätze für die Verarbeitung personenbezogener Daten**

Ähnlich wie das Bundesdatenschutzgesetz geht die Richtlinie von einem Verbot mit Erlaubnisvorbehalt aus, was bedeutet, daß jede Datenverarbeitung nur zulässig ist, wenn sie erlaubt ist. Gem. Art. 5 der Richtlinie haben die Mitgliedstaaten die Voraussetzungen unter denen die Verarbeitung personenbezogener Daten rechtmäßig ist, selbst festzulegen. Allerdings legen die Art. 6 bis 9 der Richtlinie den Rahmen für die zulässige Verarbeitung fest.



### 1. Grundsatz der Zweckbindung

Art. 6 Abs. 1 b) und c) legt fest, daß die Verarbeitung nur zu vorher festgelegten Zwecken erfolgen darf, und die Daten für diese Zwecke auch erheblich sein müssen. Der Zweckbindungsgrundsatz legt somit einerseits das Verarbeitungsziel fest und begrenzt andererseits den Verarbeitungsumfang. Während die Zweckbestimmung bei historischen, statistischen oder wissenschaftlichen Dateien im allgemeinen unterstellt wird, sind die präventive Datensammlung sowie das Sammeln von Daten auf Vorrat nicht erlaubt. Entfällt der, für die Datenverarbeitung verwendete Zweck, sind auch die dafür gespeicherten Daten zu löschen.

### 2. Grundsatz der Einwilligung und der Erforderlichkeit

Nach Art. 7 der Richtlinie ist die Verarbeitung personenbezogener Daten nur zulässig, wenn sie mit Einwilligung des Betroffenen erfolgt. Für die Einwilligung wird in Art. 2 der Richtlinie verlangt, daß sie den konkreten Willen des Betroffenen ohne jeden Zweifel ausdrückt. Damit sind konkludente Einwilligungen sowie generelle Einwilligungen, z.B. in einer AGB-Klausel nicht ausreichend. Vielmehr muß der Betroffene, selbst wenn die Umstände eine Einwilligung eindeutig nahelegen, noch einmal ausdrücklich sein Einverständnis erklären.

Liegt keine Einwilligung vor, kann die Datenverarbeitung nur dann rechtmäßig erfolgen, wenn sie erforderlich ist im Hinblick auf den Abschluß oder die Erfüllung eines für die betreffende Person bindenden Vertrages, zur Erfüllung einer gesetzlichen Verpflichtung, zur Wahrnehmung einer Aufgabe im öffentlichen Interesse, in Ausübung hoheitlicher Gewalt sowie wenn sie im Interesse einer anderen Person erforderlich ist und nicht die Interessen oder die Rechte und Freiheiten des Betroffenen überwiegen, Art. 7 der Richtlinie. Für die beiden letzten Ausnahmen vom Einwilligungsgrundsatz besteht jedoch gem. Art 14 Abs. I a) der Richtlinie ein Widerspruchsrecht, welches der Betroffene ohne Angabe von Gründen oder Kosten geltend machen kann, um gegen die Verarbeitung der ihn betreffenden Daten vorzugehen.

### 3. Verarbeitung sensibler Daten

Besondere Anforderungen stellt die Richtlinie in Art. 8 an die Verarbeitung sensibler Daten. Sensibel sind die Daten dann, wenn aus ihnen rassische oder ethnische Herkunft, die politische Meinung, religiöse oder philosophische oder die Gewerkschaftszugehörigkeit hervorgeht, sowie Daten über Gesundheit und Sexualleben. Ihre Verarbeitung ist grundsätzlich verboten wenn nicht die in den Abs. 2 bis 7 statuierten Voraussetzungen erfüllt sind. Auch hier ist eine Verarbeitung zulässig, wenn die ausdrückliche Einwilligung des Betroffenen vorliegt. Weitere Ausnahmen von dem Verbot der Verarbeitung sensibler Daten kommen beispielsweise in Betracht, wenn die Daten von Personen verarbeitet werden, die einem Berufsgeheimnis, wie z.B. Ärzte, unterliegen, oder bestimmte, nicht auf einen Erwerbszweck ausgerichtete Organisationen die Verarbeitung auf Grundlage angemessener Garantien vornehmen. Abs. IV der Richtlinie gesteht den Mitgliedstaaten das Recht zu, unter bestimmten Voraussetzungen weitere Verwendungen zuzulassen.

Die Kritik, daß vom Schutz sensibler Daten nichts übrig bleibt scheint einleuchtend, wird doch der in Abs. I aufgestellte Schutz der Bürger durch die Abs. I bis IV erheblich reduziert. Andererseits muß jedoch gesehen werden, daß die Ausnahmen nötig sind, um dem jeweiligen historischen, politischen und soziologischen Hintergrund des jeweiligen Mitgliedstaates gerecht zu werden. Während es in Deutschland beispielsweise erforderlich ist, daß der Arbeitgeber darüber informiert ist, welcher seiner Arbeitnehmer gewerkschaftlich organisiert ist, um ihn ggf. für gewerkschaftliche Veranstaltungen freizustellen, ist die Gewerkschaftsangehörigkeit in Frankreich traditionell "Geheimsache". Ähnlich verhält es sich mit der religiösen Überzeugung, von der der deutsche Arbeitgeber wissen muß, um die Kirchensteuer abzuführen.

Deutschland hatte bei der Erarbeitung der Richtlinie Zweifel an der Systematik und lehnte das Konzept der sensiblen Daten als überholt ab. Der Grund dafür mag darin liegen, daß mit der Differenzierung zwischen sensiblen und weniger sensiblen Daten die vom Bundesverfassungsgericht abgelehnte Sphärentheorie europaweit etabliert wird, wohingegen nach deutschem Verständnis auf den Verwendungszusammenhang der personenbezogenen Daten abgestellt werden muß. Das eine Richtlinie aber immer nur ein Kompromiß sein kann, liegt in ihrer Natur. Die großzügigen Ausnahmen müssen daher vor dem Hintergrund des Subsidiaritätsprinzips gesehen werden. Der den

Mitgliedstaaten zugestandene Spielraum ist erforderlich, um ihnen die Möglichkeit zu geben, Lösungen zu entwickeln, die ihren Rechtstraditionen entsprechen.

#### 4. Medienprivileg

Art. 9 der Richtlinie gewährt der Presse und den audiovisuellen Medien eine Sonderstellung. Demnach können Ausnahmen vom Datenschutz vorgesehen werden, soweit sie erforderlich sind, um das Recht auf Privatsphäre mit den für die Meinungsäußerungsfreiheit geltenden Vorschriften in Einklang zu bringen. Möglich sind Regelungen, die sämtliche journalistische Tätigkeit, von der Recherche bis hin zur Veröffentlichung umfassen können. Jedoch äußerte sich der Deutsche Presserat nach bekanntwerden des deutschen Entwurfs zur Umsetzung der Richtlinie besorgt, daß nach der Verabschiedung des Gesetzes der Quellen- und Informationsschutz praktisch nicht mehr gewährleistet sei. Auch Prof. Simitis äußerte Unbehagen und sagte, daß sich der Inhalt des Gesetzesentwurfs nicht aus der EU-Richtlinie folgern lasse. Das Bundesinnenministerium hat inzwischen eingelenkt und will den Entwurf korrigieren. Danach soll in einer Vereinbarung mit dem Deutschen Presserat festgelegt werden, daß die Medienunternehmen durch eine Selbstverpflichtung garantieren, daß die redaktionellen Daten vor dem Zugriff Unbefugter geschützt werden. Auf jeden Fall soll es keine Beeinträchtigung der Pressefreiheit durch die Umsetzung der Richtlinie geben.

### **VII. Rechte der Betroffenen**

#### 1. Informationsrecht

Art. 10 der Richtlinie und - sofern die Daten nicht bei der betroffenen Person erhoben wurden - gem. Art. 11 bei der Speicherung bzw. bei der ersten Übermittlung der Daten sehen eine umfassende Information des Betroffenen durch den Verantwortlichen vor. Diese ist die Grundvoraussetzung für eine wirksame Einwilligung, da nur Betroffene, die informiert sind selbst über die Preisgabe und Verwendungen ihrer persönlichen Daten bestimmen.

Die Information muß die Zweckbestimmung, die Identität des Verantwortlichen und weitere Einzelheiten umfassen. Während Art. 10 der Richtlinie lediglich dort Ausnahmen zuläßt, wo dem Betroffenen die jeweiligen Informationen bereits vorliegen, entfällt die Unterrichtungspflicht im Rahmen des Art. 11 der Richtlinie

zusätzlich, wenn die Speicherung oder Weitergabe durch Gesetz ausdrücklich vorgesehen ist oder wenn die Unterrichtung der betroffenen Person unmöglich oder unverhältnismäßig wäre.

## 2. Auskunftsrecht

Art. 12 der Richtlinie enthält das sich an das Informationsrecht anschließende Auskunftsrecht und stellt damit die zentrale Bestimmung der Regelung dar, räumt sie doch der betroffenen Person die ihr zukommende datenschutzrechtliche Rechtsposition ein.

Zum einen kann der Betroffene nicht nur in zeitlich angemessenen Abständen und ohne unzumutbare Verzögerung oder übermäßige Kosten Informationen über die Einzelheiten der Verarbeitung seiner Daten, wie z.B. Zweckbestimmung, Empfänger oder den Aufbau von Dateien verlangen.

Darüber hinaus beinhaltet das Auskunftsrecht das Recht auf Berichtigung, Löschung und Sperrung unvollständiger oder unrichtiger Daten, welches auch Dritten gegenüber gilt, denen die Daten bereits übermittelt wurden, soweit dies nicht unmöglich oder mit unverhältnismäßig großem Aufwand verbunden ist.

Teilweise wird kritisiert, das durch die Verkürzte Darstellung des Berichtigungs-, Lösungs-, oder Sperrungsanspruch unter der Überschrift des Auskunftsrechts der Eindruck entstehen könnte, daß dieser mit dem Auskunftsrecht verbunden sei. Richtig ist zwar, daß beide Ansprüche ihre dogmatische Wurzel im Recht auf informationelle Selbstbestimmung haben, jedoch sind sie nicht voneinander abhängig sondern stehen nebeneinander. So kann der Betroffene auch die Berichtigung von unrichtigen Daten verlangen, wenn er von ihrer Unrichtigkeit nicht durch die Geltendmachung seines Auskunftsanspruches, sondern auf anderem Wege Kenntnis erlangt hat.

## 3. Widerspruchsrecht

Das gem. Art. 14 der Richtlinie statuierte Widerspruchsrecht, enthält, neben den bereits unter VI/ 2 beschriebenen Recht, in lit. b) ein Recht auf Widerspruch gegen die Verarbeitung zum Zwecke der Direktwerbung.

Ausnahmen vom Widerspruchsrecht sind den Mitgliedstaaten vorbehalten.

Zusätzlich gewährt Art. 15 der Richtlinie dem Betroffenen das subjektive Recht, keiner automatisierten Einzelentscheidung unterworfen zu werden. Obwohl automatisierte Verfahren zunehmend z.B. bei der Beurteilung der Kreditwürdigkeit oder bei der Einstellung von Arbeitnehmern eine Rolle spielt, wird ihr Anwendungsbereich in der Praxis wohl eher gering bleiben. Der Grund dafür liegt darin, daß Art. 15 Abs. 2 wiederum eine Ausnahme für die Fälle vorsieht, in denen es um sich anbahnende bzw. bereits abgeschlossene Verträge geht, womit die Hauptanwendungsfälle, Kredit- und Arbeitsverhältnisse, erfaßt sind. Die vorgesehene Möglichkeit für den Betroffenen, seinen Standpunkt dennoch geltend machen zu können, dürfte ihn in wohl eher wenig nützen.

#### 4. Ausnahmen und Einschränkungen

Art. 13 der Richtlinie eröffnet den Mitgliedsstaaten die Möglichkeit, Ausnahmeregelungen bezüglich der Grundsätze in bezug auf die Qualität der Daten (Art. 6 Abs. I), des Informations- und Auskunftsrechts (Art 10, 11 Abs. I und 12) und der Öffentlichkeit der Verarbeitung (Art. 21) zu erlassen.

Wann dies zulässig ist, wird in einer Reihe von Generalklauseln beschrieben. Diese sind so zahlreich und exzessiv, das leicht der Eindruck entstehen kann, es solle kein Fall ausgelassen werden, in dem keine Ausnahme zulässig ist.

Jedoch sind Ausnahmen nur zulässig sind, soweit sie notwendig sind. Dieser Zusatz stellt eine immanente Schranke nationaler Ausnahmetatbestände dar, so daß die Mitgliedstaaten gehalten sind, bei Umsetzung der Richtlinie die Verhältnismäßigkeit sowie die Erforderlichkeit etwaiger Beschränkungen zu beachten.

Ob diese Regelung dazu beiträgt, den europäischen Datenschutz auszuhöhlen, oder ob sie ein Beitrag zu Wahrung des Subsidiaritätsprinzips ist, bleibt abzuwarten.

### **VIII. Datensicherung und Kontrolle**

#### 1. Datensicherung

Da das Recht auf Privatsphäre nicht nur durch die die datenverarbeitenden Stellen gefährdet ist, sondern auch durch den unbefugten Zugriff Dritter auf diese Daten, gibt Art. 17 der Richtlinie den Verantwortlichen auf, den Schutz der Daten sicherzustellen.

## 2. Kontrollstellen und Meldepflicht

Art. 28 der Richtlinie gibt den Mitgliedstaaten die Pflicht auf, auf nationaler Ebene Datenschutzaufsichtsbehörden etwa in Form von staatlichen Datenschutzbeauftragten einzurichten. Diese den Datenschutz überwachende Stelle legt regelmäßig einen Bericht über ihre Tätigkeit vor, um eine öffentliche Kontrolle des Datenschutzes zu gewährleisten.

Dieser Kontrollstelle muß der Verantwortliche einer Datenverarbeitung gem. Art. 18 der Richtlinie sieht Datenverarbeitungsvorgänge und die sie betreffenden Einzelheiten wie Zweckbestimmung, etc. im Rahmen eines Meldeverfahrens melden, um eine Überprüfung auf ihre Rechtmäßigkeit zu ermöglichen. Hierfür können die Mitgliedstaaten abermals Ausnahmen zulassen, insbesondere dann, wenn von dem Verantwortlichen ein interner weisungsunabhängiger Datenschutzbeauftragter benannt wurde, der die Einhaltung der nationalen Bestimmungen überwacht und zur Führung eines Dateiverzeichnisses verpflichtet ist (Art. 18 Abs. 2 Spiegelstrich 2 der Richtlinie). Diese Vorschrift läßt noch einmal deutlich erkennen, daß die Richtlinie, wie bereits eingangs erwähnt, keinen konzeptionellen Neuentwurf "aus einem Guß" darstellt, sondern ein "patchwork" aus unterschiedlichen Datenschutzregelungen ist. Während Frankreich bei der Erarbeitung der Richtlinie die ihr traditionell vertraute Meldepflicht favorisierte, hielt Deutschland dies für eine überflüssige Bürokratisierung des Datenschutzes und schlug vor, auf den für deutsches Recht typischen betrieblichen Datenschutzbeauftragten zurückzugreifen.

Das Ergebnis ist ein Kompromiß, der den Mitgliedstaaten die Wahl zwischen der Meldepflicht und der Bestellung eines Datenschutzbeauftragten.

Unabhängig von der nationalen Datenschutzkontrolle sieht Art. 30 der Richtlinie die Einrichtung einer gemeinschaftsweiten Datenschutzgruppe vor, die die Weiterentwicklung des Datenschutzes koordinieren soll.

Um weitere Maßnahmen, wie etwa ergänzende Regelungen, effektiv durchsetzen zu können, hat die Kommission im Ausschuß gem. Art. 31 der Richtlinie, der aus Vertretern der Mitgliedstaaten besteht und bei Durchführungsmaßnahmen zu beteiligen

ist, ein Initiativrecht, kann sogar unter Umständen Fakten gegen den Willen des Ausschusses durchsetzen.

Verhaltensregel???

### **IX. Rechtsbehelf und Haftung**

Art. 22 der Richtlinie verpflichtet die Mitgliedstaaten, jeder Person, deren sich aus der nationalen Umsetzungsvorschrift ergebenden Rechte durch eine Datenverarbeitung verletzt sind, einen effektiven Rechtsweg zu gewähren. Gem. Art. 23 kann die betreffende Person vom Verantwortlichen der Verarbeitung Schadenersatz verlangen, ohne daß ein Verschulden vorliegen muß. Allerdings können die Mitgliedstaaten einen Haftungsausschluß vorsehen, wenn der Verantwortliche nachweist, daß er geeignete Schutzmaßnahmen getroffen hatte (Art. 23 Abs. II der Richtlinie).

Als Anspruchsnorm kommt nach deutschem Recht vor allem § 823 I bzw. II iVm. datenschutzrechtlichen Vorschriften in Betracht.

### **X. Datenübermittlung in Drittländer**

Gem. Art. 26 ist die Datenübermittlung an Länder außerhalb der Gemeinschaft, sofern nicht der Betroffene ausdrücklich eingewilligt hat oder sie der Durchführung eines mit ihm geschlossenen Vertrages dient, nur zulässig, wenn diese ein angemessenes Schutzniveau gewähren. Die Frage, wann ein angemessenes Schutzniveau vorliegt ist noch nicht abschließend geklärt und Gegenstand eines Arbeitspapiers der Datenschutzgruppe. Mit Hinblick auf die Erwägungsgründe der Richtlinie, die den Schutz der Grundrechte (Erwägungsgrund 1 und 2) und die Achtung der Privatsphäre (Erwägungsgrund 2) hervorheben, muß jedoch zumindest der Kernbestand der Privatsphäre im wesentlichen geschützt sein. Stimmen aus der Literatur fordern, daß die Voraussetzung für die Datenübermittlung in Drittländer ein gleichwertiges Schutzniveau sein muß, um zu verhindern, daß sich Dateieverantwortliche der Bindung des strengen Datenschutzrechts in der EG zu entziehen versuchen, indem sie in Drittstaaten abwandern, die zwar kein gleichwertiges aber ein angemessenes Schutzniveau aufweisen, um ihre Daten dort zu verarbeiten. Um jedoch eine Beeinträchtigung des Wirtschaftsverkehrs mit Handelspartnern ohne gleichwertiges Schutzniveau, wie z.B. den USA zu vermeiden, fanden diese Forderungen keinen Eingang in die Richtlinie, ein dem der Europäischen Union gleichwertiger

Schutzstandart wird somit nicht verlangt. Jedoch bleibt es den Mitgliedstaaten vorbehalten, strengere Voraussetzungen zu verlangen.

Art. 26 der Richtlinie statuiert eine Reihe von Ausnahmen, bei deren Vorliegen Daten in Drittsaaten übermittelt werden dürfen, ohne daß diese ein angemessenes Schutzniveau gewähren. Insbesondere können Garantien, die der für die Verarbeitung Verantwortliche bietet, das Fehlen angemessener Schutzniveaus auf staatlicher Ebene ausgleichen. Diese Garantien können in Form von Verträgen, einseitigen Zusagen oder der Verpflichtung zur Verhaltensregeln im Sinne des Art. 27 der Richtlinie gegeben werden. Wie die Einhaltung dieser Garantien überwacht wird, ist noch unklar, ein Mindestmaß an Transparenz ist jedoch Voraussetzung.

## **XI. Ausblick**

Aufgrund des in Deutschland bereits bestehenden hohen Schutzstandarts, werden die notwendigen Rechtsänderungen nicht allzu umfangreich ausfallen.

Die anstehenden Änderungen im deutschen Datenschutzrecht werden insbesondere zu einer Gleichstellung zwischen öffentlichen und nicht- öffentlichen Bereichen führen.

Anzupassen sind jedoch nicht nur die allgemeinen Datenschutzgesetze-

Bundesdatenschutzgesetz und Landesdatenschutzgesetz- sondern auch eine Vielzahl bereichsspezifischer Regelungen des Bundes und der Länder. Zu wünschen wäre, daß im Zuge dieser Novellierung die zahlreichen unterschiedlichen Regelungen und Begriffsbestimmungen einander angeglichen werden.



## Literaturverzeichnis

- Brühann, Ulf  
EU- Datenschutzrichtlinie- Umsetzung in einem vernetzten Europa  
in: Datenschutz und Datensicherheit 1996  
Heft 2, S. 66- 72
- Ehmann  
Helfrich  
Die EG- Datenschutzrichtlinie: Kurzkomentar
- Ellger, Reinhard  
Konvergenz oder Konflikt bei der Harmonisierung des Datenschutzes in Europa?  
In: Computerrecht 1994, Heft 9, S. 558- 563 )??)
- Datenschutz und der europäische Binnenmarkt  
in: Recht der Datenverarbeitung 1991 (Teil 1)  
Heft 2, S. 57- 65
- Der Datenschutz im grenzüberschreitendem Datenverkehr  
1990
- Gounalakis, Georgios  
einer  
Mand, Elmar  
Die neue EG- Datenschutzrichtlinie- Grundlagen  
Umsetzung in nationales Recht (I)  
Computerrecht 1997, Heft 7, S. 431- 438
- einer  
Die neue EG- Datenschutzrichtlinie- Grundlagen  
Umsetzung in nationales Recht (II)  
Computerrecht 1997, Heft 8, S. 497- 504
- Hoeren, Thomas  
Auswirkungen  
Datenschutz in Europa- Der zweite Entwurf einer EG- Datenschutzrichtlinie und dessen  
auf die deutsche Privatwirtschaft

- in: Wertpapiermitteilungen 1994, Heft 1, S. 1- 8
- Kopp, Ferdinand  
Tendenzen der Harmonisierung des Datenschutzes  
in Europa  
in Datenschutz und Datensicherheit 1995  
Heft 4, S. 204- 212
- Das EG- Richtlinienvorhaben zum Datenschutz  
in: Recht der Datenverarbeitung 1993  
Heft 1, S. 1- 10
- Körner- Dammann  
Datenschutzrichtlinie  
Der zweite Entwurf einer EG-  
in: Recht der Datenverarbeitung 1993  
Heft 1, S. 14- 20
- Reich, Norbert  
Bürgerrechte in der Europäischen Union  
1. Auflage, Baden- Baden 1999
- Schild, Hans- Hermann  
Die EG- Datenschutzrichtlinie  
in: Europäische Zeitschrift für Wirtschaftsrecht  
1996  
Heft 18, S. 549- 555
- Simitis, Spiros  
oder Anreiz?  
Die EU- Datenschutzrichtlinie- Stillstand  
In: Neue Juristische Wochenschrift 1997  
Heft 5, S. 281- 288
- Datenschutz und Europäische Gemeinschaft  
in: Recht der Datenverarbeitung 1990  
Heft 1, S. 3- 9
- Simitis, Spiros  
Dammann, Ulrich  
Die EG- Datenschutzrichtlinie  
1. Auflage, 1997
- Walz, Stefan  
Datenschutz- Herausforderung durch neue Technik  
und Europarecht  
in: 20 Jahre Datenschutz- Individualismus oder  
Gemeinschaftssinn  
Düsseldorf 1998
- Wurst, Matthias  
Europa 1992: Auf dem Weg zu einem einheitlichen  
Datenschutzrecht in der europäischen  
Gemeinschaft

in: Juristische Schulung 1991, Heft 6, S. 448- 453