Die datenschutz-konforme Verwendung personenbezogener Daten in Informationssystemen

Hans-Jürgen Pollirer

Secur-Data Betriebsberatungs-
Gesellschaft m.b.H.
Fischerstiege 9/2
1010 Wien
hj.pollirer@secur-data.at

Abstract: Am 24. Oktober 1995 wurde die „**Richtlinie 95/46 EG des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr**“ verabschiedet. Das Ziel dieser Richtlinie ist die Harmonisierung der Datenschutzvorschriften der Mitgliedstaaten der Europäischen Union, um den freien Datenverkehr im Hinblick auf das Funktionieren des Binnenmarktes zu gewährleisten, allerdings unter gleichzeitiger Wahrung des Schutzes der Grundrechte. Alle 15 EU Mitgliedstaaten haben zwischenzeitlich diese Richtlinie in ihr nationales Recht umgesetzt bzw. ihre bereits existierenden Datenschutzgesetze an diese Richtlinie angepasst. Der nachfolgende Text geht auf jene Grundsätze und Bestimmungen ein, die bei der Verwendung personenbezogener Daten in Informationssystemen zu beachten sind und führt auch die Gründe für die zulässigen Ausnahmen vom Geheimhaltungsschutz an. Darüber hinaus geht der Text auch auf den Bericht der Europäischen Kommission über die Durchführung der Datenschutzrichtlinie ein.

1. Einleitung

Das Datenschutzrecht hat sich in Europa seit Beginn der 70er-Jahre kontinuierlich entwickelt und umfasst heute alle Bereiche des gesellschaftlichen Lebens. Bemerkenswert ist in diesem Zusammenhang die Tatsache, dass die EG dem Datenschutz lange Zeit ablehnend gegenüberstand, befürchtete sie doch negative Einflüsse auf die wirtschaftliche Entwicklung und die Integrationsbestrebungen durch die Behinderung des freien Datenflusses. Erst mit der Empfehlung vom 29. 6. 1981 [EU81] wurde den Mitgliedstaaten nahegelegt, die Datenschutzkonvention des Europarates bis Ende 1981 zu zeichnen und bis Ende 1982 zu ratifizieren. Der gleichzeitig angekündigten Maßnahme, nämlich bei Nichtunterzeichnung der Konvention des Europarates eine Datenschutz-Richtlinie auszuarbeiten und vorzuschlagen, kam die EG erst acht Jahre später nach, obwohl die Mitgliedstaaten der Empfehlung zur Ratifizierung der Datenschutz-Konvention sehr zögerlich nachkamen; so hatte bis Ende 1982 kein einziger Mitgliedstaat der EG die Konvention ratifiziert.

Erst die politische Entwicklung – hier vor allem die Vollendung des Binnenmarktes, aber auch die sich abzeichnende EU – führte dazu, dass sich die Kommission nunmehr eingehend mit der Materie des Datenschutzes auseinandersetzte. Dies führte schlussendlich dazu, dass die Kommission am 18. 6. 1990 einen Richtlinienentwurf vorlegte. Es dauerte dann noch fünf Jahre und bedurfte vieler Änderungen und Ergänzungen, bis dieser Entwurf schlussendlich als „**Richtlinie 95/46/EG des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr**“ am 24. Oktober 1995 [EU95] verabschiedet wurde (Datenschutz-Richtlinie).

Ziel dieser Datenschutz-Richtlinie (DS-RL) ist die Harmonisierung der Datenschutzvorschriften der Mitgliedstaaten der EU, die – bedingt durch den unterschiedlichen Regelungsinhalt der einzelnen nationalen Datenschutzgesetze – notwendig wurde, um einen Raum zu schaffen, in dem der freie Verkehr von Daten im Hinblick auf das Funktionieren des Binnenmarktes durch nationale Grenzen nicht behindert wird, selbstverständlich unter gleichzeitiger Beachtung des Schutzes der Grundrechte [DS97]. Die in der Richtlinie vorgesehene Umsetzungsfrist von drei Jahren – somit spätestens 24. Oktober 1998 – wurde zwar von den wenigsten Mitgliedstaaten eingehalten, in der Zwischenzeit verfügen aber alle 15 Mitgliedstaaten über nationale Datenschutzgesetze.

Gegenstand der einzelnen nationalen Datenschutzgesetze ist die Gewährleistung und Achtung der Grundrechte und -freiheiten, vor allem des in Art. 8 der Europäischen Konvention zum Schutz der Grundrechte und Grundfreiheiten (EMRK) und in den allgemeinen Grundsätzen des Gesellschaftsrechtes anerkannten Rechts auf die Privatsphäre. Art. 8 EMRK lautet vollständig:

„Recht auf Achtung des Privat- und Familienlebens

> *(1) Jedermann hat Anspruch auf Achtung seines Privat- und Familienlebens, seiner Wohnung und seines Briefverkehrs*
>
> *(2) Der Eingriff einer öffentlichen Behörde in die Ausübung dieses Rechtes ist nur statthaft, insoweit dieser Eingriff gesetzlich vorgesehen ist und eine Maßnahme darstellt, die in einer demokratischen Gesellschaft für die nationale Sicherheit, die öffentliche Ruhe und Ordnung, das wirtschaftliche Wohl des Landes, die Verteidigung der Ordnung und zur Verhinderung von strafbaren Handlungen, zum Schutz der Gesundheit und der Moral oder zum Schutz der Rechte und Freiheiten anderer notwendig ist.”*

Es darf mit Fug und Recht behauptet werden, dass nunmehr innerhalb der EU ein Grundwertekonsens besteht, der den Datenschutz und den Schutz der Privatsphäre mit einschließt.

Primäre Aufgabe des Datenschutzes ist es, das Recht auf informationelle Selbstbestimmung des Einzelnen zu gewährleisten, das heißt, dass die BürgerInnen grundsätzlich selbst über die Offenlegung und Verwendung ihrer personenbezogenen Daten bestimmen.

Diese Grundrechte und Grundfreiheiten sind bei der Gestaltung der verschiedenen Informationssysteme dann entsprechend zu beachten, wenn personenbezogene Daten verwendet werden. Unter dem Begriff „**personenbezogene Daten“** werden im Sinne der DS-RL alle Informationen über eine bestimmte oder bestimmbare natürliche Person („**betroffene Person**“) verstanden; als bestimmbar wird eine Person angesehen, die direkt oder indirekt identifiziert werden kann, insbesondere durch Zuordnung zu einer Kennnummer oder zu einem oder mehreren spezifischen Elementen, die Ausdruck ihrer physischen, physiologischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität sind.

Der Datenbegriff in der DS-RL bedeutet im Sinne der angewandten Informatik eher „Informationen“. In der angewandten Informatik bedeutet nämlich der Begriff „Daten“ physikalische Signale in einer bestimmten Ordnung (Syntax). Zu „Informationen“ werden Daten aber erst dann, wenn sie eine bestimmte Bedeutung (Semantik), Wirkung und Relevanz (Pragmatik) aufweisen [DPW02].

Unter Informationssystemen versteht man die Summe aller geregelten betriebsinternen und betriebsexternen Informationsverbindungen sowie deren technische und organisatorische Einrichtungen zur Informationsgewinnung und -verarbeitung. Zielsetzung eines Informationssystems ist die rechtzeitige Versorgung der Handlungsträger mit allen notwendigen und relevanten Informationen in wirtschaftlich sinnvoller Weise [Ga97]. Aus der Fülle der verschiedenen Informationssysteme seien an dieser Stelle nur die wichtigsten betriebswirtschaftlichen und branchenspezifischen genannt, wie Führungsinformationssysteme (FIS), Personalinformationssysteme (PIS), Managementinformationssysteme (MIS), Marketinginformationssysteme, Bankeninformationssysteme, Versicherungsinformationssysteme, Krankenhausinformationssysteme (KIS) etc.

Da die DS-RL nicht zwischen elektronisch verarbeiteten und manuellen personenbezogenen Daten differenziert, sind die Grundsätze des Datenschutzes nicht nur bei computergestützten Informationssystemen, sondern auch bei manuell geführten Informationssystemen zu beachten, wobei letztere in der Praxis kaum eine Rolle spielen werden.

Im Einzelnen sind nun bei der Verwendung personenbezogener Daten in Informationssystemen zwingend folgende Grundsätze zu beachten:

- Grundsätze in Bezug auf die Qualität der Daten
- Grundsätze in Bezug auf die Zulässigkeit der Verarbeitung von Daten
- Verarbeitung besonderer Kategorien personenbezogener Daten
- Verarbeitung personenbezogener Daten und Meinungsfreiheit
- Information der **betroffenen Person**
- Auskunftsrecht der **betroffenen Person**
- Widerspruchsrecht der **betroffenen Person**

- Automatisierte Einzelentscheidungen
- Vertraulichkeit und Sicherheit der Verarbeitung
- Pflicht zur Meldung bei der Kontrollstelle
- Vorabkontrolle
- Übermittlung personenbezogener Daten in Drittländer

2. Die Grundsätze der DS-RL im Einzelnen

2.1 Grundsätze in Bezug auf die Qualität der Daten

Art. 6 der DS-RL enthält nachstehende Qualitätsgrundsätze:

- **Fairness und Rechtmäßigkeit**; das bedeutet, dass die **betroffene Person** über die Umstände der Verarbeitung ihrer Daten informiert wird und über ihre Rechte nicht im Unklaren gelassen bzw. sogar irrgeführt werden darf.
- **Strikte Zweckbindung**; das heißt, bereits vor der Ermittlung der personenbezogenen Daten muss der Zweck dieser Datenermittlung spezifiziert werden (zB Marketinginformationssystem). Weiters ist zu beachten, dass die Daten nur für rechtmäßige Zwecke ermittelt und auch nur für diese weiterverwendet werden dürfen. Ein nicht-rechtmäßiger Zweck wird dann gegeben sein, wenn die Interessenabwägung zwischen dem vom für die **Verarbeitung Verantwortlichen** verfolgten Ziel und der Schwere des Eingriffs in die Privatsphäre zugunsten der **betroffenen Person** entschieden werden muss.
- **Begrenzung des Datenumfanges**; die Daten müssen für die Datenverarbeitung bedeutungsvoll sein, das heißt, dass ein Anlegen eines Datenvorrates für eine zum Zeitpunkt der Ermittlung noch nicht definierte Datenverarbeitung nicht gestattet ist.
- **Richtigkeit und Aktualität**; der für die **Verarbeitung Verantwortliche** ist auch für die sachliche Richtigkeit und Aktualität verantwortlich. Diese Bestimmung ist notwendig, um der **betroffenen Person** ungerechtfertigte Nachteile zu ersparen (zB Ablehnung einer Kreditgewährung, weil der bereits ausbezahlte Vorkredit noch nicht gelöscht wurde u.ä.).
- **Zeitliche Begrenzung**; Daten dürfen nur so lange aufbewahrt werden, solange sie benötigt werden. Das heißt zB bis zur Beendigung eines Kunden- oder Lieferantenverhältnisses, jedoch immer unter Beachtung allfälliger gesetzlicher Aufbewahrungsfristen.

Der für die **Verarbeitung Verantwortliche** bleibt immer Herr der Daten, auch dann, wenn er sich eines **Auftragsverarbeiters** bedient.

2.2 Grundsätze in Bezug auf die Zulässigkeit der Verarbeitung von Daten

Art. 7 der DS-RL knüpft die Zulässigkeit der Verarbeitung von personenbezogenen Daten, wobei unter dem Verarbeitungsbegriff auch die Übermittlung dieser Daten subsumiert ist, an das Vorliegen konkreter Voraussetzungen, wie

- Zustimmung der **betroffenen Person** oder
- die Datenverarbeitung ist für die Vertragserfüllung zwischen dem für die **Verarbeitung Verantwortlichen** und der **betroffenen Person** notwendig (zB Kundenverkehr) oder
- die Datenverarbeitung ist notwendig zur Erfüllung einer rechtlichen Verpflichtung des für die **Verarbeitung Verantwortlichen** (zB Meldung von Beitragsdaten an die Krankenkasse u.ä.) oder
- die Verarbeitung ist erforderlich für die Wahrnehmung lebenswichtiger Interessen der **betroffenen Person** oder
- die Verarbeitung ist notwendig für die Wahrnehmung gesetzlich übertragener Aufgaben des öffentlichen Bereiches oder
- die Abwägung zwischen dem Interesse eines für die **Verarbeitung Verantwortlichen** an einer bestimmten Verarbeitung von personenbezogenen Daten und dem Interesse der **betroffenen Person** an der Geheimhaltung der ihn betreffenden personenbezogenen Daten geht zugunsten des für die **Verarbeitung Verantwortlichen** aus.

2.3 Verarbeitung besonderer Kategorien personenbezogener Daten

Art. 8 der DS-RL sieht ein generelles Verarbeitungsverbot besonders schutzwürdiger Daten vor; das sind Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie von Daten über Gesundheit oder Sexualleben. Die Ausnahmen von diesem generellen Verarbeitungsverbot sind in Art. 8 der DS-RL taxativ aufgezählt, und zwar dürfen diese sensiblen Daten nur unter folgenden Voraussetzungen verarbeitet werden:

- Vorliegen einer ausdrücklichen Zustimmung der **betroffenen Person.**
- Die Verarbeitung ist erforderlich, um den Rechten und Pflichten des für die **Verarbeitung Verantwortlichen** auf dem Gebiet des Arbeitsrechts Rechnung zu tragen.

- Die Verarbeitung ist notwendig zum Schutz lebenswichtiger Interessen der **betroffenen Person,** und diese ist aus physischen oder rechtlichen Gründen außer Stande, eine Einwilligung zu geben.
- Verarbeitungen durch nicht auf Gewinn ausgerichtete Vereinigungen mit politischen, philosophischen, religiösen oder gewerkschaftlichen Tätigkeiten, wobei ein regelmäßiger Kontakt zwischen den **betroffenen Personen** und dem für die **Verarbeitung Verantwortlichen** besteht.
- Der Betroffene hat die Daten offenkundig selbst öffentlich gemacht oder sie sind zur Geltendmachung, Ausübung oder Verteidigung rechtlicher Ansprüche vor Gerichten erforderlich.
- Die Verarbeitung der Daten erfolgt zum Zweck der Gesundheitsvorsorge, der medizinischen Diagnostik, der Gesundheitsvorsorge oder der Behandlung sowie für die Verwaltung von Gesundheitsdaten. Allerdings ist die Verarbeitung dieser Daten an das ärztliche Personal gebunden, das einem besonderen Berufsgeheimnis unterliegt.

2.4 Verarbeitung personenbezogener Daten und Meinungsfreiheit

Art. 9 der DS-RL sieht für Medienunternehmen und Mediendienste für deren publizistische Tätigkeit eine Ausnahmeregelung vor. Dieses Medienprivileg betrifft aber nur den journalistischen Kernbereich, jedoch nicht die allgemeinen Datenverarbeitungen wie zB die Abonnentenverwaltung, die Personalverwaltung etc.

2.5 Information der betroffenen Person

Art. 10 der DS-RL sieht eine Informationspflicht des für die **Verarbeitung Verantwortlichen** an die **betroffene Person** vor der Datenermittlung vor, und zwar über die Identität des für die **Verarbeitung Verantwortlichen** sowie über die Zweckbestimmung der Verarbeitung und bei Notwendigkeit über die Empfänger der Daten sowie auch darüber, ob die Beantwortung der Fragen obligatorisch oder freiwillig ist, sowie über das Bestehen von Auskunfts- und Berichtigungspflichten.

2.6 Auskunftsrecht der betroffenen Person

Art. 12 der DS-RL sieht vor, dass der **betroffenen Person** auf ihr Verlangen hin Auskunft über die Zweckbestimmung der sie betreffenden Verarbeitungen, die Kategorien der Daten, die Herkunft der Daten (soweit verfügbar) und die Empfänger oder Kategorien der Empfänger, an die die Daten übermittelt wurden, erhält. Die Auskunft ist in verständlicher Form zu erteilen, das heißt, dass allfällige interne Codes, technische Abkürzungen und fremdsprachige Ausdrücke für eine **betroffene Person** ausreichend zu verdeutlichen oder zu erläutern sind, um unter Anlegung einer Durchschnittsbetrachtung die Verständlichkeit der Auskunft zu gewährleisten.

Falsche Daten sind richtig zu stellen, rechtswidrig ermittelte und verarbeitete Daten sind zu löschen oder zu sperren. Bei Datenübermittlungen sind die Empfänger über diese Umstände entsprechend zu informieren.

Beschränkungen des Auskunftsrechtes können sich bei überwiegenden öffentlichen Interessen, die einer Auskunftserteilung entgegenstehen, ergeben (zB für die Sicherheit des Staates, die Landesverteidigung, die öffentliche Sicherheit etc.) bzw. zum Schutz der **betroffenen Person** und der Rechte und Freiheiten anderer Personen.

2.7 Widerspruchsrecht der betroffenen Person

Art. 14 der DS-RL sieht ein Widerspruchsrecht der **betroffenen Person** gegen die Verarbeitung der sie betreffenden personenbezogenen Daten dann vor, wenn schutzwürdige Geheimhaltungsinteressen des Betroffenen verletzt werden.

Während in Art. 7 DS-RL der Regelfall angesprochen wird – also die Interessenlage einer durchschnittlichen **betroffenen Person** analysiert wird – stellt dieses Widerspruchsrecht nach Art. 14 auf den Sonderfall ab, dass die Datenverarbeitung zwar zulässig ist, eine aus der spezifischen Situation der **betroffenen Person** heraus erfolgende Interessenabwägung aber zugunsten der **betroffenen Person** ausfällt.

2.8 Automatisierte Einzelentscheidungen

Art. 15 der DS-RL sieht ein Verbot der ausschließlich computergestützt durchgeführten Entscheidungen über Lebenschancen von Menschen vor, wie zB über die Kreditwürdigkeit, Charaktereigenschaften u.ä., die die **betroffene Person** erheblich beeinträchtigen könnten. Während für die **betroffene Person** positive Entscheidungen zulässig sind, ist bei negativen Entscheidungen der **betroffenen Person** die Möglichkeit zu geben, ihren Standpunkt geltend zu machen. Art. 12 der DS-RL sieht in diesem Zusammenhang auch eine Offenlegung der Programmlogik der computergestützt durchgeführten Entscheidungen vor.

2.9 Vertraulichkeit der Verarbeitung

Personen – sowohl beim für die **Verarbeitung Verantwortlichen** als auch beim **Auftragsverarbeiter** – die Zugang zu personenbezogenen Daten haben, sind zur Vertraulichkeit zu verpflichten.

2.10 Sicherheit der Verarbeitung

Art. 17 der DS-RL verlangt zur Sicherstellung der Datensicherheit, dass je nach Art der verwendeten Daten, deren Umfang und Zweck der Verarbeitung und unter Betrachtnahme auf den Stand der technischen Möglichkeiten sowie auf die wirtschaftliche Vertretbarkeit, Maßnahmen getroffen werden, damit die Daten vor zufälliger oder unrechtmäßi-

ger Zerstörung und vor Verlust geschützt sind, sowie dass die Verarbeitung der Daten ordnungsgemäß erfolgt und diese Daten Unberechtigten nicht zur Kenntnis gelangen.

Betreibt der für die **Verarbeitung Verantwortliche** das betreffende Informationssystem nicht selbst, sondern bedient er sich eines **Auftragsverarbeiters**, so muss sich der für die **Verarbeitung Verantwortliche** davon überzeugen, dass auch der **Auftragsverarbeiter** einen angemessenen Grad an Datensicherheit gewährleistet.

Als Grundlage des Auftragsverhältnisses zwischen dem **Verantwortlichen der Verarbeitung** und dem **Auftragsverarbeiter** ist ein entsprechender Vertrag abzuschließen, der u.a. festhält, dass der **Auftragsverarbeiter** nur über Weisung des für die **Verarbeitung Verantwortlichen** handelt.

Datensicherheit wird durch eine Kombination von

- organisatorischen,
- personellen,
- technischen und
- baulichen

Sicherungsmaßnahmen erreicht. Es ist empfehlenswert – ausgehend von einem zu bearbeitendem Gefährdungskatalog, wobei sich hier als Grundlage der im IT-Grundschutzhandbuch des Bundesamtes für Sicherheit in der Informationstechnik (BSI) enthaltene Gefährdungskatalog empfiehlt – eine Risikoanalyse anzustellen und davon abhängig entsprechende Sicherheitsmaßnahmen zu treffen.

Die getroffenen Datensicherheitsmaßnahmen sind entsprechend zu dokumentieren (zB in Form eines Datensicherheitshandbuches).

2.11 Pflicht zur Meldung bei der Kontrollstelle

Art. 18 der DS-RL sieht vor, dass der für die **Verarbeitung Verantwortliche** seine Verarbeitungen an eine in den einzelnen Mitgliedstaaten eingerichtete Kontrollstelle meldet. Erleichterungen bestehen für festgelegte Verarbeitungskategorien (sogenannte Standardverarbeitungen), die von der Meldepflicht ausgenommen sind, sowie für den Sonderfall Deutschland, das als einziger Mitgliedstaat die Bestellung eines betrieblichen Datenschutzbeauftragten vorgesehen hat, der die Aufgabe eines Registers übernimmt.

2.12 Vorabkontrolle

Art. 20 der DS-RL sieht vor, dass für Verarbeitungen, welche spezifische Risken für die Rechte und Freiheiten der **betroffenen Person** beinhalten, diese Verarbeitungen vor ihrem Beginn durch in den einzelnen Mitgliedstaaten eingerichtete Kontrollstellen geprüft werden.

2.13 Übermittlung personenbezogener Daten in Drittländer

Als Ergebnis der durch die DS-RL erreichte Harmonisierung der datenschutzrechtlichen Rechtvorschriften der EU-Mitgliedstaaten ist die datenschutzrechtliche Kontrolle des Datenverkehrs zwischen den 15 EU-Mitgliedstaaten entfallen. Damit ist das Funktionieren des Binnenmarktes, das heißt der freie Verkehr von Waren, Personen, Dienstleistungen und Kapital gewährleistet.

Ein Datenexport in Drittländer ist jedoch nach den Bestimmungen des Art. 25 der DS-RL nur dann zulässig, wenn diese ein angemessenes Schutzniveau gewährleisten, oder aber es liegen gemäß Art. 26 die nachfolgenden Voraussetzungen vor:

- Die **betroffene Person** hat ohne jeden Zweifel ihre Einwilligung gegeben oder
- die Übermittlung ist für die Erfüllung eines Vertrages zwischen der **betroffenen Person** und dem für die **Verarbeitung Verantwortlichen** oder zur Durchführung von vorvertraglichen Maßnahmen notwendig oder
- die Übermittlung ist zum Abschluss oder zur Erfüllung eines Vertrages erforderlich oder
- die Übermittlung ist erforderlich bzw. gesetzlich vorgeschrieben für die Wahrung eines wichtigen öffentlichen Interesses oder für die Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen vor Gericht oder
- die Übermittlung ist für die Wahrung lebenswichtiger Interessen der **betroffenen Person** erforderlich oder
- die Übermittlung erfolgt aus einem Register, das gemäß den Rechts- oder Verwaltungsvorschriften des betreffenden EU-Mitgliedstaates zur Information der Öffentlichkeit bestimmt ist.

3. Erfahrungen mit der DS-RL

Knapp acht Jahre nach Verabschiedung der DS-RL am 24. Oktober 1995 hat die Kommission der Europäischen Gemeinschaften am 15. Mai 2003 ihren ersten Bericht über die Durchführung der DS-RL vorgelegt [EU03]. Aufgrund der Bestimmungen des Art. 32 Abs. 1 der DS-RL ist nämlich vorgesehen, dass die Kommission erstmals drei Jahre nach Ablauf der Umsetzungsfrist einen Bericht über die Durchführung dieser Richtlinie vorlegt und allenfalls Änderungsvorschläge beifügt. Der erste Bericht hätte demnach am 24. Oktober 2001 vorgelegt werden müssen.

Die Verspätung von mehr als 18 Monaten ist deshalb entstanden, weil einzelne Mitgliedstaaten die Richtlinie nicht zeitgerecht umgesetzt haben. Bereits im Dezember 1999

verklagte die Kommission Frankreich, Deutschland, Irland, Luxemburg und die Niederlande vor dem Gerichtshof der Gemeinschaften, weil diese Länder in Verzug waren.

Die Kommission stellt in ihrem Bericht richtigerweise fest, dass die Entwicklung in der Informationstechnologie einerseits und die wachsenden Sicherheitsbedenken andererseits die Datenschutzdiskussion verschärft hat. Besonders hervorgehoben werden Kameraüberwachungssysteme (CCTV) sowie Spyware. Die Kommission stellt berechtigterweise die Frage, ob die bestehenden Rechtsvorschriften dem Stand der Technik überhaupt noch entsprechen. Besonders hervorgehoben wird die Tatsache, dass Gesetze mit geographischem Geltungsbereich im Zeitalter des Internets immer mehr an Bedeutung verlieren. Die Kommission weist darauf hin, dass sie durch die „**Richtlinie 97/66/EG des Europäischen Parlaments und des Rates vom 15. Dezember 1997 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der Telekommunikation**“ [EU98] auf diese Herausforderung entsprechend reagiert hat, ebenso wie durch die „**Richtlinie 2002/58 EG vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation**“ [EU02a].

Als weiteres Problem wird die – auf Grund der steigenden Bedeutung des Humankapitals – intensivierte Datenerhebung am Arbeitsplatz angesehen. Da Art. 137 Abs. 2 des Vertrages gesetzgeberische Maßnahmen der EU in diesem Bereich zulässt, plant die EU die Schaffung eines europäischen Rahmens mit Grundsätzen und Regeln für einen verbesserten Datenschutz am Arbeitsplatz.

Weiters weist die Kommission in ihrem Bericht auf ihren Vorschlag für eine „**Richtlinie des Europäischen Parlaments und des Rates zur Harmonisierung der Rechts- und Verwaltungsvorschriften der Mitgliedstaaten über den Verbraucherschutz**“ [EU02b] hin.

Prinzipiell sieht die Kommission derzeit keinen Grund, Vorschläge zur Änderung der DS-RL zu unterbreiten, und zwar primär deshalb, weil die Erfahrung mit der Durchführung der DS-RL auf Grund der verspäteten Umsetzung durch die meisten Mitgliedstaaten sehr begrenzt ist und sie darüber hinaus der Meinung ist, dass die meisten Schwierigkeiten die bei der Überprüfung der Umsetzung ermittelt wurden, ohne Änderung der DS-RL behoben werden können. Viele dieser Vorschläge, die von den einzelnen EU-Mitgliedstaaten eingebracht wurden, würden auch zu einer Senkung des Datenschutz-Niveaus führen.

Die von der Kommission durchgeführte Analyse der Umsetzung der DS-RL in den 15 EU-Mitgliedstaaten ergab folgendes Ergebnis:

- **Verspätete Umsetzung**; die übermäßige Verzögerung bei der Umsetzung wurde von der Kommission unmissverständlich verurteilt.
- **Freier Datenverkehr**; der Hauptzweck der DS-RL ist nach Ansicht der Kommission gelungen, auch wenn es noch die eine oder andere Behinderung gibt.

- **Hohes Datenschutzniveau**; die Kommission ist der Meinung, dass das mit der DS-RL angestrebte Ziel, nämlich ein hohes Datenschutzniveau in der EU zu erreichen, gelungen ist.
- **Qualität der Daten und Grundsätze in Bezug auf die Zulässigkeit der Verarbeitung von Daten (Art. 6 und 7)**; die Umsetzung dieser Bestimmungen ist nach Meinung der Kommission nicht zufriedenstellend erfolgt, besonders hinsichtlich der Auslegung des Begriffes „Einwilligung ohne jeden Zweifel“ (Art. 7 a) und den Begriff der „ausdrücklichen“ Einwilligung (Art. 8).
- **Information der betroffenen Person (Art. 10 und 11)**; die Überprüfung ergab eine Reihe von Abweichungen gegenüber den Bestimmungen der DS-RL.
- **Meldung (Art. 18 und 19)**; hinsichtlich der Meldungen von Verarbeitungen monieren einige Staaten den hohen Verwaltungsaufwand, weil sie die Möglichkeiten der in der DS-RL vorgesehenen Vereinfachungen nicht erkannt haben.
- **Übermittlung personenbezogener Daten in Drittländer (Art. 25 und 26)**; hier wurden durch die Kommission enorme Abweichungen zwischen den Rechtsvorschriften der Mitgliedstaaten und den einschlägigen Bestimmungen der DS-RL festgestellt.

Der nächste Bericht der Kommission ist für das Jahr 2004 vorgesehen.

4. Resümee

Das rechtliche Instrumentarium der EU umfasst Verordnungen, Richtlinien, Entscheidungen sowie Empfehlungen. Richtlinien sind innerhalb festgesetzter Fristen in nationales Recht umzusetzen, wobei die Richtlinien üblicherweise wenig Raum für differenzierte Auslegungen zulassen. Die DS-RL ist allerdings eine Richtlinie, die den einzelnen EU-Mitgliedstaaten einen eher unüblich breiten Raum gelassen hat, um nationale spezifische Regelungen zu berücksichtigen. Als Beispiel sei nur die Beibehaltung des Datenschutzbeauftragen im deutschen Bundesdatenschutzgesetz (BDSG) [SW77] sowie der Schutz der Daten juristischer Personen im österreichischen Datenschutzgesetz (DSG 2000) angeführt. Diese Tatsache hat nach Meinung des Autors dazu geführt, dass es bei der Umsetzung der DS-RL zu unterschiedlichen Interpretationen und damit auch zu unterschiedlichen Umsetzungen einzelner Bestimmungen der DS-RL durch die EU-Mitgliedstaaten gekommen ist. Die einzelnen Regierungen werden noch einiges zu tun haben, um eine bessere Anwendung der DS-RL zu gewährleisten.

Literaturverzeichnis

[DPW02] Dohr, W.; Pollirer, H.-J.; Weiss, E.: Datenschutzgesetz 2000. Manz, Wien, 2002

[DS97] Dammann, U.; Simitis, S.: EG-Datenschutzrichtlinie. Nomos Verlagsgesellschaft, Baden-Baden, 1997.

[EU02a] Europäisches Parlament; Rat der Europäischen Union: ABl. L 201 vom 31. 7. 2002, S 37-47.

[EU02b] Kommission der Europäischen Gemeinschaften: KOM (2002) 443 endgültig vom 11. 9. 2002.

[EU03] Kommission der Europäischen Gemeinschaften: KOM (2003) 265 endgültig vom 15. 5. 2003.

[EU81] Empfehlung der Kommission vom 29. 6. 1981 betreffend ein Übereinkommen des Europarats zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten. ABl. EG L 241/31 vom 25. 8. 1981.

[EU95] Europäisches Parlament; Rat der Europäischen Union: ABl. L 281 vom 23. 11. 1995, S. 31.

[EU98] Europäisches Parlament; Rat der Europäischen Union: ABl. L 24 vom 30. 1. 1998, S 1-8.

[Ga97] Gabler Wirtschafts Lexikon. Gabler Verlag, Wiesbaden, 1997.

[SW77] Schaffland, H.-J.; Wiltfang, N.: Bundesdatenschutzgesetz (BDSG), Erich Schmidt Verlag, Berlin, 1977.