

## **Schlagwort: EU-Datenschutzrichtlinie**

Der Ministerrat der EU-Mitgliedsstaaten hat am 24. Juli 1995 die "Richtlinie zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr" endgültig verabschiedet. Dieser Beschluß wurde einstimmig angenommen - bei Enthaltung des Vereinigten Königreichs.

Mit dieser Rahmenrichtlinie soll gem. Ziff. 4 und 6 der Erwägungsgründe für Europa ein einheitlicher Datenschutzstandard und damit die Grundlage für einen freien, ungehinderten Datenverkehr geschaffen werden. Ziel der vorangegangenen vierjährigen Verhandlungen war, die unterschiedlichen Regelungs- und Kontrollsysteme der Mitgliedsstaaten zu erhalten, sofern sie einen äquivalenten Schutz bieten. Anderenfalls hätte man mit einem erheblichen Anstieg des bürokratischen Aufwands gerechnet, ohne das Schutzniveau für die Betroffenen zu erhöhen. Die unterschiedlichen Regelungen der Mitgliedsstaaten führten insbesondere zu Diskussionen in Bezug auf die

- Meldepflicht der Dateien,
- den Status und die Befugnisse der Kontrollbehörden und
- die Informationspflichten der Verarbeiter gegenüber den Betroffenen.

Die Richtlinie basiert auf der Verantwortung des Verarbeiters für die von ihm oder in seinem Auftrag vorgenommene Datenverarbeitung gegenüber den Betroffenen. Sie geht grundsätzlich von einem Verbot der Verarbeitung personenbezogener Daten aus; unterbestimmten in Art. 7 aufgeführten Voraussetzungen ist die Verarbeitung gleichwohl erlaubt (Erlaubnisvorbehalt).

Im folgenden sollen wesentliche Aspekte der Richtlinie dargestellt werden.

### **Inkrafttreten**

Die Richtlinie tritt entsprechend Art. 191 EG-Vertrag am 20. Tag nach ihrer Veröffentlichung im Amtsblatt der EG in Kraft.

Nach der Annahme der Richtlinie durch den Ministerrat müssen die Mitgliedsstaaten binnen einer Frist von 3 Jahren die Bestimmungen der Richtlinie in nationales Datenschutzrecht umsetzen. In Deutschland liegt die Umsetzung für die Bundesregierung in der Hand des Bundesministeriums des Innern. Die Umsetzung der Richtlinie für den öffentlichen Sektor liegt in der Hand der Bundesländer.

Nach der Anpassung der nationalen Rechtsvorschriften haben die Unternehmen gem. Art. 32 der Richtlinie 3 weitere Jahre Zeit zur Anpassung an die nationale Gesetzgebung.

Während dieser Übergangszeit können unterschiedliche Standards in der Datenschutzgesetzgebung der Mitgliedsstaaten bestehen. Dies kann sich hinderlich auf die freie Übertragung personenbezogener Daten auswirken bis zur Beeinträchtigung des freien Verkehrs personenbezogener Daten.

### **Gültigkeitsbereich**

Die Richtlinie bezieht sich sowohl auf den privaten als auch auf den öffentlichen Sektor. Sie regelt die Verarbeitung personenbezogener Daten für Behörden, Institutionen und Unternehmen - aber nicht für Privatpersonen im Rahmen persönlicher oder familiärer Tätigkeit. Von der Richtlinie ebenfalls nicht erfaßt werden alle Bereiche des sog. Unionsrechts wie die gemeinsame Außen- und Sicherheitspolitik sowie die Zusammenarbeit der Mitgliedsstaaten in den Bereichen Justiz mit dem Bereich des Strafrechts und Inneres, die Innere Sicherheit und die Landesverteidigung - weiterhin Daten, die zum wirtschaftlichen Wohl des Staates erforderlich sind.

Der Schutzbereich erstreckt sich ausschließlich auf natürliche Personen und nicht auf juristische - allerdings kann dies im nationalen Bereich ergänzt werden.

### **Daten und Dateien**

Unter personenbezogenen Daten faßt die Richtlinie gem. Art. 2 sämtliche "Informationen über eine bestimmte oder bestimmbare natürliche Person (betroffene Person)". Derartigen Informationen können gem. Ziff. 14 der Erwägungsgründe auch Ton- und Bilddaten zugrundeliegen. Notwendige Voraussetzung der Richtlinie ist gem. Ziff. 26 der Erwägungsgründe allerdings die Identifizierbarkeit des Betroffenen; Art. 2 der Richtlinie führt dazu aus: "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, wirtschaftlichen, kulturellen oder sozialen Identität sind".

Ziff. 15 der Erwägungsgründe fordert einen "leichten Zugriff" auf diese Daten als Voraussetzung für die Anwendung der Richtlinie. Derartige sog. unbestimmte Rechtsbegriffe, Generalklauseln und Wahloptionen sind in der Richtlinie enthalten und müssen durch nationale Rechtsvorschriften ausgefüllt werden.

Die Richtlinie gilt gem. Art. 2 nicht nur für automatisierte sondern auch für strukturierte manuelle Sammlungen personenbezogener Daten. Damit werden also auch Sammlungen von Karteikarten erfaßt. In jedem Fall können die Sammlungen auch verteilt geführt werden. Unstrukturierte Akten fallen nicht unter die Richtlinie.

Generell wird allerdings auf die Verarbeitung von Daten abgestellt und nicht auf den klassischen Dateibegriff. Die Richtlinie stellt insgesamt nicht auf eine bestimmte Technik der Verarbeitung ab.

Neu in der Richtlinie ist in Art. 2 der Begriff des "Empfängers", der - neben dem aus dem BDSG bekannten "Dritten" - den Betroffenen, den Auftragsdatenverarbeiter sowie die Organisationseinheiten innerhalb der speichernden Stelle einbezieht. Bei Anfragen sind diese weiteren Tatbestände mitzuteilen.

Die **Erhebung** der Daten ist gem. Art. 2 der Richtlinie ein Teil der Verarbeitung. Entsprechend ist die nationale Gesetzgebung anzupassen.

### **Datenschutzbeauftragter**

Von der deutschen Delegation gefordert und in die Art. 18 und 20 aufgenommen wurde der interne Datenschutzbeauftragte - als ein von der deutschen Wirtschaft gefordertes Kontrollinstrument.

Gem. Richtlinie kann eine Meldung der Verarbeitung personenbezogener Daten entfallen, wenn vom für die Datenverarbeitung Verantwortlichen ein Datenschutzbeauftragter bestellt worden ist. Darüberhinaus ist eine Regelung aufgenommen worden, der entsprechend sog. weniger beeinträchtigende Verarbeitung gar nicht gemeldet werden muß; hierunter fällt in der Regel die Datenverarbeitung kleinerer Gewerbebetriebe, aber auch die von Vertretern der Heilberufe und von Anwälten, weil der Bruch des Berufsgeheimnisses gem. § 203 StGB geregelt ist sowie andere Übermittlungsbeschränkungen einen ausreichenden Schutz personenbezogener Datenverarbeitung gewährleisten.

Der interne Datenschutzbeauftragte ist gem. Art. 18 unabhängig bei der Überwachung der Einhaltung der nationalen Rechtsvorschriften.

Einzelheiten zum Rechtsverhältnis zwischen Datenschutzbeauftragtem, speichernder Stelle, Beschäftigten und Aufsichtsbehörde können im nationalen Recht festgelegt werden.

Dementsprechend könnten die Formulierungen des BDSG hinsichtlich des Status des internen Datenschutzbeauftragten beibehalten werden mit den folgenden sich aus der Richtlinie ergebenden notwendigen Ergänzungen:

- Der interne Datenschutzbeauftragte übernimmt im Falle der von der Meldepflicht ausgenommenen Verarbeitung die Funktion des Bundesbeauftragten für den Datenschutz bzw. Des Landesbeauftragten und der Aufsichtsbehörden der Länder. Er führt das - das behördliche Register ersetzende - Dateiverzeichnis.
- Dementsprechend erteilt der interne Datenschutzbeauftragte auch Auskunft aus dem Dateiverzeichnis auf Anfrage gem. Art. 21.

### **Vorabkontrolle**

Bei besonders sensibler Verarbeitung sieht Art. 20 eine Vorabkontrolle vor. Die Verantwortung für diese Prüfung der Rechtmäßigkeit besonders sensibler Datenverarbeitung trägt der interne Datenschutzbeauftragte. Allerdings wird eine Vorabkontrolle nur dann gefordert, wenn eine Verarbeitung der Meldepflicht unterliegt; die Meldepflicht kann gesetzlich vorgesehen werden - auch dann, wenn ein interner Datenschutzbeauftragter vorhanden ist.

Eine risikoreiche Zweckbestimmung einer Datei (Risikodatei) ist nach Nr. 53 und 54 der Erwägungsgründe die Zielsetzung, "betroffene Personen von der Inanspruchnahme eines Rechts, einer Leistung oder eines Vertrags auszuschließen". Dabei kann an sog. Warndateien der Versicherer gedacht werden sowie an Verfahren zur Erkennung kreditwürdiger Personen (Persönlichkeitsprofile). Der Begriff der Risikodatei muß national vom Gesetzgeber konkretisiert werden.

### **Zulässigkeit der Verarbeitung**

Grundsätzlich darf die Verarbeitung personenbezogener Daten gem. Art. 7 nur erfolgen, wenn u.a. eine der folgenden Voraussetzungen erfüllt ist:

- Einwilligung des Betroffenen zur Verarbeitung,
- Erfüllung eines mit dem Betroffenen geschlossenen Vertrags oder

- die Verarbeitung zur Verwirklichung eines berechtigten Interesses eines Verantwortlichen ist erforderlich - sofern nicht das Interesse des Betroffenen überwiegt.

Damit ist die Einwilligung nicht mehr die alleinentscheidende Voraussetzung; vielmehr treten andere Tatbestände gleichberechtigt daneben.

### **Zweckbindung**

Während gem. Art. 6 Daten nur für festgelegte eindeutige und rechtmäßige Zwecke erhoben werden dürfen, dürfen sie sehr wohl in einer nur mit diesen Zweckbestimmungen zu vereinbarenden Weise weiterverarbeitet werden. Damit ist eine freiere Verarbeitung möglich als mit der Erhebung einmal geplant war.

Dies gilt, ohne den Betroffenen über die Weiterung informieren zu müssen.

### **Informationspflicht**

Die Art. 10 und 11 regeln die Information Betroffener bei der Erhebung personenbezogener Daten und bei der Weitergabe oder Speicherung. Art. 21 formuliert eine Informationspflicht auf Antrag für jedermann, sofern Verarbeitungen von der Meldung an die Kontrollstelle ausgenommen sind.

Betroffene haben nach Art. 14 ein Widerspruchsrecht. Bei Verwendung der Daten Betroffener zum Zwecke der Direktwerbung haben diese entweder das Widerspruchsrecht entsprechend BDSG Art. 14 oder - nach dem dänischen Modell - die zusätzliche Informationspflicht des Verantwortlichen der Verarbeitung gegenüber dem Betroffenen vor der ersten Weitergabe personenbezogener Daten.

### **Auskunftsinhalt**

Das Auskunftsrecht erstreckt sich gem. Art. 12 neben einer Verarbeitungsbestätigung, auf die Zweckbestimmung, Empfänger, Art und Herkunft der Daten sowie auf den "logischen Aufbau" der automatisierten Verarbeitung. Das bedeutet, daß dem Betroffenen eine Auskunft erteilt werden muß, auf welche Informationen sich das System stützt und nach welchen Kriterien die Aufnahme der Daten erfolgt ist.

### **Auskunftsrecht bei automatisierter Einzelentscheidung**

Gegen ausschließlich automatisiert herbeigeführte Entscheidungen können Betroffene ihren Standpunkt geltend machen und eine Überprüfung dieser Entscheidung durch einen Menschen verlangen. Voraussetzung ist, daß diese Entscheidungen zum Zwecke der Bewertung einzelner Aspekte ihrer Person - mit negativen rechtlichen Folgen oder mindestens erheblicher beeinträchtigender Wirkung gefällt wurden. Bei der Vorschrift wurde an Entscheidungen aufgrund gespeicherter Persönlichkeitsprofile o.ä. gedacht.

### **Besondere Kategorien personenbezogener Daten**

Untersagt ist entsprechend Art. 8 die "Verarbeitung personenbezogener 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." Allerdings gilt dieses Verarbeitungsverbot nicht generell; vielmehr findet es in den folgenden Fällen keine Anwendung:

- Der Betroffene hat in die Verarbeitung eingewilligt,
- die Verarbeitung ist zum Schutz lebenswichtiger Interessen der betroffenen Person oder eines Dritten erforderlich und der Betroffene konnte aus physischen oder rechtlichen Gründen keine Einwilligung geben oder
- eine politisch, philosophisch, religiös oder gewerkschaftlich ausgerichtete Stiftung oder Vereinigung verarbeitet die personenbezogenen Daten ihrer Mitglieder.

Die Regelung gilt ebenfalls nicht für Daten aus dem Gesundheitsbereich - die bekanntlich hinreichend durch vorhandene Geheimhaltungspflichten und Berufgeheimnisse geschützt sind.

### **Erhebung anderenorts**

Werden Daten nicht beim Betroffenen erhoben, so muß er gem. Art. 11 spätestens erst bei der ersten Übermittlung informiert werden. Die Information kann u.a. dann unterlassen werden, wenn sie einen unverhältnismäßigen Aufwand erfordert.

### **Grenzüberschreitender Datenverkehr**

Hat ein Unternehmen Niederlassungen im Hoheitsgebiet mehrerer Mitgliedsstaaten, so hat es die im jeweiligen Hoheitsgebiet geltenden Rechtsvorschriften zu beachten. Der Begriff "Niederlassung" be-

deutet nach den Erwägungsgründen die "effektive und tatsächliche Ausübung einer Tätigkeit mittels einer festen Einrichtung"; die Rechtsform der Niederlassung ist unerheblich. Sofern eine Niederlassung nicht vorhanden ist, gilt das Recht des übermittelnden Mitgliedsstaates.

Bei einer Umsetzung der Richtlinie in nationales Recht müssen die Ausnahmetatbestände und die Vertragslösung berücksichtigt werden.

### **Drittländer**

Die Übermittlung in Staaten außerhalb der EU ist gem. Art. 25 zulässig, wenn dieses Drittland ein angemessenes Schutzniveau gewährleistet.

Die Mitgliedsstaaten und die Kommission unterrichten einander über Drittländer, die kein angemessenes Schutzniveau gewährleisten und treffen erforderliche Maßnahmen, damit keine Datenübermittlungen in diese Drittländer erfolgen. Art. 25 regelt ein Konsultationsverfahren zwischen den Mitgliedsstaaten und der Kommission zur Lösung von Zweifelsfällen; dabei entscheidet ein Ausschuss von Regierungsvertretern der Mitgliedsstaaten gem. Art. 31 verbindlich über die Zulässigkeit der Übermittlung in das Drittland. Damit erhalten die Aufsichtsbehörden die Aufgabe, derartige Konsultationsverfahren einzuleiten und die von den Vertragspartnern ausgehandelten Garantien zu überprüfen; diese Garantien erlauben also einen Datentransfer in ein Drittland, in dem eine angemessene Datenschutzgesetzgebung nicht existiert.

Abweichend von dieser Regelung bestimmt Art. 26 die Voraussetzungen, unter denen gleichwohl ein Datentransfer stattfinden kann:

- Einwilligung des Betroffenen,
- Erfüllung eines mit dem Betroffenen geschlossenen Vertrags oder im Interesse des Betroffenen,
- Wahrung lebenswichtiger Interessen des Betroffenen oder
- öffentliches Interesse oder Transfer aus öffentlichen Registern.

Diese Regelungen der Richtlinie gehen über die bisherigen Bestimmungen des BDSG hinaus und müssen daher in nationales Recht umgesetzt werden.

### **Sicherheitsmaßnahmen**

Entsprechend Art. 17 sind technische und organisatorische Maßnahmen zum Schutz der Verarbeitung zu ergreifen gegen

- zufällige und unrechtmäßige Zerstörung sowie den zufälligen Verlust von Daten,
- unberechtigte Änderung und Weitergabe von Daten sowie "Zugang" - insbesondere im Netz und
- jede andere Form der unrechtmäßigen Verarbeitung.

"Diese Maßnahmen müssen unter Berücksichtigung des Standes der Technik und der bei ihrer Durchführung entstehenden Kosten ein Schutzniveau gewährleisten, das den von der Verarbeitung ausgehenden Risiken und der Art der zu schützenden Daten angemessen ist."

**Haftung:** Den Schadenersatz wegen einer rechtswidrigen Verarbeitung regelt Art. 23.

### **Sanktionen**

Gem. Art. 24 ergreifen die Mitgliedsstaaten geeignete Maßnahmen und erlassen Vorschriften, um die volle Anwendung der Bestimmungen dieser Richtlinie sicherzustellen und legen insbesondere Sanktionen fest, die bei Verstößen gegen die Vorschriften anzuwenden sind.

Die Vorschriften und die Sanktionen sind in nationalem Recht auszufüllen.

### **Inhaltlicher Spielraum**

Das in Deutschland erreichte Datenschutzniveau - sowie eine evtl. Weiterentwicklung - sollen Klarstellungen in den Art. 5, 7, 8 der Richtlinie sowie in den Ziffern 9 und 22 der Erwägungsgründe sicherstellen. Diese Regelungen geben ein Intervall vor, innerhalb dessen die Mitgliedstaaten nationale Rechtsvorschriften frei gestalten können, indem sie die Voraussetzungen der Verarbeitung personenbezogener Daten näher bestimmen. Dadurch können allerdings unter Beachtung des Gemeinschaftsrechts Unterschiede bei der Durchführung der Richtlinie auftreten, was Auswirkungen auf den Datenverkehr sowohl innerhalb eines Mitgliedsstaates als auch in der Gemeinschaft haben kann.

### **Datenschutzgruppe**

Die Art. 29 und 30 sehen eine Datenschutzgruppe mit beratender Funktion vor. Sie prüft die einzelstaatlichen Vorschriften, um zu einer einheitlichen Anwendung beizutragen; die Gruppe erstellt jährlich

einen Bericht. Die Datenschutzgruppe setzt sich aus Vertretern der Kontrollbehörden der Mitgliedsstaaten und der Gemeinschaft sowie einem Vertreter der Kommission zusammen.

#### **Ausschuß für Durchführungsmaßnahmen**

Die Kommission wird gem. Art. 31 von einem Ausschuß unterstützt, der sich aus Vertretern der Mitgliedsstaaten zusammensetzt und in dem der Vertreter der Kommission den Vorsitz führt. Der Ausschuß nimmt Stellung zu vom Vertreter der Kommission vorgeschlagenen Maßnahmen.

#### **Schlußbemerkungen**

Die Richtlinie zielt auf den - innerhalb der Europäischen Union (EU) - grenzüberschreitenden Verkehr personenbezogener Daten und legt dazu grundsätzliche Voraussetzungen fest. Damit wird der Datenschutz an die vorgegebene politische, soziale und technische Realität angepaßt. Ziel ist gem. Ziff. 3 der Erwägungsgründe, "die Errichtung und das Funktionieren des Binnenmarktes", und in dessen Rahmen eine "Angleichung" mit dem Ziel, "in der Gemeinschaft ein hohes Schutzniveau sicherzustellen".

Jedenfalls konnte bisher das unterschiedliche Schutzniveau bei der Verarbeitung personenbezogener Daten den grenzüberschreitenden Verkehr verhindern. Dieses Hemmnis ist nun - jedenfalls nach Anpassung der nationalen Rechtsvorschriften an die EU-Richtlinie - durch Festlegung eines innerhalb einer Bandbreite gleichwertigen Schutzniveaus beseitigt worden.

Art. 27 der Richtlinie und Ziff. 61 der Erwägungsgründe fordern die Mitgliedsstaaten und die Kommission auf, die betroffenen Wirtschaftskreise (Verbände) zu "ermutigen", interpretierende branchentypische Verhaltensregeln als Auslegungshilfe für die Praxis zu erarbeiten; diese werden dann von der Aufsichtsbehörde hinsichtlich ihrer Übereinstimmung mit den nationalen Rechtsvorschriften überprüft.

Insbesondere die deutsche Verhandlungsdelegation hat sich bemüht, die Regelungsdichte der Richtlinie zu reduzieren. Dies gilt für die Information des Betroffenen anlässlich der Erhebung in Art. 10 sowie die Speicherung und Weitergabe seiner Daten in Art. 11. Erreicht wurde auch die Beibehaltung des derzeitigen Status und die unterschiedlichen Kontrollrechte der Aufsichtsbehörden des Bundes und der Länder mit dem Beanstandungsrecht für die Kontrollbehörden des öffentlichen Sektors und Eingriffsbefugnisse für die Aufsichtsbehörden der Länder.

#### **Literatur:**

- Arbeitsgemeinschaft der Betriebs- und Personalräte der hochschulfreien Forschungseinrichtungen (AGBR): Europarichtlinie in neuer Fassung - Stellungnahme der AGBR. Datenschutz-Nachrichten 8 - 14, 4, 1994
- Bachmeier, R.: EG-Datenschutzrichtlinie - Rechtliche Konsequenzen für die Datenschutzpraxis. Recht der Datenverarbeitung 49 - 52, 2, 1995
- Bergmann, L.; Möhrle, R.; Herb, A.: Datenschutzrecht. Handkommentar Bundesdatenschutzgesetz, Datenschutzgesetze der Länder und Kirchen, bereichsspezifischer Datenschutz. Stuttgart 1996
- Brühann, U.: EU-Datenschutzrichtlinie - Umsetzung in einem vernetzten Europa. Datenschutz und Datensicherheit 66 - 72, 2, 1996 und Recht der Datenverarbeitung 12 - 17, 1, 1996
- Ellger, R.: Konvergenz oder Konflikt bei der Harmonisierung des Datenschutzes in Europa? EU-Datenschutzrichtlinie - Datenschutzkonvention des Europarats. Computer und Recht 558 - 569, 9, 1994
- EU: Richtlinie 95/47/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr. Amtsblatt der Europäischen Gemeinschaften L 281, 31 - 50, 38. Jahrg. 23. Nov. 1995
- Kopp, F.: Tendenzen der Harmonisierung des Datenschutzrechts in Europa. Datenschutz und Datensicherheit 204, 212, 4, 1995
- Lütke-meier, S.: EU-Datenschutzrichtlinie - Umsetzung in nationales Recht. Datenschutz und Datensicherheit 597 - 603, 10, 1995
- Rudolf, W.: Die europäische Datenschutz-Richtlinie und die Organisation der Datenschutzkontrolle. Datenschutz und Datensicherheit 446 - 447, 8, 1995
- Schneider, J.: Die EG-Richtlinie zum Datenschutz. Verbotssprinzip, betrieblicher Datenschutzbeauftragter, Haftung. Computer und Recht 35 - 39, 1, 1993
- Weber, M.: Der betriebliche Datenschutzbeauftragte im Lichte der EG-Datenschutzrichtlinie. Vortrag auf der BvD-Jahrestagung, Ulm 23. - 25. Okt. 1995. Datenschutz und Datensicherung 698 - 702, 12, 1995