Verwaltungs- und Verfassungsrecht

GEORGIOS GOUNALAKIS / ELMAR MAND

Die neue EG-Datenschutzrichtlinie – Grundlagen einer Umsetzung in nationales Recht (I)

Die EG-Richtlinie zum Datenschutz wurde am 24.10.1995 verabschiedet. Für die Umsetzung in nationales Recht steht den Mitgliedstaaten gem. Art. 32 Abs. 1 der Richtlinie ein Zeitrahmen von drei Jahren zur Verfügung. Der zweiteilige Beitrag beschreibt den Änderungsbedarf in der deutschen Datenschutzgesetzgebung, insbesondere im BDSG. Neben den notwendigen Änderungen in Einzelbestimmungen werden unter Einbeziehung der verfassungsrechtlichen Vorgaben, vor allem des Rechts auf informationelle Selbstbestimmung, auch die Auswirkungen auf die gesetzliche Regelungsstruktur erörtert. Obwohl der weite Spielraum, den die Richtlinie den Mitgliedstaaten bei der Umsetzung beläßt, die Möglichkeit eröffnet, i.S. einer Minimallösung Änderungen lediglich auf die Anpassung einzelner Vorschriften zu beschränken, erscheint im Interesse der effektiven Gewährleistung des Informationellen Selbstbestimmungsrechts und der Überschaubarkeit des Datenschutzrechts eine grundlegende Modifizierung des Regelungsgefüges jedoch unerläßlich.

I. Ausgangssituation

1. Bedeutung und Risiken der Verarbeitung personenbezogener Daten

a) Information als Produktionsfaktor

Die sich explosionsartig erweiternde Nutzung des Internet, das Drängen immer neuer Online-Dienste auf den Markt, die ständige Erreichbarkeit durch den täglich wachsenden Einsatz des Mobilfunks sind Schlaglichter einer gesellschaftlichen Entwicklung, die in ihrer Tragweite mit der industriellen Revolution verglichen werden kann: dem Übergang von der Industrie- zur postindustriellen Informationsgesellschaft[1].

Ein Großteil aller Betriebsabläufe, exemplarisch seien der bargeldlose Zahlungsverkehr, die Übermittlung von Nachrichten durch internationale Agenturen oder die Steuerung multinationaler Konzerne genannt, beruhen bereits heute auf Informationsprozessen, so daß ein effektives Informationsmanagement und eine effiziente Infrastruktur zum Transport von Informationen zu entscheidenden Wettbewerbsfaktoren geworden sind[2]. Schaffung, Verarbeitung und Verbreitung von Informationen haben sich, mit anderen Worten, zu einem vierten Produktionsfaktor neben Arbeit, Boden und Kapital entwickelt[3].

b) Neue Gefahrenlagen

Dem daraus resultierenden Interesse an einem weitgehend eingriffsfreien, unbeschränkten Datenverkehr stehen allerdings die Risiken gegenüber, die sich aus den Möglichkeiten automatisierter Datenverarbeitung

1) *Steber*, NJW 1989, 2569 f.; *Ellger*, Der Datenschutz im grenzüberschreitenden Datenverkehr, 1990, S. 56 f.; vgl. auch die umfassenden Untersuchungen von *Sonntag*, Die Zukunft der Informationsgesellschaft, 1983, und *Kiefer*, Auf dem Weg zur Informationsgesellschaft, 1982.
2) *Langer*, Informationsfreiheit als Grenze der informationellen Selbstbestimmung, 1992, S. 19; *Wenzel*, RDV 1996, 10.
3) *Geiger*, in FS für Adolf Arndt, S. 119; *Einwag*, RDV 1990 1, 2.

Prof. Dr. Georgios Gounalakis ist Professor für Bürgerliches Recht, Internationales Privatrecht, Rechtsvergleichung und Medienrecht sowie geschäftsführender Direktor des Instituts für Rechtsvergleichung und Mitglied des Direktoriums der Forschungsstelle für Medienrecht und Medienwirtschaft an der Philipps-Universität Marburg.
Elmar Mand ist stud. Mitarbeiter am Institut.

ergeben. Zu nennen ist hier insbesondere das Gefahrenpotential, das aus dem Umstand folgt, daß der Verwendungszweck der Daten durch deren Verknüpfung im Wege elektronischer Datenverarbeitung variabel, d.h. aber für den Betroffenen nicht mehr transparent und damit kontrollierbar wird[4]. Ohne größere technische Schwierigkeiten und finanziellen Aufwand ist es beispielsweise möglich, Persönlichkeitsprofile im Rahmen des Teleshopping oder Bewegungsprofile bei der Benutzung von Mobilfunk zu erstellen[5].

c) Informationelle Selbstbestimmung

Diese Entwicklung hat eine qualitativ neuartige Gefährdungslage für das allgemeine Persönlichkeitsrecht geschaffen, der das *BVerfG* durch die Ausweitung des Persönlichkeitsschutzes in Form der Anerkennung des Rechts auf informationelle Selbstbestimmung entgegengetreten ist[6]. Das Recht auf informationelle Selbstbestimmung vermittelt dem einzelnen Bürger eine rechtlich gesicherte Herrschaftsmacht über den Kreis der über seine Person vorhandenen Informationen[7]. Es dient der Gewährleistung der Kommunikationsfähigkeit des Bürgers in seinem sozialen Umfeld und hat damit grundlegende Bedeutung für das freiheitliche demokratische Gemeinwesen[8]. Als Ausfluß der Art. 2 Abs. 1, 1 Abs. 1 GG besitzt das informationelle Selbstbestimmungsrecht Grundrechtsqualität[9]. Es bindet folglich gem. Art. 1 Abs. 3 GG die öffentliche Gewalt. Über die Rechtsfigur der mittelbaren Drittwirkung ist der Gesetzgeber jedoch berufen, den Wertgehalt der Grundrechte auch im Privatrecht zu gewährleisten[10]. Insoweit besteht eine Verpflichtung, die Befugnis, selbst zu entscheiden, wann und innerhalb welcher Grenzen persönliche Lebenssachverhalte offenbart werden, nicht nur im Verhältnis Staat – Bürger, sondern auch im Verhältnis der Bürger untereinander zu schützen, sofern personenbezogene Daten verarbeitet werden[11].

d) Konkordanzanforderungen

Die Anforderungen an das Datenschutzrecht lassen sich vor diesem Hintergrund dahin gehend beschreiben, dem Grundrecht auf informationelle Selbstbestimmung durch geeignete Restriktionen der Datenverarbeitung Rechnung zu tragen, andererseits aber auch das Interesse an ungehindertem Informationszugang zu berücksichtigen. Da die Informationsfreiheit im privaten Bereich über Art. 5 Abs. 1, 2. Halbsatz GG[12] und allgemein über die wirtschaftliche Betätigungsfreiheit im Rahmen der Privatautonomie, Art. 12 Abs. 1, 14 Abs. 1 GG[13], ebenfalls grundrechtlichen Schutz genießt, sind die konfligierenden Interessen hier im Wege der Herstellung praktischer Konkordanz zu einem beiderseitig möglichst optimalen Ausgleich zu bringen[14].

2. Struktur der EG-Richtlinie

a) Optionen und Empfehlungen

Nach langem Zögern hat die EG – gestützt auf Art. 100 lit. a EGV – im Hinblick auf das eklatante Schutzgefälle der Datenschutzregelungen in den Mitgliedsstaaten[15] dem bestehenden Harmonisierungsbedarf durch den Erlaß einer Richtlinie im Verfahren der Mitbestimmung gem. Art. 189 lit. b EGV Rechnung getragen[16]. Richtlinien der EG sind nach Art. 189 S. 3 EGV für jeden Mitgliedsstaat hinsichtlich des zu erreichenden Ziels verbindlich, überlassen jedoch den innerstaatlichen Stellen die Wahl der Form und der Mittel für die Umsetzung in nationales Recht[17], wobei der jeweilige nationale Gestaltungsspielraum maßgeblich von der Regelungsdichte der Richtlinie abhängt[18]. Im Hinblick auf das angestrebte Harmonisierungsziel erscheint es deshalb bedenklich, wenn sich die Richtlinie zum Datenschutz weitgehend auf allgemeine Prinzipien beschränkt, in vielen Fällen verschiedene Optionen aufweist, z.T. auch nur Möglichkeiten aufzeigt, die als bloße Empfehlung an die Mitgliedsstaaten zu verstehen sind[19].

b) Folgerungen

Der weitgehende Spielraum bei der Umsetzung ist im Lichte des relativ kurzen Umsetzungszeitraums von drei Jahren und der Notwendigkeit zu sehen, unter Beachtung der jeweiligen Rechtstraditionen und der bereits gewachsenen Strukturen im Datenschutzrecht, einen Kompromiß zwischen den Mitgliedstaaten herbeizuführen.[20] Schließlich dient die Gestaltungsfreiheit bei der Umsetzung dem in Erwägungsgrund 9 explizit erwähnten Ziel, durch die Richtlinie ein hoch entwik-

4) *Podlech* in Hohmann (Hrsg.), Freiheitssicherung durch Datenschutz, 1987, S. 21 f.; *Simitis*, RDV 1990, 3, 20.
5) *Wenzel* (FN 2), S. 11.
6) BVerfGE 65, 1 ff. – Volkszählungsgesetz.
7) BVerfGE 65, 1, 42; 80, 367, 373; *Jakob*, RDV 1994, 57; *Simitis* in Simitis/Dammann/Geiger/Mallmann/Walz, BDSG, 4. Aufl. 1992, § 1 Rdnr. 164.
8) BVerfGE 65, 1, 42 ff.; *Sieber* (FN 1), S. 2570; *Simitis* (FN 4), S. 17.
9) *BVerfG* NJW 1984, 425; *BayVerfGH* NJW 1985, 1212, 1213 f.; *Benda* in Benda/Maihofer/Vogel (Hrsg.), Handbuch des Verfassungsrechts, 2. Aufl. 1994, S. 173 ff.; *Gola*, NJW 1985, 1196, 1197.
10) Grundlegend BVerfGE 7, 198, 205 f. – Lüth; vgl. auch 73, 261, 269.
11) *Simitis*, NJW 1984, 398, 401; *Gallwas*, NJW 1992, 2785, 2789; *Teske*, CR 1988, 670; kritisch *Ehmann*, AcP 188 (1988), 230, 303 ff.
12) *Pieroth/Schink*, Staatsrecht II, 10. Aufl. 1994, Rdnr. 615 ff.; *Maunz/Dürig/Herzog*, GG, Art. 5 I, II, Rdnr. 81 ff., 87 ff.; *Langer* (FN 2), S. 82 ff.
13) *Geis*, CR 1994, 171, 172 f.; *Breitfeld*, Berufsfreiheit und Eigentumsgarantie als Schranke des Rechts auf informationelle Selbstbestimmung, 1992, S. 13 ff., 21 ff.
14) *Simitis* in Simitis u.a. (FN 7), § 1 Rdnr. 223; *Breitfeld* (FN 13), S. 124 ff.; *Schmitt Glaeser* in Isensee/Kirchhof (Hrsg.), Handbuch des Staatsrechts, Bd. VI, § 129 Rdnr. 91; *Gallwas* (FN 11), S. 2786.
15) Vgl. dazu *Wurst*, JuS 1991, 448, 450, sowie die rechtsvergleichende Untersuchung von *Ellger* (FN 1), §§ 4–14.
16) Richtlinie zum Schutze natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr vom 24.10.1995, ABl. EG L 281 vom 23.11.95, 31 ff. (im folgenden kurz: «Ril»).
17) Vgl. im einzelnen *Wolff*, RDV 1995, 106, 109.
18) Vgl. *Geis* (FN 13), S. 176.
19) *Rüpke*, ZRP 1995, 185 f; *Wolff* (FN 17), S. 108; *Wolff*, RDV 1993, 1, 3; *Korff*, RDV 1994, 209, 212.
20) *Bachmeier*, RDV 1995, 49 ff.

keltes Datenschutzniveau, wie es in einigen Mitgliedsstaaten bereits existiert, nicht in einzelnen Bereichen abzuschwächen[21].

Damit sind die Rahmenbedingungen bei der im Zuge der Umsetzung der Richtlinie notwendigen Novellierung des Datenschutzrechts in Deutschland einerseits allgemein durch das Spannungsverhältnis zwischen Informationsfreiheit und informationellem Selbstbestimmungsrecht gekennzeichnet. Andererseits stehen sich die zum Teil gegenläufigen Interessen einer möglichst weitgehenden Rechtsangleichung und einer möglichst umfassenden Erhaltung des gegenwärtigen Schutzsystems und -niveaus gegenüber.

II. Struktureller Anpassungsbedarf im deutschen Recht

1. Verbot mit Erlaubnisvorbehalt (Art. 5, 7 Ril)

Indem die Datenschutzrichtlinie der Gemeinschaft der Gefahr der Verarbeitung personenbezogener Daten dadurch Rechnung trägt, daß sie diesbezüglich von einem prinzipiellen Verbot mit Erlaubnisvorbehalt ausgeht (Art. 5, 7 Ril), steht sie im Einklang mit der Regelungsstruktur von BDSG und Landesdatenschutzgesetzen[22]. Auch die Beschränkung der Schutzwirkung auf Daten natürlicher Personen (Art. 1 Abs. 1 Ril), die allerdings mit Blick auf Art. 3 Abs. 1 GG hinsichtlich der Ungleichbehandlung von juristischen Personen und Einzelkaufleuten unbefriedigend erscheint[23], entspricht der deutschen Rechtslage. Ein Anpassungsbedarf besteht insoweit nicht.

2. Trennung von öffentlichem und privatem Bereich

Im Gegensatz zum Deutschen Recht und auch noch zum ersten Entwurf der Richtlinie von 1990[24] trennt die EG-Richtlinie in ihrer endgültigen Fassung nicht mehr zwischen der Datenverarbeitung im öffentlichen und im privaten Bereich. Sie berücksichtigt damit, daß die rasante Zunahme der Verarbeitung personenbezogener Daten im privaten Bereich zu einer mindestens ebenso starken Gefährdung der Privatsphäre führt wie die Datenverarbeitung im öffentlichen Sektor[25]. Beispielhaft seien hier das Erstellen von Warndateien von Versicherungen und Verfahren zur Aussonderung nicht kreditwürdiger Personen, sog. credit-scoring, genannt. Hinzu kommt, daß zentrale Verwaltungsaufgaben und Versorgungsdienstleistungen, die traditionell öffentlich-rechtlich ausgestaltet waren (z.B. Post, Bahn, Telekommunikation), mit dem Ziel der Kostensenkung, Entbürokratisierung und der Steigerung der Effizienz zunehmend in privatrechtliche Organisationsformen überführt werden[26].

Dies wirft aber die Frage auf, ob die Differenzierung zwischen der Datenverarbeitung öffentlicher und privater Stellen in BDSG und Landesdatenschutzgesetzen im Rahmen der Umsetzung der Richtlinie ebenfalls aufzuheben ist.

Stellt man den Ausgangspunkt des Datenschutzes in Deutschland, die Sicherung des verfassungsrechtlich in Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG verankerten Grundrechts auf informationelle Selbstbestimmung in Rechnung, erscheint die prinzipielle Trennung zwischen öffentlichem und privatem Sektor zunächst einleuchtend. Gem. Art. 1 Abs. 3 GG ist unmittelbar nur die öffentliche Gewalt an die Grundrechte gebunden. Im Verhältnis der Privatrechtssubjekte untereinander beanspruchen die Grundrechte dagegen nur mittelbar Geltung, nämlich über die Generalklauseln des Zivilrechts[27]. So wird denn auch zur Begründung der bisherigen Unterscheidung vor allem darauf hingewiesen, daß die Datenverarbeitung im öffentlichen Bereich in der Regel zwangsweise für öffentliche Zwecke erfolge, während sich im privaten Sektor prinzipiell gleichwertige Rechtssubjekte gegenüberstünden[28].

Der Grundsatz der prinzipiellen Gleichrangigkeit der Privatrechtssubjekte, die ihre Angelegenheiten privatautonom regeln, ist indes gerade in datenschutzrelevanten Lebensbereichen zweifelhaft geworden: Im Verhältnis Patient-Arzt/(private) Krankenkasse, beim Abschluß von Versicherungsverträgen, dem Kontakt mit Banken – um nur einige Beispiele zu nennen – ist es in aller Regel gerade ausgeschlossen, die Bedingungen der Weitergabe und Verwendung personenbezogener Daten frei auszuhandeln. Dem Kunden werden diese Modalitäten durch den Datenverarbeiter vielmehr einseitig in allgemeinen Geschäftsbedingungen aufoktroyiert. Es besteht ein strukturelles Ungleichgewicht der Verhandlungsstärke, die dem Vertrag die sonst zu vermutende Richtigkeitsgewähr nimmt. Wie das *BVerfG* insbesondere in der Bürgschaftsentscheidung[29] herausgearbeitet hat, ist der Staat zum Ausgleich derartiger typisierbarer Ungleichgewichtslagen besonders verpflichtet. Die gegen eine prinzipielle Entsprechung der Datenschutzregelungen im öffentlichen und privaten Bereich erhobenen verfassungsrechtlichen Bedenken erweisen sich daher in diesen Fällen als wenig überzeugend.

Hieraus läßt sich freilich keine zwingende Antwort auf die Frage ableiten, ob der Gesetzgeber durch die grundsätzliche Anwendbarkeit einheitlicher Datenschutzstandards auch im Privatrechtsverkehr die strukturelle Ungleichgewichtslage quasi zum gesetzgeberischen Regelfall zu erklären hat oder vom Grundsatz

21) *Bachmeier* (FN 20), S. 50; *Weber*, CR 1995, 297, 298.
22) Vgl. § 4 Abs. 1 BDSG, § 7 HessDSG.
23) *Rüpke* (FN 19), S. 189; *Sasse*, Sinn und Unsinn des Datenschutzes, 1976, S. 46 ff.
24) Kapitel Abs. 2 und III, KOM (1990) 314 endg. Syn 287.
25) *Brühann*, RDV 1996, 12, 15.
26) Vgl. zu Ziel und Ausmaß der Privatisierung der öffentlichen Verwaltung und den datenschutzrechtlichen Konsequenzen *Simitis*, DuD 1995, 648 f.
27) Std. Rspr. seit BVerfGE 7, 198 – Lüth.
28) *Schmitt Glaeser* (FN 14), § 129 Rdnr. 88 ff.; *Rüpke* (FN 19), S. 187 f.; *ders.*, EuZW 1993, 149, 150; *Zöllner*, RDV 1985, 3, 16; vgl. auch *Mätsch*, RDV 1994, 67, 68; *Wind/Siegert*, RDV 1992, 118, 119.
29) *BVerfG* NJW 1994, 36, 38.

eines geringeren Datenschutzstandards im privaten Sektor ausgehen sollte und nur im Einzelfall, bei bestehenden typisierbaren Ungleichgewichtslagen, korrigierend eingreifen muß. Gesetzestechnisch sind grundsätzlich beide Wege gangbar.

Auch die Übernahme des Einheitsprinzips der Richtlinie ist keineswegs zwingend. Zwar sind bei der Transformation in nationales Recht einzelne Erleichterungen bei der Datenverarbeitung durch private Stellen zwingend aufzuheben oder abzumildern[30], jedoch eröffnet die generalklauselartige Weite vieler Begriffe der Richtlinie und die in Art. 5 Ril ausdrücklich hervorgehobene Regelungsfreiheit dem nationalen Gesetzgeber die Möglichkeit, ungeachtet dieser obligatorischen Anpassungen, die grundsätzliche Trennung zwischen öffentlichem und privatem Bereich beizubehalten.

Allerdings dürfte das Festhalten an diesem Prinzip, das eine Wiederholung der nach der Richtlinie für alle Formen der Datenverarbeitung geltenden Bestimmungen für die jeweiligen Bereiche notwendig macht, zu einem kaum zu überschauenden Regelungswust führen, wie er sich bereits heute in den Datenschutzgesetzen selbst, vor allem aber in den zahlreichen bereichsspezifischen Normen abzeichnet[31]. Um eine solche, der Effektivität des Datenschutzrechts abträgliche Unübersichtlichkeit zu vermeiden, erscheint eine prinzipielle Gleichbehandlung von öffentlichem und privaten Sektor vorzugswürdig[32]. Gesetzestechnisch ließe sie sich dadurch realisieren, daß eine Reihe allgemeiner Bestimmungen (bspw. Art. 6–8, 10, 11) im ersten Abschnitt des BDSG bzw. der Landesdatenschutzgesetze als »Allgemeiner Teil« vor die Klammer gezogen wird[33].

3. Verantwortlichkeit der Verarbeitung (Art. 3 Ril)

Ein zweiter struktureller Unterschied zwischen der Richtlinie und dem BDSG besteht darin, daß die Richtlinie die »Verantwortlichkeit der Verarbeitung«, Art. 3 i.V.m. Art. 2 lit. b), lit. d) Ril, als Ausgangspunkt des Datenschutzsystems wählt, während das BDSG im wesentlichen an den technischen Ausgangspunkt der Datei anknüpft, § 1 Abs. 2 Nr. 3, Abs. 3 u. 5 BDSG (eine Reihe von Landesdatenschutzgesetzen verfährt demgegenüber bereits wie die Richtlinie, so etwa Hessen § 2 Abs. 2, Berlin § 4 Abs. 2, Bremen § 2 Abs. 2 und Nordrhein-Westfalen § 4 Abs. 2. In diesem Konzept spiegelt sich die Erkenntnis wider, daß nicht der Verarbeitungsrahmen, sondern die Verarbeitung personenbezogener Daten als solche Anknüpfungspunkt einer gesetzlichen Regelung sein muß[34].

Auswirkungen hat der veränderte Ansatzpunkt der Verantwortlichkeit für die Verarbeitung vor allem für den örtlichen und sachlichen Anwendungsbereich der Datenschutzgesetze des Bundes und der Länder[35]. Anders als bei der Frage der Trennung von öffentlichem und privatem Sektor ergibt sich hieraus jedoch kein grundlegender Änderungsbedarf in der Gesetzessystematik. Zum einen wird auch in der Richtlinie der Dateibegriff insoweit beibehalten, als er den Rahmen für die unter ihren Anwendungsbereich fallende manuelle Datenverarbeitung personenbezogener Daten absteckt (Art. 3 Abs. 1 i.V.m. Art. 2 lit. c) Ril). Zum anderen wird bereits heute der Dateibegriff des BDSG – ähnlich der Definition in der Richtlinie (Art. 2 lit. c) – anhand des Kriteriums der Auswertbarkeit sehr weit ausgelegt[36]. Wie von der Richtlinie vorgesehen, kann der Verarbeitungsvorgang bzw. die Verantwortlichkeit hierfür deshalb ohne Systembruch den bisherigen Anknüpfungspunkt der Datei ersetzen. Allerdings wird im Interesse der Rechtssicherheit und -klarheit die Terminologie der Vorschriften insgesamt entsprechend anzupassen sein.

4. Ergebnis

Zusammenfassend ist somit festzustellen, daß die EG-Richtlinie zum Datenschutz in wesentlichen Bereichen, insbesondere bei dem Verbotsprinzip (Art. 5, 7 Ril), der Regelungsstruktur und -systematik des BDSG bzw. der Landesdatenschutzgesetze entweder entspricht oder nicht gravierend von ihr abweicht. Ein grundlegender Änderungsbedarf besteht insoweit nicht. Hingegen erscheint eine Nivellierung der in den Datenschutzgesetzen des Bundes und der Länder vorgesehenen Differenzierung zwischen privater und öffentlicher Datenverarbeitung auf dem Hintergrund der veränderten technischen und gesellschaftlichen Rahmenbedingungen der Verarbeitung personenbezogener Daten geboten. Der den nationalen Gesetzgebern bei der Umsetzung der Richtlinie eingeräumte Spielraum erlaubt allerdings die Beibehaltung des bisherigen Regelungsansatzes.

III. Notwendige Änderungen bei Einzelbestimmungen

1. Örtlicher Geltungsbereich der nationalen Vorschriften (Art. 4 Ril)

Nach Maßgabe von Art. 4 Abs. 1 lit. a) Ril bestimmt sich die örtliche Anwendbarkeit einzelstaatlichen Rechts bei der Datenübermittlung innerhalb der EU prinzipiell danach, in welchem Mitgliedsstaat der Verantwortliche der Verarbeitung ansässig ist. Das bedeutet, daß abweichend vom Territorialprinzip des deutschen Rechts (§ 1 Abs. 2 BDSG) im Grundsatz nicht mehr der Ort entscheidend ist, an dem eine bestimmte Datenverarbeitung vorgenommen wird. Grund dieses neuen Ansatzpunktes ist vor allem die Überlegung, daß der Standort einer Datei oder einer Verarbeitung gera-

30) Vgl. im einzelnen unten III.
31) *Schild*, EuZW 1996, 549, 550 und 554 f.
32) *Schild* (FN 31), S. 550; *Simitis* (FN 26), S. 650 f.
33) So auch *Brühann/Zerdick*, CR 1996, 429, 431.
34) *Körner/Dammann*, RDV 1993, 14, 16.
35) Vgl. dazu unten III 1. und 2.
36) *Auerhammer*, BDSG, 3. Aufl. 1993, § 3 Rdnr. 11; *Dörr/Schmidt*, BDSG, 2. Aufl. 1992, § 3 Rdnr. 6 ff.; *Goldenbohm/Weise*, CR 1991, 535, 536.

de im Falle der zunehmend expandierenden Datenbanken und -netze auf mehrere Mitgliedstaaten verteilt sein kann und deshalb oft nicht bestimmbar ist[37].

Das Sitzprinzip sieht sich jedoch der Kritik ausgesetzt, daß bei seiner uneingeschränkten Anwendung bereichsspezifisch für den Datenschutz möglicherweise fremdes Recht gelten könnte, im übrigen aber bspw. das Arbeits-, Gewerbe- und Baurecht des Verarbeitungsortes. Eine solche Aufspaltung der anwendbaren Rechtsnormen führt zwangsläufig zu einer Diversifikation und damit zu einer Verkomplizierung der rechtlichen Rahmenbedingungen unternehmerischer Aktivitäten in anderen Mitgliedsstaaten[38]. Dementsprechend soll, wenn das Unternehmen in einem anderen Mitgliedsstaat eine Niederlassung hat, gemäß Art. 4 Abs. 1 Ril nicht das Recht des Sitzes des Verantwortlichen der Datenverarbeitung, sondern das Recht des Ortes der Niederlassung gelten[39].

Eine Niederlassung setzt die effektive und tatsächliche Ausübung einer Tätigkeit mittels einer festen Einrichtung voraus. Auf die Rechtsform – insbesondere die Frage einer eigenen Rechtspersönlichkeit – kommt es nicht an[40]. Angesichts des weiten Anwendungsbereichs des Niederlassungsbegriffs, unter den z.B. auch bloße Agenturen zu subsumieren sind, dürfte diese Ausnahme vom Sitzprinzip der Regelfall werden und den Hauptteil der Betätigungen ausländischer Unternehmen der EU-Mitgliedstaaten abdecken[41]. Die notwendige Anpassung des BDSG an die Regelung des Art. 4 Abs. 1 lit. a) Ril wird daher in der Praxis nur geringe Auswirkungen für das jeweils anwendbare Recht haben. Der Umsetzung in deutsches Recht bedarf daneben die Bestimmung des Art. 4 Abs. 1 lit. c) Ril, die eine Umgehung der Datenschutzregelungen innerhalb der EU durch eine Verlagerung der Datenverarbeitung in »Datenoasen« bzw. »Datenparadiese« verhindern soll[42]. Sofern sich der Verantwortliche der Verarbeitung in einem Drittland niederläßt und dort personenbezogene Daten verarbeitet, ist er nach dieser Vorschrift dem Recht des Mitgliedstaates, in dem er auf automatisierte oder nicht automatisierte Mittel zurückgreift[43], d.h. in dem etwa Erhebungsbogen ausgefüllt oder Daten elektronisch abgerufen werden[44], zu unterstellen.

37) Vgl. Kommentierung zu Art. 4, Kom (92) 422 endg. Syn 287.
38) *Bachmeier* (FN 20), S. 50; vgl. zu weiteren Problemen des reinen Sitzprinzips, insbes. den Umgehungsmöglichkeiten strenger Datenschutzgesetze, *Weber* (FN 21), S. 299.
39) Vgl. Erwägungsgrund 18.
40) Vgl. Erwägungsgrund 19. Im Gegensatz dazu war im geänderten Vorschlag der Kommission 1992 noch das Sitzprinzip ohne Einschränkung vorgesehen.
41) *Bachmeier* (FN 20), S. 50.
42) *Weber* (FN 21), S. 299.
43) Erwägungsgrund 20.
44) *Weber*, DuD 1995, 698, 700
45) *Rüpke* (FN 19), S. 188, vgl. auch oben II. 3.
46) *Dammann*, in Simitis u.a. (FN 7), § 1 Rdnr. 219 f; *Büllesbach*, NJW 1991, 2593, 2596.
47) Erwägungsgrund 9.
48) Vgl. *Weber* (FN 21), S. 298.
49) Vgl. dazu auch *Walz*, CR 1991, 364, 365.
50) Erwägungsgrund 27.
51) So auch *Brühann* (FN 25), S. 15.

2. Sachlicher Geltungsbereich der nationalen Vorschriften (Art. 3 Ril)

a) Akten und Dateien

Der sachliche Anwendungsbereich der nationalen Datenschutzbestimmungen ist nach Art. 3 Abs. 1 Ril auf die ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten zu erstrecken. Nicht automatisierte Datenverarbeitungsvorgänge sollen dann erfaßt werden, wenn die Daten in Dateien gespeichert sind bzw. gespeichert werden sollen, Art. 3 Abs. 1 Satz 2 Ril.

Anders als das BDSG verzichtet die Datenschutzrichtlinie damit auf die Akte als Kriterium der Differenzierung. Den Rahmen für die Einbeziehung manueller Datenverarbeitungen bildet vielmehr allein der Dateibezug, wobei die Datei – im wesentlichen der Begriffsbestimmung des § 3 Abs. 2 Nr. 2 BDSG folgend[45] – als »strukturelle Sammlung personenbezogener Daten«, die nach bestimmten Kriterien zugänglich ist, definiert wird (Art. 2 lit. c) Richtlinie).

Soweit das deutsche Datenschutzrecht für die öffentliche Verwaltung seine Geltung auch auf die Datenverarbeitung in Akten erstreckt, ohne diesbezüglich einen Dateibezug zu verlangen (§§ 3 Abs. 3, 12 BDSG)[46], geht es folglich über den Geltungsrahmen der Richtlinie hinaus. Da die Umsetzung der Richtlinie jedoch nicht zu einer Verringerung des bereits bestehenden Schutzniveaus führen soll[47], ist die uneingeschränkte Einbeziehung aller Datenverarbeitungsvorgänge der öffentlichen Verwaltung unter den Anwendungsbereich des BDSG beizubehalten, auch wenn dadurch ein unterschiedlicher Standard in der Datenschutzgesetzgebung der Mitgliedstaaten aufrechterhalten wird[48].

Umgekehrt kann der generelle Ausschluß von Akten im privaten Sektor (§§ 1 Abs. 2 Nr. 3, 27 ff. BDSG)[49] angesichts der veränderten Prämisse bei der Bestimmung des Anwendungsbereiches nicht fortbestehen. Falls personenbezogene Daten in Akten nach bestimmten Kriterien strukturiert werden und daher für eine spätere Speicherung in Dateien verwendbar sind, muß vielmehr bereits die Datenverarbeitung in Akten gemäß Art. 3 Abs. 1 S. 2 Ril den Anforderungen der Datenschutzregelungen genügen[50].

Im Rahmen der Umsetzung der Richtlinie sollte deshalb auf die »Akte« als Differenzierungskriterium gänzlich verzichtet werden[51]. Die Aufrechterhaltung des hohen Schutzniveaus im öffentlichen Bereich durch die Einbeziehung sämtlicher personenbezogener Daten ist allerdings zu gewährleisten.

b) Datenerhebung

Der von der Richtlinie gewählte Anknüpfungspunkt der Verarbeitung personenbezogener Daten führt auch insoweit zu Unterschieden gegenüber dem deutschen Recht, als dieses zwischen der Erhebung (§ 13 BDSG) und der Verarbeitung personenbezogener Daten (§§ 14 ff., 28 ff. BDSG) unterscheidet, während die Richtlinie, unter Zugrundelegung eines umfassenden Verarbei-

tungsbegriffs, gemäß Art. 2 lit. b) die Erhebung als integralen Bestandteil der Verarbeitung ansieht.

Im öffentlichen Bereich, für den das BDSG sowohl die Verarbeitung als auch die Erhebung der Daten regelt, ergibt sich daraus kein materieller Änderungsbedarf. Im Interesse der Rechtsklarheit sollte jedoch auf die bestehende Differenzierung verzichtet werden.

Hingegen fehlt im privaten Sektor eine explizite Norm, die auch die Erhebung personenbezogener Daten dem Gesetzesvorbehalt unterwirft. Die Vorschrift des § 28 Abs. 1 Satz 2 BDSG, die Art. 5 lit. a) der Datenschutzkonvention des *Europarates* von 1981 entnommen ist, bestimmt zwar, daß personenbezogene Daten »nach Treu und Glauben« erhoben werden müssen. Sie ist jedoch als Kompromiß zwischen dem *Bundesrat*, der eine weitgehende Regelung präferierte, und dem Innenausschuß des *Deutschen Bundestages*, der dies strikt ablehnte, nicht als Gesetzesvorbehalt ausgestaltet[52].

Im Zuge der Umsetzung der Richtlinie ist nunmehr auch im privaten Bereich der gesamte Verarbeitungsvorgang unter Einschluß der Datenerhebung dem Anwendungsbereich der Datenschutzgesetze des Bundes und der Länder zu unterstellen. Da allerdings bei der Erhebung personenbezogener Daten für gesellschaftliche Zwecke schon heute regelmäßig die Anforderungen des § 28 Abs. 1 Satz 2 BDSG beachtet werden, bei dessen Auslegung auf die in § 242 BGB entwickelten Grundsätze, aber auch auf die spezifisch datenschutzrechtlichen Treu- und Glaubensgrundsätze zurückzugreifen ist, die, wie für den öffentlichen Bereich formuliert[53], auf die Erforderlichkeit der Aufgabenerfüllung abstellen[54], dürfte diese Novellierung in der Praxis ebenfalls keine nachhaltigen Konsequenzen hervorrufen.[55]

3. Zulässigkeitsbedingungen für die Verarbeitung (Art. 6–9 Ril)

a) Strukturunterschiede

Während die Richtlinie in Art. 6 und 7 allgemeine Grundsätze in bezug auf die Qualität bzw. die Zulässigkeit der Verarbeitung von Daten festlegt und diese für bestimmte Kategorien von Verarbeitungen in Art. 8 und 9 modifiziert, normiert das BDSG die Bedingungen der Datenverarbeitung im wesentlichen getrennt für einzelne Verarbeitungsvorgänge oder -bereiche. Besonders im privaten Sektor weisen die Vorschriften dabei ein hohes Maß an Unbestimmtheit auf, das Raum für unterschiedliche, z.T. sogar gegensätzliche Interpretationen läßt[56].

Da die Richtlinie ihrerseits nur einen Rahmen vorgibt, den die Mitgliedstaaten umzusetzen und auszufüllen haben[57], ist der diesbezüglich bestehende Anpassungsbedarf im deutschen Recht – über die im Interesse der Rechtsklarheit und -sicherheit dringend gebotene Präzisierung der Vorschriften gerade im privaten Bereich hinaus – deshalb schwer abzuschätzen. Der Umfang der Novellierung der allgemeinen Grundbedingungen der Datenverarbeitung wird letztlich von der rechtspolitischen Entscheidung abhängen, welche Gewichtung der Gesetzgeber – in den Grenzen der Vorgaben der Richtlinie und der Verfassung – bei der Herstellung des wechselseitigen Gleichgewichts zwischen informationellem Selbstbestimmungsrecht einerseits und der Informationsfreiheit andererseits den einzelnen Belangen beimißt.

b) Qualität der verarbeiteten Daten (Art. 6 Ril)

Ein zwingender Umsetzungsbedarf im deutschen Recht besteht allerdings mit Blick auf Art. 6 Abs. 1 lit. b) Ril. Dieser schreibt vor, daß personenbezogene Daten nur für genau umschriebene, dem Betroffenen erkennbare und nachvollziehbare Zwecke verarbeitet werden dürfen[58]. Insbesondere darf die Verarbeitung mit dem ursprünglichen Zweck nicht unvereinbar sein, und zwar auch dann nicht, wenn sie an sich gem. Art. 7 Ril rechtmäßig wäre. Insoweit kommt dem Zweckbestimmungsgrundsatz neben den Verarbeitungsprinzipien des Art. 7 Ril selbständige Bedeutung zu[59].

Anders als im öffentlichen Bereich, in dem die Zweckbindung weitgehend garantiert ist (§ 14 Abs. 1 BDSG, Art. 20 Abs. 3 GG)[60], bleibt das BDSG im privaten Sektor hinter diesen Anforderungen zurück. Zwar ist die Zweckbindung bei der Übermittlung von Daten gem. § 28 Abs. 4 S. 1 BDSG prinzipiell gewährleistet. Jedoch sind auch hier, wie bei der Verarbeitung und Nutzung von Daten im allgemeinen, zahlreiche, unterschiedlich interpretierbare Ausnahmen vorgesehen, die den angestrebten Schutz- und die Kontrollmöglichkeiten weitgehend nivellieren[61]. Dies ist deshalb besonders bedenklich, weil der Zweckbindungsgrundsatz, der einerseits das Verarbeitungsziel festlegt und andererseits den Verarbeitungsumfang eingrenzt, eine der wichtigsten Grundbedingungen für den effektiven Schutz des informationellen Selbstbestimmungsrechts ist[62]. Im Rahmen der Reform des BDSG muß daher die Zweckgebundenheit der Verarbeitung im privaten Bereich eindeutiger festgeschrieben werden[63].

c) Verarbeitungsgrundsätze (Art. 7 Ril)

Die in Art. 7 lit. a)–f) enumerativ aufgeführten Voraussetzungen, unter denen das prinzipielle Verbot der Verarbeitung personenbezogener Daten aufgehoben wird, entsprechen in weitem Umfang den Regelungen im

52) *Auerhammer* (FN 36), § 28 Rdnr. 30; *Simitis* in Simitis u.a. (FN 7), § 1 Rdnr. 55.
53) § 13 Abs. 1 BDSG.
54) *Geis* (FN 13), S. 175 f.; zu den daraus im einzelnen folgenden Pflichten, insbesondere der hinreichenden Aufklärung, *Mallmann* in Simitis u.a. (FN 7), § 29 Rdnr. 76.
55) *Geis* (FN 13), S. 176.
56) Vgl. *Simitis* (FN 26), S. 652; *Simitis* in Simitis u.a. (FN 7), Vorbem. zu § 27 Rdnr. 2 ff.
57) Siehe oben.
58) Vgl. Erwägungsgründe 28 f.
59) *Brühann* (FN 25), S. 15.
60) Vgl. dazu *Ehmann* (FN 11), S. 317 ff.
61) Vgl. z.B. § 28 Abs. 4 S. 2 i.V.m. § 28 Abs. 1 u. 2, §§ 29 ff. BDSG.
62) *Simitis* (FN 11), S. 402; *ders.* (FN 4), S. 17.
63) *Simitis* (FN 26), S. 651 f.; *Brühann* (FN 25), S. 15.

BDSG. Vor allem die in der Praxis besonders bedeutsamen Vorschriften über die Einwilligung des Betroffenen (Art. 7 lit. a) Ril), die Notwendigkeit der Verarbeitung für die Vertragserfüllung bzw. für die Durchführung vorvertraglicher Maßnahmen (Art. 7 lit. b) Ril) und die allgemeine Interessenabwägungsklausel (Art. 7 lit. f) Ril) stimmen mit den Vorschriften der §§ 4 Abs. 1 und 28 Abs. 1 Nr. 1 und 2 BDSG in ihrer Grundaussage überein. Allerdings bestehen in der Ausgestaltung im einzelnen einige Unterschiede, die bei der Umsetzung zu beachten sein werden.

Zum einen erhebt Art. 7 lit. b) die Erforderlichkeit für die Vertragserfüllung zur Zulässigkeitsvoraussetzung für die Verarbeitung personenbezogener Daten. Im BDSG ist das Erforderlichkeitskriterium hingegen nur außerhalb einer Vertragsbeziehung mit dem Betroffenen Maßstab für deren Zulässigkeit, § 28 Abs. 1 Nr. 2 BDSG. Allerdings besteht die Tendenz, den Erforderlichkeitsmaßstab auch auf Verarbeitungen im Rahmen einer Vertragsbeziehung gem. § 28 Abs. 1 Nr. 1 BDSG zu projizieren, jedenfalls die Geeignetheit für den Vertragszweck als Zulässigkeitskriterium anzunehmen[64]. Wenngleich in der Praxis somit nur ein subtiler Unterschied zwischen BDSG und Richtlinie in Gestalt der Unterscheidung zwischen Geeignetheit und Erforderlichkeit besteht, muß dennoch bei der Umsetzung der Richtlinie in nationales Recht den Anforderungen des Art. 7 lit. b) durch ein Einfügen des Erforderlichkeitskriteriums für die Vertragserfüllung Rechnung getragen werden.

Zum anderen erscheint fraglich, ob die in § 28 Abs. 1 Nr. 3 BDSG vorgesehene Privilegierung für Daten aus allgemein zugänglichen Quellen und die Erleichterung der Zulässigkeitsvoraussetzungen zugunsten listenmäßiger, gruppenbezogener Übermittlungen von Namen, Adressen etc. i.S.v. §§ 28 Abs. 2 Nr. 1 b), 29 Abs. 2 Nr. 1 b) BDSG Bestand haben können.

Da eine ausdrückliche Vorschrift hierüber in der Richtlinie nicht enthalten ist, kann der Fortbestand dieser Vorschriften nur auf die Generalklausel des Art. 7 lit. f) Ril gestützt werden, zu deren Präzisierung der nationale Gesetzgeber gem. Art. 5 Ril berechtigt und aufgefordert ist[65]. Legt man zugrunde, daß § 28 Abs. 1 Nr. 3 BDSG lediglich eine im Einzelfall widerlegbare Vermutung gegen ein der Verarbeitung entgegenstehendes, überwiegendes privates Interesse festschreibt, d.h. eine Interessenabwägung mithin nicht entbehrlich, sondern nur auf eine summarische Prüfung beschränkt ist[66], wenn die Daten aus allgemein zugänglichen Quellen entnommen wurden, so erscheint die Anerkennung dieser Vorschrift als nähere Ausgestaltung des Abwägungsgedankens des Art. 7 lit. f) durchaus denkbar[67]. Entsprechendes gilt für die Bestimmungen der §§ 28 Abs. 2 Nr. 1 b), 29 Abs. 2 Nr. 1 b) BDSG[68].

Zu berücksichtigen ist aber, daß die noch in der ersten Fassung des Richtlinienentwurfs enthaltene, der deutschen Regelung entsprechende Privilegierung für Informationen aus allgemein zugänglichen Quellen[69] mit der zutreffenden Begründung, daß in bestimmten Fällen allgemein zugängliche Quellen ebenfalls »empfindliche« personenbezogene Daten enthalten können[70], gestrichen wurde. Die Richtlinie geht mithin davon aus, daß eine entsprechende Privilegierung gerade nicht vorgesehen werden soll. Um dem Ziel der Richtlinie, der Harmonisierung der Datenschutzgesetze der Mitgliedstaaten auf hohem Niveau[71] zu entsprechen und diesem, wie von der »effet-utile-Rechtsprechung« des *EuGH*[72] gefordert, zu größtmöglicher Wirksamkeit zu verhelfen[73], müssen daher die Erleichterungen der Zulässigkeitsvoraussetzungen, die in § 28 Abs. 1 Nr. 3 und §§ 28 Abs. 2 Nr. 1 b), 29 Abs. 2 Nr. 1 b) BDSG vorgesehen sind, im novellierten BDSG entfallen[74].

d) Verarbeitung sensibler Daten (Art. 8 Ril)

Besondere Anforderungen stellt die Richtlinie gem. Art. 8 an die Verarbeitung »sensibler« Daten[75], z.B. über die rassische und ethnische Herkunft, die politische Meinung oder religiöse Überzeugung. Deren Verarbeitung, so der Wortlaut des Art. 8 Abs. 1 Ril, »wird von den Mitgliedstaaten untersagt«, wenn nicht die in den Abs. 2 bis 7 niedergelegten Voraussetzungen erfüllt sind.

Diese doppelte, gegenüber den übrigen personenbezogenen Daten weitergehende Unterwerfung einer Auswahl von Daten unter den Erlaubnisvorbehalt des Gesetzes orientiert sich an einem – wie ein Vergleich der einschlägigen Bestimmungen in den europäischen Datenschutzgesetzen unter Einschluß des Art. 6 der Datenschutzkonvention des Europarates zeigt[76] – im wesentlichen gemeineuropäischen, dem »right of privacy« zumindest ähnlichen[77] Verständnis, wonach mit Blick auf die empirisch hergeleitete besondere Schutzbedürftigkeit bestimmter Dimensionen der Persönlichkeitsentfaltung einzelne Datenverarbeitungen als gefährlicher eingestuft werden als andere[78]. Sie steht allerdings mit dem in Deutschland herrschenden Denkansatz des informationellen Selbstbestimmungsrechts, das eine Unterscheidung in sensible und triviale personenbezogene Daten nicht zuläßt, im Widerspruch.

64) *Auerhammer* (FN 36), § 28 Rdnr. 12; *Dörr/Schmidt* (FN 36), § 28 Rdnr. 11; vgl. auch *Rüpke*, EuZW 1993, 149, 153 mwN.
65) Erwägungsgrund 22.
66) *Auerhammer* (FN 36), § 28 Rdnr. 26; *Dörr/Schmidt* (FN 36), § 28 Rdnr. 32.
67) *Kopp* (FN 19), S. 6 auf der Grundlage des geänderten Vorschlags der Kommission von 1992.
68) Vgl. *Kopp* (FN 67).
69) Art. 8 Abs. 1 lit. b) des Entwurfs, KOM (90) 314 endg. – SYN 287.
70) Abschnitt II, Art. 7 der Kommentierung zum geänderten Entwurf von 1992, KOM (92) 422 endg. – SYN 287.
71) Erwägungsgründe 1 ff. (8).
72) Vgl. z.B. *EuGH* Slg. 1991, 5357 = NJW 1992, 165,167; zur Entwicklung und Kritik der effet-utile-Rechtsprechung *Möschel*, NJW 1994, 1709 f.
73) Zu den Konsequenzen des effet-utile-Prinzips für die Umsetzung der Richtlinie *Borries*, in Tagungsbericht – II. Datenschutzkolloquium, CR 1994, 440, 441.
74) So auch *Geis* (FN 13), S. 177; *Rüpke* (FN 19), S. 190; *Hoeren*, WM 1994, 1, 4; *Brühann* (FN 25), S. 15.
75) Entgegen einer verbreiteten Redeweise handelt es sich nicht um sensitive Daten. Man könnte höchstens sagen, daß für sensitive Personen der Schutz sensibler Daten besonders wichtig ist.
76) Vgl. die Darstellungen von *Simitis*, FS Pedrazzini, S. 469 ff.; *Geis* (FN 13), S. 173 ff.
77) *Ellger* (FN 1), S. 85 f.; *Rüpke*, Der verfassungsrechtliche Schutz der Privatheit, S. 35 ff., 73 ff.
78) Vgl. *Rüpke* (FN 19), S. 187.

Auf dem Hintergrund der Erkenntnis, daß eine Empfindlichkeitsskala, die in Abhängigkeit zu dem jeweiligen historischen, politischen und soziologischen Umfeld steht[79], durch eine Relativität vor dem Gesetzgeber gekennzeichnet ist[80], geht man zutreffend davon aus, daß Beeinträchtigungen des Rechts auf informationelle Selbstbestimmung entscheidend vom Kontext abhängen, in dem die Daten verwendet werden[81]. Per se belanglose personenbezogene Daten existieren damit nicht[82].

Dennoch wird der Gesetzgeber die Anforderungen des Art. 8 Ril bei der Umsetzung der Richtlinie zu beachten haben. Er ist dabei vor die Aufgabe gestellt, die in Art. 8 Abs. 1 Ril enthaltene Katalogisierung einzelner Datenkategorien ohne Systembruch mit dem abstrakten Denkansatz des informationellen Selbstbestimmungsrechts, der letztlich auch in dem generellen Erlaubnisvorbehalt der Art. 5, 7 Ril zum Ausdruck kommt, zu verbinden. Ein möglicher Lösungsansatz könnte darin liegen, die in Art. 8 Abs. 1 Ril genannten sensiblen Daten dadurch besonders zu schützen, daß man sie bei der Umsetzung als Regelbeispiele ausgestaltet, die bei der Abwägung der Interessen der Beteiligten grundsätzlich dem Schutz des informationellen Selbstbestimmungsrecht des Betroffenen den Vorrang einräumen. Dieser gesetzliche Hinweis auf die in den genannten Fällen regelmäßig bestehende erhöhte Schutzwürdigkeit des Betroffenen könnte dann als Hinweis auf eine strikte Handhabung des Grundsatzes der Verhältnismäßigkeit verstanden werden. Zugleich bestünde die Möglichkeit, die in Art. 8 Abs. 2–4 Ril vorgesehenen Ausnahmen als Abweichungen von der Vermutung des Vorrangs des Rechts auf informationelle Selbstbestimmung problemlos in das Regelungsgefüge einzubinden.

(Der Beitrag wird fortgesetzt.)

79) *Geis* (FN 13), S. 174.
80) *Simitis* (FN 76), S. 469, 471–474.
81) *Simitis* (FN 76), S. 469, 484 ff.; *ders.* (FN 11), S. 402.
82) BVerfGE 65, 1, 45 ff. Vgl. auch *Pieroth/Schlink* (FN 12), Rdnr. 415; *Podlech*, in Alternativkommentar-Grundgesetz, 1984, Art. 2 Abs. 1 Rdnr. 37; *Geis* (FN 13), S. 174 m.w.N.