

§ 2 Gemeinsame rechtliche Grundlagen und Strukturen

Bereits Art. 12 der Allgemeinen Erklärung der Menschenrechte (AEMR) kodifizierte 1948 den Schutz des Privatlebens als Vorgänger eines gemeinsamen Datenschutzrechts. Mit dem Inkrafttreten der Europäischen Konvention für Menschenrechte (EMRK) 1953 wurde zudem früh der Schutz des Privatlebens (Art. 8 EMRK) auf europäischer Ebene verbindlich festgeschrieben. Dieser Schutz alleine konnte jedoch nicht als Antwort auf die befürchteten Folgen der zunehmenden Technisierung und der damit einhergehenden automatisierten Verarbeitung von personenbezogenen Daten dienen. Die Initiative zur Verrechtlichung eines modernen Datenschutzes ging Anfang der 1970er Jahre von einzelstaatlichen Bemühungen zur Stärkung von Bürgerrechten aus. Bei diesem Datenschutz ging es nicht mehr allein um den abstrakten Schutz der Privatsphäre, sondern um die genauere Konturierung der Verarbeitungsbedingungen und schließlich um mehr parlamentarische Kontrolle über die Daten der Verwaltung.²⁷ Es traten bald auch inter- und supranationale Institutionen für einen gemeinsamen Regelungsrahmen ein. Trotz der bis dahin unterschiedlichen nationalen Modelle²⁸ konnte man sich zu Beginn der 1980er Jahre schließlich im Rahmen der Zusammenarbeit im Europarat auf eine gemeinsame europäische Datenschutzkonvention²⁹ einigen. Selbst über die Grenzen Europas hinaus konnten internationale Mindestanforderungen - wenngleich unverbindlich - durch die Vereinten Nationen (UN)³⁰ und die Organisation für wirtschaftliche Zusammenarbeit und Entwicklung (OECD)³¹ formuliert werden. Vor diesem geschichtlichen Hintergrund erscheinen die DSRL von 1995 sowie die 2009 erfolgte Integration der Europäischen Grundrechtecharta (GRC) in die Verträge der EU – insbesondere von Art. 8 GRC – lediglich als vorläufige Höhepunkte gemeinsamer gesetzgeberischer Bemühungen auf dem Gebiet des Datenschutzes.

²⁷ Simitis/Simitis, BDSG, Einleitung Rn. 13 ff.

²⁸ Simitis/Simitis, BDSG, Einleitung Rn. 127 ff.

²⁹ Übereinkommen Nr. 108 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten vom 28.1.1981.

³⁰ „Guidelines for the Regulation of Computerized Personal Data Files“, Entschließung 45/95 der Generalversammlung der Vereinten Nationen vom 14.12.1990.

³¹ „Richtlinien über Datenschutz und grenzüberschreitende Ströme personenbezogener Daten“ der Organisation für wirtschaftliche Zusammenarbeit und Entwicklung vom 23.09.1980; hierzu *Tinnefeld/Buchner/Petri*, Einführung in das Datenschutzrecht, S. 71 ff. sowie ausführlich *Chassigneux*, La protection des informations à caractère personnel, S. 270 f.

I. Datenschutzregelungen in multilateralen Abkommen

1. Datenschutz als Teil des Schutzes des Privatlebens

a. Datenschutz im Rahmen der Vereinten Nationen

Weder die AEMR noch andere Dokumente der Vereinten Nationen enthalten eigenständige Datenschutzgrundrechte. Dennoch erstreckt sich der Schutzbereich einzelner Abkommen auf den Schutz personenbezogener Daten, und zwar im Rahmen des Schutzes des Privatlebens. Der Internationale Pakt über bürgerliche und politische Rechte, der am 23. März 1976 in Kraft trat, schützt in seinem Art. 17 S. 1 unter anderem vor Eingriffen in das Privatleben bzw. die „Privatsphäre“.³² Die Vorschrift ist dem Wortlaut des Art. 12 AEMR entlehnt, umfasst jedoch nicht nur den Schutz vor willkürlichen, sondern zusätzlich den Schutz vor rechtswidrigen Eingriffen. Der Pakt ist für die Signatarstaaten, darunter Deutschland und Frankreich, verbindlich. Der UN-Menschenrechtsausschuss, welcher über die Einhaltung des Paktes wacht, gab in einer seiner allgemeinen Bemerkungen nach Art. 40 Abs. 4 S. 1 IPbPr aus dem Jahr 1988 die maßgeblichen Vorgaben zur Auslegung des Art. 17 IPbPr bekannt³³: Der Begriff der „Privatsphäre“ sei notwendig relativ und demnach sei eine strikte Abgrenzung zum nichtprivaten Bereich nicht möglich.³⁴ Grundsätzlich seien jedoch persönliche Daten vom Schutz des Privatlebens umfasst.³⁵ Durch Sammlung und Speicherung von personenbezogenen Daten auf Computern, Datenbanken und ähnlichen Vorrichtungen durch staatliche oder private Einrichtungen könne in das Schutzrecht eingegriffen werden. Zur Rechtfertigung müssten diese jedoch gesetzlich fixiert sein; auch müssten effektive staatliche Maßnahmen getroffen werden, welche Daten, die zum Privatleben einer Person gehören, vor nicht autorisierten Zugriffen von staatlichen oder privaten Einrichtungen schützen.³⁶

Da beim IPbPr der Datenschutz lediglich als Teil des Schutzes des Privatlebens angesehen wird und daher nur sehr allgemein ausgeprägt ist, ergeben sich datenschutzspe-

³² Engl. *privacy*; die deutsche Übersetzung („Privatleben“), abgedruckt in BGBl. 1973 II 1533, gehört nicht zu den nach Art. 53 Abs. 1 IPbPr verbindlichen Vertragstexten.

³³ UN-Menschenrechtsausschuss, Allgemeine Bemerkung Nr. 16 vom 8.4.1988 („Article 17 – The right to respect of privacy, family, home and correspondence, and protection of honour and reputation”).

³⁴ Ebenda, Ziffer 7.

³⁵ Ebenda, Ziffer 10; UN-Menschenrechtsausschusses, Jahresbericht 2007/2008 (A/63/40), Vol. I, S. 77; vgl. auch Nowak, U.N. Covenant on Civil and Political Rights, Art. 17 Rn. 23.

³⁶ Die Pflicht zum staatlichen Schutz vor Eingriffen Dritter leitet sich unmittelbar aus Art. 17 Abs. 2 IPbPr ab; vgl. Klein, Meinungsfreiheit und Persönlichkeitsschutz nach dem Internationalen Pakt über bürgerliche und politische Rechte, S. 9.

zifische Anforderungen allenfalls aus Einzelfallentscheidungen.³⁷ Der UN-Menschenrechtsausschuss ist befugt, Individualbeschwerden von Bürgern entgegenzunehmen, deren Staaten das erste Zusatzprotokoll zum IPbPR unterzeichnet haben.³⁸ Hierzu gehören auch Deutschland und Frankreich. Eine inhaltliche Befassung des Ausschusses mit Beschwerden von Bürgern gegen Eingriffe in ihre Privatsphäre ist jedoch ausgeschlossen, wenn bereits der EGMR in derselben Angelegenheit vorbefasst war. Möglich ist dies durch entsprechende Vorbehalte zahlreicher europäischer Staaten (so auch Deutschland und Frankreich) gegen Art. 5 Abs. 2 des ersten Zusatzprotokolls des IPbPR.³⁹ Dies mag einer der Gründe sein, warum sich bis heute eine spezifische Judikatur zum Schutz personenbezogener Daten als Teilaspekt des Schutzes des Privatlebens seitens des Ausschusses nicht entwickeln konnte.⁴⁰

Neben Art. 17 IPbPR normiert Art. 16 des Übereinkommens über die Rechte des Kindes (Kinderrechtskonvention) den Schutz des Privatlebens. Dieser deckt sich im Wortlaut mit Artikel 17 IPbPR und gilt nur für Kinder im Sinne von Art. 1 Kinderrechtskonvention. Dagegen stellt Art. 22 Abs. 2 des Übereinkommens über die Rechte von Menschen mit Behinderungen (Behindertenrechtskonvention) eine Besonderheit dar: Es wird explizit Bezug zum Schutz persönlicher Informationen als Teil des Schutzes der Privatsphäre genommen, indem „auf der Grundlage der Gleichberechtigung mit anderen die Vertraulichkeit von Informationen über die Person, die Gesundheit und die Rehabilitation von Menschen mit Behinderungen“ geschützt werden soll.

b. Art. 8 der Europäischen Menschenrechtskonvention

Art. 8 Abs. 1 Var. 1 der Europäischen Menschenrechtskonvention (EMRK) garantiert in seinem Geltungsbereich jeder Person die Achtung ihres Privat- und Familienlebens, ihrer Wohnung und ihrer Korrespondenz als ein Menschenrecht. In diese Rechte dürfen die Signatarstaaten der EMRK nur aufgrund eines Gesetzes und zum Schutz der in Abs. 2 der Vorschrift aufgezählten Rechtsgüter eingreifen. Die EMRK hat als völkerrechtlicher Vertrag gemäß Art. 55 der frz. Verfassung übergesetzlichen Rang, geht also demnach - mit Ausnahme der Verfassung selbst - der französischen Gesetzgebung

³⁷ So die Enquete-Kommission „Internet und digitale Gesellschaft“, Fünfter Zwischenbericht vom 15.3.2012, BT-Drs. 17/8999, S. 8.

³⁸ Hierzu näher *Althoff*, AnwBl. 2012, S. 52 f.

³⁹ *Klein*, Der Schutz der Grund- und Menschenrechte durch den Europäischen Gerichtshof für Menschenrechte, § 150 Rn. 70.

⁴⁰ Erwähnenswert ist etwa der Fall *Sayadi et al. gg. Belgien* (Löschung von Namen aus Anti-Terror-Datei), Entscheidung des UN-Menschenrechtsausschusses, CCPR/C/89/D/1472/2006 vom 22.10.2008.

vor.⁴¹ In Deutschland besitzt die EMRK zwar grundsätzlich nur den Rang eines einfachen Bundesgesetzes; das Bundesverfassungsgericht (BVerfG) zieht sie jedoch als Kontrollmaßstab gegen die Rechtsprechung, die Exekutive und (mittelbar) die Legislative heran und stellt sie *de facto* über das einfache Recht.⁴² Im Unterschied zu den später verfassten Bestimmungen der EU, namentlich der GRC, des EUV, des AEUV und der DSRL, behandelt die EMRK⁴³ in ihrem Art. 8 Abs. 1 grundsätzlich nur den Schutz des Privatlebens des Menschen und knüpft nicht an den Begriff des personenbezogenen Datums an. Der Wortlaut gebietet es daher, den Schutzbereich nur auf solche Informationen zu erstrecken, die eine Nähe zur Privatsphäre des Betroffenen aufweisen.⁴⁴

Dennoch kann Art. 8 EMRK, vermittelt durch die extensive Rechtsprechung des EGMR, mittlerweile als ein Motor des Datenschutzgrundrechts auf europäischer Ebene bezeichnet werden.⁴⁵ Denn nach anfänglicher Zurückhaltung sowohl der damaligen Europäischen Kommission für Menschenrechte (EKMR) als auch des EGMR hat sich, insbesondere nach Erlass der Datenschutzkonvention des Europarates im Jahr 1981 eine ausgedehnte Judikatur zum Datenschutz entwickelt.⁴⁶ Diese ist auf den vom EGMR weit verstandenen sachlichen Schutzbereich der Vorschrift zurückzuführen: Das Privatleben umfasse die physische und geistige Integrität einer Person, wobei Art. 8 EMRK in erster Linie die Entwicklung der Persönlichkeit jedes Einzelnen ohne Beeinträchtigung von außen in seinen Beziehungen zu anderen Menschen intendiere.⁴⁷ In seiner Entscheidung *Leander gg. Schweden*⁴⁸ aus dem Jahr 1987 legte der Gerichtshof erstmals fest, dass schon die bloße Speicherung von persönlichen Daten eines Betroffenen durch eine öffentliche Stelle eine Beeinträchtigung des Rechts aus Art. 8 EMRK darstelle. Auf den Verwendungszusammenhang komme es für diese Feststellung nicht an.⁴⁹ Mit seinen Entscheidungen *Kopp gg. die Schweiz* und *Amann gg. die*

⁴¹ *Fromont*, DÖV 2005, S. 1 ff. (S. 2); *Grabenwarter/Pabel*, Europäische Menschenrechtskonvention, § 3 Rn. 3.

⁴² BVerfG NVwZ 2007, 808 (811); *Pieroth/Schlink*, Grundrechte – Staatsrecht II, Rn. 58.

⁴³ Frankreich ist der EMRK erst 1974 beigetreten und hat 1981 das Individualbeschwerderecht nach Art. 25 a.F. EMRK anerkannt. Vgl. den Signatur- und Ratifikationsstatus der EMRK:

<http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=005&CL=GER>.

⁴⁴ So auch *Viethen*, Datenschutz als Aufgabe der EG, S. 28.

⁴⁵ *Britz*, Das Grundrecht auf Datenschutz in Art. 8 der Grundrechtecharta, S. 4.

⁴⁶ *Viethen*, Datenschutz als Aufgabe der EG, S. 28; Zum Ganzen: *Gridl*, Datenschutz in globalen Telekommunikationssystemen, S. 107 ff; *Albers*, Informationelle Selbstbestimmung, S. 288 ff; *Siemen*, Datenschutz als europäisches Grundrecht, S. 51 ff.

⁴⁷ EGMR, Slg. 1998-I, S. 422, Nr. 32 – *Botta/Italien*.

⁴⁸ EGMR, 1987, Serie A, Band 116, S. 22, Nr. 48 – *Leander/Schweden*.

⁴⁹ Siehe auch EGMR NJOZ 2010, S. 696 ff. (697 f.) – *Marper/Vereinigtes Königreich*.

Schweiz⁵⁰ festigte der Gerichtshof diese Rechtsprechung und nahm explizit Bezug zur Europäischen Datenschutzkonvention. Art. 8 EMRK ist demnach sowohl auf die Erhebung und Speicherung als auch auf die Übermittlung von Daten durch öffentliche Stellen anwendbar, sofern ein Bezug zum Privatleben des Betroffenen besteht. Dabei legt der EGMR den Begriff „Privatleben“ weit aus⁵¹: Zwar könne der Begriff wohl kaum vollends definiert werden. Eine Beschränkung des Schutzbereichs auf den „inneren Kreis“ der Persönlichkeitsentfaltung sei jedoch zu restriktiv. Der Begriff umfasse auch die äußeren Beziehungen zu anderen Menschen. Selbst geschäftliche Beziehungen könnten in das Privatleben des Betroffenen fallen. Eine Ausdehnung dieses gerichtlichen Schutzes dergestalt, dass die Signatarstaaten für legislative Versäumnisse zum Schutz des Privatlebens im nicht-öffentlichen Bereich haftbar gemacht werden, erscheint möglich,⁵² wurde jedoch bislang nicht entschieden. Darüber hinaus schützt Art. 8 EMRK Daten juristischer Personen (wie z.B. Wirtschaftsunternehmen).⁵³

Zusammenfassend bleibt festzuhalten, dass unter Zugrundelegung der Rechtsprechung des EGMR zum Schutz der Privatlebens nach Art. 8 EMRK, für die beiden untersuchten Rechtsordnungen eine gemeinsame grundrechtliche Kontrolle auf europäischer Ebene von illegitimer und/oder unverhältnismäßiger Datenverarbeitung im öffentlichen Bereich vorhanden ist.

2. Die Datenschutzkonvention des Europarates

Am 28.01.1981 wurde die Datenschutzkonvention des Europarates⁵⁴ (DSK) unterzeichnet. Es handelt sich um den ersten völkerrechtlich verbindlichen Vertrag zur Sicherstellung eines einheitlichen Datenschutzniveaus.⁵⁵ Deutschland und Frankreich gehören zu den Erstunterzeichnern der Konvention, die am 01.10.1985 in Kraft trat. Obwohl es für eine Reihe von Mitgliedstaaten zu keinen Anpassungen der nationalen Gesetzgebungen kam,⁵⁶ gilt die Konvention als Meilenstein in der Entwicklung eines

⁵⁰ EGMR, Slg. 1998-II, S. 541, Nr. 51 ff. – *Kopp/Schweiz*; EGMR, Slg. 2000-II, Nr. 69 – *Amann/Schweiz*.

⁵¹ EGMR NJW 1993, S. 718 ff. (718 f.) – *Niemitz/Deutschland*.

⁵² Hierzu *Viechten*, Datenschutz als Aufgabe der EG, S. 28 mit Verweis auf EGMR EuGRZ 1985, S. 297 ff. – *X. und Y./Niederlande*; *Bodenschatz*, Der europäische Datenschutzstandard, S. 46 mit Verweis auf EGMR GRUR 2004, S. 1051 ff. – *Von Hannover/Deutschland*.

⁵³ *Grabenwarter/Pabel*, Europäische Menschenrechtskonvention, § 22 Rn. 4.

⁵⁴ Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten, Konvention Nr. 108.

⁵⁵ *Hochreiter*, Die heimliche Überwachung internationaler Kommunikation, S. 53 ff.; vgl. zum Ganzen das Werk von *Henke*, Die Datenschutzkonvention des Europarates.

⁵⁶ Darunter Deutschland, Frankreich und Luxemburg; vgl. hierzu *Burkert*, Die Konvention des Europarates zum Datenschutz, S. 753.

gemeinsamen europäischen Datenschutzrechts⁵⁷: Erstmals wurden verbindliche und spezifisch datenschutzrechtliche Mindeststandards (sog. „common core“, Art. 5 - 11 DSK) für die Signatarstaaten festgesetzt, die diese auch gegenüber Dritten in ihrem Hoheitsbereich durchsetzen müssen.

Die wichtigsten Datenverarbeitungsprinzipien enthält Art. 5 DSK⁵⁸:

- Der Grundsatz der begrenzten Datenerfassung und -verarbeitung nach Art. 5 lit. a DSK, wonach personenbezogene Daten nach Treu und Glauben und auf rechtmäßige Weise⁵⁹ beschafft und verarbeitet werden müssen. Während die „Rechtmäßigkeit“ eine gesetzliche Grundlage für die Datenverarbeitung erfordert, soll die Datenverarbeitung nach „Treu und Glauben“ einen gerechten Ausgleich zwischen den Interessen und Erwartungen der Beteiligten sowie die Informierung des Betroffenen über seine Rechte sicherstellen.⁶⁰ Die Einwilligung des Betroffenen als Rechtmäßigkeitsvoraussetzung nennt die Konvention allerdings nicht.⁶¹
- Der Grundsatz der Zweckbindung nach Art. 5 lit. b DSK. Hiernach müssen die Datenverarbeiter durch die Signatarstaaten verpflichtet werden, die Zwecke der Datenverarbeitung konkret festzulegen und sich sodann an diese zu halten.
- Der Grundsatz der Datenqualität nach Art. 5 lit. c und d DSK. Die personenbezogenen Daten müssen den Zwecken, für welche sie gespeichert wurden, „entsprechen“, d.h. im Verhältnis zu ihnen angemessen und erheblich sein. Zudem verlangt der Grundsatz, dass die Daten vom Verwender präzise und aktuell gehalten werden.
- Der Grundsatz des Vorrangs der anonymen Datenverarbeitung nach Art. 5 lit. e DSK, wonach personenbezogene Daten nur solange durch den Verarbeiter aufbewahrt werden dürfen, wie es für die Zweckerreichung notwendig ist.
- Hervorzuheben ist zudem der besondere Schutz sensibler Daten nach Art. 6 DSK, wozu auch Gesundheitsdaten zählen.

⁵⁷ Rächle, Online-Profiling, S. 74.

⁵⁸ Ausführlich Henke, Die Datenschutzkonvention des Europarates, S. 96 ff.; Vgl. auch die Aufzählungen bei Bodenschatz, Der europäische Datenschutzstandard, S. 51 f.; Rächle, Online-Profiling, S. 76 ff.; Knaub, La protection des données, S. 365 ff.

⁵⁹ engl. „fairly and lawfully“ bzw. frz. „loyalement et licitement“; gemäß der Schlussformel der DSK ist ihr Text nur in englischer und französischer Sprache verbindlich.

⁶⁰ Karanja, Transparency and Proportionality in the Schengen Information System and Border Control Co-operation, S. 148 f.; Viethen, Datenschutz als Aufgabe der EG, S. 33: „Beteiligung des Betroffenen“; Knaub, La protection des données, S. 375.

⁶¹ Hierzu Artikel 29-Datenschutzgruppe, Arbeitspapier 187, S. 7.

Im Gegensatz zur EMRK stellt die DSK kein unmittelbar anwendbares Recht in den Mitgliedstaaten dar. Ihre Vergünstigungen kommen den Bürgern nur mittels Umsetzungsakten, zu denen die Mitgliedstaaten gemäß Artikel 4 Nr. 1 DSK verpflichtet sind, zugute. Ihr sachlicher Anwendungsbereich ist beschränkt auf automatisierte Dateien bzw. Datensammlungen und automatische Verarbeitungen von personenbezogenen Daten. Geschützt sind durch sie nur natürliche Personen, was jedoch einen weitergehenden Schutz juristischer Personen durch gesetzliche Bestimmungen der Signatarstaaten nicht ausschließt.⁶² Zudem ist die Datenerhebung vom Anwendungsbereich der DSK grundsätzlich nicht mitumfasst (Ausnahme: Der Grundsatz der begrenzten Datenerfassung und -verarbeitung nach Art. 5 lit. a DSK).⁶³ Es greift daher der in Art. 5 lit. b DSK normierte Zweckbindungsgrundsatz erst ab der Verarbeitungsphase der Datenspeicherung, was die DSK von der DSRL unterscheidet.⁶⁴ Andererseits gilt die Konvention gemäß Art. 3 Nr. 1 DSK auch für die Datenverarbeitung im privaten Bereich.

Die Datenschutzkonvention sieht in Art. 9 Abs. 3 DSK für den Bereich der wissenschaftlichen Forschung Ausnahmen von den in Art. 8 lit. a-d DSK aufgeführten Rechten der Betroffenen vor. Die Mitgliedstaaten dürfen zugunsten der Zwecke der wissenschaftlichen Forschung die Rechte der Betroffenen auf Auskunft nach den eigenen personenbezogenen Daten, auf Berichtigung bzw. Löschung dieser Daten sowie auf ein Rechtsmittel gegen Entscheidungen der verantwortlichen Stelle einschränken. Die Konvention stellt damit klar, dass die Rechtmäßigkeit der Verarbeitung personenbezogener Daten zu Forschungszwecken grundsätzlich keinen Sonderregeln unterworfen ist, erkennt jedoch andererseits an, dass besondere Transparenzbedingungen zum Schutze der Forschungszwecke notwendig sein können. Den Signatarstaaten soll die Möglichkeit erhalten bleiben, die Abwägung zwischen wissenschaftlicher Forschung und dem Schutz der Probandendaten selbständig vorzunehmen. Eine Privilegierung kommt nach dem Wortlaut der Vorschrift jedoch nur in Frage, „wenn offensichtlich keine Gefahr besteht, dass der Persönlichkeitsbereich der Betroffenen beeinträchtigt wird“. Welche Regulierungswirkung dieser Einschränkung konkret zukommt, ist damit allerdings nicht klar, zumal die DSK selbst hierzu keinerlei Vorgaben macht. Es handelt

⁶² Simitis/*Simitis*, BDSG, Einleitung Rn. 155 ff.

⁶³ Vgl. Art. 2 lit. c. DSK; hierzu *Henke*, Die Datenschutzkonvention des Europarates, S. 80 ff., der durch ergänzende Auslegung der Konvention versucht, diese „Lücke“ zu schließen.

⁶⁴ *Fink/Cole/Keber*, Europäisches und Internationales Medienrecht, Rn. 293; *Viethen*, Datenschutz als Aufgabe der EG, S. 33; wohl a.A. ohne Begründung *Kühling/Seidel/Sivridis*, Datenschutzrecht, S. 10.

sich um eine Vorgabe, welche die Signatarstaaten zur strikten Anwendung des Verhältnismäßigkeitsgrundsatzes anhält, sofern sie von dem Forschungsprivileg Gebrauch machen wollen.⁶⁵

Als Ergänzung zur Datenschutzkonvention beschloss das Ministerkomitee des Europarats 1983 konkretisierende Empfehlungen für den Bereich der wissenschaftlichen Forschung und 1997 zum Schutz medizinischer Daten.⁶⁶ Die Empfehlungen sind nicht bindend, können jedoch als Auslegungshilfe für die Datenschutzkonvention dienen.⁶⁷ Die Konvention wurde durch das Zusatzprotokoll (ETS No. 181) vom 08.11.2001 zeitgemäß erweitert. Nach Art. 1 ETS No. 181 sehen die Vertragsstaaten unabhängige Kontrollstellen zur Gewährleistung der Rechte und Grundfreiheiten bei der Datenverarbeitung, d. h. staatliche Datenschutzbeauftragte oder -kommissionen, vor. Nach Art. 2 ETS No. 181 sollen personenbezogene Daten an Drittstaaten oder -organisationen grundsätzlich nur übermittelt werden dürfen, wenn dort ein angemessenes Datenschutzniveau gewährleistet wird, wobei Abweichungen von diesem Grundsatz möglich bleiben.

Seit 2011 wird die mittlerweile über 30 Jahre alte Konvention durch den Europarat überarbeitet.⁶⁸ Es steht u.a. zu erwarten, dass die Begrenzung des Anwendungsbereichs der Konvention auf die automatische Datenverarbeitung aufgehoben wird und „sensitive Daten“ künftig als solche angesehen werden, deren Verarbeitung eine Gefährdung der Interessen, der Rechte und der Freiheiten des Betroffenen bedeuten könnten.

3. Die Biomedizin-Konvention des Europarates

Die Biomedizin-Konvention des Europarates vom 04.04.1997 (BMK)⁶⁹ enthält Mindeststandards zum Schutz der Menschenwürde und der Identität im Hinblick auf die Anwendung von Medizin und Biologie. Sie versteht sich als Konkretisierung der

⁶⁵ Ähnlich *Schiedermaier*, Der Schutz des Privaten als Internationales Grundrecht, S. 323; Siehe auch die Dokumente des Europarates „Explanatory Memorandum Recommendation No. R (97) 5 of the Committee of Ministers to Member States on the protection of medical data“, Rz. 161 und „Explanatory Memorandum Recommendation No. R (97) 18 of the Committee of Ministers to Member States concerning the protection of personal data collected and processed for statistical purposes“, Rz. 89.

⁶⁶ Empfehlungen des Europarats Nr. R (83) 10 und Nr. R (97) 5.

⁶⁷ *Pöttgen*, Medizinische Forschung und Datenschutz, S. 46; *Tinnefeld*, DuD 1999, S. 35 ff. (37).

⁶⁸ Überblick auf http://www.coe.int/t/dghl/standardsetting/dataprotection/modernisation_en.asp; hierzu *Simitis/Simitis*, BDSG, Einleitung Rn. 177 ff.

⁶⁹ Übereinkommen zum Schutz der Menschenrechte und der Menschenwürde im Hinblick auf die Anwendung von Biologie und Medizin: Übereinkommen über Menschenrechte und Biomedizin vom 4. April 1997; auch genannt „Bioethik-Konvention“ oder „Oviedo Convention“.

EMRK in Bezug auf medizinische Therapie und zugleich auf die biomedizinische Forschung (Art. 15 ff. BMK).⁷⁰ Neben der Menschenwürde und der körperbezogenen Selbstbestimmung gehört die informationelle Selbstbestimmung zu den Grundrechten, welche vor der Biomedizin geschützt werden soll, auch wenn weitestgehend datenschutzrechtliche Detailregelungen fehlen.⁷¹ Trotz der Möglichkeit Vorbehalte bezüglich jeder einzelnen Vorschrift gemäß Art. 36 Nr. 1 BMK auszusprechen, haben von den 47 Mitgliedstaaten des Europarates 18 die Konvention nicht oder noch nicht ratifiziert. Dies betrifft u.a. das Vereinigte Königreich, Österreich und Deutschland.⁷² Die Gründe für die Zurückhaltung bei der Ratifizierung dieses umstrittenen Übereinkommens sind unterschiedlich. Während im Vereinigten Königreich die Konvention als zu restriktiv und forschungshemmend erachtet wird,⁷³ hat sich Deutschland bei der Abstimmung im Ministerrat über die BMK der Stimme enthalten, um der öffentlichen Diskussion über die Zulässigkeit biomedizinischer Forschung nicht vorzugreifen.⁷⁴ Nach Angaben der Bundesregierung ist die öffentliche Meinungsbildung zur Konvention bislang nicht abgeschlossen.⁷⁵ Tatsächlich wird die Konvention von einem großen Teil der (Fach-) Öffentlichkeit kontrovers diskutiert. Der Widerstand regt sich vor allem gegen die Möglichkeit, bei einwilligungsunfähigen Patienten und/oder Probanden unter bestimmten Voraussetzungen Blut- und Gewebeproben zu entnehmen und sog. „verbrauchende Embryonenforschung“ durchzuführen, d.h. Forschung unter Zerstörung des frühen menschlichen Embryos.⁷⁶ Darüber hinaus bestehen Vorbehalte gegen die gruppennützige Forschung mit Minderjährigen.⁷⁷ Frankreich hat hingegen die Konvention ratifiziert. Diese wurde teilweise sogar durch die französische Gesetzgebung zur Bioethik inspiriert⁷⁸ und das Land gehört zu den Erstunterzeichnern. Die Konvention trat dort dennoch erst nach 15 Jahren am 1.4.2012 in Kraft. Der Grund für diese Verzögerung war weniger in der inhaltlichen Umstrittenheit der Konvention in Frankreich zu suchen, denn vielmehr in der Absicht, eine Präjudizwirkung auf den

⁷⁰ Radau, Die Biomedizinkonvention des Europarates, S. 39 f.

⁷¹ Radau, Die Biomedizinkonvention des Europarates, S. 25 ff.; Tinnefeld/Buchner/Petri, Einführung in das Datenschutzrecht, S. 75.

⁷² Stand 25.8.2015.

⁷³ De Wachter, Hastings Center Report 1997, Heft 1, S. 13 ff. (13 ff.); Andorno, Journal of International Biotechnology Law 2005, Heft 2, S. 133 ff. (133).

⁷⁴ Quaaß/Zuck, Medizinrecht, § 67 Rn. 15, dort Fn. 21.

⁷⁵ BT-Drs. 17/5315, S. 3 f.; davor bereits BT-Drs. 16/21, S. 4.

⁷⁶ Eine Zusammenfassung der Diskussion findet sich bei Taupitz, Einführung in die Thematik: Die Menschenrechtskonvention zur Biomedizin zwischen Kritik und Zustimmung, S. 1 ff. m.w.N.; vgl. auch König, MedR 2005, S. 22 ff. (22 ff.).

⁷⁷ Hierzu Sprecher, Medizinische Forschung mit Kindern und Jugendlichen, S. 188.

⁷⁸ Goffin/Borry/Dierickx/Nys, Health Policy 2008 (Nr. 86), S. 222 ff. (225) mit Bezug auf die französischen Bioethikgesetze von 1994, hierzu unten § 3, II., 1., a., (3), (a), (aa).

französischen Gesetzgeber zu vermeiden.⁷⁹ Von den vier Zusatzprotokollen, welche die Konvention über die Jahre erhielt, hat Frankreich drei unterzeichnet und noch keines ratifiziert.⁸⁰

Zum Schutz personenbezogener Daten sind insbesondere die Präambel, welche auf die Datenschutzkonvention des Europarates verweist, sowie Art. 5 und Art. 10 BMK hervorzuheben. Der Einwilligungsvorbehalt nach Art. 5 BMK legt fest, dass jedwede Intervention im Gesundheitsbereich grundsätzlich der informierten Einwilligung des Betroffenen bedarf. Auch sind Eingriffe zu Forschungszwecken vom Einwilligungsvorbehalt umfasst, was sich aus einem Umkehrschluss aus Artikel 16 V BMK ergibt. Die Einwilligung zu Forschungszwecken muss danach schriftlich erfolgen. Art. 10 BMK, welcher in seiner amtlichen Überschrift explizit auf den Schutz der Privatsphäre deutet, garantiert den Betroffenen das Recht auf Verschwiegenheit der behandelnden Ärzte oder anderer Institutionen in Bezug auf die erhobenen Gesundheitsdaten sowie das Recht auf Information. Eine „Intervention im Gesundheitsbereich“ (engl. *intervention in the health field*) als ein zentraler Begriff wird in der BMK nicht näher definiert. Bedenkt man die Ambitionen des Europarates, einen möglichst umfassenden Schutz der Würde und der Identität aller Menschen im Bereich der Medizin und Biologie zu gewährleisten, so muss von einem weiten Verständnis ausgegangen werden. Er bezeichnet daher jedwede Form von therapeutischen oder präventiven medizinischen Eingriffen.⁸¹ Sowohl Eingriffe in die körperliche als auch in die psychische Integrität des Betroffenen sind umfasst. Fragebögen, Interviews oder Beobachtungen können in diesem Sinne nur dann eine Intervention darstellen, wenn sie ein Risiko für die Gesundheit des Betroffenen darstellen.⁸² Einfache Fragen und Beobachtungen stellen daher in aller Regel keine Intervention dar, erst Recht keine Forschung, die ausschließlich unter Abwesenheit des Betroffenen erfolgt.⁸³

⁷⁹ Goffin/Borroy/Dierickx/Nys, Health Policy 2008 (Nr. 86), S. 222 ff. (225); Teboul, Éthique et santé 2012, S. 39 ff. (40 f.).

⁸⁰ Stand: Dezember 2015; die Zusatzprotokolle über das Verbot zum Klonen von menschlichen Lebewesen (ETS Nr. 168), bezüglich der Transplantation von menschlichen Organen und Gewebe (ETS Nr. 186) und betreffend der Gentests zu gesundheitlichen Zwecken (ETS Nr. 203) wurden unterzeichnet, jedoch das Zusatzprotokoll betreffend der biomedizinischen Forschung (ETS Nr. 195) nicht.

⁸¹ Siehe hierzu Europarat, Convention on Human Rights and Biomedicine – Explanatory Report, Rz. 29.

⁸² Lõuk, Rethinking the Ethics of Human Biomedical Non-Interventional Research, S. 177; Niedziolka, Rechtliche Rahmenbedingungen der Anwendungsbeobachtung bei Arzneimitteln, S. 61 f. m.w.N.

⁸³ Lõuk, Rethinking the Ethics of Human Biomedical Non-Interventional Research, S. 176 f.

II. Datenschutzbestimmungen der EU

1. Datenschutz als EU-Grundrecht

Im Primärrecht der EU ist das Grundrecht auf Schutz von personenbezogenen Daten, welches die Gemeinschaftsorgane und -einrichtungen sowie die Mitgliedstaaten bei der Ausführung des EU-Rechts bindet, gleich an zwei Stellen verankert: Art. 8 der Europäischen Grundrechtecharta (GRC) und Art. 16 Abs. 1 AEUV. Mit der Kodifizierung des Datenschutzgrundrechtes in den Verträgen und der bindenden Verrechtlichung der GRC haben die Veränderungen durch den Vertrag von Lissabon zu einer deutlichen Aufwertung des Datenschutzes im Primärrecht geführt.⁸⁴ Vor der ausdrücklichen Anerkennung verstand sich der Datenschutz im Unionsrecht primär als Ausprägung des durch Art. 8 EMRK geschützten Rechts auf Privatsphäre, wie Art. 1 Abs. 1 DSRL zeigt.⁸⁵ Auf die Herleitung eines Datenschutzgrundrechts als Teil des allgemeinen Grundsatzes auf Achtung des Privatlebens nach Art. 6 Abs. 3 EUV i.V.m. Art. 8 Abs. 1 EMRK kommt es aufgrund der vorstehenden expliziten Regelungen jedoch nicht mehr an.

Die Vorschrift des Art. 8 Abs. 1 GRC, welche als Teil des Rechts der Grundrechtecharta gemäß Art. 6 Abs. 1 S. 1 EUV mit den EU-Verträgen gleichrangig ist, umfasst das Recht jeder Person „auf Schutz der sie betreffenden personenbezogenen Daten“. Neben dem Recht der Person auf Achtung ihres Privat- und Familienlebens, ihrer Wohnung sowie ihrer Kommunikation nach Art. 7 GRC statuiert die Vorschrift damit ein eigenständiges Datenschutzgrundrecht. Erfasst ist von Art. 8 GRC in Anlehnung an Art. 2 lit. a) und b) DSRL und Art. 2 lit. a) und b) VO EG/45/2001 jedwede Verarbeitung, d.h. die Erhebung, Speicherung, Verwendung, Sperrung oder Löschung⁸⁶ von Informationen über eine bestimmte oder bestimmbare natürliche Person. Der Schutzbereich ist damit - parallel zu der Rechtsprechung des EGMR zum Datenschutz im Rahmen des Art. 8 EMRK - weit gefasst. Auf die Sensitivität der Daten oder eventuelle Nachteile infolge der Datenverarbeitung kommt es nicht an.⁸⁷ Die unter Berufung auf den EuGH vertretene Ansicht, die bloße Speicherung personenbezogener Daten über die an das Personal gezahlten Gehälter durch einen Arbeitgeber ohne Wei-

⁸⁴ So auch die Enquete-Kommission „Internet und digitale Gesellschaft“, Fünfter Zwischenbericht vom 15.3.2012, BT-Drs. 17/8999, S. 9.

⁸⁵ Grabitz/Hilf/Nettesheim/Sobotta, Das Recht der Europäischen Union, Art. 16 AEUV, Rn. 5.

⁸⁶ Callies/Ruffert/Kingreen, EUV/AEUV, Art. 8 EU-GRCharta, Rn. 12; Jarass, EU-GRCharta, Art. 8 Rn. 8.

⁸⁷ Jarass, EU-GRCharta, Art. 8 Rn. 8.

tergabe an Dritte sei kein Eingriff in den Schutzbereich,⁸⁸ verkennt die in der Zwischenzeit eingetretene Verselbständigung des Datenschutzgrundrechts gegenüber dem Schutz der Privatsphäre.⁸⁹ Dem weiten Schutzbereich steht die Schrankenregelung des Art. 8 Abs. 2 GRC gegenüber. Das Grundrecht nach Art. 8 Abs. 1 GRC kann gemäß Art. 8 Abs. 2 GRC eingeschränkt werden, wenn die Datenverarbeitung nach Treu und Glauben für festgelegte Zwecke und mit Einwilligung der betroffenen Person oder auf einer sonstigen gesetzlich geregelten legitimen Grundlage erfolgt.

Bereits bevor die GRC durch den Vertrag von Lissabon für die Gemeinschaft unmittelbare Verbindlichkeit erlangte, erkannte der EuGH unter Hinweis auf Art. 8 GRC ein Grundrecht auf den Schutz personenbezogener Daten an, gleichwenn der inhaltliche Bezug zum Schutz des Privatlebens nach Art. 8 EMRK und Art. 7 GRC betont und die Rechtsprechung des EGMR stets als vergleichender Maßstab herangezogen wurde.⁹⁰ Die Linie des EGMR spielt in der Rechtsprechung des EuGH auch nach der Verselbständigung des Datenschutzgrundrechts eine gewichtige Rolle. Denn der Datenschutz steht nach Ansicht des Gerichts, dargelegt im Urteil „Schecke“, in einem engen Zusammenhang mit dem in Art. 7 GRC verankerten Recht auf Achtung des Privatlebens.⁹¹ Bei dessen Auslegung nimmt der Gerichtshof – gestützt auf Art. 52 Abs. 3 und Art. 53 GRC – die Rechtsprechung des EGMR zu Art. 8 EMRK als Maßstab und geht davon aus, „dass sich die in den Art. 7 und 8 GRC anerkannte Achtung des Privatlebens hinsichtlich der Verarbeitung personenbezogener Daten auf jede Information erstreckt, die eine bestimmte oder bestimmbare natürliche Person betrifft und zum anderen, dass Einschränkungen des Rechts auf Schutz der personenbezogenen Daten gerechtfertigt sein können, wenn sie denen entsprechen, die im Rahmen von Art. 8 EMRK geduldet werden“.⁹² Damit bejaht der EuGH zugleich die Frage, ob das EG-Datenschutzgrundrecht den durch die EMRK garantierten Rechten gemäß Art. 53 Abs. 3 GRC entspricht. Diese Rechtsprechung steht zwar somit im offenen Widerspruch zu einer teilweise vertretenen gegenläufigen Annahme in der Literatur⁹³ und ist insbeson-

⁸⁸ Callies/Ruffert/Kingreen, EUV/AEUV, Art. 8 EU-GRCharta, Rn. 12 a.E.

⁸⁹ EuGH EuR 2004, S. 276 ff. (286) – Österreichischer Rundfunk, verneint explizit nur einen Eingriff in die „Privatsphäre“ und nicht in den Schutz „personenbezogener Daten“.

⁹⁰ vgl. z.B. EuGH GRUR 2008, S. 241 ff. (244) – Promusicae; EuGH EuR 2004, S. 276 ff. (285) – Österreichischer Rundfunk u.a.

⁹¹ EuGH GewArch 2011, S. 24 ff. (24) – Schecke.

⁹² EuGH GewArch 2011, S. 24 ff. (25) – Schecke; zur Schutzbereichermittlung des Art. 8 Abs. 1 GRC im Rahmen des Art. 53 GRC vgl. Wehlau/Lutzhöft, EuZW 2012, S. 45 ff. (47).

⁹³ Britz, EuGRZ 2009, S. 1 ff. (6); Callies/Ruffert/Kingreen, EUV/AEUV, Art. 8 EU-GRCharta, Rn. 4 m.w.N.; a.A. wohl Jarass, EU-GRCharta, Art. 8 Rn. 11.

dere aus rechtsdogmatischer Sicht problematisch.⁹⁴ Auch nach der Ansicht des Europäischen Konvents zur Grundrechtecharta gehört das Recht aus Art. 8 GRC nicht zu denjenigen Rechten, welche inhaltlich gemäß Art. 52 Abs. 3 GRC den durch die EMRK garantierten Rechten entsprechen.⁹⁵ Jedoch kann der EuGH durch die strikte Anlehnung an die Rechtsprechung des EGMR unnötige Abweichungen vermeiden und erspart sich mittelbar mit der Festlegung auf Art. 52 Abs. 3 GRC die ansonsten sich aufdrängende Abgrenzung des Art. 8 GRC zum vorbehaltlos gewährten Datenschutz nach Art. 16 Abs. 1 AEUV über Art. 52 Abs. 2 GRC.

Probleme mit der Bindungswirkung des Art. 8 GRC gegenüber den Mitgliedstaaten bestehen nicht. Neben Art. 16 AEUV besteht mit der DSRL Unionsrecht, welches durch die Mitgliedstaaten durchzuführen ist i.S.d. Art. 51 Abs. 1 S. 1 GRC. Es ist dabei zu bedenken, dass der EuGH den Anwendungsbereich des Vertrages, der die Bindung des Mitgliedstaates begründet sehr weit versteht. So hat der EuGH die in einem österreichischen Gesetz enthaltene Verpflichtung, die Bezüge von Spitzenfunktionären im öffentlichen Dienst zu veröffentlichen, zunächst am Maßstab der DSRL geprüft um letztlich das betreffende nationale Gesetz an den Grundrechten aus dem GRC zu messen.⁹⁶

Mit dem Vertrag von Lissabon wurde zudem Art. 16 AEUV eingeführt, dessen Vorgängerregelung (Art. 286 EGV a.F.) die Rechtsakte der Gemeinschaft zum Datenschutz für die Gemeinschaftsorgane und -einrichtungen für anwendbar erklärte und die Schaffung einer unabhängigen Kontrollinstanz für den Datenschutz anordnete. Art. 16 Abs. 1 AEUV bestimmt an herausgehobener Stelle im Titel II (Allgemein geltende Bestimmungen), dass jede Person „das Recht auf Schutz der sie betreffenden personenbezogenen Daten“ habe. Die Vorschrift enthält damit ebenfalls ein primärrechtliches eigenständiges Grundrecht auf Datenschutz, das gegenüber den Gemeinschaftsorganen, -einrichtungen und sonstigen Stellen der EU sowie gegenüber den Mitgliedstaaten gilt, soweit sie im Anwendungsbereich des Unionsrechts handeln.⁹⁷ Art. 16 Abs. 1 AEUV ist mit Art. 8 Abs. 1 GRC im Wortlaut identisch. Differenzen bezüglich

⁹⁴ *Brink/Wolff*, JZ 2011, S. 206 ff. (S. 206 ff.).

⁹⁵ Siehe hierzu Europäischer Konvent, Charta-Entwurf „Charte 4473/1/00 REV 1“ vom 19.10.2000 in abschließlich frz. Version mit Erläuterungen des Konventpräsidiums, S. 11.

⁹⁶ EuGH EuR 2004, S. 276 ff. (285 f.) – Österreichischer Rundfunk; hierzu Callies/Ruffert/Kingreen EUV/AEUV, Art. 8 EU-GRCharta, Rn. 8.

⁹⁷ Vgl. Geiger/Khan/Kotzur/Kotzur, EUV/AEUV, Art. 16 AEUV, Rn. 2; Callies/Ruffert/Kingreen, EUV/AEUV, Art. 16 AEUV, Rn. 6.

des Schutzgegenstandes bestehen keine.⁹⁸ Auch werden durch die Vorschriften gleichermäßen die Institutionen der EU sowie die Mitgliedstaaten bei Entscheidungen mit Bezug zum Europarecht gebunden. Art. 16 AEUV gewährt den Datenschutz jedoch ohne explizite Schranken. Der EuGH zieht bislang lediglich Art. 8 Abs. 1 GRC heran und erspart sich eine Abgrenzung.⁹⁹

2. Die EG-Datenschutzrichtlinie

Die EG-Datenschutzrichtlinie (DSRL) aus dem Jahr 1995¹⁰⁰ errichtete erstmals und bildet seitdem einen einheitlichen und verbindlichen Rechtsrahmen für den Datenschutz in den Mitgliedstaaten der Europäischen Union. Die DSRL ist von enormer Bedeutung für die nationale Gesetzgebung und Rechtsanwendung, da sie innerhalb der Grenzen ihres Anwendungsbereichs als Auslegungsmaßstab für das nationale Recht gilt und der EuGH in zahlreichen Entscheidungen die einheitliche Auslegung sichergestellt hat.¹⁰¹ Der Richtlinie sind lange Verhandlungen vorausgegangen, welche sich u.a. aufgrund von Kompetenzfragen als schwierig erwiesen und bei denen sich die bis dahin unterschiedlichen nationalen Gepflogenheiten offenbarten.¹⁰² Wie jede EG-Richtlinie bedurfte sie der Umsetzung durch die Mitgliedstaaten. Diese erfolgte in Deutschland im Jahr 2001.¹⁰³ In Frankreich wurde die Richtlinie erst im Jahr 2004 mit dem Gesetz Nr. 2004-801 vom 6. August 2004¹⁰⁴ umgesetzt.

Der weite sachliche Anwendungsbereich der Richtlinie erstreckt sich gemäß Art. 3 Abs. 1 DSRL auf „die ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten sowie [...] die nicht automatisierte Verarbeitung personenbezogener Daten,

⁹⁸ *Schiedermaier*, Der Schutz des Privaten als Internationales Grundrecht, S. 343; von der Groeben/Schwarze/Hatje/Brühann, Europäisches Unionsrecht, Art. 16 AEUV Rn. 30; Calliess/Ruffert/Kingreen, EUV/AEUV, Art. 16 AEUV, Rn. 3 („Dopplung“).

⁹⁹ Das Gericht hat mittlerweile mehrmals die Gelegenheit für eine Befassung mit Art. 16 AEUV nicht genutzt; vgl. EuGH GewArch 2011, S. 24 ff. (24 f.) – Schecke; EuGH EuZW 2012, S. 37 ff. (39 f.) – ASNEF; EuGH MMR 2014, S. 455 ff. (461) – Google.

¹⁰⁰ Richtlinie 95/46/EG des europäischen Parlamentes und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr.

¹⁰¹ Z.B. EuGH MMR 2004, S. 95 ff. – Lindqvist; EuGH EuR 2004, S. 276 ff. – Österreichischer Rundfunk; EuGH GRUR 2008, S. 241 ff. – Promusicae; EuGH MMR 2009, S. 175 ff. – Satakunnan Markkinapörssi; EuGH MMR 2009, S. 171 ff. – Huber; EuGH MMR 2010, S. 252 ff. – Kommission gg. Deutschland; EuGH EuZW 2012, S. 37 ff. – ASNEF.

¹⁰² Frz. Senat, Bericht Nr. 218 vom 19.3.2003, Berichterstatter Türk, S. 24 spricht insofern von unterschiedlichen „Kulturen“.

¹⁰³ Gesetz zur Änderung des Bundesdatenschutzgesetzes und anderer Gesetze vom 18. Mai 2001, BGBl I 2001, 904, in Kraft seit dem 23.05.2001.

¹⁰⁴ Loi n° 2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, JORF Nr. 182 vom 7.8.2004, S. 14063.

die in einer Datei gespeichert sind oder gespeichert werden sollen“. Die in dieser Formel verwendeten unbestimmten Rechtsbegriffe „personenbezogenen Daten“, „Verarbeitung“ und „Datei“ werden in Art. 2 lit. a - c definiert, wobei weitere Präzisierungen den Erwägungsgründen entnommen werden können. Demnach sind personenbezogene Daten alle Informationen über eine bestimmte oder bestimmbare natürliche Person. Bei der Entscheidung, ob eine Person bestimmbar ist, sind alle Mittel zu berücksichtigen, die vernünftigerweise von dem Verantwortlichen oder von einem Dritten eingesetzt werden könnten, um die betreffende Person zu bestimmen.¹⁰⁵ Dabei wird wie bei der Datenschutzkonvention des Europarates keine Unterscheidung zwischen dem privaten und dem öffentlichen Sektor gemacht. Aus Art. 2 lit. b) DSRL folgt weiterhin, dass für die Anwendbarkeit der Richtlinie die Bestimmung einer konkreten Verarbeitungsphase („Erhebung“, „Übermittlung“, usw.) keine Rolle spielt, da jeglicher Umgang mit einem personenbezogenem Datum als „Verarbeitung“ definiert wird, wobei mit diesem Begriff sowohl einzelne Vorgänge als auch miteinander verknüpfte Vorgangsreihen gemeint sein können.¹⁰⁶ Die DSRL gilt gemäß Art. 3 Abs. 1 DSRL sowohl für die „automatisierte Verarbeitung“ unter Zuhilfenahme von Datenverarbeitungsanlagen als auch die „nicht-automatisierte“, also die manuelle Verarbeitung. Letzteres gilt jedoch nur, sofern diese in Dateien erfolgt, die nach bestimmten personenbezogenen Kriterien strukturiert sind und einen leichten Zugriff auf die Daten ermöglichen. Unsortierte Akten, welche personenbezogene Daten enthalten, fallen demnach nicht in den Anwendungsbereich der DSRL.

Bezüglich der räumlichen Anwendbarkeit ordnet Art. 4 Abs. 1 DSRL an, dass die Umsetzungsvorschriften der Mitgliedstaaten auf Datenverarbeitungsvorgänge anzuwenden sind, die verantwortliche Stelle „im Rahmen der Tätigkeiten einer Niederlassung“ im betroffenen Mitgliedstaat ausführt oder dort auf „automatisierte oder nicht automatisierte Mittel“ zurückgreift. Eine Niederlassung setzt nach Erwägungsgrund 19 der Richtlinie die effektive und tatsächliche Ausübung einer Tätigkeit mittels einer festen Einrichtung voraus, wobei die Rechtsform nicht maßgeblich ist.¹⁰⁷ Der Umstand, dass die Niederlassung die Datenverarbeitung lediglich wirtschaftlich fördert, soll nach An-

¹⁰⁵ Vgl. Erwägungsgrund 26 der DSRL; Hierzu *Boulanger/de Terwangne/Léonard/Louveau/Moreau/Poullet*, JTDE 1997, S. 121 ff. (124).

¹⁰⁶ *Kopp*, DuD 1995, S. 204 ff. (207).

¹⁰⁷ Vgl. EuGH, Slg. 1985, I-2251, Rn. 19 – Berkholz.

sicht des EuGH bereits dafür reichen, dass die verantwortliche Stelle „im Rahmen der Tätigkeit“ dieser Niederlassung personenbezogene Daten verarbeitet.¹⁰⁸

Im Kern sieht die Richtlinie im Unterschied zur Datenschutzkonvention ein generelles Verbot der Verarbeitung personenbezogener Daten mit Erlaubnisvorbehalt vor, Art. 7 DSRL. Nur in den Fällen des Art. 7 lit. a bis f DSRL bleibt die Datenverarbeitung erlaubt, demnach zumeist dann, wenn die betroffene Person in die Datenverarbeitung eingewilligt hat (Art. 7 lit. a DSRL), die Datenverarbeitung notwendig ist im Hinblick auf den Abschluss oder die Erfüllung eines für die betroffene Person bindenden Vertrags (Art. 7 lit. b DSRL) oder zur Wahrnehmung einer Aufgabe, die in Ausübung hoheitlicher Gewalt erfolgt (Art. 7 lit. e, 2. Alt. DSRL). Die gesetzliche Konkretisierung der öffentlichen Aufgaben, für die Behörden Daten verarbeiten dürfen, bleibt den Mitgliedstaaten selbst vorbehalten. Gemäß Art. 8 DSRL genießen die Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen (sensitive Daten), besonderen Schutz. Zwar gilt auch für sie das generelle Verbot der Datenverarbeitung mit Erlaubnisvorbehalt. Die Hürden der für sie vorgesehenen Ausnahmeregelungen in Art. 8 Abs. 2 DSRL sind jedoch ungleich höher. Zusätzlich stützt sich die DSRL auf die aus der Datenschutzkonvention bekannten Prinzipien, so insbesondere auf den Grundsatz der begrenzten Datenerfassung und -verarbeitung nach Art. 6 Abs. 1 lit. a DSRL. Nach dem Grundsatz der Zweckbindung nach Art. 6 Abs. 1 lit. b und e DSRL dürfen die verantwortlichen Stellen eine Verarbeitung personenbezogener Daten nur vornehmen, sofern (Art. 6 Abs. 1 lit. b DSRL) und solange (Art. 6 Abs. 1 lit. e DSRL) sie die Daten für die zuvor festgelegten Zwecke verwenden.

3. Die Artikel 29-Datenschutzgruppe

Benannt nach der zugrundeliegenden Vorschrift in der DSRL hat die Art. 29 - Datenschutzgruppe für die Auslegung und Konkretisierung der DSRL und die Entwicklung von allgemeinen Leitlinien zu datenschutzrechtlichen Fragestellungen auf europäischem Level eine hohe Bedeutung.¹⁰⁹ Die Entscheidungen dieses Gremiums besitzen zwar keine Bindungswirkung; die Gruppe hat gemäß Art. 29 Abs. 1 S. 2 DSRL „nur“ beratende Funktion. Sie als reines Beratungsorgan der Europäischen Kommission zu qualifizieren, würde jedoch dem Status der überwiegenden Anzahl ihrer Mit-

¹⁰⁸ EuGH MMR 2014, S. 455 ff. (459 f.) – Google; Vgl. dagegen Artikel 29-Datenschutzgruppe, Arbeitspapier 179, S. 20 f.

¹⁰⁹ *Boulanger/de Terwangne/Léonard/Louveau/Moreau/Poullet*, JTDE 1997, S. 121 ff. (178).

glieder als nationale Datenschutzkontrolleure nicht gerecht. Bei der Gruppe handelt sich nämlich um ein unabhängiges Gremium mitgliedstaatlicher – ihrerseits unabhängiger – Kontrollinstanzen, wobei jeder Mitgliedstaat je einen Vertreter entsendet. Deutschland wird durch den Bundesbeauftragten für den Datenschutz und Informationsfreiheit vertreten, während der französische Vertreter der Präsident der *Commission nationale de l'informatique et des libertés* (CNIL) ist. Vervollständigt wird das Gremium durch den Europäischen Datenschutzbeauftragten als Kontrollstelle für die Institutionen und Organe der Gemeinschaft sowie einem Vertreter der Kommission. Letzterer besitzt jedoch kein Stimmrecht. Das Gremium besteht demnach derzeit aus 30 Vertretern (28 + 1 + 1). Es wird weiterhin bei seinen Sekretariatsgeschäften durch die Kommission unterstützt, wobei das Sekretariat derzeit bei der Generaldirektion Justiz angesiedelt ist.¹¹⁰ Aufgrund dieser Mitgliederstruktur und der damit verbundenen datenschutzrechtlichen Expertise wird die Gruppe gemeinhin mit den „aggregierten Datenschutzinteressen in der Union identifiziert“.¹¹¹ Da kein vergleichbares Fachgremium in Europa existiert, kommt ein Alleinstellungsmerkmal hinzu. Relativiert wird die Doppelrolle als Expertengruppe einerseits und zentrales Kollektiv der Vollzugsbehörden andererseits lediglich durch die divergierende nationale Gesetzgebung zum Datenschutz sowie die damit ebenfalls einhergehende Möglichkeit, mehrere Kontrollinstanzen mit unterschiedlichen Funktionen zu schaffen. Sind in einem Mitgliedstaat mehrere Kontrollinstanzen vorhanden, so müssen diese sich auf einen Vertreter einigen (Beispiel Deutschland: BFDI und die Datenschutzbeauftragten der Länder).

Die Aufgaben der Art. 29-Datenschutzgruppe ergeben sich aus Art. 30 DSRL und Art. 15 der Datenschutzrichtlinie für elektronische Kommunikation. Demnach berät die Gruppe vornehmlich die Kommission durch Stellungnahmen zu allen Fragen bezüglich der Datenschutzrichtlinien und deren Umsetzung in den Mitgliedstaaten. Die Gruppe kann gemäß Art. 30 Abs. 3 DSRL aber auch von sich aus Empfehlungen zu allen Fragen abgeben, die den Schutz von Personen bei der Verarbeitung personenbezogener Daten in der Gemeinschaft betreffen. Dies hat die Datenschutzgruppe in der Vergangenheit häufig genutzt, um entscheidenden Einfluss auf das europäische Datenschutzniveau auszuüben.¹¹² Wichtig sind die in diesem Rahmen von der Gruppe erstellten und veröffentlichten Arbeitspapiere, welche zu aktuellen Themen des Daten-

¹¹⁰ Zu den damit verbundenen Implikationen und Problemen siehe Simitis/*Simitis*, BDSG, Einleitung, Rn. 227.

¹¹¹ Burkert in: Roßnagel, Handbuch Datenschutzrecht, S. 106 f.; Vgl. auch Tinnefeld/Ehmann/Gerling, Einführung in das Datenschutzrecht, 4. Auflage, S. 131.

¹¹² Tinnefeld/Ehmann/Gerling, Einführung in das Datenschutzrecht, 4. Auflage, S. 131.

schutzes Stellung nehmen.¹¹³

Relevant für den Bereich des Forschungsdatenschutzes im Bereich der Medizin sind insbesondere die Arbeitspapiere über genetische Daten, über die Verarbeitung von Patientendaten in elektronischen Patientenakten, die Stellungnahme zum Begriff „personenbezogene Daten“, die Stellungnahme zu den Entwicklungen im Bereich biometrischer Technologien, die Stellungnahme zum Zweckbindungsgrundsatz sowie die Stellungnahme zu Open Data und der Weiterverwendung von Informationen des öffentlichen Sektors.¹¹⁴ In diesen Dokumenten konturiert die Gruppe den Forschungsdatenschutz punktuell und kontextbezogen, wobei sie die Anforderungen der DSRL, insbesondere die Definition des personenbezogenen Datums¹¹⁵ und die Ausnahme vom Zweckbindungsgrundsatz für Forschungszwecke¹¹⁶ näher umschreibt und anhand von Beispielen erläutert.

4. Besondere Bestimmungen für den Bereich der medizinischen Forschung

a. Besondere Bestimmungen der DSRL

Für die wissenschaftlichen Forschung hält die Richtlinie besondere Bestimmungen bereit: So können die Mitgliedstaaten vom Grundsatz der Zweckbindung zugunsten der wissenschaftlichen Forschung abweichen und insofern das Recht auf informationelle Selbstbestimmung einschränken, Art. 6 Abs. 1 lit. b S. 2 und lit. e S. 2 DSRL. Auch kann das Recht auf Information des Betroffenen für den Fall, dass die Daten nicht bei dieser Person erhoben wurden (Art. 11 Abs. 1 DSRL), sowie das Auskunftsrecht (Art. 12 DSRL) beschränkt werden. Die Mitgliedstaaten müssen für diese Ausnahmen jedoch „geeignete Garantien“ vorsehen. Dieses Erfordernis stellt ein Pendant zu dem aus Art. 9 Abs. 3 DSK des Europarates bekannten Anforderung „wenn offensichtlich keine Gefahr besteht, dass der Persönlichkeitsbereich der Betroffenen beeinträchtigt wird“ dar. Zwar definiert die Richtlinie nicht, welche regulatorischen Vorkehrungen hierunter zu fassen sein sollen und lässt somit den Mitgliedstaaten einen weiten Interpretationsspielraum.¹¹⁷ In Frage kommen letztlich alle Vorkehrungen rechtlicher,

¹¹³ Download der Arbeitspapiere unter: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/index_en.htm.

¹¹⁴ Artikel 29-Datenschutzgruppe, Arbeitspapiere 91, 131, 136, 193, 203, 207.

¹¹⁵ Artikel 29-Datenschutzgruppe, Arbeitspapier 136, S. 15 f..

¹¹⁶ Artikel 29-Datenschutzgruppe, Arbeitspapier 131, S. 16, Arbeitspapier 203, S. 28 ff. und Arbeitspapier 207, S. 22 f.

¹¹⁷ Pöttgen, Medizinische Forschung und Datenschutz, S. 49 f.

technischer und organisatorischer Art.¹¹⁸ Jedoch müssen die Vorkehrungen im Hinblick auf den Schutzgegenstand (Art. 1 Abs. 1 und Abs. 2 DSRL) zum einen auf einen Ausgleich des Eingriffs in das informationelle Selbstbestimmungsrechts gerichtet sein und zum anderen ausschließen, „dass die Daten für Maßnahmen oder Entscheidungen gegenüber einzelnen Betroffenen verwendet werden“.¹¹⁹

b. Besondere Bestimmungen für klinische Prüfungen mit Arzneimitteln

(1) Richtlinie 2001/20/EG

Die Richtlinie 2001/20/EG (GCP-RL)¹²⁰ behandelt die Voraussetzungen und die Bedingungen, insbesondere die Schutzvorkehrungen, bei klinischen Prüfungen von Arzneimitteln, jenem Teil der angewandten medizinischen Forschung also, welche die Wirksamkeit von Prüfpräparaten am lebenden Menschen untersucht. Ihr ausgewiesenes Ziel ist neben der Glaubwürdigkeit der Ergebnisse von klinischen Prüfungen der Schutz der Rechte, der Sicherheit und des Wohlergehens der Prüfungsteilnehmer (Art. 1 Abs. 2 S. 2 GCP-RL), wozu sie auch den Schutz der personenbezogenen Probandendaten zählt.¹²¹ Zu diesem Zweck bestimmt Art. 3 Abs. 2 lit. c) RL 2001/20/EG, dass im Rahmen von klinischen Prüfungen auf die Vorgaben der DSRL zu achten sei. Insbesondere sind daher die Aufklärungspflichten nach Art. 10 und Art. 11 DSRL bedeutsam. Vor diesem Hintergrund ist wohl die in Erwägungsgrund 16 der RL 2001/20/EG vorausgesetzte Informationspflicht, dass es bei Inspektionen der Prüfungsdokumentationen zu einer Aufdeckung der Personenidentität kommen kann, nicht in den Richtlinientext übernommen worden.

(2) Verordnung 536/2014/EU

Die am 16.4.2014 erlassene Verordnung 536/2014/EU¹²² (EU-AMVO) ersetzt mit Wirkung frühestens ab dem 28. Mai 2016 die GCP-RL.¹²³ Im Verhältnis zu ihrer Vorgängerregelung sind aus datenschutzrechtlicher Perspektive die folgenden Änderungen von Relevanz: Die Verordnung gestattet dem Sponsor, gleich bei Gelegenheit der klinischen Prüfung die Prüfungsteilnehmer an einem anderen wissenschaftlichen For-

¹¹⁸ *Tinnefeld*, DuD 1999, S. 35 ff. (36 ff.).

¹¹⁹ Erwägungsgrund 29 der DSRL.

¹²⁰ Richtlinie 2001/20/EG des europäischen Parlaments und des Rates vom 4. April 2001 zur Angleichung der Rechts- und Verwaltungsvorschriften der Mitgliedstaaten über die Anwendung der guten klinischen Praxis bei der Durchführung von klinischen Prüfungen mit Humanarzneimitteln.

¹²¹ Siehe die Erwägungsgründe 2 (Satz 2), 16 und 17 der Richtlinie 2001/20/EG.

¹²² Verordnung (EU) Nr. 536/2014 des Europäischen Parlaments und des Rates vom 16. April 2014 über klinische Prüfungen mit Humanarzneimitteln und zur Aufhebung der Richtlinie 2001/20/EG.

¹²³ Zummendfassend *Richter*, Ethik in der Medizin 2015, S. 89 ff.

schungsvorhaben außerhalb des Prüfungsplans zu beteiligen, sofern deren Einwilligung auch zu diesen Projekten eingeholt wird (Art. 28 Abs. 2 S. 1 EU-AMVO). Hierbei ist beachtlich, dass eine Beschränkung für medizinische Forschungszwecke nicht vorgesehen ist, wohl aber für wissenschaftliche Forschungszwecke im Allgemeinen. Es dürfte in einem solchen Fall für den Sponsor eine gesteigerte Aufklärungspflicht des Probanden gelten, um Irritationen bezüglich des Forschungszwecks und/oder der Datenempfänger zu vermeiden. Neu geregelt sind auch die Folgen eines Widerrufs der Einwilligungserklärung: Gemäß Art. 28 Abs. 3 S. 2 EU-AMVO gilt der Widerruf bezüglich der Datenverarbeitungsprozesse *ex nunc*. Der Widerruf hat keine Auswirkungen auf Tätigkeiten, die auf der Grundlage der Einwilligung bereits vor deren Widerruf durchgeführt wurden, oder auf die Verwendung der auf dieser Grundlage erhobenen Daten. Eine dem § 40 Abs. 2a S. 3 AMG entsprechende Vorschrift, wonach im Falle eines Widerrufs der Teilnahme die verantwortliche Stelle unverzüglich zu prüfen hat, inwieweit die gespeicherten Daten für die wesentlichen Zwecke der klinischen Prüfung noch erforderlich sein können, fehlt im Verordnungstext. Schließlich ist die Pflicht des Sponsors, „eine Beschreibung der Vorkehrungen für die Einhaltung der geltenden Vorschriften zum Schutz personenbezogener Daten, insbesondere der organisatorischen und technischen Maßnahmen, die getroffen werden, um die verarbeiteten Informationen und personenbezogenen Daten vor unbefugtem Zugriff, unbefugter Bekanntgabe, Verbreitung und Veränderung sowie vor Verlust zu schützen“¹²⁴ zu nennen. Die genannte Beschreibung ist Bestandteil des Prüfplans, den der Sponsor bei der zuständigen Ethik-Kommission einzureichen hat.

¹²⁴ Anhang I, D, Nr. 17 ak) EU-AMVO.

Der Schutz von Patientendaten für die medizinische
Forschung in Krankenhäusern

Eine rechtsvergleichende Untersuchung der
Regelungen in Deutschland und Frankreich

Karaalp, R.N.

2017, XVIII, 373 S., Softcover

ISBN: 978-3-658-16184-2