Berufsbegleitender Masterstudiengang
Informationsrecht (LL.M.)

Center für lebenslanges Lernen

Prof. Dr. Jürgen Taeger

Datenschutzrecht

Carl von Ossietzky Universität Oldenburg, 2017
10. Auflage

Impressum

Autor: Prof. Dr. Jürgen Taeger

Herausgeber: Carl von Ossietzky Universität
Center für lebenslanges Lernen (C3L)

Auflage: 10. überarbeitete Auflage

Oldenburg, Februar 2017

INHALTSVERZEICHNIS

I. EINFÜHRUNG IN DAS DATENSCHUTZRECHT

1 Entwicklung des nationalen, europäischen und internationalen Datenschutzrechts

Datenschutz kann nicht allein eine nationale Angelegenheit sein.[1] Die grenzüberschreitende Übermittlung personenbezogener Daten im Internet durch das weltumspannende World Wide Web und durch E-Mail-Dienste ist offensichtlich und allgemein bekannt. Aber schon vor dem Siegeszug des Web wurden Daten elektronisch über Datenleitungen und Satelliten nach Übersee übermittelt, so beispielsweise Arbeitnehmerdaten von der deutschen Konzerntochter an die Konzernmutter in den USA zur Verarbeitung der Personaldaten.[2] Heute beunruhigen Informationen darüber, dass für den grenzüberschreitenden Datentransfer von Arbeitnehmerdaten und – gefördert durch eCommerce und elektronische Versteigerungen – von Kundendaten, die für Individualisierungsstrategien im Marketing genutzt werden, große Teilen der Bevölkerung datenschutzrechtlich kaum sensibilisiert sind.

Mehr Sensibilisierung im Umgang mit den eigenen Daten, die häufig einschließlich Fotos freiwillig auf der eigenen Webseite, in Blogs, Tagebüchern und in virtuellen ‚Communities' öffentlich einsehbar dargeboten werden, wäre auch deswegen wünschenswert, weil das WWW nichts vergisst; einmal eingestellte Informationen über eine Person bleiben selbst dann zugänglich, wenn die Webquelle die Daten – aus welchem Grund auch immer – längst wieder gelöscht hat. Einmal in das Internet gelangte Informationen können nicht mehr zuverlässig entfernt werden. Auch Jahre nach der „Entfernung" von Informationen aus der eigenen Webseite können frühere Versionen des Webauftritts durch die Nutzung von Internet-Archiven wieder sichtbar gemacht werden. Forderungen nach einem gesetzlichen „Recht auf Vergessenwerden" erscheinen deshalb wenig realitätsnah.[3]

Personensuchmaschinen wie zoominfo.com, peoplecheck.de oder yasni.de durchsuchen das Netz nach personenbezogenen Informationen und stellen sie gebündelt zur Verfügung. Auch community-Portale wie Xing, Facebook oder linkedIn werden gescannt und ausgelesen. Das heutige „Web 2.0" ermöglicht eine weltweite Kommunikation und Interaktion über Plattformen, in die Nutzer selbst Inhalte – häufig mit sehr persönlichen Daten über sich selbst und Dritte – einstellen. „Social networks" sind Ausdruck einer Verlagerung des realen Lebens in das Internet.

---

[1] So auch *Grimm,* JZ 2013, S. 585 (589).

[2] Siehe dazu *Kilian*, Personalinformationssysteme in deutschen Großunternehmen, 1982, S. 62.

[3] Siehe *Feldmann*, Zum „Recht auf Vergessenwerden", in: Taeger, IT und Internet, 2012, S. 675; *Gerling/Gerling,* DuD 2013, S. 445; *Kodde*, ZD 2013, S. 115; *Hornung/Hofmann,* JZ 2013, S. 163; *Jandt/Kieselmann/Wacker*, DuD 2013, S. 235.

„Big Data“ ist das aktuelle Stichwort, unter dem neue technische Entwicklungen der Aufbereitung personenbezogener Daten im gewerblichen Bereich diskutiert werden.[4] Die weltweit verteilten Datenbestände mit personenbezogenen Daten sind bei Wirtschaftsunternehmen aufgrund des technischen Fortschritts bei der mobilen Kommunikation, durch den Einsatz von Cloud Computing, durch Social Media-Anwendungen erheblich angewachsen; die Datenmengen über Personen werden in kürzester Zeit exponentiell weiter wachsen. Aktuelle Techniken zur Nutzung großer Datenbanken etwa für Zwecke von Kundenbindungsmaßnahmen und individualisierter Werbung werden unter den Stichworten Data Warehousing und Data Mining diskutiert, deren Möglichkeiten sind angesichts der unstrukturierten Informationsmenge aber begrenzt. „Big Data“-Lösungen zielen darauf ab, extrem große Datenmengen zu strukturieren und als „vierte[n] Produktionsfaktor neben Kapital, Arbeitskraft und Rohstoffe[n]“[5] beispielsweise für Wissenschaft und Forschung, für das Marketing oder für die Korruptionsbekämpfung nutzbar zu machen. Auch damit wird das Datenschutzrecht vor neue Herausforderungen gestellt.

Weiterentwicklungen der Informations- und Kommunikationstechnik und neue Einsatzmöglichkeiten waren schon immer Herausforderungen für das Datenschutzrecht und Beschleuniger für seine Anpassungen an neue Realitäten. Die Lektüre der Tätigkeitsberichte der Aufsichtsbehörden, die über das „Zentralarchiv für Tätigkeitsberichte des Bundes- und der Landesdatenschutzbeauftragten und der Aufsichtsbehörden für den Datenschutz (ZAfTDa)“ erschlossen werden können,[6] zeigt das vielfältige Bild täglich neuer Herausforderungen für die Aufsichtsbehörden. Vor dem Hintergrund aktueller Überwachungsszenarien resümierte der Landesdatenschutzbeauftragte *Bos* aus Sachsen-Anhalt in seinem im Dezember 2013 vorgelegten Tätigkeitsbericht, dass „der Mensch zur Sache [wird], algorithmengesteuerte Verfahren und prädiktive Analysen bestimmen das Verhalten vor. Ein Innenraum freier Selbstbestimmung (vgl. BVerfGE 27, 1, 6-7) verkommt zur Hülse. Das Gemeinwohl der demokratischen Gesellschaft leidet angesichts der Überwachungssysteme mit.“[7]

Auch wenn technische Entwicklungen und ihr Einsatz in Wirtschaft und Verwaltung immer neuen Herausforderungen für die Gewährleistung des Betroffenenschutzes durch das Datenschutzrecht schaffen werden, sollte nicht verkannt werden, dass die Bevölkerung trotz des bisweilen sorglosen Umgangs mit den eigenen Daten insbesondere in sozialen Netzwerken und Unternehmen, die personenbezogene Daten von Arbeitnehmern und Kunden verarbeiten, sensibler geworden sind.

---

[4] *Weichert,* ZD 2013, S. 251; *Zieger*/*Smirra,* MMR 2013, S. 418; *Schaar*, RDV 2013, S. 223; *Ulmer,* RDV 2013, S. 227; *Bornemann,* RDV 2013, S. 232; *Roßnagel,* ZD 2013, S. 562; *Piltz*, Benötigen wir Big Data-Kommissionen?, in: Jürgen Taeger (Hrsg.), Big Data & Co – Neue Herausforderungen für das Informationsrecht, DSRI-Tagungsband 2014, 2014, S. 141; *Werkmeister*/*Brandt*, CR 2016, S. 233; *Boehme-Neßler*, DuD 2016, S. 419; *Marnau*, DuD 2016, S. 428; *Sarunski*, DuD 2016, S. 424; *Roßnagel*, DuD 2016, S. 561; *Ehlen*/*Brandt*, CR 2016, S. 570; *Dammann*, ZD 2016, S. 307.

[5] BITKOM Leitfaden „Big Data im Praxiseinsatz“, S. 7.

[6] www.zaftda.de; von *Lewinski,* RDV 2009, S. 267.

[7] XI. Tätigkeitsbericht des Landesbeauftragten für den Datenschutz Sachsen-Anhalt, LT-Drs. 6/2602, S. 3.

Die Diskussion über Compliance, also die Gewährleistung rechtskonformen Handelns im Unternehmen, hat ein Übriges dafür getan, dass dem Datenschutz ein höherer Stellenwert beigemessen wird. Als ein Hauptproblem erweisen sich solche Unternehmen, deren Unternehmenszweck die Sammlung von personenbezogenen Daten ist, um sie ‚veredelt', mit anderen Daten zu einem Profil zu verknüpfen und sie dann gewinnbringend zu veräußern oder für individualisierte Marketingstrategien zu nutzen. Häufig sind sie im Ausland, vornehmlich in den USA, angesiedelt und entziehen sich trotz ihres auf die deutschen Nutzer ausgerichteten Engagements unserer Rechtsordnung und dem Zugriff der deutschen Aufsichtsbehörden.[8]

Im öffentlichen Bereich stehen die grenzüberschreitenden Informationssysteme im Fokus, die im Europa der offenen Grenzen auf der Grundlage des Schengener Abkommens im Interesse der öffentlichen Sicherheit errichtet wurden und ausgebaut werden (Europäisches Informationssystem und Zollinformationssystem). Die Datenanalyse des transnationalen Zahlungsverkehrs über SWIFT und die Passagierdatenübermitteilung der Fluggesellschaften an Sicherheitsbehörden der USA als Maßnahme der Terrorbekämpfung, die Abhöraffären der Geheimdienste NSA und CIA und die Überwachung der elektronischen Kommunikation mit dem Programm PRISM unter mutmaßlicher Beteiligung von Microsoft, Google, Facebook und anderen großen Kommunikationsdiensteanbietern geben Hinweise auf die beängstigende Dimension, die das Thema Datenschutz im hoheitlichen Bereich angenommen hat.

1.1 Entwicklung des Datenschutzrechts in Deutschland

Vor diesem Hintergrund ist es evident, den Entwicklungsstand des Schutzes von Persönlichkeitsrechten im digitalen Zeitalter zu beleuchten. Erste explizite Überlegungen zur Regelung des Datenschutzes gehen in die 70er Jahre zurück, als an das Ausmaß heutiger Vernetzung und Datenflüsse noch gar nicht zu denken war. Immerhin gab es parallel zu der Entwicklung der Computertechnik, die den Aufbau großer Datenbanken mit jederzeitiger Zugriffsmöglichkeit von jedem Ort auch auf ältere Daten ermöglichte, die in einem Ordner im Archiv möglicherweise sonst die „Gnade des Vergessens" erlangten, auch eine Anfang der 60er Jahre beginnende Diskussion über die Gefährdung der Privatsphäre. Die Sorge bestand vornehmlich darin, dass verteilt bestehende Datenbestände in einer großen Datensammlung zusammengeführt würden und dadurch die Person mit den von ihr in verschiedenen Lebenszusammenhängen hinterlassenen Spuren mit einem kompletten Persönlichkeitsprofil abgebildet würde (Big Brother). Insbesondere in den USA gab es eine kritische Diskussion,[9] die 1974 zur Verabschiedung des Privacy Act führte. Die Diskussion knüpfte an die Rechtstradition eines *Right to be let alone* an (seit 1934), die besonders mit dem Werk von *Samuel D. Warren* und *Louis D. Brandeis*, The Right to Privacy,[10] verbunden war. Der Privacy

[8] Siehe dazu das Editorial von *Thilo Weichert*, Landesbeauftragter für den Datenschutz in Schleswig-Holstein: Wer ist für was im Internet verantwortlich, ZD 2014, S. 1.

[9] Siehe etwa *Alan F. Westin*, Privacy and Freedom, 1967.

[10] Harvard Law Review, IV (1890) 5.

Act untersagt den US-Bundesbehörden die zweckentfremdete Verwendung personenbezogener Daten und räumt Benachrichtigungs-, Auskunfts- und Berichtigungsansprüche und auch einen Schadensersatzanspruch ein.

Zu diesem Zeitpunkt gab es in Hessen seit 1970 bereits das erste Landesdatenschutzgesetz, das die Verarbeitung personenbezogener Daten durch landesunmittelbare Stellen regelt.[11] Im gleichen Jahr erteilte das Bundesministerium des Innern einen Forschungsauftrag, mit dem die Erforderlichkeit eines Datenschutzgesetzes festgestellt und ein Datenschutzkonzept entwickelt werden sollte.[12] Auf dieser Grundlage wurde sieben Jahre später das erste Bundesdatenschutzgesetz[13] verabschiedet, das am 1.1.1978 in Kraft trat.[14] Andere Länder folgten dem Beispiel der USA und Deutschlands und verabschiedeten eigene Datenschutzgesetze.[15]

1990 folgte die erste Neufassung des BDSG.[16] Die nächste Reform, mit der die EG-Datenschutzrichtlinie[17] verspätet umgesetzt wurde, kam 2001.[18] Eine Reihe von Datenschutzaffären auch bei großen deutschen Konzernen wie der Deutschen Bahn AG und der Deutschen Telekom AG waren Anlass für drei Reformgesetze zum Datenschutz im Jahr 2009, die überwiegend 2010 in Kraft traten. Die sog. BDSG-Novelle I[19] erfolgte durch das Gesetz zur Änderung des Bundesdatenschutzgesetzes vom 29.7.2009.[20] Sie trat zum 1.4.2010 in Kraft und befasst sich mit Scoring, Rating und dem Recht der Auskunfteien. Die Novelle brachte Neuerungen des Datenschutzrechts insbesondere in vier Bereichen; so werden Mitteilungs- und Erklärungspflichten bei automatisierten Einzelentscheidungen, Zulässigkeitsregeln für Verfahren sowie die Übermittlung von Daten an Auskunfteien und Auskunftspflichten in Bezug auf Scorewerte neu geregelt.

---

11 Datenschutzgesetz vom 7.10.1970, Hess. GVBl. I, S. 625.

12 *Steinmüller*/*Lutterbeck*/*Mallmann*/*Harbort*/*Kolb*/*Schneider*, Grundfragen des Datenschutzes, Gutachten im Auftrag des Bundesministeriums des Innern, Juli 1971, BT-Drs. 6/3826, S. 5; siehe dazu *Steinmüller,* RDV 2007, S. 158.

13 Siehe zur Gesetzgebungskompetenz für den Datenschutz im Bund und in den Ländern Taeger/Gabel-*Taeger*/*Schmidt*, BDSG, 2. Aufl., 2013, Einleitung Rn. 7 ff.

14 Gesetz zum Schutz vor Missbrauch personenbezogener Daten bei der Datenverarbeitung (Bundesdatenschutzgesetz – BDSG) vom 27.1.1977, BGBl. I, S. 201; siehe dazu *Buchner*, Informationelle Selbstbestimmung im Privatrecht, S. 26ff.

15 Empfehlenswert: *Steinmüller,* RDV 2007, S. 158. Siehe zur frühen Entwicklung in Deutschland *R. Kamlah,* Right of Privacy, 1969; *Kilian*/*Lenk*/*Steinmüller,* Datenschutz, 1973; *Podlech,* DVR 1972/73, S. 149; *Steinmüller,* Datenverkehrsrecht, Film und Recht 1977, S. 440. Die Entwicklung des Datenschutzrechts von 1600 bis 1977“ beleuchtet von *Lewinski,* in: Arndt et al., Freiheit – Sicherheit – Öffentlichkeit, 48. Assistententagung Öffentliches Recht 2009, S. 196.

16 BGBl. I, S. 2954.

17 Richtlinie zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (EG-Datenschutzrichtlinie), 95/46/EG, ABl. EG 1995, L 281, 31.

18 BGBl. I, S. 904.

19 BGBl. I, S. 2954.

20 BGBl. I, S. 2254.

Sodann wurde als Teil der Novelle II mit § 32 BDSG eine Vorschrift zum Beschäftigtendatenschutz eingefügt, die weitgehend zum 1.9.2009 in Kraft trat.[21] Die Vorschrift enthält in Abs. 1 Erlaubnistatbestände für die Erhebung, Verarbeitung und Nutzung von Daten solcher Personen, die in einem Beschäftigungsverhältnis stehen. Wer zu den Beschäftigten gehört, definiert § 3 Abs. 11 BDSG. Nach der Gesetzesbegründung sollen in § 32 BDSG die bisherigen Grundsätze für den Datenschutz im Beschäftigungsverhältnis lediglich zusammengefasst worden sein. Schon lange vor der Einführung des § 32 BDSG gab es Bemühungen, den Beschäftigtendatenschutz ausführlicher und konkreter zu regeln. Die langjährigen Beratungen zur Einführung eines speziellen Beschäftigtendatenschutzgesetzes endeten nach der ersten Lesung im Deutschen Bundestag mit dem Rückzug des Entwurfs im Januar 2013.

Die BDSG-Novelle II änderte auch die Anforderungen an die Zulässigkeit personalisierter Werbung, verschärfte die Anforderungen an die Auftragsdatenverarbeitung gemäß § 11 BDSG, führte Informationspflichten für die Unternehmen bei Datenschutzpannen ein, erweiterte Kompetenzen der Aufsichtsbehörden und stärkte die Rechtsstellung des betrieblichen Datenschutzbeauftragten durch Kündigungsschutz und einen Anspruch auf Fort- und Weiterbildung.

Die Novelle III von 2009[22] ergänzte § 29 BDSG um zwei Absätze zu den Auskunftspflichten von Auskunfteien über die gesammelten Daten zur Bonität von Kunden.

Neben die allgemeinen Datenschutzgesetze des Bundes und der Länder traten die sogenannten bereichsspezifischen Datenschutzgesetze. Die Gesetzgeber des Bundes und der Länder sahen sich durch das Urteil des Bundesverfassungsgerichts zur Volkszählung veranlasst, die Erhebung und Verarbeitung personenbezogener Daten insbesondere durch öffentliche Stellen gesetzlich zu regeln und damit hoheitliche Eingriffsbefugnis zu schaffen. Das Bundesverfassungsgericht hatte die Verfassungsbeschwerde gegen die Volkszählung 1983 zum Anlass genommen, sich grundlegend und die weitere Entwicklung prägend zum Grundrecht auf Informationelle Selbstbestimmung (Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG) zu äußern.[23] Das Urteil besagt im Kern, dass jede hoheitliche Erhebung und Verarbeitung personenbezogener Daten einen Grundrechtseingriff darstellt und deshalb nur auf der Grundlage einer gesetzlichen Eingriffserlaubnis außerhalb des Bundesdatenschutzgesetzes oder der Landesdatenschutzgesetze zulässig ist. In der Folge wurden zahlreiche bereichsspezifische Datenschutzgesetze verabschiedet, um verfassungsrechtlich gebotene Eingriffstatbestände zu schaffen.

Die bereichsspezifischen Datenschutzvorschriften schaffen für hoheitliche Stellen erst die Eingriffsbefugnis und gestalten die Verarbeitung der Daten näher aus.[24] Sie

---

21 BGBl. I, S. 2814. Siehe aus der umfangreichen Literatur zur neuen Vorschrift etwa *Heldmann,* DB 2010, S. 1235; *B. Schmidt,* RDV 2009, S. 193; *Thüsing,* NZA 2009, S. 865; *Robrecht,* ZD 2011, S. 23

22 Gesetz vom 29.7.2009, BGBl. I, S. 2355. Die Änderungen traten am 11.6.2010 in Kraft.

23 BVerfGE 65, 1. Siehe dazu neben vielen *Simitis*, NJW 1984, S. 398; *Vogelgesang,* Grundrecht auf informationelle Selbstbestimmung?, 1987.

24 Ausführlich dazu Taeger/Gabel-*Taeger*, BDSG, 2013, § 4 Rn. 16 ff. und 24-29.

verdrängen die allgemeinen Vorschriften nur soweit, wie sie Einzelfragen näher regeln. Im Übrigen bleiben die allgemeinen Datenschutzgesetze anwendbar (§ 1 Abs. 3 BDSG).[25] Teilweise schränken sie die Befugnisse der verantwortlichen Stellen ein oder beschränken Rechte der Betroffenen. Entgegen den allgemeinen Datenschutzvorschriften knüpfen bereichsspezifische Regelungen an die Erhebung und Verarbeitung beispielsweise an besondere Voraussetzungen, so etwa beim Telemediengesetz (TMG) oder dem Telekommunikationsgesetz (TKG). Anderes bereichsspezifisches Datenschutzrecht kann die Rechte der Betroffenen aufgrund einer von der Legislative vorgenommenen Interessenabwägung einschränken, wie beispielsweise durch § 15 Abs. 2 Bundesverfassungsschutzgesetz (BVerfschG).

Die großen christlichen Kirchen regeln den Datenschutz aufgrund der Freiheitsgarantie des Art. 140 GG i.V.m. Art. 137 Abs. 3 Satz 1 WRV und des daraus folgenden kirchlichen Selbstbestimmungsrechts selbst;[26] sie agieren allerdings nicht in einem datenschutzfreien Raum, sondern orientierten sich mit kirchlichen Datenschutzgesetzen weitgehend an den allgemeinen Datenschutzgesetzen. Ob öffentlich-rechtliche Religionsgemeinschaften nicht doch als öffentliche Stellen gem. § 2 BDSG anzusehen sind und damit unter den Anwendungsbereich des Bundesdatenschutzgesetzes fallen, ist umstritten.[27] Unstreitig fallen rein wirtschaftliche Betriebe der Religionsgemeinschaften als nicht-öffentliche Stellen unter das Bundesdatenschutzgesetz.

Derzeit befindet sich der Kabinettsentwurf für ein Gesetz zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 (Datenschutz-Anpassungs- und -Umsetzungsgesetz EU – DSAnpUG-EU) im Gesetzgebungsverfahren. Es soll die Öffnungsklauseln der EU-Datenschutz-Grundverordnung, die ab dem 25. Mai 2018 in Europa gilt, ausfüllen. Das BDSG wird in der jetzt geltenden Fassung dann nicht mehr anzuwenden sein. Bis dahin soll ein Anpassungsgesetz als Artikelgesetz, das mit Art. 1 ein Allgemeines Bundesdatenschutzgesetz (BDSG-neu) einführt, verabschiedet werden. Es wird die zwingend bis zum 25. Mai 2018 vorzunehmenden Regelungsaufträge berücksichtigen und die aufgrund sogenannter Öffnungsklauseln bestehenden Regelungsoptionen wahrnehmen. Das Anpassungsgesetz darf dabei kein gegenüber der Datenschutzgrundverordnung höheres Schutzniveau zu bestimmten, in der DSGVO enthaltenen Regelungen enthalten, soweit eine Öffnungsklausel dies nicht ausdrücklich vorsieht (Art. 6 Abs. 2 und 3 DSGVO). Im Anschluss daran werden auch die bereichspezifischen Vorschriften angepasst, sofern dies erforderlich ist und sie nicht auf andere EU-Vorschriften zurückgehen. Auch die Ländergesetze werden noch anzupassen sein.

---

[25] Dazu Taeger/Gabel-*Schmidt*, BDSG, 2013, § 1 Rn. 33 ff.

[26] *Weichert*, in: Däubler/Klebe/Wedde/Weichert, BDSG, 2016, § 2 Rn. 9. Siehe dazu etwa *Ziekow,* Datenschutz und evangelisches Kirchenrecht, 2002; *Germann,* ZevKR 48, S. 446; *Fachet,* RDV 1996, S. 177; *Claessen*, DuD 1995, S. 8; *Lorenz,* DVBl. 2001, S. 428; *Dammann,* NVwZ 1992, S. 1147.

[27] Vgl. Taeger/Gabel-*Buchner,* BDSG, 2013, § 2 Rn. 12; *Dammann,* in: Simitis, BDSG, 2014, § 2 Rn. 84ff.; *Gola*/*Schomerus,* BDSG, 2015, § 2 Rn. 14a; *Schreiber,* in: Plath, BDSG, 2013, § 2 Rn. 11.

1.2 Entwicklung des internationalen und europäischen Datenschutzrechts

Auch die Internationalen Organisationen und die Europäische Gemeinschaft bzw. jetzt die Europäische Union erkannten in der Entwicklung der Informations- und Kommunikationstechnik (IuK) schon früh Gefährdungen für die Persönlichkeitsrechte und reagierten mit Empfehlungen und völkerrechtlichen Verträgen, um den Schutz von Persönlichkeitsrechten in den Verfassungsrang zu erheben und einfachgesetzliche Schutzvorschriften zu initiieren.

1.2.1 Vereinte Nationen

Die Vereinten Nationen nahmen sich des Problems der Folgen der automatisierten Datenverarbeitung verstärkt 1985 an, als sie einen ersten Richtlinienentwurf zum Datenschutz durch die UN-Menschenrechtskommission erarbeiteten. 1990 beschloss die UN-Generalversammlung „Richtlinien zur Verarbeitung personenbezogener Daten in automatisierten Dateien“.[28] Allerdings enthält diese Richtlinie kein die Mitgliedstaaten und ihre Organisationen bindendes Völkerrecht, sondern Empfehlungen zum Datenschutz bei öffentlichen und nicht-öffentlichen Stellen. Dazu gehörte auch die Empfehlung, unabhängige Datenschutzinstanzen einzurichten.

Vor dem Hintergrund der sog. NSA-Affäre verabschiedete die UN-Vollversammlung am 18. Dezember 2013 eine von Brasilien und Deutschland eingebrachte Resolution mit dem Titel „Das Recht auf Privatsphäre im digitalen Zeitalter“,[29] mit der die Totalüberwachung der Menschheit über das Internet verurteilt wird. Eine Resolution bindet niemanden, richtet aber doch die Aufmerksamkeit auf ein wesentliches Thema.

1.2.2 OECD

Noch früher, nämlich schon 1980, wurden vom Rat der Organisation für Wirtschaftliche Zusammenarbeit und Entwicklung (OECD) die „Guidelines on the Protection of Privacy and Transborder Flows of Personal Data“ (offizielle Übersetzung: Richtlinien über Datenschutz und grenzüberschreitende Ströme personenbezogener Daten) als Empfehlung verabschiedet, um ihre Ziele pluralistische Demokratie, Achtung der Menschenrechte und freie Marktwirtschaft zu fördern. Dazu sollten in den Mitgliedstaaten nationale Gesetze die folgenden Grundsätze durch ordnungsrechtliche oder selbstregulierende Maßnahmen sicherstellen:

---

[28] United Nations, Guidelines on the Use of Computerized Personal Data Flow, Resolution 44/132, 14.12.1990, E/CN.4/Sub.2/1988/22. Siehe zur Geschichte des Datenschutzes bei Internationalen Organisationen *Ennulat,* Datenschutzrechtliche Verpflichtungen der Gemeinschaftsorgane und -einrichtungen, 2008, S. 64 ff.

[29] General Assembly GA/11475 vom 18.12.2013, http://www.un.org/News/Press/docs//2013/ga11475.doc.htm. Zuvor war die Resolution “The right to Privacy in the digital age” vom Menschenrechtsausschuss der UNO gebilligt worden, allerdings nach Intervention der USA in einer gegenüber der Entwurfsfassung abgeschwächten Form, A/C.3/68/L.45.

Grundsatz

- der begrenzten Datenerhebung,
- der Datenqualität,
- der Zweckbestimmung,
- der Nutzungsbegrenzung,
- der Sicherung,
- der Offenheit,
- des Mitspracherechts,
- der Rechenschaftspflicht.

In dem Vorwort der OECD-Richtlinien über Datenschutz und grenzüberschreitende Ströme personenbezogener Daten[30] heißt es:

> „Im Zuge der Einführung der Informationstechnologien in verschiedene Bereiche der Wirtschaft und Gesellschaft und mit der zunehmenden Bedeutung und Leistungsstärke der elektronischen Datenverarbeitung beschloss die Organisation für Wirtschaftliche Zusammenarbeit und Entwicklung (OECD) 1980, Richtlinien für eine internationale Politik über Datenschutz und grenzüberschreitende Ströme personenbezogener Daten herauszugeben.
>
> Die rasch alle Bereiche durchdringende Entwicklung der Informations- und Kommunikationstechnologien, gekennzeichnet durch Erscheinungen wie das Internet, trug in jüngster Zeit zur beschleunigten Entstehung einer globalen Informationsgesellschaft bei. Die OECD hat sich daraufhin mit der Frage befasst, wie diese Richtlinien im 21. Jahrhundert bestmöglich umgesetzt werden können, um die Achtung der Privatsphäre und den Schutz personenbezogener Daten online zu gewährleisten."

Am 12.6.2007 wurde dann die 27 Jahre alte Richtlinie durch den Beschluss des Rates der OECD revidiert, weil die Menge an Daten, die grenzüberschreitend ausgetauscht wird, und die Veränderungen der Art und Weise, wie dieser Austausch vor sich geht, die Risiken für den Datenschutz bei Einzelpersonen erhöht haben. Die Arbeitsgruppe für Informationssicherheit und Datenschutz (WPISP) des OECD-Komitees für Information, Computer und Kommunikationspolitik (ICCP) hat deshalb einen Rahmenbeschluss entwickelt, der in die neue OECD-Empfehlung zur grenzüberschreitenden Zusammenarbeit bei der Umsetzung von Gesetzen zum Datenschutz aufgenommen wurde, um die Effizienz der nationalen Datenschutzgesetze angesichts der gestiegenen Risiken zu erhöhen.

Aus den "OECD Recommendation on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy" vom Juni 2007:[31]

---

30 http://www.oecd.org/sti/ieconomy/15589558.pdf.

31 http://www.oecd.org/sti/ieconomy/38770483.pdf.

„Globalisierung, das Aufkommen von „Follow-the Sun"-Unternehmensmodellen, die Entwicklung des Internets und fallende Kommunikationskosten steigern die Menge an grenzüberschreitenden personenbezogenen Informationsströmen drastisch. Dieser Anstieg an grenzüberschreitenden Informationsströmen dient sowohl Organisationen als auch Einzelpersonen, indem dabei Kosten gesenkt werden, die Effizienz gesteigert und die Verbraucherfreundlichkeit verbessert wird. Gleichzeitig vertiefen diese personenbezogenen Informationsströme die Bedenken im Bereich des Datenschutzes, und stellen neue Herausforderungen in Bezug auf den Schutz von personenbezogener Information über Einzelpersonen dar."

Bei den OECD-Richtlinien und -Empfehlungen handelt es sich nicht um verbindliches Völkerrecht, so dass kein Umsetzungszwang besteht. Bedeutung kommt ihnen jedoch durch die Etablierung des Datenschutzrechts als Gegenstand internationaler Regulierung zu.

1.2.3 Europarat

Mit der Europäischen Menschenrechtskonvention (EMRK) von 1950,[32] die in Deutschland den Rang eines einfachen Gesetzes hat, strebt der Europarat einen effizienten Menschenrechtsschutz an. Zur Durchsetzung dient als Rechtsschutzinstanz der Europäische Gerichtshof für Menschenrechte. Mit Art. 8 Abs. 1 EMRK wird der Anspruch jedes Menschen auf Achtung des Privatlebens, des Familienlebens, der Wohnung und des Briefverkehrs gewährleistet. Zur Konkretisierung verabschiedete das Ministerkomitee das „Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten (Europäische Datenschutzkonvention), das 2001 um einen Zusatz mit der Forderung, unabhängige Überwachungsbehörden einzurichten, ergänzt wurde.[33] Diese erste völkerrechtlich verbindliche Normierung des Datenschutzrechts wurde 1985 mit der Verabschiedung des Ratifizierungsgesetzes in Deutschland geltendes Recht. Sie regelt den Datenschutz bei der automatischen Verarbeitung personenbezogener Daten natürlicher Personen und enthält Prinzipien des Datenschutzes, wie den Grundsatz der rechtmäßigen Datenerhebung nach Treu und Glauben (Art. 5a), den Zweckbindungsgrundsatz der Datenerhebung und Verarbeitung (Art. 5 b und 5 c), den Grundsatz der richtigen Datenerhebung (Art. 5 d), den Grundsatz der Anonymisierung (Art. 5 e) sowie den Grundsatz der Datensicherheit (Art. 7). In Art. 12 werden zudem Regelungen zum grenzüberschreitenden Datenverkehr getroffen. Das Übereinkommen differenziert, anders als das BDSG, aber nicht zwischen der Datenverarbeitung durch öffentliche und private Stellen, sondern unterwirft sie den gleichen Regelungen.

---

[32] Vom 4.11.1950, 213 UNTS 221, zuletzt geändert durch Protokoll Nr. 14 vom 13.5.2004. http://www.echr.coe.int/Documents/Convention_deu.pdf.

[33] European Treaty Series No. 8; http://conventions.coe.int/treaty/ger/treaties/html/108.htm.

Vom Europarat stammen darüber hinaus bereichsspezifische datenschutzrechtliche Empfehlungen, wie etwa zum Arbeitnehmerdatenschutz.[34]

In der Cybercrime-Convention, die neben der Vereinheitlichung des materiellen Computerstrafrechts auch eine Angleichung der strafprozessualen Möglichkeiten des Zugriffs auf Telekommunikations- und Computerdaten anstrebt, sind daraus resultierende Datenschutzbelange nicht thematisiert worden.[35]

1.2.4 Europäische Union

1.2.4.1 Sekundäres Gemeinschaftsrecht

Seit 1974 hatte sich das Europäische Parlament mit zahlreichen Entschließungen bemüht, die zögerliche EG-Kommission zu Beschlüssen über Maßnahmen zum Schutz der Rechte des Einzelnen angesichts der fortschreitenden technischen Entwicklung auf dem Gebiet der elektronischen Datenverarbeitung zu veranlassen.[36] Erst 1995 wurde eine Datenschutz-Richtlinie verabschiedet.[37] Mit der Transformation in nationales Recht soll ein einheitlicher Rechtsrahmen für die Verarbeitung personenbezogener Daten im europäischen Binnenmarkt mit einem einheitlichen Schutzniveau erreicht werden, der die „Grundrechte und Grundfreiheiten und insbesondere den Schutz der Privatsphäre natürlicher Personen gewährleisten“ (Art. 1 Abs. 1 DSRl) und zum wirtschaftlichen und sozialen Fortschritt, zur Entwicklung des Handels sowie zum Wohlergehen der Menschen beitragen soll (Erwägungsgrund 2 der DSRl). Intendiert ist mit der Herstellung des einheitlichen Schutzniveaus innerhalb der Europäischen Union der freie personenbezogene Datenverkehr zwischen den EU-Mitgliedstaaten im Sinne des EU-Binnenmarktes. Im nationalen Recht spiegelt sich dies beispielsweise in § 1 Abs. 5 BDSG wieder, wonach das BDSG dann keine Anwendung findet, sofern eine in einem anderen Mitgliedstaat der Europäischen Union verantwortliche Stelle von dort – nicht über eine Niederlassung im Inland – personenbezogene Daten im Inland erhebt oder verarbeitet, weil davon ausgegangen werden kann, dass im EU-Ausland

---

34 Empfehlung Nr. R (89)2 vom 18.1. 1989, EU DS, EuRAT-Conv.

35 Convention on Cybercrime v. 23.11.2001, European Treaty Series No. 185, in Kraft getreten 1.7.2014. Bis November 2013 ratifizierten 41 Staaten die Convention, weitere 11 unterzeichneten sie. Die Stagnation bei den Ratifizierungen beklagt *Gercke,* ZUM 2012, S. 625. Siehe zur Cybercrime Convention *Gercke*, CR 2004, S. 782; *Gercke*/*Brunst,* Praxishandbuch Internetstrafrecht, 2009.

36 Dazu auch *Kort,* DB 2012, S. 1020. Zur Entwicklung des Datenschutzrechts in der EG und der EU: *Taeger,* EWS 1995, S. 69; *Taeger,* Grenzüberschreitender Datenverkehr und Datenschutz in Europa, 1995; *Brühann,* RDV 1996, S. 12; *Zilkens,* RDV 2007, S. 196; *Kuner,* European Data Protection Law: Corporate Compliance and Regulation, 2. Aufl., 2007; *Boehm,* JA 2009, S. 435; *von Lewinski,* Geschichte des Datenschutzrechts von 1600 bis 1977, in: Arndt et al., Freiheit – Sicherheit – Öffentlichkeit, 2009, S. 196; *Bäcker*/*Hornung*, ZD 2012, S. 195; *Gürtler,* RDV 2012, S. 126; *Ronellenfitsch,* DuD 2012, S. 561; *Reding,* JD 2012, S. 195.

37 Richtlinie 95/46/EG zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (EG-Datenschutzrichtlinie/DSRl) 95/46/EG, ABl. EG Nr. L 281/31.

das gleiche Datenschutzniveau besteht. Es wird also vom Sitzprinzip und nicht vom Territorialprinzip ausgegangen.[38]

Zu den wesentliche Regelungen gehört auch das Zweckbindungsprinzip (Art. 6 Abs. 1 Buchst. b DSRl). Darüber hinaus enthält sie Regelungen für die Datenübermittlung in Drittstaaten außerhalb der Europäischen Union (EU) und des Europäischen Wirtschaftsraums (EWR), die nur zulässig ist, wenn im Empfängerstaat ein ‚angemessenes Schutzniveau' gewährleistet ist. Am 5.2.2010 wurden von der Kommission neue Standardvertragsklauseln beschlossen, durch die eine datenschutzkonforme Übermittlung von personenbezogenen Daten in Drittländer außerhalb des Europäischen Wirtschaftsraums (EWR), die kein angemessenes Datenschutzniveau vorweisen können, möglich ist.[39]

Die Datenschutzrichtlinie enthielt auch neue Elemente, die dem deutschen Datenschutzrecht noch nicht bekannt waren und deshalb durch eine Änderung des BDSG – nach Ablauf der Änderungsfrist am 18.5.2001 – aufgenommen wurden, darunter das Verbot automatisierter Einzelentscheidungen (§ 6a BDSG), die Regelung über besonders sensible Daten (§§ 3 Abs. 9, 28 Abs. 6 BDSG) und Vorstellungen von einer Selbstregulierung (§ 38a BDSG).

Nach Art. 29 der Allgemeinen Datenschutzrichtlinie ist eine unabhängige Gruppe einzusetzen, die sich aus einem Vertreter der Kommission und aus den Vertretern der nationalen Aufsichtsbehörden zusammensetzt (Art. 29-Gruppe). Sie hat die Aufgabe, die Kommission zu beraten und kann auch (Art. 30 Abs. 3 DSRl) von sich aus Empfehlungen aussprechen, was sie intensiv nutzt.[40]

Neben dieser allgemeinen Datenschutzrichtlinie folgten bereichsspezifische Harmonisierungsrichtlinien: die EG-Telekommunikationsdatenschutz-Richtlinie von 1997,[41] die durch die EG-Richtlinie über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation revidiert wurde.[42]

Das Europäische Parlament und der Rat der Europäischen Union beschlossen am 25.11.2009 (Cookie-Richtlinie)[43] Änderungen der Datenschutzrichtlinie für die

---

38 Siehe auch Art. 4 DSRl. Das Territorialitätsprinzip findet allerdings Anwendung, sofern aus dem EU-/EWR-Ausland eine strafbare Datenschutzverletzung in Deutschland begangen wird (§ 44 BDSG). Siehe zur internationalen Anwendbarkeit des deutschen Datenschutzrechts ausführlich *Voigt*, ZD 2014, S. 15.

39 ABl. Nr. L 39 v. 12.2.2010, S. 5; http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2010:039:0005:0018:DE:PDF.

40 http://ec.europa.eu/justice/data-protection/article-29/index_de.htm.

41 Richtlinie 97/66/EG des Europäischen Parlaments und des Rates vom 15.12.1997 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre im Bereich der Telekommunikation, ABl. EG Nr. L 24 v. 30.1.1998, S. 1.

42 Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12.7.2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation), ABl. EG Nr. L 201 v. 31.7.2002, S. 37.

43 Richtlinie 2009/136/EG; ABl. EG Nr. L 337 v. 18.12.2009, S. 11. Siehe dazu *Ohlenburg*, MMR 2003, S. 83, *Eckhardt*, MMR 2003, S. 557

elektronische Kommunikation (E-Privacy-Richtlinie)[44] oder). Das nationale Recht, berührt sind hier das Telemediengesetz (TMG) und das Telekommunikationsgesetz (TKG), hätte bis zum 25.5.2011 angepasst werden müssen. Wegen nicht rechtzeitiger Umsetzung leitete die EU-Kommission ein Vertragsverletzungsverfahren ein. Eingeführt werden sollen eine Mitteilungspflicht bei Datenschutzverletzungen und eine opt-in-Einwilligung in das Setzen von Cookies.[45]

Die Auseinandersetzung über die Rechtsetzungskompetenz der EU zur Verabschiedung der EG-Richtlinie über die Vorratsspeicherung von Daten[46] hielt auch nach einer Entscheidung des EuGH auf eine abgewiesene Nichtigkeitsklage an.[47] Der EuGH hatte die Klage von EU-Mitgliedern, die die Richtlinie aus formellen Gründen für nichtig hielten, mit einer nicht überzeugenden Begründung deshalb abgewiesen,[48] weil die EG-Richtlinie zur Vorratsdatenspeicherung im Wesentlichen die Tätigkeiten der Telekommunikationsdiensteanbieter im betroffenen Sektor des Binnenmarkts regeln würde, was in überwiegendem Maß das Funktionieren des Binnenmarkts betreffe. Der Zugang zu den Daten durch die zuständigen nationalen Strafverfolgungsbehörden und die Frage der Verwendung und des Austauschs dieser Daten zwischen diesen Behörden werde durch die Richtlinie nicht geregelt.

Das deutsche Transformationsgesetz führte zu einer großen Zahl von Verfassungsbeschwerden. Das Bundesverfassungsgericht entschied am 2.3.2010, dass die §§ 113a und 113b TKG verfassungswidrig und nichtig sind.[49] Daraufhin kündigte die EU-Kommission an, auch ihre RL zur Vorratsdatenspeicherung überprüfen zu wollen. Allerdings hat die EU-Kommission inzwischen ein Vertragsverletzungsverfahren wegen der Nicht-Umsetzung der Richtlinie auch gegen die Bundesrepublik Deutschland eingeleitet, wo aufgrund politischer Differenzen innerhalb der Regierung eine neue Regelung bislang nicht beschlossen wurde. Die Erfolgsaussichten des Verfahrens wurden als gering eingestuft.[50] Das galt umso mehr, als am 12.12.2013 der Generalanwalt beim EuGH in seinem Gutachten die EU-Richtlinie zur Vorratsdatenspeicherung für grundrechtswidrig erklärte

---

44 Richtlinie 2002/58/EG (Datenschutzrichtlinie für elektronische Kommunikation; ePrivacy-RL) v. 31.7.2002 (ABl. EG Nr. L 201 S. 37).

45 Siehe dazu *Schleipfer,* RDV 2011, S. 170.

46 Richtlinie 2006/24/EG des Europäischen Parlaments und des Rates vom 15.3.2006 über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste erzeugt oder verarbeitet werden, und zur Änderung der Richtlinie 2002/58/EG, ABl. EU Nr. L 105 v. 13.4.2006, S. 54.

47 Siehe zur Diskussion über die Verfassungsmäßigkeit der Vorratsdatenspeicherung und die Regelungskompetenz der EU u.a. *Albrecht,* VR 2013, S. 84; *Alvaro,* Recht und Politik 2012, S. 207; *Szuba,* Vorratsdatenspeicherung, 2011; *Wybitu*l, BB 2010, S. 889; *Orantek*, 2010, S. 193; *Petri,* EuZW 2009, S. 214; *Petri,* DuD 2012; S. 607; *Gundel,* Europarecht 2009, S. 536; *Kind,* MMR 2009, S. 661; *Simitis,* NJW 2009, S. 1782; *Terhechte,* EuZW 2009, S. 199; *Klesczewski,* HRRS 2009, S. 250.

48 EuGH, Urt. v. 10.2.2009 – C-301/06, ZUM 2009, 398.

49 1 BvR 256/08 - BVerfGE 125, 260 = K&R 2010, 248; vgl. auch Taeger/Gabel-*Munz*, BDSG, 1. Aufl., 2010, §§ 113a, 113 b TKG Rn. 4 ff.;

50 Siehe nur *Petri,* DuD 2012, S. 607.

und Änderungen empfahl. Der Bundesjustizminister der Großen Koalition erklärte daraufhin, die im Dezember 2013 in der Koalitionsvereinbarung vereinbarten Pläne zur Regelung einer Vorratsdatenspeicherung in der beabsichtigten Form aufzugeben.[51] Der EuGH erklärte die EU-Richtlinie zur Vorratsdatenspeicherung als mit der Charta der Grundrechte der Europäischen Union nicht vereinbar.[52] Der BGH erlaubte dementsprechend den Internetprovidern die Speicherung der IP-Adressen von Nutzern für sieben Tage allein für interne Zwecke bei Störungen der technischen Anlagen.[53] In einem Vorabentscheidungsverfahren bekräftigte der EuGH, dass eine nationale Regelung, die eine Vorratsdatenspeicherung zum Gegenstand hat, gegen die Grundrechte-Charta verstößt, wenn sie nicht im Rahmen der Bekämpfung von Straftaten diesen Zugang ausschließlich auf die Zwecke einer Bekämpfung schwerer Straftaten beschränkt, nicht den Zugang einer vorherigen Kontrolle durch ein Gericht oder eine unabhängige Verwaltungsbehörde unterwirft und nicht vorsieht, dass die betreffenden Daten im Gebiet der Union auf Vorrat gespeichert werden.[54]

Es wurde in Deutschland schließlich mit § 113b TKG doch wieder eine Vorratsdatenspeicherung durch Gesetz eingeführt, die ab 1.7.2017 zu erfüllen ist.[55] Hiergegen wurde wieder Verfassungsbeschwerde eingelegt.[56] Eine Vorratsdatenspeicherung mit Zugriff des Verfassungsschutzes findet sich auch im Bayerischen Verfassungsschutzgesetz.[57]

Auf der Grundlage der EG-Richtlinie 2004/82/EG137 werden Fluggastdaten („Advance Passenger Information" – API-Daten) zur Verbesserung von Grenzkontrollen und zur Bekämpfung der illegalen Einwanderung verarbeitet und auf Anfrage an Behörden übermittelt und 24 Stunden nach der Ankunft des Passagiers gelöscht; bei den empfangenden Stellen kann die Löschung bei Vorliegen von Ausnahmetatbeständen auch später erfolgen. Die Richtlinie wurde in Deutschland mit § 31a BPolG umgesetzt. Mit den USA wurde über ein weitergehendes Fluggastdatenabkommen verhandelt („Passenger Name Records" – PNR-Abkommen), das am 1.7.2012 in Kraft trat.[58] Zu der Mitteilung der Kommission über das sektorübergreifende Konzept für die Übermittlung von Fluggastdatensätzen (PNR) an Drittländer hat der Europäische Datenschutzbeauftragte kritisch Stellung genommen

---

51 FAZ v. 13.12.2013.

52 EuGH, Urt. v. 8.4.2014 – C-293/12, K&R 2014, 405 m. Anm. *Westphal* =ZD 2014, 296 m. Anm. *Petri* = NJW 2014, 2169.

53 Urt. v. 3.7.2014 – III ZR 391/13 –, K&R 2014, 593 = ZD 2014, 461 m. Anm. Eckhardt; vgl. dazu

54 EuGH, Urt. v. 21.12.2016 – C-203/15 und C-698/15, K&R 2017, 105

55 Gesetz 10.12.2015 zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten (VerkDSpG), BGBl. I S. 2218. Siehe dazu *Forgó*/*Heermann*, K&R 2015, S. 753;

56 http://www.vorratsdatenspeicherung.de/content/view/772/1/lang,de/.

57 Art. 15 Abs. 3 Bayer. VerfSchutzG von 2016. Dazu *Dieterle*, ZD 2016, 517.

58 Siehe zur Entwicklung des Abkommens *Westpha*l, EuZW 2006, S. 406; *McGinley*, DuD 2010, S. 250; *Szczekall*, DVBl. 2006, S. 896.

und wegen des beabsichtigten zur Risikobewertung vorgenommenen Massentransfers von Daten unschuldiger Personen ernsthafte Zweifel an der Verhältnismäßigkeit angemeldet.[59]

Ähnlich umstritten wie das Fluggastdatenabkommen ist das sog. SWIFT (Society for Worldwide Interbank Financial Telecommunication)-Abkommen zwischen der EU und den USA zur Übermittlung von Bankdaten zum Zweck der Terrorismusbekämpfung. Der Rat der Europäischen Justiz- und Innenminister billigte das Abkommen am 30.11.2009, so dass es am 1.2.2010 in Kraft treten konnte. Kritisiert wird, dass vertrauliche Zusatzabkommen nicht veröffentlicht werden, dass der Begriff „Terrorismus" sehr weit definiert wird, im Vertrag die Pflicht zur Übermittlung von Daten über Banktransfers innerhalb der Union und die Übermittlung von Daten durch die USA an Drittstaaten nicht ausdrücklich ausgenommen werden, die Betroffenen über die Übermittlung nicht informiert werden und ein Rechtsschutz nicht vorgesehen ist.[60] Das Europäische Parlament teilte diese Kritik und verweigerte dem Abkommen aufgrund von Bedenken im Hinblick auf europäisches Datenschutzrecht sowie den Grundsatz der Verhältnismäßigkeit und Gegenseitigkeit die Zustimmung und erklärte den Text für ungültig. Die Kommission verhandelte daraufhin eine geänderte Fassung, die das Europäische Parlament am 8.7.2010 billigte.[61]

Nach Artikel 15 des Abkommens stehen allen Unionsbürgern ein Auskunftsrecht und nach Artikel 16 Rechte zur Berichtigung, Löschung oder Sperrung unrichtiger Daten zu. Im März 2011 hatte die Gemeinsame Kontrollinstanz von Europol massive Defizite bei der Umsetzung des SWIFT-Abkommens offengelegt. Europol ist nach dem Abkommen verpflichtet, alle US-Ersuchen auf die Beachtung dieser Beschränkungen und damit auf die Erforderlichkeit der Datenübermittlung zu überprüfen.

Auch die europäischen Datenschutzbeauftragten (Art. 29-Gruppe) haben sich im Juni 2011 gegenüber der US-Regierung in einem gemeinsamen Schreiben für einen besseren Datenschutz nach dem Terrorist Finance Tracking Program (TFTP) eingesetzt, bei dem US-Behörden Zugriff auf weltweite Finanzdaten des Zahlungsnetzwerkes SWIFT erhalten. Sie sandten einen Zehn-Punkte-Katalog an das zuständige US-Finanzministerium, in denen Fragen zu Verfahren und Umfang der Rechte der Betroffenen gestellt werden, weil bisher eine Durchsetzung der Rechte der Betroffenen gegenüber den US-Behörden sehr erschwert wird.

---

59 Stellungnahme des Europäischen Datenschutzbeauftragten zu der Mitteilung der Kommission über das sektorübergreifende Konzept für die Übermittlung von Fluggastdatensätzen (PNR) an Drittländer, ABl. C 357 v. 30.12.2010, S. 7.

60 Kritisch etwa *Starosta*, Datenaustausch zwischen der EU und den USA am Beispiel des TFTP II-Abkommens (SWIFT-Abkommen), 2012.

61 Siehe zum neuen Abkommen *Schulte*, RIW 2012, S. 129; *Stefan*, jurisPR-BKR 1/2011 Anm 1; *Höhne*, AnwZert ITR 10/2010 Anm 3.

Nach Bekanntwerden der Späh-Aktionen des US-Geheimdienstes NSA[62] verlangte das Europäische Parlament allerdings am 23.10.2013 das Aussetzen des Abkommens bis zur Klärung der Frage, ob sich die NSA unter Verletzung der Vereinbarung in unzulässiger Weise einen Zugang zu SWIFT-Daten verschafften.

Einen weiteren Impuls für die Fortentwicklung des nationalen Datenschutzrechts im Hinblick auf die Organisation der Datenschutzaufsicht setzte am 9.3.2010 der EuGH mit seiner Entscheidung, dass Deutschland gegen Art. 28 Abs. 1 der Richtlinie 95/46/EG verstößt, weil die deutschen Datenschutzaufsichtsbehörden im nicht-öffentlichen Bereich nicht unabhängig organisiert seien.[63] Der EuGH befürchtet, durch die Unterstellung unter die Aufsicht eines Ministeriums könnten diese die ihnen zugewiesenen Aufgaben nicht in völliger Unabhängigkeit wahrnehmen. Die von diesem Urteil betroffenen, nach Landesrecht zuständigen Aufsichtsbehörden sind inzwischen bereits anders organisiert worden.

1.2.4.2 Primäres Gemeinschaftsrecht

Am 7.12.2000 wurde die Charta der Grundrechte bei der Eröffnung der Regierungskonferenz in Nizza feierlich proklamiert. Sie sollte als Teil II in den Europäischen Verfassungsvertrag (Vertrag über eine Verfassung für Europa – VVE) Eingang finden, der den EG- und den EU-Vertrag ablösen und der EU eine einheitliche Struktur und Rechtspersönlichkeit geben sollte. Der Verfassungsvertrag erlangte aber keine Rechtskraft, weil er von Frankreich und den Niederlanden wegen gescheiterter Volksabstimmungen nicht ratifiziert werden konnte. Stattdessen wurde am 13. Dezember 2007 der Vertrag von Lissabon unterzeichnet,[64] nach dem die bestehenden Vertragswerke nicht mehr ersetzt, sondern geändert wurden. Mit dem Vertrag von Lissabon wurde einerseits der EU-Vertrag (EUV)[65] reformiert und der folgende Art. 39 eingefügt:

> **Art. 39 EU-Vertrag:**
> Gemäß Artikel 16b des Vertrags über die Arbeitsweise der Europäischen Union und abweichend von Absatz 2 des genannten Artikels erlässt der Rat einen Beschluss zur Festlegung von Vorschriften über den Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Mitgliedstaaten im Rahmen der Ausübung von Tätigkeiten, die in den Anwendungsbereich dieses Kapitels fallen, und über den freien Datenverkehr. Die Einhaltung dieser Vorschriften wird von unabhängigen Behörden überwacht.

---

62 Siehe dazu *Harris*, ZD 2013, S. 369; *Lejeune*, CR 2013, 755; *Gercke,* CR 2013, 749.

63 ABl EU 2010, Nr. C 113, S. 3 = EuGRZ 2010, 58-62, mit zustimmender Anm. von *Roßnagel,* EuZW 2010, S. 296. Sehr kritisch wird das Urteil besprochen von *Bull,* EuZW 2010, S. 488. Die Missachtung der Souveränität der Mitgliedstaaten beklagt *Frenzel,* DÖV 2010, S. 925. Siehe auch *Ziebarth*, CR 2013, S. 60; *Taeger*, K&R 2010, S. 330. Allgemein zur Rechtsprechung des EuGH zum Datenschutz *Streinz*, DuD 2011, S. 602.

64 Vertrag von Lissabon zur Änderung des Vertrags über die Europäische Union und des Vertrags zur Gründung der Europäischen Gemeinschaft (2007/C 306/01), ABl. EU Nr. C 306 v. 17.12.2007, S. 1.

65 ABl. EU Nr. C 115 v. 9.5.2008, S. 13

Im Vertrag über die Arbeitsweise der Europäischen Union (AEUV)[66] wurde der folgende, den Art. 286 ersetzende Art. 16 eingefügt:

Art. 16 AEUV:

(1) Jede Person hat das Recht auf Schutz der sie betreffenden personenbezogenen Daten.

(2) Das Europäische Parlament und der Rat erlassen gemäß dem ordentlichen Gesetzgebungsverfahren Vorschriften über den Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe, Einrichtungen und sonstigen Stellen der Union sowie durch die Mitgliedstaaten im Rahmen der Ausübung von Tätigkeiten, die in den Anwendungsbereich des Unionsrechts fallen, und über den freien Datenverkehr. Die Einhaltung dieser Vorschriften wird von unabhängigen Behörden überwacht.

Die auf der Grundlage dieses Artikels erlassenen Vorschriften lassen die spezifischen Bestimmungen des Artikels 25a des Vertrags über die Europäische Union unberührt.

Mit dem Inkrafttreten des Vertrages von Lissabon am 1.12.2009 erlangte auch die Charta der Grundrechte der EU[67] Rechtskraft. Dazu bestimmt der neue Art. 6 EU-Vertrag:[68]

Artikel 6 EU-Vertrag

(1) Die Union erkennt die Rechte, Freiheiten und Grundsätze an, die in der Charta der Grundrechte der Europäischen Union vom 7. Dezember 2000 in der am 12. Dezember 2007 in Straßburg angepassten Fassung niedergelegt sind; die Charta der Grundrechte und die Verträge sind rechtlich gleichrangig. Durch die Bestimmungen der Charta werden die in den Verträgen festgelegten Zuständigkeiten der Union in keiner Weise erweitert. Die in der Charta niedergelegten Rechte, Freiheiten und Grundsätze werden gemäß den allgemeinen Bestimmungen des Titels VII der Charta, der ihre Auslegung und Anwendung regelt, und unter gebührender Berücksichtigung der in der Charta angeführten Erläuterungen, in denen die Quellen dieser Bestimmungen angegeben sind, ausgelegt.

(2) Die Union tritt der Europäischen Konvention zum Schutz der Menschenrechte und Grundfreiheiten bei. Dieser Beitritt ändert nicht die in den Verträgen festgelegten Zuständigkeiten der Union.

(3) Die Grundrechte, wie sie in der Europäischen Konvention zum Schutz der Menschenrechte und Grundfreiheiten gewährleistet sind und wie sie sich aus den gemeinsamen Verfassungsüberlieferungen der Mitgliedstaaten ergeben, sind als allgemeine Grundsätze Teil des Unionsrechts.

---

66 Konsolidierte Fassungen des Vertrags über die Europäische Union und des Vertrags über die Arbeitsweise der Europäischen Union 2008/C 115/01), ABl. EU Nr. C 115 v. 9.5.2008, S. 1.

67 Charta der Grundrechte der Europäischen Union, ABl. EU Nr. C 303 v. 14.12.2007, S. 1.

68 Vertrag über die Europäische Union (konsolidierte Fassung), ABl. EU Nr. C 326/13 v. 26.10.2012.

Damit haben nun auch die Datenschutz-Grundrechte aus der EU-Grundrechte-Charta Rechtsverbindlichkeit erhalten. Von Bedeutung für den Datenschutz sind die Art. 7 und 8:

> **Artikel 7**
>
> Achtung des Privat- und Familienlebens
>
> Jede Person hat das Recht auf Achtung ihres Privat- und Familienlebens, ihrer Wohnung sowie ihrer Kommunikation.
>
> **Artikel 8**
>
> Schutz personenbezogener Daten
>
> (1) Jede Person hat das Recht auf Schutz der sie betreffenden personenbezogenen Daten.
>
> (2) Diese Daten dürfen nur nach Treu und Glauben für festgelegte Zwecke und mit Einwilligung der betroffenen Person oder auf einer sonstigen gesetzlich geregelten legitimen Grundlage verarbeitet werden. Jede Person hat das Recht, Auskunft über die sie betreffenden erhobenen Daten zu erhalten und die Berichtigung der Daten zu erwirken.
>
> (3) Die Einhaltung dieser Vorschriften wird von einer unabhängigen Stelle überwacht.

Mit dem Vertrag von Lissabon wurde das 3-Säulen-Modell der Europäischen Union, die Europäischen Gemeinschaften (EG), die Gemeinsame Außen- und Sicherheitspolitik (GASP) und die polizeiliche und justizielle Zusammenarbeit in Strafsachen (PJZS), aufgegeben. Zum primären Unionsrecht gehören damit der EU-Vertrag und der Vertrag über die Arbeitsweise der Europäischen Union sowie die Grundrechte-Charta. Mit Art. 16 Abs. 2 AEUV ist nun die Zuständigkeit für den Erlass von Datenschutzvorschriften als Teil des sekundären Unionsrechts umfassend geregelt. Parlament und Rat erlassen die Vorschriften im ordentlichen Gesetzgebungsverfahren, was zu einer Zustimmungspflicht des Parlaments für sämtliche datenschutzrelevante Rechtsakte führt und dessen Kompetenzen erheblich vergrößert.

Der Vertrag von Lissabon erweitert die Kompetenzen der EU insofern auch inhaltlich, als diese nun die Verarbeitung personenbezogener Daten für die Mitgliedstaaten regeln kann. Neben der Kompetenzerweiterung wurde – wie gezeigt – mit dem Vertrag von Lissabon auch die Europäische Grundrechte-Charta rechtsverbindlich. In ihr gewährleistet Art. 8 das Grundrecht auf den Schutz personenbezogener Daten. Der Art. 16 AEUV[69] wiederholt dieses Europäische Grundrecht wörtlich. Damit ist das Sekundärrecht der Europäischen Union nicht mehr, wie noch die Datenschutz-Richtlinie, auf die Binnenmarktkompetenz angewiesen.[70]

---

[69] Vertrag über die Arbeitsweise der Europäischen Union (konsolidierte Fassung), ABl. EU Nr. C 326/47 v. 26.10.2012.

[70] Vgl. dazu *Grimm,* JZ 2013, S. 585 (589). Zur Entwicklung des europäischen Datenschutzes auch *Ronellenfitsch*, DVBl. 2013, S. 1521 (1522).

Die hohe Relevanz des Datenschutz-Grundrechts aus Art. 8 der EU-Grundrechte-Charta spiegelt sich in der Entscheidung des EuGH[71] über die Veröffentlichung der Namen von Subventionsempfängern wieder. Erstmals spielen das Grundrecht auf Achtung des Privat- und Familienlebens (Art. 7) und das Grundrecht auf Datenschutz (Art. 8) eine zentrale Rolle bei der Auslegung von Richtlinien durch das Gericht. Bei der Prüfung von Verhältnismäßigkeit und Erforderlichkeit kommt das Gericht bei der Abwägung des Transparenzgrundsatzes, der aus Art. 1 II und X EU sowie Art. 15 AEUV folgt, mit dem Datenschutzgrundrecht zu dem Ergebnis, dass die Veröffentlichung von Daten über die Empfänger von Agrarsubventionen unzulässig ist. Das Bundesverfassungsgericht hat in seinem Urteil zur Antiterrordatei[72] allerdings auf das Grundrecht aus Art. 2 Abs. 1 GG und nicht auf Art. 8 Grundrechte-Charta abgestellt und damit aufgezeigt, dass noch nicht entscheiden ist, in welchem Verhältnis Grundrechte-Charta und Grundgesetz zueinander stehen.[73]

1.2.4.3 Perspektiven durch eine EU-Datenschutzgrundverordnung

Das Europäische Parlament verabschiedete am 14.4.2016 die „Verordnung des Rates und des Europäischen Parlaments zum Schutz natürlicher Personen“ (DS-GVO). Sie trat bereits am 25.5.2016 in Kraft und gilt nach Art. 99 DS-GVO ab dem 25. Mai 2018.

Am 25.1.2012 hatte die EU-Kommission einen Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Grundverordnung)[74] und für eine Richtlinie für die behördliche Datenverarbeitung zu Zwecken der Aufklärung und Verhinderung von Straftaten[75] vorgelegt. Eine Datenschutz-Grundverordnung (EU-DSGVO-E) sollte an die Stelle der allgemeinen Datenschutz-Richtlinie 95/46/EG treten und das europäische Datenschutzrecht grundlegend reformieren.[76] Sie würde gem. Art. 288 Abs. 2 AEUV in den Mitgliedstaaten unmittelbar gelten. Nachdem auch das Europäische Parlament einen geänderten Entwurf vorgelegt hatte, fand der sog. Trilog statt, der mit einer Einigung der beteiligten Institutionen am 15.12.2015 endete. Eine offizielle deutsche Übersetzung wurde am 28. Januar 2016 vorgelegt.[77]

---

71 EuGH, Urteil vom 9.11.2010, C 92/09, ABl EU 2011, Nr C 13, 6 = MMR 2011, 122 (Schecke GbR). Siehe dazu *Kilian*, NJW 2011, S. 1325.

72 BVerfG, Urt. v. 24.4.2013, NJW 2013, 1499 = CR 2013, 369 = ZD 2013, 328 m.Anm. *Petri,* S. 348 = JZ 2013, 621 m. Anm. *Gärditz*, S. 633.

73 Näher dazu *Grimm*, JZ 2013, S. 585 (591). Vgl. auch *Ronellenfitsch*, DVBl. 2013, S. 1523 („Das BVerfG ist ausgeschaltet.“, S. 1528).

74 KOM (2012) 11/4 v. 25.1.2012, dazu *Reding*, JD 2012, S. 195.

75 KOM (2012) 10, siehe hierzu *Bäcker*/*Hornung*, ZD 2012, S. 195.

76 *Masing*, SZ v. 9.1.2012, spricht kritisch davon, dass die EU-DSGVO das Potential einer tiefgreifenden Verfassungsänderung hätte.

77 Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Grundverordnung) – politische Einigung, vom 28.1.2016, 5455/16.

Wesentliche Prinzipien wie der auch das deutsche Datenschutzrecht leitende alternativlose „Grundsatz des Verbots mit Erlaubnisvorbehalt“ [78] wurden beibehalten. Gleichwohl ist das Datenschutzrecht in Europa neu zu denken und an der harmonisierten DS-GVO auszurichten. Ein nationales Anpassungsgesetz, das als Kabinettsentwurf vorliegt, wird aufgrund von Öffnungsklauseln gebotene und mögliche Ergänzungen vornehmen. Deshalb wird die Datenschutz-Grundverordnung am Ende in einem eigenen Kapitel näher vorgestellt werden.

Kontrollfragen:

1. *Was ist die „Art. 29-Gruppe“ und welche Aufgaben hat sie?*
2. *In welchen Fällen der Verarbeitung personenbezogener Daten mit Auslandsberührung findet das BDSG Anwendung und unter welchen zusätzlichen Voraussetzungen neben dem gesetzlichen Erlaubnistatbestand dürfen nicht-öffentliche Stellen personenbezogene Daten an Stellen im Ausland übermitteln?*

2 Entwicklungsstufen des nationalen Datenschutzrechts

Auch wenn 2018 ein unmittelbar anzuwendendes Europäisches Datenschutzrecht in Kraft treten wird, das durch nationale Regelungen flankiert sein wird, so sollen doch die nationalen Entwicklungen zu dem bekannt strengen und detailliert geregelten deutschen Datenschutzrecht aufgezeigt werden.

Als das weltweit erste allgemeine Datenschutzgesetz gilt das Landesdatenschutzgesetz von Hessen, das bereits 1970 verabschiedet wurde. Auf nationaler Ebene trat dann zuerst ein Datenschutzgesetz in Schweden in Kraft, bevor Deutschland mit dem Bundesdatenschutzgesetz (BDSG)1977 folgte. Das erste BDSG ging auf einen fraktionsübergreifenden Referentenentwurf zurück, der bereits 1971 vorgelegt worden war; aber erst 1973 wurde mit dem Regierungsentwurf das Gesetzgebungsverfahren eingeleitet, in dem der Entwurf mehrfach geändert wurde, bevor er gegen die Stimmen der Opposition angenommen wurde. Das Gesetz musste aber wegen der Änderungswünsche des Bundesrates in den Vermittlungsausschuss, der die teilweise Berücksichtigung der Änderungen empfahl. Nach der Zustimmung durch Bundestag und Bundesrat wurde das BDSG schließlich am 1. Februar 1977 in seiner ersten Fassung verkündet.

---

[78] Für die Beibehaltung und Stärkung des Verbotsprinzips, Taeger/Gabel-*Taeger*, BDSG, 2013§ 4 Rn. 6; *Karg*, DuD 2013, S. 75; *Weichert*, DuD 2013, S. 246; *Bäcker*, in: Wolff/Brink, Beck’scher Online-Kommentar Datenschutzrecht, § 4 Rn. 3; *Pfeiffer,* K&R 2011, S. 543; Spindler, Persönlichkeitsschutz im Internet, Gutachten F zum 69. DJT, S. 102. Zum Grundsatz des Verbots mit Erlaubnisvorbehalt kritisch oder ablehnend: *Bull*, Netzpolitik, 2013, S. 136; *Kramer*, DuD 2013, S. 380; *Nettesheim*, VVDStRL Bd. 170 (2011), S. 7, und *Franzen*, ZfA 2012, S. 172 (180 ff., mit Bezug auf den Beschäftigtendatenschutz), sowie *Härting* und *Schneider*: *Härting*, in: Taeger, IT und Internet, S. 687; *Härting*/*Schneider*, ZRP 2011, S. 233; *Härting*, AnwBl2012, S. 716; *Härting*, BB2012, S. 459; *Härting*, in: Leible/Kutschke, Schutz der Persönlichkeit im Internet, 2013, S. 55; *Härting*/*Schneider,* ZRP 2011, S. 233; *Härting*/*Schneider*, CRi 2013, Supplement 1, S. 19; *Schneider*, ITRB 2011, S. 243; *Schneider,* AnwBl 2011, S. 233; S*chneider*, ITRB 2012, S. 180; *Schneider*/*Härting*, ZD 2012, S. 199.