Datenschutz und Informationsfreiheit

Textsammlung

Bearbeitet von
Von Alexander Dix, LL.M.

2. Auflage 2018. Buch. 940 S. Kartoniert
ISBN 978 3 8487 4231 8

NomosGesetze

Dix

Datenschutz und Informationsfreiheit

Europarecht, Bundes- und Landesrecht, Völkerrecht

Textsammlung

2. Auflage

Nomos

NomosGesetze

Dr. Alexander Dix, LL.M.

Datenschutz und Informationsfreiheit

Europarecht, Bundes- und Landesrecht, Völkerrecht

2. Auflage

Stand: 1. Februar 2018

Nomos

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.d-nb.de abrufbar.

ISBN 978-3-8487-4231-8

2. Auflage 2018

Einleitung

In den fast fünfzig Jahren, die seit dem Inkrafttreten des weltweit ersten Datenschutzgesetzes in Hessen 1970 vergangen sind, hat der Datenschutz in den nationalen und internationalen Regelwerken eine bemerkenswerte Ausbreitung erfahren. Die Bestrebungen, einen regulatorischen Rahmen für die immer schneller fortschreitende Verarbeitung personenbezogener Daten in einer vernetzten Welt zu formulieren, haben auf nationaler, regionaler, aber auch auf globaler Ebene zugenommen. In mehr als einhundert Staaten gelten mittlerweile gesetzliche Regeln für den Umgang mit personenbezogenen Daten, die sich allerdings stark voneinander unterscheiden. Zudem hat sich die Erkenntnis durchgesetzt, dass die grenzüberschreitende und auch technisch zunehmend entgrenzte Datenverarbeitung eines Regelungsrahmens bedarf, der das Problem des unterschiedlichen Schutzniveaus bei internationalen Datenflüssen adressiert.

Am weitesten entwickelt ist die Angleichung der rechtlichen Rahmenbedingungen des Datenschutzes auf einem im weltweiten Vergleich hohen Niveau in der Europäischen Union. Wer in Deutschland wissen will, welche rechtlichen Voraussetzungen bei der Verarbeitung personenbezogener Daten gelten, wird deshalb in erster Linie die Europäische Datenschutz-Grundverordnung zu beachten haben, die am 25. 5. 2018 in Kraft tritt (Nr. 4) Dem folgt auch die geänderte Struktur dieser Neuauflage. Der Vorrang des Unionsrechts führt dazu, dass die Datenschutzgesetze des Bundes und der Länder ebenso wie das bereichsspezifische Datenschutzrecht nach ihrer Anpassung an den neuen europäischen Rechtsrahmen zwar parallel anzuwenden sind, das innerstaatliche Recht aber an Bedeutung verlieren wird.

Auch auf internationaler Ebene wird seit Gründung der Vereinten Nationen verstärkt versucht, den Schutz der Privatsphäre ebenso wie den Schutz des Einzelnen bei der Verarbeitung personenbezogener Daten sowohl durch *soft law* zu verbessern als auch in verbindlichen Konventionen zu verankern. Das ist aufgrund der erheblichen rechtlichen, sozialen und kulturellen Unterschiede ein Prozess, der sich noch in einem frühen Stadium befindet. Es ist daher wenig erstaunlich, dass nicht nur in Europa, sondern auch in anderen Erdteilen regionale Regelwerke formuliert worden sind, was als Indiz für die wachsende globale Bedeutung des Datenschutzes angesehen werden kann.

Verglichen mit dem Datenschutz hat die Informationsfreiheit zumindest in einzelnen Ländern eine sehr viel längere Geschichte. Das erste Gesetz zur Informationsfreiheit trat 1766 in Schweden in Kraft. Auch hier gibt es mittlerweile rund einhundert Länder weltweit, die diesem Beispiel gefolgt sind. In Deutschland hat die Informationsfreiheitsgesetzgebung erst ab 1998 Ergebnisse gezeitigt und noch immer haben nicht alle Bundesländer entsprechende Gesetze. Die Europäische Union hat in Ermangelung einer Rechtssetzungskompetenz für den allgemeinen Informationszugang nur bestimmte Bereiche geregelt. Auf internationaler Ebene gibt es eine erste Konvention, die vom Europarat initiiert wurde, allerdings (bei Redaktionsschluss für diese 2. Auflage der Textsammlung) noch nicht in Kraft getreten ist.

Sowohl der Schutz der Privatsphäre und der Datenschutz als auch die Informationsfreiheit sind mittlerweile auf regionaler und globaler Ebene in unterschiedlicher Form als Menschenrechte anerkannt und bilden die gemeinsame Basis für die unterschiedlichen Gesetze und Konventionen.

I. Europäische Union

Das Datenschutzrecht in Deutschland und Europa steht vor einer grundlegenden Veränderung. Mit dem Inkrafttreten der Europäischen Datenschutz-Grundverordnung am 25. 5. 2018 gilt diese in Deutschland wie in allen anderen EU-Mitgliedstaaten unmittelbar. Gleichzeitig wird das bisher geltende Bundesdatenschutzgesetz durch ein neues Gesetz ersetzt, mit dem ein wesentlicher Teil des Datenschutzrechts in Deutschland an die Vorgaben des Unionsrechts angepasst werden soll (Nr. 20).

Die Bemühungen der Europäischen Union um einen harmonisierten Rechtsrahmen für den Datenschutz in Europa fanden erstmals Ausdruck in der Richtlinie 95/46/EG. Diese überließ den Mitgliedstaaten weitgehend die Umsetzung der formulierten Standards in das innerstaatliche Recht, auch wenn der Europäische Gerichtshof in jüngster Zeit zumindest bestimmte Regelungen der Richtlinie für un-

mittelbar anwendbar erklärte, soweit die Mitgliedstaaten abweichende Vorschriften vorsahen oder von einer Umsetzung der Richtlinie abgesehen hatten.[1)] Mit der Europäischen Grundrechte-Charta (2000 Nr. 3) und dem Vertrag von Lissabon (2007) erhielten zum einen der Schutz der Privatsphäre und der Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten in Europa den Rang von Menschenrechten (Art. 7 u. 8 GRCh); zum anderen wurden das Europäische Parlament und der Rat mit der Ausarbeitung eines Europäischen Datenschutzgesetzes beauftragt (Art. 16 Abs. 2 AEUV) (Nr. 2). Dieser Auftrag und die beschränkte Harmonisierungswirkung der Richtlinie 95/46/EG veranlassten die Kommission dazu, im Januar 2012 Entwürfe für eine Datenschutz-Grundverordnung und für eine Richtlinie zum Datenschutz im Bereich der Strafverfolgung und Strafvollstreckung vorzulegen. Beide Rechtsakte wurden nach vierjährigen Verhandlungen 2016 verabschiedet und treten im Mai 2018[2)] in Kraft (Nrn. 4 u. 8). Sie sind der erste Teil eines umfassenden Rechtsrahmens für den Datenschutz in der Europäischen Union.

Die Datenschutz-Grundverordnung basiert einerseits in wesentlichen Teilen auf der Richtlinie von 1995 und greift wie diese auf Grundprinzipien des deutschen Datenschutzrechts zurück. Andererseits enthält sie eine Reihe von wichtigen Klarstellungen und Neuerungen. So legt sie bezüglich ihres Anwendungsbereichs anknüpfend an die Rechtsprechung des Europäischen Gerichtshofes ausdrücklich das Marktortprinzip fest, wonach europäisches Datenschutzrecht auch auf die Datenverarbeitung außereuropäischer Unternehmen anzuwenden ist, die dazu dient, betroffenen Personen in der Union Waren und Dienstleistungen anzubieten oder das Verhalten dieser Personen zu beobachten (Art. 3 Abs. 2 DS-GVO).

In materieller Hinsicht sieht die Grundverordnung ein strikteres Koppelungsverbot vor, so dass künftig die Vertragserfüllung oder Erbringung einer Dienstleistung nicht mehr von einer Einwilligung in die Verarbeitung solcher Daten anhängig gemacht werden darf, die für die Erfüllung des Vertrages nicht erforderlich sind (Art. 7 Abs. 4 DS-GVO). Wesentliche Neuerungen enthält die Grundverordnung zudem bezüglich der Transparenz der Datenverarbeitung (Art. 12 - 23, 33 u. 34 DS-GVO). Nicht nur die Rechte der Betroffenen auf Information über die sie betreffenden Verarbeitungsprozesse, sondern auch die selbständigen Pflichten der Verantwortlichen in diesem Bereich werden deutlich erweitert. Die zunehmende Intransparenz der Datenverarbeitung soll dadurch zumindest teilweise kompensiert werden. Zugleich werden neuartige Rechte der Betroffenen statuiert, die das bisherige Datenschutzrecht nicht kannte: das Recht auf Löschung im Internet (Art. 17 Abs. 2 DS-GVO, irreführend als „Recht auf Vergessenwerden“ bezeichnet) wird weitergehend geregelt als dies der Europäische Gerichtshof zunächst beschränkt auf Suchmaschinen-Anbieter entschieden hatte.[3)] Ein Recht auf Datenübertragbarkeit (Portabilität, Art. 20 DS-GVO) soll den betroffenen Personen die Möglichkeit eröffnen, auch außerhalb von sozialen Netzwerken ihre Daten von einem Anbieter zu einem anderen „mitzunehmen“. Damit wird das Recht auf informationelle Selbstbestimmung durch ein wichtiges Instrument ergänzt, das zugleich eine wettbewerbssteigernde Wirkung haben könnte.

Neu sind auch mehrere Bestimmungen in der Grundverordnung, die Bedingungen für die rechtmäßige Verarbeitung der Daten von Kindern formulieren (Art. 6 Abs. 1 lit. f, Art. 8, Art. 12 Abs. 1 S. 1, Art. 57 Abs. 1 lit. b DS-GVO). Erstmals hat der Unionsgesetzgeber in Art. 25 DS-GVO die Prinzipien der Privacy by Design und Privacy by Default in das verpflichtende Sekundärrecht aufgenommen. Bereits bei der Entscheidung über den Einsatz der technischen Mittel (Hard- und Software) muss der Verantwortliche das Prinzip der Datenminimierung berücksichtigen und technisch-organisatorische Maßnahmen treffen, die die Risiken für die Rechte der betroffenen Personen hinreichend begrenzen. Die schon in der Richtlinie von 1995 vorgesehenen Verhaltensregeln (Codes of Practice) können künftig von der Kommission für unionsweit verbindlich erklärt werden (Art. 40 Abs. 9 DS-GVO). Neu ist auch die Verpflichtung der Mitgliedstaaten, der Aufsichtsbehörden, des Europäischen Datenschutzausschusses und der Kommission, unionsweit die Entwicklung datenschutzspezifischer Zertifizie-

1) Vgl. z.B. EuGH Urt. v. 24. 11. 2011 Rs. C-468/10 u. 469/10, ECLI:EU:C:2011:777 (ASNEF), Rn. 50 ff.

2) Die DS-GVO tritt am 25. 5. 2018 unionsweit mit unmittelbarer Wirkung in Kraft; die Richtlinie (EU) 2016/680 ist von den Mitgliedstaaten bis zum 6. 5. 2018 umzusetzen.

3) EuGH, Urt. v. 13. 5. 2014, Rs. C-131/12, ECLI:EU:C:2014:317 (Google Spain.).

rungsverfahren und Datenschutzsiegel zu fördern, mit deren Hilfe die Einhaltung der Grundverordnung nachgewiesen werden kann (Art. 42 DS-GVO).
In formeller Hinsicht sieht die Grundverordnung eine wesentliche Straffung der Entscheidungsprozesse und stärkere Zusammenarbeit der Aufsichtsbehörden auf europäischer Ebene vor. Im Interesse der außereuropäischen Unternehmen, die Niederlassungen in der Union haben, dürfte vor allem die Bestimmung einer federführenden Behörde liegen, die – im Anschluss an die bisherige Praxis der europäischen Aufsichtsbehörden bei Genehmigung von bindenden Unternehmensregeln – als einziger Ansprechpartner („One-Stop Shop") in Fällen grenzüberschreitender Datenverarbeitung vorgesehen ist (Art. 56 DS-GVO). Aber auch die betroffenen Personen können sich bei einer Aufsichtsbehörde (nicht notwendigerweise in dem Mitgliedstaat, in dem sie sich aufhalten) beschweren und dann verlangen, dass diese Behörde sie über das Ergebnis dieser Beschwerde informiert (Art. 77 DS-GVO). Auch für die betroffene Person gilt insoweit ein „One-Stop Shop". Die europäischen Aufsichtsbehörden kooperieren im Europäischen Datenschutzausschuss, der – versehen mit mit eigener Rechtspersönlichkeit – an die Stelle der Gruppe nach Art. 29 der Richtlinie von 1995 tritt und wichtige Funktionen bei der Sicherstellung der einheitlichen Anwendung der Grundverordnung hat (Art. 68 - 76 DS-GVO). Vor allem aber kann der Datenschutzausschuss in bestimmten Streitfällen, für die ein Kohärenzverfahren vorgesehen ist, verbindliche Entscheidungen mit unionsweiter Wirkung treffen (Art. 63 - 65 DS-GVO). Daneben behalten die Aufsichtsbehörden der Mitgliedstaaten das Recht, unter außergewöhnlichen Umständen Dringlichkeitsmaßnahmen zu treffen, um Datenschutzverstöße zu unterbinden (Art. 66 DS-GVO).
Die Datenschutz-Grundverordnung ist das Ergebnis langjähriger Verhandlungen, das zwangsläufig Kompromisscharakter trägt. Während sich die Kommission ursprünglich selbst das Recht vorbehalten wollte, die Verordnung durch Tertiärrechtsakte (Durchführungs- und delegierte Rechtsakte) zu konkretisieren, sieht der verabschiedete Rechtsakt vor, dass diese Konkretisierungen, soweit sie nicht bereits in den Verordnungstext selbst aufgenommen wurden, entweder vom Europäischen Datenschutzausschuss oder von den Mitgliedstaaten vorgenommen werden sollen. Dabei hat der Unionsgesetzgeber zum einen der Tatsache Rechnung getragen, dass in bestimmten Bereichen keine unionsweit einheitlichen Massstäbe vorhanden sind (etwa im Bereich von Medien- und Informationsfreiheit, Art. 85, 86 DS-GVO, oder beim Beschäftigtendatenschutz, Art. 89 DS-GVO). Zum anderen ist der Harmonisierungsanspruch in Teilen relativiert worden, um überhaupt zu einer Einigung über das Gesamtpaket zu kommen. Das betrifft z.B. die zahlreichen Möglichkeiten der Beschränkung von Betroffenenrechten durch das Recht der Union oder der Mitgliedstaaten (Art. 23 DS-GVO), die allerdings an enge grundrechtliche Voraussetzungen geknüpft sind.
Insgesamt handelt es sich bei all diesen Vorschriften, die abweichende oder konkretisierende Regelungen zulassen, nach richtiger Auffassung nicht um „Öffnungsklauseln", die dem Unionsgesetzgeber oder den Mitgliedstaaten völlig freie Hand lassen, sondern um „Spezifizierungsklauseln", bei deren Ausfüllung die grundsätzlichen Vorgaben der Grundverordnung zu beachten sind. Gleichwohl sind die Mitgliedstaaten trotz der unmittelbaren Wirkung der Grundverordnung gehalten, bestimmte innerstaatliche Vorschriften zu erlassen, um ihr bisheriges Datenschutzrecht an das neue Unionsrecht anzupassen. Hier besteht das Risiko, dass die nationalen Gesetzgeber ihren Spielraum überschätzen und damit ihrerseits das Ziel der größtmöglichen Harmonisierung des Datenschutzrechts in Europa gefährden.
Die Regelungen für den Export personenbezogener Daten in Drittländer sind gegenüber der Richtlinie von 1995 nur unwesentlich verändert worden. Auch weiterhin gilt die Grundregel, dass personenbezogene Daten nur dann in außereuropäische Länder exportiert werden dürfen, wenn in dem jeweiligen Zielland ein im Wesentlichen gleichwertiges Datenschutzniveau besteht (Art. 44 - 50 DS-GVO). Damit soll verhindert werden, dass in einer vernetzten Welt das regional kodifizierte europäische Datenschutzrecht nicht durch eine Verlagerung der Datenverarbeitung in ein nicht-europäisches Land umgangen werden kann (Art. 44 S. 2 DS-GVO). Zur Gewährleistung eines im Wesentlichen gleichwertigen Datenschutzniveaus im Zielland können Angemessenheitsbeschlüsse der Kommission, Standardvertragsklauseln und verbindliche interne Datenschutzvorschriften (Binding Corporate Rules) herangezogen werden. Letztere sind im Anschluss an die von den europäischen Datenschutzbehörden

schon unter der Geltung der Richtlinie von 1995 geübte Praxis jetzt auch formell legalisiert worden. Das europäische Datenexportregime ist ein wesentlicher Grund dafür, dass zahlreiche außereuropäische Unternehmen das Unionsrecht und insbesondere die Grundverordnung als globalen Standard für den Datenschutz ansehen und ihre Datenverarbeitung daran orientieren. Denn sie können ihre Prozesse auf internationalen Märkten nur dann rechtskonform organisieren, wenn sie gewährleisten, dass die hohen europäischen Schutzstandards auch außerhalb der Union eingehalten werden.

Von besonderer Bedeutung ist in diesem Zusammenhang der transatlantische Datenverkehr. Unter der Richtlinie von 1995 hatte die Kommission die Angemessenheit des Datenschutzniveaus in den USA, wo bisher eine umfassende Datenschutzgesetzgebung für die Wirtschaft fehlt, nach Abschluss des Abkommens über den „sicheren Hafen" festgestellt. Diese Entscheidung hat der Europäische Gerichtshof 2015 aufgehoben, weil die Kommission die Angemessenheit des Datenschutzniveaus in den USA unzureichend geprüft hatte.[1)] Für den Gerichtshof spielten auch die bekannt gewordenen exzessiven Überwachungsaktivitäten der National Security Agency eine wesentliche Rolle, auch wenn er sie nicht explizit erwähnte. Insbesondere widersprechen nach Ansicht des Gerichtshofs solche Regelungen den Grundprinzipien des europäischen Datenschutzrechts, die eine undifferenzierte Speicherung aller aus der EU in die USA übermittelten Daten und den Zugriff auf die Inhalte elektronischer Kommunikation vorsehen und die zudem den betroffenen Personen keine Möglichkeit eröffnen, mittels eines Rechtsbehelfs Zugang zu den über sie gespeicherten Daten zu erlangen oder die Rechtmäßigkeit der Verarbeitung dieser Daten im Zielland gerichtlich überprüfen zu lassen.[2)] Die Kommission hat mit Durchführungsbeschluss v. 12. 7. 2016 die Angemessenheit des durch den - nach dem Urteil des EuGH vereinbarten - EU-US-Datenschutzschild *(Privacy Shield)* garantierten Schutzniveaus in den USA festgestellt (Nr. 5). Gegen diesen Beschluss der Kommission sind ebenso wie gegen die von ihr bereits vor dem Urteil von 2015 als angemessene Garantien anerkannten Standardvertragsklauseln (Nr. 6) Klagen vor dem EuGH anhängig. Es bleibt abzuwarten, wie der Gerichtshof diese Rechtsinstrumente zum Datenexport bewerten wird.

Schließlich ist eine wesentliche Neuerung in der Datenschutz-Grundverordnung die Einführung und deutliche Verschärfung der Sanktionsmöglichkeiten, die den Aufsichtsbehörden bei Verletzungen der Grundverordnung zur Verfügung stehen. Je nach Art des Verstoßes können Geldbußen von bis zu 10 Mio. oder 20 Mio. Euro bzw. 2 % oder 4 % des gesamten weltweit erzielten Jahresumsatzes des verantwortlichen Unternehmens verhängt werden (Art. 83 Abs. 4 - 6 DS-GVO). Auch diese Sanktionsandrohung des Unionsgesetzgebers trägt dazu bei, dass sich die Unternehmen nicht nur in Europa verstärkt mit den Anforderungen des neuen europäischen Rechtsrahmens auseinandersetzen. Für die praktische Wirkung der Grundverordnung wird viel davon abhängen, dass die Aufsichtsbehörden die neuen Sanktionsmöglichkeiten intelligent einsetzen.

Die nahezu zeitgleich mit der Grundverordnung umzusetzende Richtlinie zum Datenschutz bei Strafverfolgung und Strafvollstreckung (Nr. 8) enthält teilweise gleichlautende, aber auch abweichende Bestimmungen für Polizei- und Justizbehörden in den Mitgliedstaaten. Die Abgrenzung der Anwendungsbereiche von Grundverordnung und Richtlinie kann im Einzelfall schwierig sein. Jedenfalls wollte der Unionsgesetzgeber keinen Bereich der öffentlichen Verwaltung mit geringeren Datenschutzanforderungen versehen, als sie die Grundverordnung und die Richtlinie enthalten, auch wenn die Mitgliedstaaten im Bereich der öffentlichen Verwaltung größeren Spielraum für eigene Regelungen haben.

Bisher nicht an die Datenschutz-Grundverordnung angepasst wurde die Verordnung (EG) 45/2001 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe und Einrichtungen der Gemeinschaft und zum freien Datenverkehr. Die Kommission ist aber in der Pflicht, die Regeln für die Datenverarbeitung der Unionsorgane alsbald der Grundverordnung anzugleichen.

Eine entsprechende ausdrückliche Aufforderung zur Anpassung des bereichsspezifischen Sekundärrechts enthält die Datenschutz-Grundverordnung für den Bereich der elektronischen Kommunikati-

1) EuGH, Urt. v. 6. 10. 2015, Rs. C-362/14, ECLI:EU:C:2015:650 (Schrems), Rnrn. 79 ff.
2) EuGH, ebda., Rnrn. 93 ff.

on.[1] Hier gilt bisher noch die Richtlinie 2002/58/EG über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (e-Privacy-Richtlinie). Das Verhältnis zur Datenschutz-Grundverordnung regeln spezielle Konkurrenzvorschriften (Art. 95 Abs. 2, Art. 96 DS-GVO). Die Kommission hat aber bereits im Januar 2017 einen Entwurf für eine e-Privacy-Verordnung vorgelegt (Nr. 9), die mit dem Inkrafttreten der Grundverordnung die e-Privacy-Richtlinie ersetzen und zusätzliche Regeln für einen besseren Datenschutz in der elektronischen Kommunikation enthalten soll. Gegenwärtig hat der Trilog über dieses Rechtsinstrument noch nicht begonnen, deshalb ist unwahrscheinlich, dass ein synchrones Inkrafttreten der beiden Verordnungen erreicht werden kann. Die E-Privacy-Richtlinie wird deshalb noch solange neben der Datenschutz-Grundverordnung auf die elektronische Kommunikation anzuwenden sein, bis die spezielle Verordnung ebenfalls in Kraft tritt.

Im Bereich der allgemeinen Informationsfreiheit fehlt trotz zahlreicher Bezüge auf das Transparenzprinzip im Vertrag von Lissabon (Nr. 1) eine Rechtssetzungskompetenz der Europäischen Union. Diese hat allerdings die Verordnung (EG) Nr. 1049/2001 über den Zugang der Öffentlichkeit zu Dokumenten des Europäischen Parlaments, des Rates und der Kommission erlassen (Nr. 11), deren geplante Modernisierung wegen Differenzen zwischen Kommission und Parlament ins Stocken geraten ist. Bereits 1999 hatte die Europäische Union erstmals Regeln für den Zugang zu Umweltinformationen erlassen. Die entsprechende spezielle Richtlinie[2] ist 2003 im Zuge der Umsetzung der Aarhus-Konvention der UN-Wirtschaftskommission für Europa[3] novelliert und erweitert worden. Vom Abdruck dieser umweltrechtlichen Rechtsgrundlagen wurde hier abgesehen.

Schließlich hat der Unionsgesetzgeber von seiner Rechtssetzungskompetenz im Bereich der Weiterverwendung von Informationen des öffentlichen Sektors erstmals 2003 durch den Erlass einer entsprechenden Richtlinie Gebrauch gemacht[4] (Nr. 12). Damit sollen gleiche Wettbewerbsbedingungen im Binnenmarkt beim Umgang mit Informationen des öffentlichen Sektors geschaffen werden. Ein allgemeines Zugangsrecht zu Informationen der Verwaltung enthält dieses Rechtsinstrument nicht.

II. Bundes- und Landesrecht

Die Datenschutz-Grundverordnung überlässt es an mehreren Stellen den Mitgliedstaaten, ihre notwendigerweise allgemein gehaltenen Regelungen zu spezifizieren. Als erster Mitgliedstaat hat Deutschland dem mit der Verabschiedung des Gesetzes zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 (Datenschutz-Anpassungs- und -Umsetzungsgesetz EU) v. 30. 6. 2017 entsprochen und insbesondere das Bundesdatenschutzgesetz (BDSG) neu gefasst (Nr. 20). Es löst mit dem Inkrafttreten der Grundverordnung am 25. 5. 2018 das bisher geltende BDSG ab. Das von der Kommission ursprünglich verfolgte Ziel und die von Seiten der Politik geäußerte Erwartung, die Grundverordnung werde die innerstaatlichen Datenschutzgesetze insgesamt ersetzen, haben sich schon aufgrund des Kompromisscharakters der Grundverordnung nicht verwirklichen lassen. Der Grad der Harmonisierung des Datenschutzrechts ist durch die Verordnung gegenüber der Richtlinie von 1995 zwar erhöht worden, eine vollständige Harmonisierung war aber schon aufgrund der unterschiedlichen nationalen Vorstellungen etwa im Medienbereich oder beim Beschäftigtendatenschutz nicht realistisch.

Die Bundesregierung war bei den Verhandlungen im Rat bestrebt, zum einen wesentliche Elemente des geltenden deutschen Datenschutzrechts beizubehalten und auch gegen Vorschläge von Kommission und Parlament für einen weitergehenden Datenschutz zu verteidigen. Dabei war sie allerdings nur zum Teil erfolgreich. Das neue Bundesdatenschutzgesetz dokumentiert das fortgesetzte Bestreben, so viel wie möglich von der bisherigen Rechtslage selbst dann zu konservieren, wenn das Unionsrecht dafür im Grunde keinen Raum lässt. Auch hat der Bundesgesetzgeber die Möglichkeiten zur Spezifi-

1) EG 173 DS-GVO.

2) Richtlinie 2003/4/EG des Europäischen Parlaments und des Rates vom 28. Januar 2003 über den Zugang der Öffentlichkeit zu Umweltinformationen und zur Aufhebung der Richtlinie 90/313/EWG des Rates, ABl.EU *L 41 v.* 14. 2. 2003, S. 26 ff.

3) Übereinkommen über den Zugang zu Informationen, die Öffentlichkeitsbeteiligung an Entscheidungsverfahren und den Zugang zu Gerichten in Umweltangelegenheiten v. 25. 6. 1998 (BGBl. 2006 II S. 1251, 2007 II S. 1392.).

4) Die Richtlinie 2003/98/EG wurde durch die Richtlinie 2013/37/EU geändert.

zierung der Grundverordnung teilweise bis über die Grenze des unionsrechtlich Zulässigen hinaus ausgeschöpft.

Insofern ergibt sich ein paradoxes Bild: Während die Grundverordnung selbst – wie schon die Richtlinie von 1995 - zahlreiche Elemente des deutschen Datenschutzrechts aufgreift und in erweiterter Form „europäisiert", hat Deutschland spätestens mit der Verabschiedung des neuen Bundesdatenschutzgesetzes seine seit dem Inkrafttreten des Hessischen Datenschutzgesetzes eingenommene Rolle als Vorreiter des Datenschutzes aufgegeben. Zugleich hat der Bundesgesetzgeber für die Praxis in Deutschland durch das Nebeneinander zwischen Datenschutz-Grundverordnung und Bundesdatenschutzgesetz die Komplexität in unnötiger Weise erhöht.

Rechtsanwender sollten jedoch in jedem Fall ihren Entscheidungen primär die Grundverordnung zugrunde legen und nur ergänzend prüfen, welche Sonderregelungen das Bundesdatenschutzgesetz enthält. Bestehen Zweifel, ob das Bundesrecht unionskonform ist, ist stets vom Vorrang des Unionsrechts auszugehen. So widersprechen beispielsweise bestimmte Beschränkungen der Betroffenenrechte (z.B. §§ 29 Abs. 1, 32 Abs. 1 Nr. 1, 33 Abs. 3 BDSG) ebenso der Grundverordnung wie der weitgehende Ausschluss der unabhängigen Datenschutzkontrolle gegenüber Berufsgeheimnisträgern (§ 29 Abs. 3 S. 1 BDSG).

Das bereichsspezifische Datenschutzrecht hat der Bundesgesetzgeber bisher nur im Steuer- und Sozialrecht an die Grundverordnung angepasst. Mit der Novelle zum Bundesversorgungsgesetz und anderen Vorschriften v. 17. 7. 2017 sind u.a. sowohl die Abgabenordnung als auch das Sozialgesetzbuch mit Wirkung v. 25. 5. 2018 neu gefasst worden (Nrn. 25-27). Die entsprechenden Vorschriften sind teilweise an das novellierte Bundesdatenschutzgesetz angelehnt und begegnen in Teilen wie dieses unionsrechtlichen Einwänden. Immerhin hat der Gesetzgeber dem Vorrang des Unionsrechts durch eine ausdrückliche Vorschrift Rechnung getragen, die die datenschutzrechtlichen Bestimmungen des Steuer- und Sozialrechts insoweit für unanwendbar erklärt, als die Grundverordnung unmittelbar gilt (§§ 2a Abs. 3 AO, 35 Abs. 2 Satz 1 SGB I, vgl. auch § 1 Abs. 5 BDSG).

Das übrige bereichsspezifische Datenschutzrecht des Bundes muss noch an die Grundverordnung angepasst werden. Das gilt auch für das Telekommunikationsgesetz (Nr. 21) und das Telemediengesetz (Nr. 22). Für beide Gesetzgebungsmaterien hat das Unionsrecht aber bereits jetzt unmittelbare Auswirkungen aufgrund der Rechtsprechung des Europäischen Gerichtshofs: Dieser hat zum einen seine Rechtsprechung bekräftigt, nach der die anlasslose Speicherung von Verkehrsdaten gegen Unionsrecht verstößt.[1)] Dementsprechend hat ein deutsches Gericht bereits die entsprechende im Dezember 2015 novellierte Bestimmung des deutschen Telekommunikationsrechts (§ 113b TKG) für unanwendbar erklärt.[2)] Daraufhin hat die Bundesnetzagentur die Vorratsdatenspeicherung bundesweit ausgesetzt. Zum anderen hat der Europäische Gerichtshof auch in der Regelung des § 15 TMG einen Verstoß gegen die Datenschutz-Richtlinie von 1995 gesehen.[3)]

Auch die Landesdatenschutzgesetze sind an die Grundverordnung anzupassen, selbst wenn der Änderungsbedarf sich insoweit in Grenzen hält, zumal die Verordnung gerade auf Betreiben Deutschlands den Mitgliedstaaten für den öffentlichen Bereich ein größeres Maß an Flexibilität einräumt als im Bereich der Wirtschaft. Allerdings darf der Anpassungsbedarf auch im Bereich der Landes- und Kommunalverwaltung nicht unterschätzt werden. Bei Redaktionsschluss dieser Sammlung lagen noch keine an das neue Unionsrecht angepassten Landesdatenschutzgesetze sondern nur Entwürfe vor. Soweit die Länder nicht bis zum Inkrafttreten der Grundverordnung ihre Gesetze anpassen, wird zu prüfen sein, inwieweit die Verordnung auch für die Behörden in Ländern und Gemeindeverwaltungen unmittelbar gilt. Diese Textsammlung enthält deshalb lediglich die Landesdatenschutzgesetze in der bei Redaktionsschluss geltenden Fassung.

Im Bereich der Informationsfreiheit und Informationsweiterverwendung hat der Bundesgesetzgeber allein das Informationsweiterverwendungsgesetz (Nr. 24) an das geänderte europäische Sekundärrecht angepasst. Auf Landesebene bietet sich ein disparates Bild der Rechtsentwicklung: während einerseits

1) EuGH, Urteile v. 8. 4. 2014, Rs. C-293/12 u. C-594/12, ECLI:EU:C:2014:238 (Digital Rights Ireland), und v. 21. 12. 2016, Rs. C-203/15 u. 698/15, ECLI:EU:C:2016:970 (Tele 2 Sverige.).

2) OVG Münster, Beschl. v. 22. 6. 2017, AZ 13 B 238/17.

3) EuGH, Urt. v. 19. 10. 2016, Rs. C-582/14, ECLI:EU:C:2016:779 (Breyer.).

mittlerweile 12 von 16 Bundesländern Gesetze für den freien Zugang zu Informationen der öffentlichen Verwaltung verabschiedet haben, stehen solche Gesetze in Bayern, Hessen, Niedersachsen und Sachsen noch aus. Zudem zeichnet sich eine interessante Weiterentwicklung des Informationszugangsrechts dadurch ab, dass Hamburg und Rheinland-Pfalz Transparenzgesetze beschlossen haben (Nrn. 35a u. 40a), die nach ersten entsprechenden Ansätzen in den Informationsfreiheitsgesetzen Bremens (Nr. 34a) und Berlins (Nr. 32a) das Prinzip der proaktiven Veröffentlichung von Informationen der öffentlichen Verwaltung zusätzlich zum antragsgebundenen Zugangsrecht der Bürgerinnen und Bürger statuieren. Es bleibt abzuwarten, wann der Bund und andere Länder diesem innovativen Konzept der Informationsfreiheit folgen werden.

III. Völkerrecht

1. Vereinte Nationen

Auch wenn bisher ein verbindlicher völkerrechtlicher Vertrag mit globaler Geltung zu Fragen des Datenschutzes fehlt, gibt es doch menschenrechtliche Garantien der Privatsphäre, namentlich in Art. 12 der Allgemeinen Erklärung der Menschenrechte von 1947 (Nr. 51) und in Art. 17 des Internationalen Pakts über bürgerliche und politische Rechte von 1966 (Nr. 52). Die Vollversammlung der Vereinten Nationen hat zudem 1990 Richtlinien betreffend personenbezogene Daten in automatisierten Dateien beschlossen (Nr. 51), die den Charakter von *soft law* haben. Gleiches gilt für die drei – hier nicht abgedruckten – Resolutionen, die die Vollversammlung nach den Enthüllungen von Edward Snowden 2013, 2014 und 2016 zum Schutz der Privatsphäre im digitalen Zeitalter verabschiedet hat.[1)] Zudem hat der UN-Menschenrechtsrat einen Sonderberichterstatter zum Recht auf Privatsphäre ernannt, der sich mit den besonderen Gefährdungen der Privatheit in der vernetzten Weltgesellschaft auseinanderzusetzen hat.

2. Organisation für wirtschaftliche Zusammenarbeit und Entwicklung

Die von der Organisation für wirtschaftliche Zusammenarbeit und Entwicklung (OECD) 1980 beschlossenen Leitlinien für den Schutz des Persönlichkeitsrechts und den grenzüberschreitenden Verkehr personenbezogener Daten sind das erste – wenngleich nicht rechtsverbindliche – internationale Dokument, das sich mit dem Problem des grenzüberschreitenden Datenverkehrs befasst. Diese Leitlinien sind insofern ein Vorläufer der – allerdings strengeren - Datenexportvorschriften der Europäischen Union. Dreißig Jahre nach Annahme der ersten Leitlinien begann die OECD mit einer Überarbeitung, die 2013 mit der Verabschiedung neu gefasster Leitlinien abgeschlossen werden konnte (Nr. 60). Zu den neu aufgenommenen Regelungselementen gehören die Meldepflicht über Datenlecks (Security Breach Notification) und das Prinzip der Verantwortlichkeit (Accountability), die sich beide auch in der Europäischen Datenschutz-Grundverordnung wiederfinden. Schon 2007 hatte der OECD-Ministerrat eine Empfehlung zur grenzüberschreitenden Zusammenarbeit bei der Durchsetzung von Datenschutzgesetzen beschlossen.[2)]

3. Europarat

Im Rahmen des Europarates garantiert die 1953 in Kraft getretene Europäische Menschenrechtskonvention sowohl den Schutz des Privat- und Familienlebens (Art. 8) als auch die Informationsfreiheit (Art. 10) (Nr. 70). Zum Schutz des Privatlebens hat der Europäische Gerichtshof für Menschenrechte eine umfangreiche Judikatur entwickelt, die auch die Rechtsprechung des Europäischen Gerichtshofs zur Europäischen Grundrechte-Charta beeinflusst hat. Am 28. Januar 1981 wurde mit dem Übereinkommen des Europarates zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten (Konvention No. 108) der weltweit erste völkerrechtlich verbindliche Vertrag zum Datenschutz unterzeichnet (Nr. 71). Diese Konvention hat sich als sehr einflussreich erwiesen und ist

1) Resolutions 68/167 v. 18. 12. 2013, 69/166 v. 18. 12. 2014 und A/C.3/71/1.39/.
2) OECD, The OECD Privacy Framework (2013), S. 129 ff.

nicht nur vor den Mitgliedstaaten des Europarates, sondern auch von mehreren außereuropäischen Staaten ratifiziert worden.[1] Die Konvention wird ergänzt durch ein Zusatzprotokoll bezüglich der Aufsichtsbehörden und des grenzüberschreitenden Datenverkehrs (Nr. 72). Die Modernisierung der Datenschutzkonvention, die zeitgleich mit der Überarbeitung der OECD-Leitlinien 2010 begonnen wurde und bei der in vergleichbarer Weise neue Konzepte des Datenschutzes in den Text der Konvention aufgenommen werden sollen, steht kurz vor ihrem Abschluss. Auch der Europarat war es auch, der als erster einen Mustervertrag für den grenzüberschreitenden Datenverkehr ausgearbeitet hat (Nr. 73). Das Ministerkomitee des Europarates hat zudem zahlreiche Empfehlungen zu speziellen Problemen des Datenschutzes beschlossen. Diese vom Beratenden Ausschuss vorbereiteten Empfehlungen betrafen zuletzt z.B. Themen wie Big Data, Profiling und den Umgang mit Flugpassagierdaten. Schließlich hat der Europarat auch den weltweit ersten völkerrechtlichen Vertrag zum Zugang zu amtlichen Dokumenten initiiert. Er ist am 18. Juni 2009 in Tromsö unterzeichnet worden, allerdings noch nicht in Kraft getreten[2] (Nr. 74). Auch dieser Konvention können außereuropäische Staaten beitreten.

4. Organisation amerikanischer Staaten

Im Rahmen der Organisation amerikanischer Staaten (OAS) ist 1969 in San José die Amerikanische Menschenrechtskonvention unterzeichnet worden und 1978 in Kraft getreten. Auch der Vertrag von San José enthält Garantien des Schutzes der Privatsphäre und der Informationsfreiheit (Nr. 80). Allerdings verfügt der zur Entscheidung von Streitfällen errichtete Interamerikanische Menschenrechtsgerichtshof nicht über vergleichbare Befugnisse zur Durchsetzung seiner Urteile wie der Europäische Gerichtshof für Menschenrechte.

5. Afrikanische Union

Die Afrikanische Union (AU, früher Organisation für afrikanische Einheit – OAU) hat 1981 in Nairobi die Afrikanische Charta der Menschenrechte und Rechte der Völker verabschiedet, die 1986 in Kraft getreten ist.[3] Sie enthält neben der Verpflichtung zur Achtung der Menschenwürde und dem Recht des Menschen, Informationen zu erhalten auch die Verpflichtung der Staaten zum Schutz der Familie (Nr. 91). Ein ausdrückliches Recht auf Schutz des Privatlebens enthält diese Konvention dagegen nicht. Die Afrikanische Union hat darüber hinaus 2014 auch eine Konvention zur Cybersicherheit und zum Datenschutz ausgearbeitet, die bisher allerdings erst von einem afrikanischen Staat ratifiziert wurde[4] und noch nicht in Kraft getreten ist.[5] Diese Konvention enthält neben Regelungen zur elektronischen Kommunikation in ihrem zweiten Kapitel Bestimmungen zum Datenschutz und zu nationalen Datenschutzbehörden, die sich in vieler Hinsicht am europäischen Vorbild orientieren. Als neues Element enthält die Konvention zudem die Verpflichtung des Verantwortlichen, personenbezogene Daten in nachhaltiger Form zu speichern, so dass sie unabhängig von der verwendeten Technik genutzt werden können (Nr. 51). Darüber hinaus sind in bestimmten Regionen Afrikas weitergehende internationale Initiativen zur Sicherung des Datenschutzes ergriffen worden.[6]

6. Asiatisch-Pazifische Wirtschaftsgemeinschaft

Auch die Asiatisch-Pazifische Wirtschaftsgemeinschaft (Asia-Pacific Economic Cooperation - APEC), der die Pazifik-Anrainer-Staaten einschließlich der Vereinigten Staaten und Kanadas angehören, hat sich mit dem Datenschutz und insbesondere mit dem grenzüberschreitenden Datenverkehr

1) Bisher sind dies Uruguay, Mauritius, Senegal und Tunesien.
2) Bisher haben neun Staaten (darunter nicht die Bundesrepublik) die Konvention unterzeichnet. Mit der Hinterlegung der zehnten Ratifikationsurkunde tritt die Tromsö-Konvention in Kraft.
3) Nach der Hauptstadt Gambias, in der wesentliche Vorarbeiten stattfanden, wird sie gemeinhin „Banjul-Charta“ genannt.
4) Senegal.
5) 15 Ratifikationen sind für das Inkrafttreten der Konvention erforderlich.
6) So in der South African Development Community (SADC), der Economic Community of West African States (ECOWAS) und in der East African Community (EAC), vgl. https://cipesa.org/2017/07/what-african-countries-can-learn-from-european-privacy-laws-and-policies/ (gesehen am 2. 12. 2017.).

auseinandergesetzt. Das entsprechende Rahmen-Regelwerk (APEC Privacy Framework) von 2004 und das ergänzende Regelsystem für grenzüberschreitende Datenflüsse (Cross Border Privacy Rules System) von 2009[1)] orientiert sich an den OECD-Leitlinien und ist wie diese rechtlich nicht verbindlich. Dennoch hat es Kontakte zwischen den entsprechenden APEC-Gremien und der Art. 29-Gruppe der europäischen Datenschutzbehörden gegeben, um Möglichkeiten einer Kooperation bei der praktischen Anwendung der bisher noch unterschiedlichen Regeln zum grenzüberschreitenden Datenverkehr zwischen diesen Systemen auszuloten. Auch hier wird das Bestreben deutlich, weltweit zu einheitlichen Kriterien zumindest für den grenzüberschreitenden Datenverkehr zu kommen.

1) www.cbprs.org (gesehen am 3. 12. 2017.).

Inhalt

Europäische Union

Inhalt

Inhalt