Markus Kring

Big Data und der Grundsatz der Zweckbindung

im Datenschutzrecht

Big Data und der Grundsatz der Zweckbindung im Datenschutzrecht

Inauguraldissertation
zur Erlangung des Doktorgrades
des Fachbereichs Rechtswissenschaft
der Johann Wolfgang Goethe-Universität,
Frankfurt am Main

von
Markus Kring
Geboren in Iserlohn

Erscheinungsjahr: 2019
Datum der Promotion: 6. März 2019

Erstgutachterin: Frau Prof. Dr. Indra Spiecker genannt Döhmann, LL.M. (Georgetown Univ.)
Zweitgutachter: Herr Prof. Dr. Roland Broemel

In Memoriam

Renate Kring

Vorwort

Die vorliegende Arbeit wurde vom Fachbereich Rechtswissenschaft der Johann Wolfgang Goethe-Universität Frankfurt am Main im Wintersemester 2018/2019 als Dissertation angenommen. Rechtsprechung und Literatur befinden sich auf dem Stand vom 22. Mai 2018.

Mein herzlicher Dank gebührt zuerst Frau Prof. Dr. Indra Spiecker genannt Döhmann, LL.M. (Georgetown Univ.) für die Betreuung und Förderung dieser Arbeit. Herrn Prof. Dr. Roland Broemel danke ich für die Erstellung des Zweitgutachtens.

Während meiner Zeit als wissenschaftlicher Mitarbeiter am Lehrstuhl für Öffentliches Rechts des Instituts für Informations- und Wirtschaftsrecht am Zentrum für Angewandte Rechtswissenschaft des Karlsruher Instituts für Technologie war ich für mehrere Lehrstuhlvertreter und -inhaber tätig. Dies waren Herr Prof. Dr. Gernot Sydow, M.A., Herr Prof. Dr. Matthias Bäcker und Herr Prof. Dr. Nikolaus Marsch, D.I.A.P. (ENA). Jedem Einzelnen von ihnen bin ich für die lehrreichen Einblicke in Wissenschaft und Lehre zu besonderem Dank verpflichtet.

Meinen ehemaligen Kolleginnen und Kollegen am Institut für Informations- und Wirtschaftsrecht danke ich für die stets angenehme Zusammenarbeit.

Zu guter Letzt möchte ich meinem Vater, Herrn Dr. Reinhard Kring und insbesondere meiner Frau, Dr. Lisa Heinzmann, LL.M., für die Unterstützung bei der Erstellung dieser Arbeit ganz herzlich danken. Ohne ihren steten Rückhalt wäre diese Dissertation nie fertiggestellt worden.

Stuttgart, im Juli 2019 *Markus Kring*

Inhaltsverzeichnis

Literaturverzeichnis

Agentur der europäischen Union für Grundrechte: Handbuch zum europäischen Datenschutzrecht, Luxemburg 2014.

Albers, Marion: Zur Neukonzeption des grundrechtlichen "Daten"schutzes, in: Haratsch, Andreas / Kugelmann, Dieter / Repkewitz, Ulrich (Hrsg.), Herausforderungen an das Recht der Informationsgesellschaft - 36. Tagung der Wissenschaftlichen Mitarbeiterrinnen und Mitarbeiter der Fachrichtung "Öffentliches Recht", Stuttgart, München, Hannover, Berlin, Weimar, Dresden 1996, S. 113-139.

Albers, Marion: Informationelle Selbstbestimmung, Baden-Baden 2005.

Albers, Marion: Umgang mit personenbezogenen Informationen und Daten, in: Hoffmannn-Riem, Wolfgang / Schmidt-Aßmann, Eberhard / Voßkuhle, Andreas (Hrsg.), Grundlagen des Verwaltungsrechts, Band II: Informationsordnung, Verwaltungsverfahren, Handlungsformen, 2. Auflage, München 2012, S. 107-234.

Albrecht, Jan Philipp: Das neue EU-Datenschutzrecht - von der Richtlinie zur Verordnung - Überblick und Hintergründe zum finalen Text für die Datenschutz-Grundverordnung der EU nach der Einigung im Trilog, CR 2016, S. 88-98.

Albrecht, Jan Philipp / Jotzo, Florian: Das neue Datenschutzrecht der EU, Baden-Baden 2017.

Arming, Marian Alexander: Datenpools - Big Data datenschutzkonform umsetzen, K&R Beihefter 3/2015 zu Heft 9 2015, S. 7-12.

Arndt, Hans-Wolfgang / Fetzer, Thomas / Scherer, Joachim / Graulich, Kurt (Hrsg.): Telekommunikationsgesetz - Kommentar, 2. Auflage, Berlin 2015.

Artikel-29-Datenschutzgruppe: Stellungnahme 7/2003 zur Weiterverwendung von Informationen des öffentlichen Sektors und Schutz personenbezogener Daten - Interessenabwägung -, angenommen am 12. Dezember 2003, WP 83.

Artikel-29-Datenschutzgruppe: Stellungnahme 10/2004 zu einheitlicheren Bestimmungen über Informationspflichten, angenommen am 25. November 2004, WP 100.

Artikel-29-Datenschutzgruppe: Stellungnahme 4/2007 zum Begriff "personenbezogene Daten", angenommen am 20. Juni 2007, WP 136.

Artikel-29-Datenschutzgruppe: Stellungnahme 2/2009 zum Schutz der personenbezogenen Daten von Kindern (Allgemeine Leitlinien und Anwendungsfall Schulen), angenommen am 11. Februar 2009, WP 160.

Artikel-29-Datenschutzgruppe: Stellungnahme 16/2011 zur Best-Practice-Empfehlung von EASA und IAB zu verhaltensorientierter Online-Werbung, angenommen am 8. Dezember 2011, WP 188.

Artikel-29-Datenschutzgruppe: Opinion 03/2013 on purpose limitation, adopted on 2 April 2013, WP 203.

Artikel-29-Datenschutzgruppe: Stellungnahme 01/2014 zur Anwendung der Begriffe der Notwendigkeit und der Verhältnismäßigkeit sowie des Datenschutzes im Bereich der Strafverfolgung, angenommen am 27. Februar 2014, WP 211.

Artikel-29-Datenschutzgruppe: Stellungnahme 5/2014 zu Anonymisierungstechniken, angenommen am 10. April 2014, WP 216.

Artikel-29-Datenschutzgruppe: Statement on the role of a risk-based approach in data protection legal frameworks, adopted on 30 May 2014, WP 218.

Artikel-29-Datenschutzgruppe: Erklärung der nach Artikel 29 eingesetzten Datenschutzgruppe über die Auswirkungen der Entwicklung von Big-Data-Technologien auf den Schutz natürlicher Personen im Hinblick auf die Verarbeitung ihrer personenbezogenen Daten in der EU, angenommen am 16. September 2014, WP 221.

Artikel-29-Datenschutzgruppe: Stellungnahme 8/2014 zu den jüngsten Entwicklungen im Internet der Dinge, angemommen am 16. September 2014, WP 223.

Auernhammer, Herbert: Bundesdatenschutzgesetz: Kommentar, 3. Auflage, Köln, Berlin, Bonn, München 1993.

Auer-Reinsdorff, Astrid / Conrad, Isabell (Hrsg.): Handbuch IT- und Datenschutzrecht, 2. Auflage, München 2016.

Badura, Peter: Anhörungsbeitrag in der öffentlichen Anhörung des Innenausschusses des Deutschen Bundestages vom 19. Juni 1989, in: Deutscher Bundestag (Hrsg.), Fortentwicklung der Datenverarbeitung und des Datenschutzes, Zur Sache 17/1990, Bonn 1990, S. 15-16.

Badura, Peter: Schriftliche Stellungnahme zur öffentlichen Anhörung des Innenausschusses des Deutschen Bundestages vom 19. Juni 1989, in: Deutscher Bundestag (Hrsg.), Fortentwicklung der Datenverarbeitung und des Datenschutzes, Zur Sache 17/1990, Bonn 1990, S. 148-160.

Bäcker, Matthias: Grundrechtlicher Informationsschutz gegen Private, Der Staat 51 (2012), S. 91-116.

Baeriswyl, Bruno: Data Mining und Data Warehousing: Kundendaten als Ware oder geschütztes Gut?, RDV 2000, S. 6-11.

Baeriswyl, Bruno: «Big Data» ohne Datenschutz-Leitplanken, digma 2013, S. 14-17.

Bäumler, Helmut: Datenschutz beim Verfassungsschutz, AöR 110 (1985), S. 30-54.

Barth, Armin P.: Algorithmik für Einsteiger, 2. Auflage, Wiesbaden 2013.

Baum, Gerhart: Wacht auf, es geht um die Menschenwürde, DuD 2013, S. 583-584.

Beckhusen, G. Michael: Der Datenumgang innerhalb des Kreditinformationssystems der SCHUFA - Unter besonderer Berücksichtigung des Scoring-Verfahrens ASS und der Betroffenenrechte, Baden-Baden 2004.

Beckhusen, G. Michael: Das Scoring-Verfahren der Schufa im Wirkungsbereich des Datenschutzrechts, BKR 2005, S. 335-344.

Benda, Ernst: Privatsphäre und "Persönlichkeitsprofil" - Ein Beitrag zur Datenschutzdiskussion, in: Leibholz, Gerhard / Faller, Hans Joachim / Mikat, Paul / Reis, Hans (Hrsg.), Menschenwürde und freiheitliche Rechtsordnung - Festschrift für Willi Geiger zum 65. Geburtstag, Tübingen 1974, S. 23-44.

Bergmann, Lutz / Möhrle, Roland / Herb, Armin: Datenschutzrecht - Kommentar, Bundesdatenschutzgesetz, Datenschutzgesetze der Länder und Kirchen, bereichsspezifischer Datenschutz, Stand: 50. Ergänzungslieferung Mai 2016, Stuttgart u. a.

Bergt, Matthias: Die Bestimmbarkeit als Grundproblem des Datenschutzrechts - Überblick über den Theorienstreit und Lösungsvorschlag, ZD 2015, S. 365-371.

Bischoff, Stefan: Zur Komplementierung des Datenschutzes unter organisatorischen Aspekten: Das Konzept der Zweckbindung, in: Traunmüller, R. / Fiedler, H. / Grimmer, K. / Reinermann, H. (Hrsg.), Neue Informationstechnologien und Verwaltung - Fachtagung 14. - 16. September 1983, Berlin, Heidelberg, New York, Tokyo 1984, S. 193-211.

BITKOM (Hrsg.): Big Data im Praxiseinsatz - Szenarien, Beispiele, Effekte, https://www.bitkom.org/Publikationen/2012/Leitfaden/Leitfaden-Big-Data-im-Praxiseinsatz_Szenarien_Beispiele_Effekte/BITKOM_LF_big_data_2012_online(1).pdf, (abgerufen am 11.5.2018).

BITKOM (Hrsg.): Management von Big-Data-Projekten, https://www.bitkom.org/Publikationen/2013/Leitfaden/Management-von-Big-Data-Projekten/130618_Management-von-Big-Data-Projekten.pdf, (abgerufen am 11.05.2018).

BITKOM (Hrsg.): Big-Data-Technologien - Wissen für Entscheider, https://www.bitkom.org/noindex/Publikationen/2014/Leitfaden/Big-Data-Technologien-Wissen-fuer-Entscheider/140228-Big-Data-Technologien-Wissen-fuer-Entscheider.pdf, (abgerufen am 11.05.2018).

Bitter, Till / Buchmüller, Christoph / Uecker, Philip: IV. Datenschutzrecht, in: Hoeren, Thomas (Hrsg.), Big Data und Recht, München 2014, S. 58-94.

Bizer, Johann: Forschungsfreiheit und informationelle Selbstbestimmung - Gesetzliche Forschungsregelungen zwischen grundrechtlicher Förderungspflicht und grundrechtlichem Abwehrrecht, Baden-Baden 1992.

Bizer, Johann: Zweckbindung durch Willenserklärung, DuD 1998, S. 552.

Bizer, Johann: Ziele und Elemente der Modernisierung des Datenschutzrechts, DuD 2001, S. 274-277.

Bock, Kirsten / Meissner, Sebastian: Datenschutz-Schutzziele im Recht, DuD 2012, S. 425-431.

Boehme-Neßler, Volker: Zwei Welten? Big Data und Datenschutz - Entwicklungslinien des Datenschutzes in der digitalen Gesellschaft, in: Rehbinder, Manfred (Hrsg.), UFITA - Archiv für Urheber- und Medienrecht 2015 I, Bern 2015, S. 19-66.

Boehme-Neßler, Volker: Das Ende der Anonymität - Wie Big Data das Datenschutzrecht verändert, DuD 2016, S. 419-423.

Bornemann, Dirk: Big Data - Chancen und rechtliche Hürden, RDV 2013, S. 232-235.

Boyd, Danah / Crawford, Kate: Critical Questions for Big Data, Information, Communication & Society 2012, S. 662-679.

Bräutigam, Peter: Das Nutzungsverhältnis bei sozialen Netzwerken - Zivilrechtlicher Austausch von IT-Leistung gegen personenbezogene Daten, MMR 2012, S. 635-641.

Bramer, Max: Principles of Data Mining, 3. Auflage, London 2016.

Breinlinger, Astrid: Datenschutzrechtliche Probleme bei Kunden- und Verbraucherbefragungen zu Marketingzwecken, RDV 1997, S. 247-253.

Bretthauer, Sebastian: Compliance-by-Design-Anforderungen bei Smart Data - Rahmenbedingungen am Beispiel der Datennutzung im Energiesektor, ZD 2016, S. 267-274.

Brink, Stefan / Eckhardt, Jens: Wann ist ein Datum ein personenbezogenes Datum? - Anwendungsbereich des Datenschutzrechts, ZD 2015, S. 205-212.

Britz, Gabriele: Europäisierung des grundrechtlichen Datenschutzes?, EuGRZ 2009, S. 1-11.

Brouwer, Evelien: Legality and Data Protection Law: The Forgotten Purpose of Purpose Limitation, in: Besselink, Leonard / Pennings, Frans / Prechal, Sacha (Hrsg.), The Eclipse of the Legality Principle in the European Union, Alphen aan den Rijn 2011, S. 273-294.

Brühann, Ulf: EU-Datenschutzrichtlinie - Umsetzung in einem vernetzten Europa, DuD 1996, S. 66-72.

Brühann, Ulf: Europarechtliche Grundlagen, in: Roßnagel, Alexander (Hrsg.), Handbuch Datenschutzrecht - Die neuen Grundlagen für Wirtschaft und Verwaltung, München 2003, Kapitel 2.4, S. 131-155.

Brühann, Ulf: Richtlinie 95/46/EG zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, Ergänzungslieferung 13, Mai 1999, in: Grabitz, Eberhard / Hilf, Meinhard / Nettesheim, Martin (Hrsg.), Das Recht der Europäischen Union, Band IV - Sekundärrecht, A. Verbraucher- und Datenschutzrecht, München 2004, Teil A 30.

Brühann, Ulf: Mindeststandards oder Vollharmonisierung des Datenschutzes in der EG - Zugleich ein Beitrag zur Systematik von Richtlinien zur Rechtsangleichung im Binnenmarkt in der Rechtsprechung des Europäischen Gerichtshofs, EuZW 2009, S. 639-644.

Buchner, Benedikt: Die Einwilligung im Datenschutzrecht, DuD 2010, S. 39-43.

Buchner, Benedikt: Grundsätze und Rechtmäßigkeit der Datenverarbeitung unter der DS-GVO, DuD 2016, S. 155-161.

Büllesbach, Alfred: Datenschutz bei Data Warehouses und Data Mining, CR 2000, S. 11-17.

Bull, Hans Peter: Zur verfassungsrechtlichen Verankerung des Datenschutzes, ÖVD 11/1979, S. 3-9.

Bull, Hans Peter: Neue Konzepte, neue Instrumente?, ZRP 1998, S. 310-314.

Bull, Hans Peter: Europol, der Datenschutz und die Informationskultur, in: Lamnek, Siegfried / Tinnefeld, Marie-Theres (Hrsg.), Globalisierung und informationelle Rechtskultur in Europa - Informationelle Teilhabe und weltweite Solidarität, Baden-Baden 1998, S. 217-230.

Bull, Hans Peter: Aus aktuellem Anlass: Bemerkungen über Stil und Technik der Datenschutzgesetzgebung, RDV 1999, S. 148-153.

Bull, Hans Peter: Zweifelsfragen um die informationelle Selbstbestimmung - Datenschutz als Datenaskese, NJW 2006, S. 1617-1624.

Bull, Hans Peter: Informationelle Selbstbestimmung - Vision oder Illusion, 2. Auflage, Tübingen 2011.

Bull, Hans Peter: Persönlichkeitsschutz im Internet: Reformeifer mit neuen Ansätzen, NVwZ 2011, S. 257-263.

Bull, Hans Peter: Sinn und Unsinn des Datenschutzes, Tübingen 2015.

Bunte, Stefan / Krohn-Grimberghe, Artus: Was bringt Big Data? - Begriffserklärung, Nutzen und Umsetzung, zfo 2014, S. 372-378.

Burkert, Herbert: Internationale Grundlagen, in: Roßnagel, Alexander (Hrsg.), Handbuch Datenschutzrecht - Die neuen Grundlagen für Wirtschaft und Verwaltung, München 2003, Kapitel 2.3, S. 85-130.

Bygrave, Lee A.: Data Privacy Law, Oxford 2014.

Cate, Fred H.: The Failure of Fair Information Practice Principles, in: Winn, Jane K. (Hrsg.), Consumer Protection in the Age of the Information Economy, Aldershot, Burlington 2006, S. 343-379.

Cate, Fred H. / Cullen, Peter / Mayer-Schönberger, Viktor: Data Protection Principles for the 21st century: Revising the 1980 OECD Guidelines., 2013, https://www.oii.ox.ac.uk/publications/Data_Protection_Principles_for_the_21st_Century.pdf, (abgerufen am 11.05.2018).

Cate, Fred H. / Mayer-Schönberger, Viktor: Notice and consent in a world of Big Data, International Data Privacy Law, Vol. 3 No. 2, 2013, S. 67-73.

Cavoukian, Ann: Personal Data Ecosystem (PDE) - A Privacy by Design Approach to an Individual's Pursuit of Radical Control, in: Hildebrandt, Mireille / O'Hara, Kieron / Waidner, Michael (Hrsg.), Digital Enlightenment Yearbook 2013, S. 89-101.

Cavoukian, Ann: Data Mining: Staking a Claim on Your Privacy, Toronto, http://docplayer.net/storage/33/16673687/1526146575/aOLgRcuQBjPZuXub-_nu5w/16673687.pdf, (abgerufen am 11.05.2018).

Cavoukian, Ann / Jonas, Jeff: Privacy by Design in the Age of Big Data, Toronto, www.ontla.on.ca/library/repository/mon/26006/318163.pdf, (abgerufen am 11.05.2018).

Chirco, Claudio G.: Industrie 4.0 in der Praxis - Die Auswirkungen der Vernetzung von Wertschöpfungsketten auf die anwaltliche Beratung, in: Taeger, Jürgen (Hrsg.), Internet der Dinge - Digitalisierung von Wirtschaft und Gesellschaft - Tagungsband Herbstakademie 2015, Edewecht 2015, S. 519-535.

Citron, Danielle Keats: Technological Due Process, Washington University Law Review, Vol. 85, 2008, S. 1249-1313.

Cleve, Jürgen / Lämmel, Uwe: Data Mining, München 2014.

Coudert, Fanny / Dumortier, Jos / Verbruggen, Frank: Applying the purpose specification principle in the age of "big data": the example of integrated video surveillance platforms in France, 25. April 2012, ICRI Working Paper 6/2012, https://lirias.kuleuven.be/bitstream/123456789/389699/1/Coudert_Dumortier_Verbruggen_2012_ICRI+Working+paper+6-2012.pdf, (abgerufen am 11.05.2018).

Crawford, Kate / Schultz, Jason: Big Data and Due Process: Toward a Framework to Redress Predictive Privacy Harms, Boston College Law Review, Vol. 55, 2014, S. 93-128.

Culik, Nicolai / Döpke, Christian: Zweckbindungsgrundsatz gegen unkontrollierten Einsatz von Big Data-Anwendungen, ZD 2017, 226-230.

Cumbley, Richard / Church, Peter: Is "Big Data" creepy?, CLSR 29 (2013), S. 601-609.

Däubler, Wolfgang / Klebe, Thomas / Wedde, Peter / Weichert, Thilo (Hrsg.): Bundesdatenschutzgesetz - Kompaktkommentar zum BDSG, 5. Auflage, Frankfurt am Main 2016.

Dammann, Ulrich / Simitis, Spiros (Hrsg.): EG-Datenschutzrichtlinie: Kommentar, Baden-Baden 1997.

Dammann, Ulrich: Erfolge und Defizite der EU-Datenschutzgrundverordnung - Erwarteter Fortschritt, Schwächen und überraschende Innovationen, ZD 2016, S. 307-314.

Dapp, Thomas F. / Heine, Veronika: Big Data - Die ungezähmte Macht - Deutsche Bank Research, Frankfurt am Main, 4. März 2014, https://www.deutsche-bank.de/fk/de/docs/Big_Data_die_ungezaehmte_Macht.pdf, (abgerufen am 11.05.2018).

Datenschutzkonferenz des Bundes und der Länder: Entschließung der 57. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 25./26. März 1999 zu: Modernisierung des Datenschutzrechts jetzt – umfassende Novellierung des BDSG nicht aufschieben, abgedruckt in: 18. Tätigkeitsbericht des BfD, BT-Drs. 14/555, Anlage 9, S. 212.

Datenschutzkonferenz des Bundes und der Länder: Entschließung zu Data Warehouse, Data Mining und Datenschutz, 59. Konferenz der Datenschutzbeauftragten des Bundes und der Länder, Hannover, 14./15. März 2000, Text abrufbar unter: https://www.datenschutz.rlp.de/fileadmin/lfdi/Konferenzdokumente/Datenschutz/DSK/Entschliessungen/059_datamining.html, (abgerufen am 11.05.2018).

Datenschutzkonferenz des Bundes und der Länder: Ein modernes Datenschutzrecht für das 21. Jahrhundert, verabschiedet von der Konferenz der Datenschutzbeaufgtragen des Bundes und der Länder am 18. März 2010, www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2013/10/Modernisierung_DS-Recht_-_Eckpunkte_-_Maerz_2010.pdf#, (abgerufen am 11.05.2018).

Datenschutzkonferenz des Bundes und der Länder: Stellungnahme der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 11. Juni 2012 zur Datenschutz-Grundverordnung, https://www.bfdi.bund.de/SharedDocs/Publikationen/Entschliessungssammlung/DSBundLaender/StellungnahmeDSK2012ZurDSGVO.pdf?__blob=publicationFile&v=1, (abgerufen am 11.05.2018).

Datenschutzkonferenz des Bundes und der Länder: Positionspapier der DSK zur Datenschutzgrundverordnung, DuD 2015, S. 722.

Dean, Jeffrey / Ghemawat, Sanjay: Map Reduce: Simplified Data Processing on Large Clusters, https://research.google.com/archive/mapreduce-osdi04.pdf, (abgerufen am 11.05.2018).

Deutscher Bundestag - Unterabteilung Europa: Zur Vereinbarkeit des Gesetzes zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten mit dem EuGH-Urteil vom 21. Dezember 2016 zur Vorratsdatenspeicherung, https://www.bundestag.de/blob/492116/.../pe-6-167-16-pdf-data.pdf, (abgerufen am 11.05.2018).

Dippoldsmann, Peter: EG-Datenschutz - "Zwiedenken" auf europäisch - Zum Gebrauch des Datenschutzes als Instrument seiner Vereitelung, Kritische Justiz 1994, S. 369-380.

Dix, Alexander / Schaar, Peter: Der EuGH zur Vorratsdatenspeicherung: Wegweisend für den gesamten Datenschutz, in: Dix, Alexander / Franßen, Gregor / Kloepfer, Michael / Schaar, Peter / Schoch, Friedrich / Voßhoff, Andrea / Deutsche Gesellschaft für Informationsfreiheit (Hrsg.), Informationsfreiheit und Informationsrecht - Jahrbuch 2014, Berlin 2015, S. 17-28.

Dörr, Erwin / Schmidt, Dietmar: Neues Bundesdatenschutzgesetz, 2. Auflage, Köln 1992.

Dorner, Michael: Big Data und "Dateneigentum" - Grundfragen des modernen Daten- und Informationshandels, CR 2014, S. 617 - 628.

Dreier, Thomas / Spiecker genannt Döhmann, Indra: Die systematische Aufnahme des Straßenbildes - Zur rechtlichen Zulässigkeit von Online-Diensten wie "Google Street View", Baden-Baden 2010.

Drews, Hans-Ludwig: Mehrgeteilter Datenschutz, CR 1988, S. 364-367.

Dudenredaktion (Hrsg.): Duden - Die deutsche Sprache - Wörterbuch in drei Bänden, Band 3: Q-ZZGL, Berlin u. a. 2014.

Düsseldorfer Kreis, Arbeitsgruppe internationaler Datenverkehr / Konferenz der Datenschutzbeauftragten, Arbeitskreis Technik und Medien: Orientierungshilfe Cloud Computing Version 2.0, Stand: 09.10.2014, https://www.datenschutz-bayern.de/technik/orient/oh_cloud.pdf, (abgerufen am 11.05.2018).

Ehmann, Eugen: Der weitere Weg zur Datenschutzgrundverordnung - Näher am Erfolg, als viele glauben?, ZD 2015, S. 6-12.

Ehmann, Eugen (Hrsg.): Lexikon für das IT-Recht 2017-2018, Heidelberg 2017.

Ehmann, Eugen / Helfrich, Marcus: EG-Datenschutzrichtlinie: Kurzkommentar, Köln 1999.

Ehmann, Eugen / Selmayr, Martin (Hrsg.): Datenschutz-Grundverordnung, München 2017.

Ehmann, Horst: Informationsschutz und Informationsverkehr im Zivilrecht, AcP 188 1988, S. 230-380.

Ehmann, Horst: Zur Zweckbindung privater Datennutzung - Zugleich ein Beitrag des Datenschutzrechts mit einer Stellungnahme zu den Entwürfen zur Änderung des Bundesdatenschutzgesetzes - Teil 1, RDV 1988, S. 169-180.

Ehmann, Horst: Zur Zweckbindung privater Datennutzung - Zugleich ein Beitrag zum Rechtsgut des Datenschutzrechts mit einer Stellungnahme zur Änderung des Bundesdatenschutzgesetzes - Teil 2, RDV 1988, S. 221-247.

Eifert, Martin: Zweckvereinbarkeit statt Zweckbindung als Baustein eines modernisierten Datenschutzes, in: Gropp, Walter / Lipp, Martin / Steiger, Heinhard (Hrsg.), Rechtswissenschaft im Wandel - Festschrift des Fachbereichs Rechtswissenschaft zum 400jährigen Gründungsjubiläum der Justus-Liebig-Universität Gießen, Tübingen 2007, S. 139-152.

Eßer, Martin / Kramer, Philipp / Lewinski, Kai von (Hrsg.): Auernhammer, Kommentar zum Bundesdatenschutzgesetz, 4. Auflage, Köln 2014.

Europäischer Datenschutzbeauftragter: Stellungnahme des Europäischen Datenschutzbeauftragten zum Datenschutzreformpaket vom 7. März 2012, Brüssel, https://edps.europa.eu/sites/edp/files/publication/12-03-07_edps_reform_package_de.pdf, (abgerufen am 11.05.2018).

Europäischer Datenschutzbeauftragter: Privatsphäre und Wettbewerbsfähigkeit im Zeitalter von "Big Data": das Zusammenspiel zwischen Datenschutz, Wettbewerbsrecht und Verbraucherschutz in der digitalen Wirtschaft, Brüssel, März 2014, https://edps.europa.eu/data-protection/our-work/publications/opinions/privacy-and-competitiveness-age-big-data_de (abgerufen am 11.05.2018).

Europäischer Datenschutzbeauftragter: Opinion 3/2015 - Europe's big opportunity - EDPS recommendations on the EU's options for data protection reform, Brüssel, 27. Juli 2015, https://edps.europa.eu/data-protection/our-work/publications/opinions/edps-recommendations-eu%E2%80%99s-options-data-protection_en (abgerufen am 11.05.2018).

Europäischer Datenschutzbeauftragter: Opinion 7/2015 - Meeting the challenges of big data, 19. November 2015, https://edps.europa.eu/sites/edp/files/publication/15-11-19_big_data_en.pdf, (abgerufen am 11.05.2018).

Europarat: Guidelines on the Protection of Individuals with regard to the processing of personal data in a world of Big Data, https://rm.coe.int/16806ebe7a, (abgerufen am 11.05.2018).

Federal Trade Commission: Protecting Consumer Privacy in an Era of Rapid Change - Recommendations for Businesses and Policymakers, März 2012, https://www.ftc.gov/reports/protecting-consumer-privacy-era-rapid-change-recommendations-businesses-policymakers, (abgerufen am 11.05.2018).

Feiler, Lukas / Fina, Siegfried: Datenschutzrechtliche Schranken für Big Data, medien und recht 2013, S. 303-309.

Forgó, Nikolaus / Krügel, Tina: Die Subjektivierung der Zweckbindung - Datenschutz - Bremsklotz oder Motor des E-Government, DuD 2005, S. 732-735.

Forgó, Nikolaus / Krügel, Tina / Rapp, Stefan: Zwecksetzung und informationelle Gewaltenteilung - Ein Beitrag zu datenschutzgerechtem E-Government, Baden-Baden 2006.

Frenz, Walter: Handbuch Europarecht, Band 4: Europäische Grundrechte, Berlin, Heidelberg 2009.

Gallwas, Hans-Ullrich: Verfassungsrechtliche Grundlagen des Datenschutzes, Der Staat 1979, S. 507-520.

Geiselberger, Heinrich / Moorstedt, Tobias, (Red.): Big Data das neue Versprechen der Allwissenheit, Berlin 2013.

Geppert, Martin / Schütz, Raimund (Hrsg.): Beck'scher TKG-Kommentar, 4. Auflage, München 2013.

Gierschmann, Sibylle: Was "bringt" deutschen Unternehmen die DS-GVO? - Mehr Pflichten, aber die Rechtsunsicherheit bleibt, ZD 2016, S. 51-55.

Giesen, Thomas: Zivile Informationsordnung im Rechtsstaat: Aufräumen!, RDV 2010, S. 266-274.

Gillespie, Tarleton: The Relevance of Algorithms, in: Gillespie, Tarleton / Boczkowski, Pablo J. / Foot, Kirsten A. (Hrsg.), Media Technologies: Essays on communication, materiality, and society, Cambridge, Mass., London, S. 167-193.

Ginsberg, Jeremy / Mohebbi, Matthew H. / Patel, Rajan S. / Brammer, Lynnette/Smolinski, Mark S. / Brilliant, Larry: Detecting influenza epidemics using search engine query data, nature 2009, S. 1012-1015.

Globig, Klaus: Zulässigkeit der Erhebung, Verarbeitung und Nutzung im öffentlichen Bereich, in: Roßnagel, Alexander (Hrsg.), Handbuch Datenschutzrecht - Die neuen Grundlagen für Wirtschaft und Verwaltung, München 2003, Kapitel 4.7, S. 627-677.

Göres, Ulrich: Rechtmäßigkeit des Zugriffs der Strafverfolgungsbehörden auf die Daten der Mauterfassung, NJW 2004, S. 195-198.

Gola, Peter: Verbandsklagen - ein neues Schwert des Datenschutzes?, RDV 2016, S. 17-22.

Gola, Peter (Hrsg.): Datenschutz-Grundverordnung - Kommentar, München 2017.

Gola, Peter / Klug, Christoph / Reif, Yvette: Datenschutz- und presserechtliche Bewertung der "Vorratsdatenspeicherung", NJW 2007, S. 2599-2602.

Gola, Peter / Schomerus, Rudolf (Hrsg.): BDSG, 12. Auflage, München 2015.

Gola, Peter / Schulz, Sebastian: Listenprivileg, Drittinteresse, Zweckbindung - Anmerkungen zum postalischen Direktmarketing in den Entwürfen für eine EU-Datenschutzgrundverordnung, K&R 2015, S. 609-615.

Grafenstein, Maximilian von: Das Zweckbindungsprinzip zwischen Innovationsoffenheit und Rechtssicherheit, DuD 2015, S. 789-795.

Grafenstein, Maximilian von: Die Auswirkungen des Zweckbindungsprinzips auf Innovationsprozesse in Startups, in: Taeger, Jürgen (Hrsg.), Smart World - Smart Law? - Weltweite Netze mit regionaler Regulierung - Tagungsband Herbstakademie 2016, Edewecht 2016, S. 233-246.

Greenleaf, Graham: Five years of the APEC Privacy Framework: Failure or promise, CLSR 25 (2009), S. 28-43.

Grimm, Rüdiger: Spuren im Netz, DuD 2012, S. 88-91.

Groeben, Hans von der / Schwarze, Jürgen / Hatje, Armin (Hrsg.): Europäisches Unionsrecht - Vertrag über die Europäische Union - Vertrag über die Arbeitsweise der Europäischen Union - Charta der Grundrechte der Europäischen Union, 7. Auflage, Baden-Baden 2015.

Grund, Roland: Wertvolles Wissen entdecken und Risiken vermeiden - Data Mining in der Praxis, in: Deggendorfer Forum zur digitalen Datenanalyse e.V. (Hrsg.), Big Data - Systeme und Prüfung, Berlin 2013, S. 29-44.

Gusy, Christoph: Informationelle Selbstbestimmung und Datenschutz: Fortführung oder Neuanfang?, KritV 2000, S. 52-64.

Haase, Martin Sebastian: Datenschutzrechtliche Fragen des Personenbezugs, Tübingen 2015.

Härting, Niko: Datenschutz zwischen Transparenz und Einwilligung - Datenschutzbestimmungen bei Facebook, Apple und Google, CR 2011, S. 169-175.

Härting, Niko: Internetrecht, 5. Auflage, Köln 2014.

Härting, Niko: Profiling: Vorschläge für eine intelligente Regulierung - Was aus der Zweistufigkeit des Profilings für die Regelung des nicht-öffentlichen Datenschutzbereichs folgt, CR 2014, S. 528-536.

Härting, Niko: Zweckbindung und Zweckänderung im Datenschutzrecht, NJW 2015, S. 3284-3288.

Härting, Niko: Datenschutz-Grundverordnung, Köln 2016.

Hallermann, Ulrich: Der "Teilzeit-Datenschutzbeauftragte" und das Verfahrensverzeichnis: Praxistipps für eine schlanke Umsetzung der BDSG-Vorgaben, RDV 2013, S. 173-178.

Hartzog, Woodrow / Selinger, Evan: Big Data in Small Hands, 66 Stanford Law Review Online 2013, S. 81-88.

Heckel, Christian: Behördeninterne Geheimhaltung - Ein Beitrag zum amtsinternen Datenaustausch, NVwZ 1994, S. 224-229.

Heckmann, Dirk (Hrsg.): jurisPK-Internetrecht , 4. Auflage, 2014.

Heibey, Hanns-Wilhelm / Lutterbeck, Bernd / Rohlfs, Sabine / Töpel, Michael: Einige Bemerkungen zum Zusammenhang von Computereinsatz, Innovation und Gesellschaft, in: Dierstein, R. / Fiedler, H. / Schulz, A. (Hrsg.), Datenschutz und Datensicherung - Referate der gemeinsamen Fachtagung der Österreichischen Gesellschaft für Informatik (ÖGI) und der Gesellschaft für Informatik (GI), Johannes-Kepler-Universität, Linz/Österreich, 21. bis 23. September 1976, Köln 1976, S. 298-310.

Helbing, Thomas: Big Data und der datenschutzrechtliche Grundsatz der Zweckbindung, K&R 2015, S. 145-150.

Helbing, Dirk / Frey, Bruno S. / Gigerenzer, Gerd / Hafen, Ernst / Hagner, Michael / Hofstetter, Yvonne / Hoven, Jeroen van den / Zicari, Roberto V. / Zwitter, Andrej: Digital-Manifest (I) - Digitale Demokratie statt Datendiktatur, Spektrum der Wissenschaft Spezial - Physik, Mathematik, Technik, 1. 2017, S. 7-14.

Heller, Christian: Post-Privacy – Prima leben ohne Privatsphäre, München 2011.

Hert, Paul de / Papakonstantinou, Vagelis: The proposed data protection Regulation replacing Directive 95/46/EC: A sound system for the protection of individuals, CLSR 28 (2012), S. 130-142.

Hert, Paul de / Papakonstantinou, Vagelis: The new General Data Protection Regulation: Still a sound system for the protection of individuals?, CLSR 32 (2016), S. 179-194.

Heußner, Hermann: Zur Zweckbindung und zur informationellen Gewaltenteilung in der Rechtsprechung des Bundesverfassungsgerichts, in: Brandt, Willy / Gollwitzer, Helmut / Henschel, Johann Friedrich (Hrsg.), Ein Richter, ein Bürger, ein Christ - Festschrift für Helmut Simon, Baden-Baden 1987, S. 231-242.

Hildebrandt, Mireille: The Dawn of a Critical Transparency Right for the Profiling Era, in: Bus, Jacques / Crompton, Malcom / Hildebrandt, Mireille / Metakides, George (Hrsg.), Digital Enlightenment Yearbook, Amsterdam u. a. 2012, S. 41-56.

Hoeren, Thomas: Anonymität im Web - Grundfragen und aktuelle Entwicklungen, ZRP 2010, S. 251-253.

Hoeren, Thomas / Sieber, Ulrich / Holznagel, Bernd (Hrsg.): Handbuch Multimedia-Recht, 45. Ergänzungslieferung, München Juli 2017.

Hoffmann, Bernhard: Zweckbindung als Kernpunkt eines prozeduralen Datenschutzansatzes: Das Zweckproblem aus theoretischer und praktischer Sicht, Baden-Baden 1991.

Hoffmann-Riem, Wolfgang: Datenschutz als Schutz eines diffusen Interesses in der Risikogesellschaft, in: Krämer, Ludwig / Micklitz, Hans-W. / Tonner, Klaus (Hrsg.), Law and diffuse Interests in the European Legal Order - Recht und diffuse Interessen in der europäischen Rechtsordnung - Liber amicorum Norbert Reich, Baden-Baden 1997, S. 777-788.

Hoffmann-Riem, Wolfgang: Informationelle Selbstbestimmung in der Informationsgesellschaft - Auf dem Wege zu einem neuen Konzept des Datenschutzes -, AöR 123 (1998), S. 513-540.

Hornung, Gerrit: Datensparsamkeit - Zukunftsfähig statt überholt, Spektrum der Wissenschaft Spezial - Physik, Mathematik, Technik, 1.2017, S. 63-67.

Hornung, Gerrit / Hofmann, Kai: Ein "Recht auf Vergessenwerden"? - Anspruch und Wirklichkeit eines neuen Datenschutzrechts, JZ 2013, S. 163-170.

Hornung, Gerrit / Sädtler, Stephan: Europas Wolken - Die Auswirkungen des Entwurfs für eine Datenschutz-Grundverordnung auf das Cloud Computing, CR 2012, S. 638-645.

Horvath, Sabine: Wissenschaftliche Dienste - Deutscher Bundestag - Aktueller Begriff: Big Data, https://www.bundestag.de/blob/194790/.../big_data-data.pdf, (abgerufen am 11.05.2018).

Hustinx, Peter J.: Referat: Bild der internationalen Situation, in: Hassemer, Winfried / Möller, Klaus Peter (Hrsg.), 25 Jahre Datenschutz - Bestandsaufnahme und Perspektiven, Baden-Baden 1996, S. 20-28.

ISO IEC JTC 1 - Information technology: Big Data - Preliminary Report 2014, Genf 2014, https://www.iso.org/iso/big_data_report-jtc1.pdf, (abgerufen am 11.05.2018).

Jandt, Silke / Laue, Philip: Voraussetzungen und Grenzen der Profilbildung bei Location Based Services, K&R 2006, S. 316-322.

Jarass, Hans D.: Charta der Grundrechte der Europäischen Union - Unter Einbeziehung der vom EuGH entwickelten Grundrechte, der Grundrechtsregelungen der Verträge und der EMRK - Kommentar, 2. Auflage, München 2013.

Jhering, Rudolph von: Der Zweck im Recht, Erster Band, 5. Auflage, Leipzig 1916.

Jonas, Hans: Das Prinzip Verantwortung - Versuch einer Ethik für die technologische Zivilisation, Frankfurt am Main 2003.

Jotzo, Florian: Der Schutz personenbezogener Daten in der Cloud, Baden-Baden 2013.

Kamlah, Ruprecht: Right of Privacy, Köln, Berlin, Bonn, München, 1969.

Kamlah, Ruprecht: Datenüberwachung und Bundesverfassungsgericht, DÖV 1970, S. 361-364.

Kamlah, Ruprecht: Datenschutz im Spiegel der anglo-amerikanischen Literatur - Ein Überblick über die Vorschläge zur Datenschutzgesetzgebung, BT-Drs. VI/3826 S. 195-211.

Kamlah, Wulf: Das SCHUFA-Verfahren und seine datenschutzrechtliche Zulässigkeit, MMR 1999, S. 395-404.

Karg, Moritz: Die Rechtsfigur des personenbezogenen Datums - Ein Anachronismus des Datenschutzes?, ZD 2012, S. 255-260.

Karg, Moritz: Anonymität, Pseudonymität und Personenbezug revisited?, DuD 2015, S. 520-526.

Karjoth, Günther: Viele kleine Daten, grosse Wirkung, digma 2013, S. 4-5.

Karsten, Till / Leonhardt, Andreas: Datenschutzrechtliche Anforderungen bei intelligenten Messsystemen - Das neue "Gesetz zur Digitalisierung der Energiewende", RDV 2016, S. 22-24.

Katko, Peter / Babaei-Beigi, Ayda: Accountability statt Einwilligung? - Führt Big Data zum Paradigmenwechsel im Datenschutz?, MMR 2014, 360-364.

Kilian, Wolfgang / Heussen, Benno (Hrsg.): Computerrechts-Handbuch - Informationstechnologie in der Rechts- und Wirtschaftspraxis, Teil 14 Multimedia-Recht - Datenschutzrechtliche Fragen, 32. Ergänzungslieferung, München, August 2013.

Klausnitzer, Rudi: Das Ende des Zufalls - Wie Big Data unser Leben vorhersehbar macht, Salzburg 2013.

Kloepfer, Michael: Geben moderne Technologien und die europäische Integration Anlaß, Notwendigkeit und Grenzen des Schutzes personenbezogener Informationen neu zu bestimmen? - Gutachten D für den 62. Deutschen Juristentag, München 1998.

Koch, Frank A.: Big Data und der Schutz der Daten - Über die Vereinbarkeit des deutschen und europäischen Datenschutzrechts mit Big Data, itrb 2015, S. 13-20.

Kring, Markus: Big Data und der Grundsatz der Zweckbindung, in: Plödereder, Erhard / Grunske, Lars / Schneider, Eric / Ull, Dominik (Hrsg.), 44. Jahrestagung der Gesellschaft für Informatik - Informatik 2014, Big Data - Komplexität meistern, Bonn 2014, S. 551-562.

Kring, Markus / Marosi, Johannes: Ein Elefant im Porzellanladen - Der EuGH zu Personenbezug und berechtigtem Interesse, K&R 2016, S. 773-776.

Kroes, Neelie: The big data revolution, 26. März 2013, EIT Foundation Annual Innovation Forum, Brüssel, Speech/13/261, europa.eu/rapid/press-release_SPEECH-13-261_en.pdf, (abgerufen am 11.05.2018).

Kühling, Jürgen: Datenschutz in einer künftigen Welt allgegenwärtiger Datenverarbeitung - Aufgabe des Rechts?, Die Verwaltung 2007, S. 153-172.

Kühling, Jürgen / Bohnen, Simon: Zur Zukunft des Datenschutzrechts - Nach der Reform ist vor der Reform, JZ 2010, S. 600-610.

Kühling, Jürgen / Buchner, Benedikt (Hrsg.): Datenschutz-Grundverordnung, München 2017.

Kühling, Jürgen / Martini, Mario: Die Datenschutz-Grundverordnung: Revolution oder Evolution im europäischen oder deutschen Datenschutzrecht?, EuZW 2016, S. 448-454.

Kühling, Jürgen / Martini, Mario / Heberlein, Johanna / Kühl, Benjamin / Nink, David / Weinzierl, Quirin / Wenzel, Michael: Die Datenschutz-Grundverordnung und das nationale Recht - Erste Überlegungen zum innerstaatlichen Regelungsbedarf, Münster 2016.

Kühling, Jürgen / Schall, Tobias / Biendl, Michael: Telekommunikationsrecht, 2. Auflage, Heidelberg u. a. 2014.

Kühling, Jürgen / Seidel, Christian / Sivridis, Anastasios: Datenschutzrecht, 3. Auflage, Heidelberg 2015.

Küpper, Johanna: Personenbezug von Gruppendaten? - Eine Untersuchung am Beispiel von Scoring- und Geo-Gruppendaten, München 2016.

Kutscha, Martin: Datenschutz durch Zweckbindung - ein Auslaufmodell?, ZRP 1999, S. 156-160.

Ladeur, Karl Heinz: Datenschutz - vom Abwehrrecht zur planerischen Optimierung von Wissensnetzwerken - Zur "objektiv-rechtlichen Dimension" des Datenschutzes, DuD 2000, S. 12-19.

Landau, Susan: Control use of data to protect privacy, Science 2015, Vol. 347, Issue 6221, S. 504-506.

Laney, Doug: 3D Data management: controlling Data Volume, Velocity, and Variety, Meta Group File: 949, 6. Februar 2001, https://blogs.gartner.com/doug-laney/files/2012/01/ad949-3D-Data-Management-Controlling-Data-Volume-Velocity-and-Variety.pdf, (abgerufen am 11.05.2018).

Laue, Philip / Nink, Judith / Kremer, Sascha: Das neue Datenschutzrecht in der betrieblichen Praxis, Baden-Baden 2016.

Lazer, David / Kennedy, Ryan / King, Gary / Vespignani, Alessandro: The Parable of Google Flu: Traps in Big Data Analysis, Science 2014, S. 1203-1205.

Liedke, Bernd: BIG DATA - small information: muss der datenschutzrechtliche Auskunftsanspruch reformiert werden?, K&R 2014, S. 709-714.

Louis, Hans Walter: Grundzüge des Datenschutzrechts, Köln u. a. 1981.

Lüdemann, Volker / Ortmann, Manuel Christian / Pokrant, Patrick: Datenschutz beim Smart Metering - Das geplante Messstellenbetriebsgesetz (MsbG) auf dem Prüfstand, RDV 2016, S. 125-133.

Lütkemeier, Sven: EU-Datenschutzrichtlinie - Umsetzung in nationales Recht, DuD 1995, S. 597-603.

Luhmann, Niklas: Zweckbegriff und Systemrationalität, 2. Auflage, Frankfurt am Main 1977.

Mallmann, Otto: Das Spannungsverhältnis zwischen Justiz und Datenschutz - Ist der Datenschutz Sand im Getriebe der Justiz?, DRiZ 1987, S. 377-381.

Mallmann, Otto: Zweigeteilter Datenschutz, CR 1988, S. 93-98.

Manovich, Lev: Trending: The Promises and the Challenges of Big Social Data, in: Gold, Matthew K. (Hrsg.), Debates in the Digital Humanities, Minneapolis 2012, S. 460-475.

Mantelero, Alessandro: Personal Data for decisional purposes in the age of analytics: From an individual to a collective dimension of data protection, CLSR 32 (2016), S. 238-255.

Mantz, Reto: Verwertung von Standortdaten und Bewegungsprofilen durch Telekommunikationsdiensteanbieter, K&R 2013, S. 7-11.

Mantz, Reto / Spittka, Jan: EuGH: Speicherung von IP-Adressen beim Besuch einer Webseite - Urteilsanmerkung, NJW 2016, S. 3582- 3583.

Marenbach, Ulrich: Die informationellen Beziehungen zwischen Meldebehörde und Polizei in Berlin: Historische, verfassungsrechtliche und dogmatische Aspekte der Zusammenarbeit, Berlin 1995.

Marnau, Ninja: Anonymisierung, Pseudonymisierung und Transparenz für Big Data, DuD 2016, S. 428-433.

Martini, Mario: Big Data als Herausforderung für den Persönlichkeitsschutz und das Datenschutzrecht, DVBl 2014, S. 1481-1489.

Masing, Johannes: Transparente Verwaltung: Konturen eines Informations-verwaltungsrechts, VVDStRL (63) 2004, S. 377-441.

Masing, Johannes: Herausforderungen des Datenschutzes, NJW 2012, S. 2305-2311.

Mattern, Friedemann: Die technische Basis für das Internet der Dinge, in: Fleisch, Edgar / Mattern, Friedemann (Hrsg.), Das Internet der Dinge - Ubiquitous Computing und RFID in der Praxis: Visionen, Technologien, Anwendungen, Handlungsanleitungen, Berlin, Heidelberg 2005, S. 39-66.

Mayer-Schönberger, Viktor / Cukier, Kenneth: Big Data - A Revolution that will transform how we live, work, and think, Boston, New York 2013.

Mayer-Schönberger, Viktor / Mack, Leonard: Zeitenwechsel - Wie Big Data Open Data verändert, in: Dix, Alexander / Franßen, Gregor / Kloepfer, Michael / Schaar, Peter / Schoch, Friedrich / Voßhoff, Andrea / Deutsche Gesellschaft für Informationsfreiheit (Hrsg.), Informationsfreiheit und Informationsrecht - Jahrbuch 2014, Berlin 2015, S. 1-16.

McDonald, Aleecia M. / Cranor, Lorrie Faith: The Cost of Reading Privacy Policies, I/S A Journal of Law and Policy for the Information Society, Vol. 4:3 2008, S. 540-565.

McKinsey Global Institute (Hrsg.): Big data: The next frontier for innovation, competition and productivity, http://www.mckinsey.com/insights/business_technology/big_data_the_next_frontier_for_innovation, (abgerufen am 11.05.2018).

Meyer, Jürgen (Hrsg.): Charta der Grundrechte der Europäischen Union, 4. Auflage, Baden-Baden 2014.

Meyerdierks, Per: Sind IP-Adressen personenbezogene Daten, MMR 2009, S. 8-13.

Möller, Frank: Data Warehouse als Warnsignal an die Datenschutzbeauftragten, DuD 1998, S. 555-560.

Möller, Jan / Florax, Björn-Christoph: Datenschutzrechtliche Unbedenklichkeit des Scoring von Kreditrisiken, NJW 2003, S. 2724-2726.

Möncke, Ulrich: Data Warehouses - eine Herausforderung für den Datenschutz, DuD 1998, S. 561-569.

Moerel, Lokke: Big Data Protection - How to make the draft EU regulation on data protection future proof, www.debrauw.com/wp-content/uploads/NEWS%20-%20PUBLICATIONS/ Moerel_oratie.pdf (abgerufen am 11.05.2018).

Monreal, Manfred: Weiterverarbeitung nach einer Zweckänderung in der DS-GVO - Chancen nicht nur für das europäische Verständnis des Zweckbindungsgrundsatzes, ZD 2016, S. 507-512.

Montjoye, Yves-Alexandre de / Radaelli, Laura / Singh, Vivek Kumar / Pentland, Alex "Sandy": Unique in the shopping mall: On the reidentifiability of credit card metadata, Science, Vol. 347, Issue 6221, 30.01.2015, S. 536-539.

Moos, Flemming: Die Entwicklung des Datenschutzrechts im Jahr 2014, K&R 2015, S. 158-166.

Müller-Broich, Jan D.: Telemediengesetz, TMG, Baden-Baden 2012.

Müller-Glöge, Rudi / Preis, Ulrich / Schmidt, Ingrid (Hrsg.): Erfurter Kommentar zum Arbeitsrecht, München 2016.

Müllmann, Dirk: Zweckkonforme und zweckändernde Weiternutzung - Die Konsolidierung der Rechtsprechung des BVerfG zur Weiterverwendung zweckgebunden erhobener Daten im Urteil zum BKA-Gesetz vom 20.04.2016, NVwZ 2016, S. 1692-1696.

Nachbaur, Andreas: Vorratsdatenspeicherung "light" - Rechtswidrig und allenfalls bedingt von Nutzen, ZRP 2015, S. 215-217.

Narayanan, Arvind / Shmantikov, Vitaly: Robust De-anonymization of Large Sparse Datasets, Proceedings of the 2008 IEEE Symposium on Security and Privacy 2008, S. 111-125.

National Institute of Standards and Technology: NIST Big Data Interoperability Framework: Volume 1, Definitions, Final Version 1, September 2015, http://dx.doi.org/10.6028/NIST.SP.1500-1, (abgerufen am 11.05.2018).

Niehaus, Holger: Erhebung von Mautdaten durch Strafverfolgungsbehörden?, NZV 2004, S. 502-504.

Ohm, Paul: Broken Promises of Privacy: Responding to the surprising Failure of Anonymisation, UCLA Law Review, Vol. 57, 2010, S. 1701-1777.

Ohm, Paul: Response, The Underwhelming Benefits of Big Data, U. PA. L. Rev. Online, Vol. 161, 2013, S. 339-346.

Ohrtmann, Jan-Peter / Schwiering, Sebastian: Big Data und Datenschutz - Rechtliche Herausforderungen und Lösungsansätze, NJW 2014, S. 2984-2990.

Paal, Boris P. / Pauly, Daniel A. (Hrsg.): Datenschutz-Grundverordnung, München 2017.

Pahlen-Brandt, Ingrid: Datenschutz braucht scharfe Instrumente - Beitrag zur Diskussion um "personenbezogene Daten", DuD 2008, S. 34-40.

Pahlen-Brandt, Ingrid: Zur Personenbezogenheit von IP-Adressen - Zugleich eine Replik auf Eckhardt, K&R 2007, 602 ff., K&R 2008, S. 288-290.

Peifer, Karl-Nikolaus: Verhaltensorientierte Nutzeransprache - Tod durch Datenschutz oder Moderation durch das Recht?, K&R 2011, S. 543-547.

Peschel, Christopher / Rockstroh, Sebastian: Big Data in der Industrie - Chancen und Risiken neuer datenbasierter Dienste, MMR 2014, S. 571-576.

Piltz, Carlo: Die Datenschutz-Grundverordnung, K&R 2016, S. 557-567.

Pitschas, Rainer: Referat zum Thema: Geben moderne Technologien und die Europäische Integration Anlaß, Notwendigkeit und Grenzen des Schutzes personenbezogener Informationen neu zu bestimmen?, in: Ständige Deputation des Deutschen Juristentages (Hrsg.), Verhandlungen des zweiundsechzigsten Deutschen Juristentages - Bremen 1998, Band II/1, Teil M, München 1998, S. M 9-M 74.

Plath, Kai-Uwe (Hrsg.): BDSG - DSGVO - Kommentar, 2. Auflage, Köln 2016.

Podlech, Adalbert: Datenschutz im Bereich der öffentlichen Verwaltung: Entwürfe eines Gesetzes zur Änderung des Grundgesetzes (Art. 75 GG) zur Einführung einer Rahmenkompetenz für Datenschutz und eines Bundesdatenschutz-Rahmengesetzes (DVR Beiheft 1), Berlin 1973.

Podlech, Adalbert: Gesellschaftstheoretische Grundlage des Datenschutzes, in: Dierstein, R. / Fiedler, H. / Schulz, A. (Hrsg.), Datenschutz und Datensicherung - Referate der gemeinsamen Fachtagung der Österreichischen Gesellschaft für Informatik (ÖGI) und der Gesellschaft für Informatik (GI), Johannes-Kepler-Universität, Linz/Österreich, 21. bis 23. September 1976, Köln 1976, S. 311-326.

Podlech, Adalbert / Pfeifer, Michael: Die informationelle Selbstbestimmung im Spannungsverhältnis zu modernen Werbestrategien, RDV 1998, S. 139-154.

Pohle, Jörg: Zweckbindung revisited, DANA 2015, S. 141-145.

Polzer, Georg: Big Data - Eine Einführung, digma 2013, S. 6-9.

Priebe, Reinhard: Reform der Vorratsdatenspeicherung - strenge Maßstäbe des EuGH, EuZW 2014, S. 456-459.

Raabe, Oliver / Wagner, Manuela: Verantwortlicher Einsatz von Big Data - Ein Zwischenfazit zur Entwicklung von Leitplanken für die digitale Gesellschaft, DuD 2016, S. 434-439.

Rachor, Frederik: Vorbeugende Straftatenbekämpfung und Kriminalakten, Baden-Baden 1989.

Rammos, Thanos: Datenschutzrechtliche Aspekte verschiedener Arten "verhaltensbezogener" Onlinewerbung, K&R 2011, S. 692-698.

Ranger, Colby / Raghuraman, Ramanan / Penmetsa, Arun / Bradski, Gary / Kozyrakis, Christos: Evaluating MapReduce for Multi-core and Multiprocessor Systems, 2007 IEEE 13th International Symposium on High Performance Computer Architecture 2007, S. 13-24.

Richards, Neil M. / King, Jonathan H.: Three Paradoxies of Big Data, 66 STAN. L. REV. ONLINE 2013, S. 41-46.

Richter, Philipp: Datenschutz zwecklos? - Das Prinzip der Zweckbindung im Ratsentwurf der DSGVO, DuD 2015, S. 735-740.

Richter, Philipp: Big Data, Statistik und die Datenschutz-Grundverordnung, DuD 2016, S. 581-586.

Roßnagel, Alexander: Modernisierung des Datenschutzrechts für eine Welt allgegenwärtiger Datenverarbeitung, MMR 2005, S. 71-75.

Roßnagel, Alexander: Datenschutz im 21. Jahrhundert, APuZ, Heft 5-6 2006, S. 9-15.

Roßnagel, Alexander: Datenschutz in der künftigen Verkehrstelematik, NZV 2006, S. 281-288.

Roßnagel, Alexander: Datenschutz in einem informatisierten Alltag - Gutachten im Auftrag der Friedrich-Ebert-Stiftung, Berlin 2007, library.fes.de/pdf-files/stabsabteilung/04548.pdf, (abgerufen am 11.05.2018).

Roßnagel, Alexander: Die Novellen zum Datenschutzrecht - Scoring und Adresshandel, NJW 2009, S. 2716-2722.

Roßnagel, Alexander (Hrsg.): Beck'scher Kommentar zum Recht der Telemediendienste, München 2013.

Roßnagel, Alexander: Big Data - Small Privacy? - Konzeptionelle Herausforderungen für das Datenschutzrecht, ZD 2013, S. 562-567.

Roßnagel, Alexander: Die neue Vorratsdatenspeicherung - Der nächste Schritt im Ringen um Sicherheit und Grundrechtsschutz, NJW 2016, S. 533-539.

Roßnagel, Alexander (Hrsg.): Europäische Datenschutz-Grundverordnung - Vorrang des Unionsrechts - Anwendbarkeit des nationalen Rechts, Baden-Baden 2017.

Roßnagel, Alexander / Geminn, Christian / Jandt, Silke / Richter, Philipp: Datenschutzrecht 2016 - "Smart genug für die Zukunft? - Ubiquitous Computing und Big Data als Herausforderungen des Datenschutzrechts, Kassel 2016.

Roßnagel, Alexander / Laue, Philip: Zweckbindung im Electronic Government, DÖV 2007, S. 543-549.

Roßnagel, Alexander / Nebel, Maxi: (Verlorene) Selbstbestimmung im Datenmeer - Privatheit im Zeitalter von Big Data, DuD 2015, S. 455-459.

Roßnagel, Alexander / Nebel, Maxi: Die neue Datenschutz-Grundverordnung - Ist das Datenschutzrecht nun für heutige Herausforderungen gerüstet?, https://www.forum-privatheit.de/forum-privatheit-de/publikationen-und-downloads/veroeffentlichungen-des-forums/positionspapiere-policy-paper/PolicyPaper-5-Die-neue-DSGVO_1.-Auflage_Mai_2016.pdf, (abgerufen am 11.05.2018).

Roßnagel, Alexander / Nebel, Maxi / Richter, Philipp: Was bleibt vom Europäischen Datenschutzrecht? - Überlegungen zum Ratsentwurf der DS-GVO, ZD 2015, S. 455-460.

Roßnagel, Alexander / Pfitzmann, Andreas / Garstka, Hansjürgen: Modernisierung des Datenschutzrechts - Gutachten im Auftrag des Bundesministeriums des Innern, https://www.bfdi.bund.de/SharedDocs/Publikationen/Arbeitshilfen/2001GutachtenModernisierungDSRecht.pdf?__blob=publicationFile&v=3, (abgerufen am 11.05.2018).

Roßnagel, Alexander / Scholz, Philip: Datenschutz durch Anonymität und Pseudonymität - Rechtsfolgen der Verwendung anonymer und pseudonymer Daten, MMR 2000, S. 721-731.

Rogosch, Patricia Maria: Die Einwilligung im Datenschutzrecht, Baden-Baden 2013.

Ronellenfitsch, Michael / Schriever-Steinberg, Angelika / Berg, Nina: Datenschutzrechtliche Kernpunkte für die Trilogverhandlungen zur Datenschutz-Grundverordnung, DANA 2015, S. 126-127.

Rotenberg, Marc: Fair Information Practices and the Architecture of Privacy (What Larry Doesn't Get), Stanford Technology Law Review, 1 2001.

Rubinstein, Ira S.: Big Data: The End of Privacy or a New Beginning, International Data Privacy Law 2013, S. 74-87.

Ruckriegel, Werner: Datenschutz und Datenübermittlung in der öffentlichen Verwaltung, ÖVD 11/1979, S. 10-15.

Rüpke, Giselher: Aspekte zur Entwicklung eines EU-Datenschutzrechts, ZRP 1995, S. 185-190.

Säcker, Franz Jürgen (Hrsg.): Telekommunikationsgesetz Kommentar, 3. Auflage, Frankfurt am Main 2013.

Schaar, Peter: Datenschutz im Internet - Die Grundlagen, München 2002.

Schaar, Peter: Zwischen Big Data und Big Brother - zehn Jahre als Bundesbeauftragter für den Datenschutz und die Informartionsfreiheit, RDV 2013, 223-227.

Schaar, Peter: Überwachung total - Wie wir in Zukunft unsere Daten schützen, Berlin 2014.

Schaffland, Hans-Jürgen / Wiltfang, Noeme: Bundesdatenschutzgesetz (BDSG) - ergänzbarer Kommentar nebst einschlägigen Rechtsvorschriften, Stand: Ergänzungslieferung 1/2015, Berlin 2015.

Schantz, Peter: Die Datenschutz-Grundverordnung - Beginn einer neuen Zeitrechnung im Datenschutzrecht, NJW 2016, S. 1841-1847.

Schantz, Peter / Wolff, Heinrich Amadeus (Hrsg.): Das neue Datenschutzrecht - Datenschutz-Grundverordnung und Bundesdatenschutzgesetz in der Praxis, München 2017.

Schefzig, Jens: Big Data = Personal Data? Der Personenbezug von Daten bei Big Data-Analysen, K&R 2014, S. 772-778.

Scheja, Gregor / Haag, Nils Christian: Teil 5. Datenschutzrecht, in: Leupold, Andreas / Glossner, Silke (Hrsg.), Münchener Anwaltshandbuch IT-Recht, 3. Auflage, München 2013.

Schild, Hans-Hermann: Meldepflichten und Vorabkontrolle, DuD 2001, S. 282-286.

Schleutermann, Markus: Datenverarbeitung im Konzern - Ein Vergleich Schweiz, Österreich und Deutschland, CR 1995, S. 577-585.

Schlink, Bernhard: Datenschutz und Amtshilfe, NVwZ 1986, S. 249-256.

Schmidt, Walter: Die bedrohte Entscheidungsfreiheit, JZ 1974, S. 241-250.

Schmidtmann, Karin / Schwiering, Sebastian: Datenschutzrechtliche Rahmenbedingungen bei Smart-TV - Zulässigkeit von HbbTV-Applikationen, ZD 2014, S. 448-453.

Schmitz, Peter: TDDSG und das Recht auf informationelle Selbstbestimmung, München 2000.

Schneider, Jochen: Datenschutz und neue Medien, NJW 1984, 390-398.

Schneider, Jochen / Härting, Niko: Datenschutz in Europa - Plädoyer für einen Neubeginn - Zehn "Navigationsempfehlungen", damit das EU-Datenschutzrecht internettauglich und effektiv wird, CR 2014, S. 306-312.

Schoch, Friedrich: Das Recht auf informationelle Selbstbestimmung in der Informationsgesellschaft, in: Sachs, Michael / Siekmann, Helmut (Hrsg.), Der grundrechtsgeprägte Verfassungsstaat - Festschrift für Klaus Stern zum 80. Geburtstag, Berlin 2012, S. 1491-1512.

Scholz, Philip: Datenschutz bei Data Warehousing und Data Mining, in: Roßnagel, Alexander (Hrsg.), Handbuch Datenschutzrecht - Die neuen Grundlagen für Wirtschaft und Verwaltung, München 2003, Kapitel 9.2, S. 1833-1875.

Scholz, Rupert / Pitschas, Rainer: Informationelle Selbstbestimmung und staatliche Informationsverantwortung, Berlin 1984.

Scholz, Rupert / Pitschas, Rainer: Informationstechnik zwischen Bürokratie und Datenschutz, AöR 110 (1985), S. 489-527.

Schulz, Sebastian: Datenschutz als überindividuelles Interesse? - Anmerkungen zur geplanten Reform des UKlaG, ZD 2014, S. 510-514.

Schulz, Thomas / Roßnagel, Alexander / David, Klaus: Datenschutz bei kommunizierenden Assistenzsystemem - Wird die informationelle Selbstbestimmung von der Technik überrollt?, ZD 2012, S. 510-515.

Schumacher, Florian: Quantified Self, Wearable Technologies und persönliche Daten, in: Langkafel, Peter (Hrsg.), Big Data in der Medizin und Gesundheitswirtschaft, Heidelberg 2014, S. 227-241.

Schwan, Eggert: Datenschutz, Vorbehalt des Gesetzes und Freiheitsgrundrechte, VerwArch 1975, S. 120-150.

Schwartz, Paul M.: Preemption and Privacy, The Yale Law Journal, Vol. 118, 2009, S. 902-947.

Schwartz, Paul M.: Information Privacy in the Cloud, University of Pennsylvania Law Review, Vol. 161, 2013, S. 1623-1662.

Schwartz, Paul M.: The EU-U.S. Privacy Collision: A turn to institutions and procedures, Harvard Law Review, Vol. 126, 2013, S. 1966-2009.

Schwartz, Paul M. / Solove, Daniel J.: The PII Problem: Privacy and a New Concept of Personally Identifiable Information, 86 N.Y.U. L.Q. Rev. 1814, (2011), S. 1814-1894.

Schwartz, Paul M. / Treanor, William M.: The New Privacy, Michigan Law Review, (Vol. 101), 2003, S. 2163-2184.

Schwarze, Jürgen (Hrsg.): EU-Kommentar, 3. Auflage, Baden-Baden 2012.

Seidel, Ulrich: Das aktuelle Thema: Datenschutz - Teil III: Schutz-Sicherungs-Strukturen, Online - ZfD 1973, S. 359-366.

Seidel, Ulrich: Das Grundrecht auf Datensouveränität - Nowendige Erweiterung - rechtsökonomische und rechtsstaatliche Auswirkungen, ZG 2014, S. 153-165.

Simitis, Spiros: Bundesdatenschutzgesetz - Ende der Diskussion oder Neubeginn?, NJW 1977, S. 729-737.

Simitis, Spiros: Datenschutz: Voraussetzung oder Ende der Kommunikation?, in: Horn, Norbert (Hrsg.), Europäisches Rechtsdenken in Geschichte und Gegenwart, Band II - Festschrift für Helmut Coing zum 70. Geburtstag, München 1982, S. 495-520.

Simitis, Spiros: Die informationelle Selbstbestimmung - Grundbedingung einer verfassungskonformen Informationsordnung, NJW 1984, S. 398-405.

Simitis, Spiros: Von der Amtshilfe zur Informationshilfe - Informationsaustausch und Datenschutzanforderungen in der öffentlichen Verwaltung, NJW 1986, S. 2795-2805.

Simitis, Spiros: Programmierter Gedächtnisverlust oder reflektiertes Bewahren: Zum Verhältnis von Datenschutz und historischer Forschung, in: Fürst, Walther / Herzog, Roman / Umbach, Dieter C. (Hrsg.), Festschrift für Wolfgang Zeidler, Band 2, Berlin, New York 1987, S. 1475-1506.

Simitis, Spiros: Vom Markt zur Polis: Die EU-Richtlinie zum Datenschutz, in: Tinnefeld, Marie-Theres / Philipps, Lothar / Heil, Susanne (Hrsg.), Informationsgesellschaft und Rechtskultur in Europa, Baden-Baden 1995, S. 51-70.

Simitis, Spiros: Die EU-Datenschutzrichtlinie - Stillstand oder Anreiz?, NJW 1997, S. 281-288.

Simitis, Spiros: Datenschutz - Rückschritt oder Neubeginn, NJW 1998, S. 2473-2479.

Simitis, Spiros: Der Transfer von Daten in Drittländer - ein Streit ohne Ende?, CR 2000, S. 472-481.

Simitis, Spiros: Auf dem Weg zu einem neuen Datenschutzkonzept, DuD 2000, S. 714-726.

Simitis, Spiros (Hrsg.): Bundesdatenschutzgesetz, 8. Auflage, Baden-Baden 2014.

Simitis, Spiros: Die Vorratsspeicherung - ein unverändert zweifelhaftes Privileg, NJW 2014, S. 2158-2160.

Sinn, Dieter K.: Das Internet der Dinge - Vernetzt - erst das Büro, dann die Menschen, jetzt die Dinge, CA 2013, S. 4-8.

Skistims, Hendrik / Voigtmann, Christian / David, Klaus / Roßnagel, Alexander: Datenschutzrechtliche Gestaltung von kontextvorhersagenden Algorithmen, DuD 2012, S. 31-36.

Smart-Data-Begleitforschung: Smart Data - Smart Privacy? - Impulse für eine interdisziplinär rechtlich-technische Evaluation, https://www.digitale-technologien.de/DT/Redaktion/DE/Downloads/Publikation/SmartData_Thesenpapier_smart_Privacy.pdf?__blob=publicationFile&v=7, (abgerufen am 11.05.2018).

Sokol, Bettina / Tiaden, Roul: Big Brother und die schöne neue Welt der Vermarktung personenbezogener Informationen, in: Bizer, Johann / Lutterbeck, Bernd / Riß, Joachim (Hrsg.), Umbruch von Regelungssystemen in der Informationsgesellschaft, Stuttgart 2002, S. 161-168.

Solove, Daniel J.: Introduction: Privacy Self-Management and the Consent Dilemma, Harvard Law Review, Vol. 126, 2013, S. 1880-1903.

Solove, Daniel J. / Schwartz, Paul M.: Information Privacy Law, 3. Auflage, New York 2009.

Specht, Louisa / Müller-Riemenschneider, Severin: Dynamische IP-Adressen: Personenbezogene Daten für den Webseitenbetreiber? - Aktueller Stand der Diskussion um den Personenbezug, ZD 2014, S. 71-75.

Spiecker genannt Döhmann, Indra: Big Data intelligent genutzt: Rechtskonforme Videoüberwachung im öffentlichen Raum, K&R 2014, S. 549-556.

Spiecker genannt Döhmann, Indra: Bundesverfassungsgericht kippt BKA-Gesetz: Ein Pyrrhus-Sieg der Freiheitsrechte, VerfBlog, 2016/4/21, http://dx.doi.org/10.17176/20160421-230550, (abgerufen am 11.05.2018).

Spiecker genannt Döhmann, Indra: Big und Smart Data - Zweckbindung zwecklos?, Spektrum der Wissenschaft Spezial - Physik, Mathematik, Technik, 1. 2017, S. 56-61.

Spindler, Gerald / Schuster, Fabian (Hrsg.): Recht der elektronischen Medien, 3. Auflage, München 2015.

Steinmüller, Wilhelm: Informationstechnologie und Gesellschaft - Einführung in die Angewandte Informatik, Darmstadt 1993.

Steinmüller, Wilhelm / Lutterbeck, Bernd / Mallmann, Christoph / Harbot, U. / Kolb, G. / Schneider, Jochen: Grundfragen des Datenschutzes - Gutachten im Auftrag des Bundesministeriums des Innern, Bundestagsdrucksache VI/3826, 1971 S. 5-193.

Stiemerling, Oliver: § 5 Grundlagen der Datenauswertung, in: Conrad, Isabell / Grützmacher, Malte (Hrsg.), Recht der Daten und Datenbanken im Unternehmen, Köln 2014, S. 62-70.

Stiemerling, Oliver: § 6 Aktuelle Herausforderungen: Unstructured, Real-Time und Big Data, in: Conrad, Isabell / Grützemacher, Malte (Hrsg.), Recht der Daten und Datenbanken im Unternehmen, Köln 2014, S. 71-78.

Stollhof, Sabine: Datenschutzgerechtes E-Government: Eine Untersuchung am Beispiel des Einheitlichen Ansprechpartners nach der Europäischen Dienstleistungsrichtlinie, Baden-Baden 2012.

Streinz, Rudolf (Hrsg.): EUV / AEUV - Vertrag über die Europäische Union und Vertrag über die Arbeitsweise der Europäischen Union, 2. Auflage, München 2012.

Sydow, Gernot (Hrsg.): Europäische Datenschutzgrundverordnung, Baden-Baden-2017.

Taeger, Jürgen: Kundenprofile im Internet - Customer Relationship Management und Datenschutz, K&R 2003, S. 220-227.

Taeger, Jürgen: Anmerkung zu BGH, Urteil vom 28.1.2014 - VI ZR 156/13, MMR 2014, S. 492-494.

Taeger, Jürgen: Datenschutzrecht, Frankfurt am Main 2014.

Taeger, Jürgen: Scoring in Deutschland nach der EU-Datenschutzgrundverordnung, ZRP 2016, S. 72-75.

Taeger, Jürgen / Gabel, Detlev (Hrsg.): Kommentar zum BDSG und zu den Datenschutzvorschriften des TKG und des TMG, 2. Auflage, Frankfurt am Main 2013.

Tene, Omer / Polonetsky, Jules: Privacy in the Age of Big Data: A time for big decisions, Stanford Law Review Online 2012, S. 63-69.

Tene, Omer / Polonetsky, Jules: Big Data for All: Privacy and User Control in the Age of Analytics, Northwestern Journal of Technology and Intellectual Property 2013, Vol. 11, Issue 5, S. 239-273.

The President's Council of Advisors on Technology: Big Data and Privacy: A Technological Perspective, Mai 2014, https://obamawhitehouse.archives.gov/sites/default/files/microsites/ostp/PCAST/pcast_big_data_and_privacy_-_may_2014.pdf, (abgerufen am 11.05.2018).

The White House: Consumer Data Privacy in a Networked World - A framework for protecting privacy and promoting innovation in the global digital economy, February 2012, https://www.hsdl.org/?view&did=700959, (abgerufen am 11.05.2018).

Tinnefeld, Marie-Theres: Geschützte Daten, in: Roßnagel, Alexander (Hrsg.), Handbuch Datenschutzrecht - Die neuen Grundlagen für Wirtschaft und Verwaltung, München 2003, Kapitel 4.1, S. 485-500.

Tinnefeld, Marie-Theres / Buchner, Benedikt / Petri, Thomas: Einführung in das Datenschutzrecht - Datenschutz und Informationsfreiheit in europäischer Sicht, 5. Auflage, München 2012.

Tinnefeld, Marie-Theres / Ehmann, Eugen / Gerling, Rainer W.: Einführung in das Datenschutzrecht, 4. Auflage, München 2005.

Treacy, Bridget / Bapat, Anita: Purpose limation - clarity at last?, Privacy & Data Protection Volume 13, Issue 6 2013, S. 11-13.

Trute, Hans-Heinrich: Der Schutz personenbezogener Informationen in der Informationsgesellschaft, JZ 1998, S. 822-831.

Trute, Hans-Heinrich: Verfassungsrechtliche Grundlagen, in: Roßnagel, Alexander (Hrsg.), Handbuch Datenschutzrecht - Die neuen Grundlagen für Wirtschaft und Verwaltung, München 2003, Kapitel 2.5, S. 156-187.

Tuner, Lotte: Zur Notwendigkeit einer Entflechtung von Amtshilfe und Datenschutz, CR 1986, S. 591-596.

U.S. Department of Health, Education & Welfare: Records, Computers, and the Rights of Citizens: Report of the Secretary's Advisory Committee on Automated Personal Data Systems, Washington D.C. 1973.

Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein / GP Forschungsgruppe: Scoring nach der Datenschutz-Novelle 2009 und neue Entwicklungen, www.bmjv.de/SharedDocs/Downloads/DE/PDF/Scoring-Studie.pdf?__blob=publicationFile&v=3, (abgerufen am 11.05.2018).

Ulmer, Claus-Dieter: BIG DATA - neue Geschäftsmodelle, neue Verantwortlichkeiten, RDV 2013, S. 227-232.

Veil, Winfried: DS-GVO: Risikobasierter Ansatz statt rigides Verbotsprinzip, ZD 2015, S. 347-353.

Venzke-Caprarese, Sven: Internet der Dinge - Digitalisierung des Alltags und datenschutzrechtliche Auswirkungen auf den Einzelnen, in: Taeger, Jürgen (Hrsg.), Internet der Dinge - Digitalisierung von Wirtschaft und Gesellschaft - Tagungsband der Herbstakademie 2015, Edewecht 2015, S. 377-392.

Voßhoff, Andrea / Hermerschmidt, Sven: "Wo sind die roten Linien, die bei den Trilog-Verhandlungen in den kommenden Monaten nicht überschritten werden dürfen?", DANA 2015, S. 117.

Wachter, Joren de: Intellectual Property in an Age of Big Data: an Exercise in Futility? - An examination of Big Data's impact on patents and database protection, CRi 2014, S. 1-7.

Waidner, Michael (Hrsg): SIT Technical Reports, Begleitpapier Bürgerdialog - Chancen durch Big Data und die Frage des Privatsphärenschutzes, Stuttgart 2015, https://www.sit.fraunhofer.de/fileadmin/dokumente/studien_und_technical_reports/Big-Data-Studie2015_FraunhoferSIT.pdf, (abgerufen am 11.05.2018).

Walden, Marcus: Zweckbindung und -änderung präventiv und repressiv erhobener Daten im Bereich der Polizei, Berlin 1996.

Wartala, Ramon: Hadoop - Zuverlässige, verteilte und skalierbare Big-Data-Anwendung, München 2012.

Weichert, Thilo: Datenschutz als Verbraucherschutz, DuD 2001, S. 264-270.

Weichert, Thilo: Datenschutzrechtliche Anforderungen an Data-Warehouse-Anwendungen bei Finanzdienstleistern, RDV 2003, S. 113-122.

Weichert, Thilo: Der Personenbezug von Geodaten, DuD 2007, S. 17-23.

Weichert, Thilo: Big Data und Datenschutz - Chancen und Risiken einer neuen Form der Datenanalyse, ZD 2013, S. 251-259.

Weichert, Thilo: Big Data, Gesundheit und der Datenschutz, DuD 2014, S. 831-838.

Weichert, Thilo: Scoring in Zeiten von Big Data, ZRP 2014, S. 168-171.

Werkmeister, Christoph / Brandt, Elena: Datenschutzrechtliche Herausforderungen für Big Data, CR 2016, S. 233-238.

Wespi, Andreas: Big Data: der nächste IT-Sicherheits-Trend?, digma 2013, S. 10-13.

Wiebe, Andreas: Datenschutz in der Zeit von Web 2.0 und BIG DATA - dem Untergang geweiht oder auf dem Weg zum Immaterialgüterrecht, ZIR 2014/1, S. 35-54.

Wittig, Petra: Die datenschutzrechtliche Problematik der Anfertigung von Persönlichkeitsprofilen zu Marketingzwecken, RDV 2000, S. 59-62.

Woertge, Hans-Georg: Die Prinzipien des Datenschutzrechts und ihre Realisierung im geltenden Recht, Heidelberg 1984.

Wolber, Tanja: Datenschutzrechtliche Zulässigkeit automatisierter Kreditentscheidungen - Rechtliche Rahmenbedingungen für die elektronische Risikobewertung, CR 2003, S. 623-626.

Wolff, Heinrich Amadeus / Brink, Stefan (Hrsg.): Beck'scher Online Kommentar Datenschutzrecht, 23. Edition. Stand 01.02.2018, München 2018.

World Economic Forum: Unlocking the Value of Personal Data: From Collection to Usage, Februar 2013, http://www3.weforum.org/docs/WEF_IT_UnlockingValuePersonalData_CollectionUsage_Report_2013.pdf, (abgerufen am 11.05.2018).

Wuermeling, Ulrich: Scoring von Kreditrisiken, NJW 2002, S. 3508-3510.

Wójtowicz, Monika: Wirksame Anonymisierung im Kontext von Big Data, PinG 2013, S. 65-69.

Wybitul, Tim: EU-Datenschutz-Grundverordnung in der Praxis - Was ändert sich durch das neue Datenschutzrecht?, BB 2016, S. 1077-1081.

Zezschwitz, Friedrich von: Konzept der normativen Zweckbegrenzung, in: Roßnagel, Alexander (Hrsg.), Handbuch Datenschutzrecht - Die neuen Grundlagen für Wirtschaft und Verwaltung, München 2003, Kapitel 3.1, S. 219-268.

Ziegenhorn, Gero / Heckel, Katharina von: Datenverarbeitung durch Private nach der europäischen Datenschutzreform - Auswirkungen der Datenschutz-Grundverordnung auf die materielle Rechtmäßigkeit der Verarbeitung personenbezogener Daten, NVwZ 2016, S. 1585-1591.

Zöllner, Wolfgang: Die gesetzgeberische Trennung des Datenschutzes für öffentliche und private Datenverarbeitung, RDV 1985, S. 3-16.

Zscherpe, Kerstin A.: Anforderungen an die datenschutzrechtliche Einwilligung im Internet, MMR 2004, S. 723-727.

Zuiderveen Borgesius, Frederik J.: Singling out people without knowing their names - Behavioural targeting, pseudonymous data, and the new Data Protection Regulation, CLSR 32 (2016), S. 256-271.

Zwart, Melissa de / Humphreys, Sal / Dissel, Beatrix van: Surveillance, Big Data and Democracy: Lessons for Australia from the US and UK, UNSW Law Journal, Volume 37 (2), 2014, S. 713-747.

Abkürzungsverzeichnis

A.	Auflage
a. A.	andere Ansicht
ABl.	Amtsblatt
Abs.	Absatz
a. F.	alte Fassung
AG	Amtsgericht
APEC	Asiatisch-Pazifische Wirtschaftsgemeinschaft
Art.	Artikel
Az.	Aktenzeichen
BDSG a. F.	Bundesdatenschutzgesetz alter Fassung
BDSG 2018	Bundesdatenschutzgesetz in der Fassung von Art. 1 des Datenschutz-Anpassungs- und Umsetzungsgesetzes EU – DSAnpUG-EU vom 30. Juni 2017, BGBl. I, S. 2097
BFStrMG	Bundesfernstraßenmautgesetz
BGBl.	Bundesgesetzblatt
BGH	Bundesgerichtshof
BKAG	Bundeskriminalamtgesetz
BMI	Bundesministerium des Innern
BR-Drs.	Bundesratsdrucksache
BSG	Bundessozialgericht
BStatG	Bundesstatistikgesetz
BT-Drs.	Bundestagsdrucksache
BVerfG	Bundesverfassungsgericht
bzw.	beziehungsweise
d. h.	das heißt
DSGVO	Datenschutz-Grundverordnung
DSGVO-E-Komm	Kommissionsentwurf der Datenschutz-Grundverordnung
DSGVO-E-Rat	Ratsentwurf der Datenschutz-Grundverordnung
DSRL	EU-Datenschutzrichtlinie

DSRL-E[1]	erster Kommissionsentwurf der Datenschutzrichtlinie
DSRL-E[2]	zweiter Kommissionsentwurf der Datenschutzrichtlinie
dt.	deutsch
EG	Europäische Gemeinschaft
EGMR	Europäischer Gerichtshof für Menschenrechte
Einl.	Einleitung
EnWG	Energiewirtschaftsgesetz
endg.	endgültig
EMRK	Europäische Menschenrechtskonvention
ErwG	Erwägungsgrund
etw.	etwas
EU	Europäische Union
EuGH	Europäischer Gerichtshof
EWG	Europäische Wirtschaftsgemeinschaft
f., ff.	folgende
FIPs	Fair Information Practices
Fn.	Fußnote
FS	Festschrift
GenDG	Gendiagnostikgesetz
GG	Grundgesetz
GPS	Global Positioning System
GRCh	EU-Grundrechtecharta
HDSG a. F.	Landesdatenschutzgesetz Hessen alter Fassung
Hrsg.	Herausgeber
InfrAG	Infrastrukturabgabengesetz
IP-Adresse	Internetprotokoll-Adresse
i. S.	im Sinne
i. S. d.	im Sinne des
i. S. v.	im Sinne von
IT-System	informationstechnisches System
i. V. m.	in Verbindung mit
Jh.	Jahrhundert
jmd.	jemand
Kap.	Kapitel

LDSG BW a. F.	Landesdatenschutzgesetz Baden-Württemberg alter Fassung
LDSG SH a. F.	Landesdatenschutzgesetz Schleswig-Holstein alter Fassung
LG	Landgericht
lit.	littera (Buchstabe)
LKHG BW	Landeskrankenhausgesetz Baden-Württemberg
Ls.	Leitsatz
m. w. N.	mit weiteren Nachweisen
MsbG	Messstellenbetriebsgesetz
No.	number
NoSQL	not only structured query language
Nr.	Nummer
o. Ä.	oder Ähnliches
OECD	Organisation für wirtschaftliche Zusammenarbeit und Entwicklung
PolG BW	Polizeigesetz Baden-Württemberg
RiS	Recht auf informationelle Selbstbestimmung
Rn.	Randnummer
Rs.	Rechtssache
S.	Seite
SGB I	Sozialgesetzbuch I
sog.	sogenannte
SQL	structured query language
StPO	Strafprozessordnung
TDDSG	Teledienstedatenschutzgesetz
TKG	Telekommunikationsgesetz
TMG	Telemediengesetz
u.	und
u. a.	und andere
UKlaG	Unterlassungsklagengesetz
UN	Vereinte Nationen
USA	Vereinigte Staaten von Amerika
UWG	Gesetz gegen den unlauteren Wettbewerb
v.	versus, von, vom
v. d.	von dem, von der

vgl.	vergleiche
VGH	Verwaltungsgerichtshof
VO	Verordnung
Vol.	volume
z. B.	zum Beispiel

A. Einleitung

I. Problemaufriss

Aufgrund des technischen Fortschritts ist es mittlerweile möglich sehr große Datenmengen dauerhaft zu speichern und auszuwerten. Im Vergleich zu früher besteht ein wesentlicher Unterschied darin, dass die Daten in Echtzeit analysiert werden können. Dieses Phänomen wird als „Big Data" bezeichnet. Eine allgemein anerkannte Definition gibt es aber bislang noch nicht.

Gerade von Seiten der Wirtschaft wird Big Data momentan forciert. Zwar wird dem Thema derzeit eine womöglich unangemessen große Aufmerksamkeit zuteil; man kann es angesichts seiner Unbestimmtheit auch als ein Modethema auffassen. Der voraussichtlich in Zukunft immer günstigere Speicherplatz und die leistungsfähigeren Computer lassen aber vermuten, dass diese Art der Datenanalyse weiter an Bedeutung gewinnen wird. Denn die Möglichkeit mit Hilfe von großen Datenmengen und Algorithmen neue Erkenntnisse zu gewinnen, erscheint zu verlockend und ist bereits jetzt Grundlage einer Reihe von erfolgreichen und Erfolg versprechenden Geschäftsmodellen. So ist es nicht verwunderlich, dass personenbezogene Daten wiederholt als das „neue Öl" in einer vernetzten Welt[1] und Standortdaten als „das Datengold des 21. Jahrhunderts"[2] bezeichnet worden sind.

Während Big Data datenschutzrechtlich unproblematisch ist, solange nicht mit personenbezogenen Daten umgegangen wird bzw. kein Perso-

---

1 So z. B. die damalige Vizepräsidentin der EU-Kommission *Kroes*, Rede, S. 2; siehe *Cavoukian*, in: Hildebrandt/O'Hara/Waidner (Hrsg.), Digital Enlightenment Yearbook, S. 89 (90); ähnlich *Dorner*, CR 2014, 617 (618), der schlicht vom neuen Öl spricht; ebenso *Arming*, K&R Beihefter 3/2015 zu Heft 9 2015, 7.

2 *Martini*, DVBl 2014, 1481 (1482).

nenbezug herstellbar ist, stellt sich die Frage, ob es mit den datenschutzrechtlichen Grundprinzipien im Falle des Umgangs mit personenbezogenen Daten im Einklang steht und stehen kann. Big Data zielt oftmals gerade darauf ab, bislang unbekannte Korrelationen zu entdecken und überraschende Schlüsse aus diesen Zusammenhängen zu ziehen. Daher ist der Zweck der Verarbeitung personenbezogener Daten bei deren Erhebung häufig noch nicht konkret bestimmbar. Gleichwohl ist aber bei der Erhebung von Daten nach derzeitiger Rechtslage grundsätzlich die Angabe des Zwecks oder der Zwecke der Erhebung, Verarbeitung oder Nutzung erforderlich. Zudem werden Daten genutzt, deren ursprünglicher Erhebungszweck möglicherweise längst erfüllt ist.

Um Big Data in rechtskonformer Weise nutzen zu können, stellt sich daher die Frage, inwiefern ein Spannungsverhältnis zum Zweckbindungsgrundsatz besteht und wie dieses gegebenenfalls aufgelöst werden kann.[3]

Einerseits sieht sich das Zweckbindungsprinzip erheblicher Kritik ausgesetzt. Die Zweckbindung sei die Antithese zu Big Data.[4] Im Rahmen der Reform des europäischen Datenschutzrechts wurde sogar die Abschaffung der Zweckbindung gefordert, da sie dem Ziel des größtmöglichen Erkenntnisgewinns im Rahmen von Big-Data-Analysen entgegenstehe.[5] Die bei der Datenerhebung nicht vorhergesehenen Sekundärnut-

---

3 Aufgrund neuer technischer Entwicklungen sah auch die *Artikel-29-Datenschutzgrupppe* eine Auseinandersetzung mit dem Zweckbindungsprinzip als notwendig an: *Artikel-29-Datenschutzgruppe*, WP 203, S. 14.

4 *Tene/Polonetsky*, Northwestern Journal of Technology and Intellectual Property 2013, Vol. 11, Issue 5, 239 (242); ähnlich *Ohrtmann/Schwiering*, NJW 2014, 2984, die einen Widerspruch zwischen Big Data und der Zweckbindung feststellen.

5 BITKOM, EU-Datenschutzverordnung muss Innovationen ermöglichen. Pressemitteilung v. 24.06.2015, abrufbar unter: https://www.bitkom.org/Presse/Presseinformation/EU-Datenschutzverordnung-muss-Innovationen-ermoeglichen.html, (abgerufen am 11.05.2018); ähnlich *Cate/Mayer-Schönberger*, International Data Privacy Law, Vol. 3 No. 2, 2013, 67 (72), die in einem Bericht der Ergebnisse einer von *Microsoft* gesponserten Tagung eine „Inkonsistenz mit der Datennutzung in der heutigen Welt" ausmachten; erhebli-

zungen seien die Kronjuwelen von Big Data.[6] Die Zweckbindung gehöre „auf den Prüfstand“ da die Datenverwendung für bislang unbekannte Zwecke die „innovative Kraft“ von Big Data darstelle.[7] Die Zweckbindung versuche die Zukunft abzuwehren und stehe zukünftigen technischen Notwendigkeiten des Datenumgangs entgegen.[8] Das derzeitige Regelungsregime müsse überdacht werden, denn aufgrund der neuen Möglichkeiten der Bevorratung und Auswertung von Daten sei offensichtlich, dass Daten nicht nur einem Zweck dienen könnten, wie dies früher der Fall gewesen sei.[9] Big Data ziele gerade darauf die Daten aus ihrem ursprünglichen Erhebungskontext herauszureißen.[10] Das Ziel von Big-Data-Analysen sei möglichst viele Daten auf Vorrat zu speichern und sodann für zunächst unbestimmte Zwecke auszuwerten, weshalb sie der Zweckbindung entgegenstünden.[11] Bei der Zusammenführung vieler Daten werde deren jeweilige Zweckbindung verletzt, da diese aus ihren ursprünglichen Kontexten gelöst würden.[12] Big Data sehe weder eine Zweckbestimmung noch eine Zweckbindung vor.[13] Eine starke Betonung der Zweckbindung würde daher für auf personenbezogene Daten angewiesene Big-Data-Analysen eine große Einschränkung bedeuten.[14] Mit einer

---

che Kritik aufgrund geschäftlicher Interessen ist allerdings kein neues Phänomen, siehe die Forderung nach einer „in einer Marktwirtschaft unabdingbaren Flexibilität“ bei *Lütkemeier*, DuD 1995, 597 (599); vgl. zu frühzeitigen Forderungen dieser Art.: *Simitis*, DuD 2000, 714 (717).

6 *Tene/Polonetsky*, Northwestern Journal of Technology and Intellectual Property 2013, Vol. 11, Issue 5 239 (259); ähnlich, d. h. ebenfalls auf die Bedeutung der zweckändernden Sekundärnutzungen abstellend: *Mayer-Schönberger/Cukier*, Big Data, S. 153; es finden sich auch warnende Stimmen vor Sekundärverwendungen und Profilbildungen, siehe *Klausnitzer*, Big Data, S. 200.

7 *Härting*, Internetrecht, Annex, Rn. 48, der als (fiktives) Beispiel die zukünftige Heilung von Krankheiten mittels heutiger Tweets anführt.

8 Vgl. *Moerel*, Big Data, S. 53.

9 *Mayer-Schönberger/Mack*, in: Dix/Franßen/Kloepfer/Schaar/Schoch/Voßhoff/Deutsche Gesellschaft für Informationsfreiheit (Hrsg.), Jahrbuch 2014, S. 1 (4).

10 *Helbing*, K&R 2015, 145 (146).

11 *Roßnagel/Nebel*, DuD 2015, 455 (458).

12 *Roßnagel*, ZD 2013, 562 (565); *Schaar*, RDV 2013, 223 (225).

13 *Roßnagel*, ZD 2013, 562 (564).

14 *Roßnagel/Nebel*, DuD 2015, 455 (459).

Welt der allgegenwärtigen Datenverarbeitung („ubiquitous computing“)[15] sei die Zweckbindung aufgrund der Schwierigkeit der vorherigen Zweckfestlegung nicht zu vereinbaren.[16] Die Multifunktionalität vieler Geräte lasse die klare Bestimmung eines Zwecks nicht mehr zu.[17] Auch sei ein maschinelles Lernen nicht mit dem Verbot der Vorratsspeicherung von Daten vereinbar.[18] Big-Data-Analysen mit personenbezogenen Daten stellten in aller Regel einen „klaren Verstoß“ gegen das Zweckbindungsprinzip dar.[19]

Zwar sei eine Umgehung des Problems durch eine weite Fassung des Zwecks denkbar, dadurch gehe aber die Steuerungsfunktion verloren[20] und es bestehe die Gefahr von Abwägungen im Rahmen von Generalklauseln, die letztlich regelmäßig zu einer Zulässigkeit des Datenumgangs führten.[21] Die Konzepte des Datenschutzes sollten überdacht und an die technischen Entwicklungen angepasst werden.[22]

Die Zweckbindung habe zu einer „geradezu inflationären Datenschutzgesetzgebung“ geführt,[23] wodurch die Fülle an Regelungen entgegen dem Ziel der Transparenz immer unübersichtlicher geworden sei.[24] Sie werde

---

15 Siehe hierzu: *Mattern*, in: Fleisch/Mattern (Hrsg.), Internet der Dinge, S. 39 ff.

16 *Roßnagel*, APuZ, Heft 5-6 2006, 9 (12); *Roßnagel/Geminn/Jandt/Richter*, Datenschutzrecht 2016, S. 26; *Kühling*, Die Verwaltung 2007, 153 (159), hält die Zweckbindung zumindest für erschwert und sieht sogar die Möglichkeit eines „endgültigen Todesstoßes“ für die Zweckbindung.

17 *Roßnagel*, APuZ, Heft 5-6 2006, 9 (12).

18 Vgl. *Roßnagel*, APuZ, Heft 5-6 2006, 9 (12). *Roßnagel*, MMR 2005, 71 (72).

19 *Roßnagel/Geminn/Jandt/Richter*, Datenschutzrecht 2016, S. 26.

20 Ähnlich *Forgó/Krügel*, DuD 2005, 732 (733), die von einer „sehr niedrigen Hürde“ für die Feststellung der Zweckidentität sprechen.

21 Vgl. *Roßnagel*, APuZ, Heft 5-6 2006, 9 (12 f.), der von einer „Freikarte“ zum Datenumgang für die verantwortliche Stelle spricht; ähnlich *Simitis*, NJW 1998, 2473 (2478), der die Gefahr einer Verwandlung in eine Leerformel durch Generalklauseln und unbestimmte Rechtsbegriffe sieht.

22 *Schulz/Roßnagel/David*, ZD 2012, 510 (515).

23 *Eifert*, in: Gropp/Lipp/Steiger (Hrsg.), FS Uni Gießen, S. 139 (142).

24 *Eifert*, in: Gropp/Lipp/Steiger (Hrsg.), FS Uni Gießen, S. 139 (141 f.); *Hoffmann-Riem*, in: Krämer/Micklitz/Tonner (Hrsg.), Recht und diffuse Interessen, S. 777 (779).

durch zahllose Ausnahmen „ausgehöhlt“[25] und müsse überdacht werden.[26] Aufgrund zahlreicher Zweckänderungsmöglichkeiten sei die Bezeichnung „Zweckbeschränkungsgrundsatz“ besser.[27] Das Zweckbindungsprinzip sei „(…) theoretisch eindrucksvoll, praktisch aber außerordentlich schwierig, wenn nicht unvollziehbar.“[28]

Andererseits wird in der Literatur die Bedeutung der Zweckbindung betont: Es gebe keine Alternativen, die die Leistungen der Zweckfestlegung in gleichwertiger Weise erfüllen könnten.[29] Die Zweckbindung sei „Dreh- und Angelpunkt eines wirklich effizienten Datenschutzes“[30]; werde sie gelockert, so schwinde die Transparenz und die Kontrolle gehe verloren.[31] Eine Aufweichung der Zweckbindung werde den „zentralen Stützpfeiler des bisherigen datenschutzrechtlichen Regulierungskonzepts destabilisieren.“[32] Die Zweckbindung diene als „Prüfanker“ der Rechtmäßigkeit des Datenumgangs während des gesamten Prozesses[33] und werde aufgrund zunehmender Verknüpfungen moderner IT-Systeme zum Schutz der Autonomie des Betroffenen immer wichtiger.[34] Die Multifunktionalität von IT-Systemen sei gerade der Grund für die Einführung der Zweckbindung, weshalb es heutzutage keinen Änderungsbedarf auf-

---

25 Es wird vertreten, dass die Zweckbindung nur noch bei für die LKW-Maut erhobenen Daten gewährleistet sei: *Bergmann/Möhrle/Herb*, BDSG, Systematik Ziff. 2.1.3.; auch im Rahmen der LKW-Maut gab es aber Versuche zur Durchbrechung der Zweckbindung, siehe AG Gummersbach, NJW 2004, 240 f.; eine Zulässigkeit der Zweckdurchbrechung für Zwecke der Strafverfolgung ablehnend *Niehaus*, NZV 2004, 502 (504); ebenso *Göres*, NJW 2004, 195 (197 f.).

26 *Bull*, ZRP 1998, 310 (314).

27 *Helbing*, K&R 2015, 145 (146).

28 *Badura*, in: Deutscher Bundestag (Hrsg.), Anhörungsbeitrag, S. 15 (16).

29 *Albers*, Informationelle Selbstbestimmung, S. 500.

30 So *Simitis*, CR 2000, 472 (474); ähnlich *Masing*, VVDStRL (63) 2004, 377 (399), der von einem „unangefochtenen Eckpfeiler jeden modernen Datenschutzes“ spricht; vgl. auch *Roßnagel/Laue*, DÖV 2007, 543 (545); *Kutscha*, ZRP 1999, 156 (157); *Simitis*, NJW 1984, 398 (402), die hierin das zentrale Element im Datenschutzkonzept des Bundesverfassungsgerichts sehen.

31 *Simitis*, CR 2000, 472 (474).

32 *Richter*, DuD 2015, 735.

33 *Pohle*, DANA 2015, 141 (142 f.).

34 *Jotzo*, Der Schutz personenbezogener Daten in der Cloud, S. 44.

grund technischer Weiterentwicklungen gebe.[35] Die Vielzahl von Daten, die in der heutigen Welt des Internets der Dinge anfalle, führe zu neuen Risiken aufgrund der Erkenntnisse durch die Zusammenführung von Daten aus unterschiedlichen Quellen[36] und der damit einhergehenden Lösung der Daten aus dem ursprünglichen Verwendungskontext.[37] Zwar werde die Zweckbindung durch Generalklauseln eingeschränkt, aber gerade aufgrund neuer technischer Entwicklungen solle ihr zu stärkerer Geltung verholfen werden.[38] Statt den Zweckbindungsgrundsatz abzuschaffen, bedürfe dieser einer „stärkeren Geltungskraft und Konkretisierung", da jede Restriktion zu einer Einschränkung der informationellen Selbstbestimmung führe.[39] Darüber hinaus wird die Bedeutung der Zweckbindung auch aus wettbewerbsrechtlicher Sicht zur Vermeidung eines ungebührlichen Vorteils eines marktbeherrschenden Unternehmens gegenüber Neueinsteigern betont.[40]

II. Gang der Untersuchung

Ziel der Arbeit ist die Analyse der Vereinbarkeit von Big Data mit dem Grundsatz der Zweckbindung und das Aufzeigen von Lösungsmöglichkeiten im Falle der Nichtvereinbarkeit mit dem derzeit geltenden Recht.[41]

Es soll zunächst eine Definition des Begriffs Big Data erarbeitet werden. Dann soll untersucht werden, ob und inwiefern Big Data und der da-

---

35 *Pohle*, DANA 2015, 141 (143).

36 Vgl. *Artikel-29-Datenschutzgruppe*, WP 223, S. 8 f.

37 Auf dieses Risiko der automatisierten Datenverarbeitung wies *Simitis*, NJW 1984, 398 (402) schon frühzeitig hin.

38 *Kutscha*, ZRP 1999, 156 (160).

39 *Scholz*, in: Roßnagel (Hrsg.), Handbuch DSR, Kap. 9.2 Rn. 74; für eine Stärkung der Zweckbindung siehe auch: *Datenschutzkonferenz des Bundes und der Länder*, DSR 21. Jh., S. 6 und 10 f.

40 Vgl. *Artikel-29-Datenschutzgruppe*, WP 221, S. 3.

41 Dabei wird sich zeigen, ob tatsächlich durch Big Data keine neuen rechtlichen Fragen aufgeworfen werden, wie *Bull*, Sinn und Unsinn, S. 36, behauptet, der davon ausgeht, dass es sich um eine Summe bereits bekannter Einzelfragen handele.

tenschutzrechtliche Zweckbindungsgrundsatz miteinander kollidieren. Hierzu werden Regelungen zur Zweckbindung im BDSG a. F., der DSRL, der DSGVO und dem BDSG 2018 betrachtet. Zum Abschluss werden verschiedene in der Literatur genannte Lösungsvorschläge diskutiert und ein eigener Vorschlag formuliert.

Die Untersuchung bezieht sich in weiten Teilen auf seit dem 25. Mai 2018 nicht mehr geltende Rechtsvorschriften. Da das Zweckbindungsprinzip auch in der DSGVO enthalten ist, können viele Überlegungen aber auch unter diesem neuen Rechtsregime fortgelten. Auch die Aussagen des BVerfG sind aufgrund der weiteren Europäisierung des Datenschutzrechts mit der DSGVO – zumindest für den nichtöffentlichen Bereich – nur sehr vorsichtig nutzbar.

B. Big Data

Zunächst gilt die Frage zu klären, was genau sich hinter dem Schlagwort „Big Data“ verbirgt. Problematisch ist hierbei, dass es sich nicht um einen klar definierbaren Begriff handelt. Daher ist eine Erläuterung des Begriffs mithilfe mehrerer Merkmale notwendig. Zudem soll auf den technischen Hintergrund eingegangen und zur Veranschaulichung einige Anwendungsbeispiele geschildert werden.

I. Definition

1. Problem der Definition

Der Begriff Big Data oder auch Smart Data[42] findet sich derzeit in einer Vielzahl von Publikationen.[43] Gleichwohl hat sich keine eindeutige Begriffsdefinition herausgebildet.[44] Der Begriff ist vielmehr zu Recht als „schillernd“ [45] bezeichnet worden. Nicht zuletzt deswegen bemühen sich

42 *Bornemann*, RDV 2013, 232 (234); *Boehme-Neßler*, in: Rehbinder (Hrsg.), UFITA 2015 I, 19 (22) scheint unter Smart Data die mittels Analyse aus einer Datenmenge (Big Data) gewonnenen Informationen zu verstehen; ähnlich *Bretthauer*, ZD 2016, 267 (268), der den Schwerpunkt bei der Betrachtung der Analyseergebnisse sieht. *Raabe/Wagner*, DuD 2016, 434 (437) sehen ein wesentliches Merkmal in einer gezielten Selektion der Daten bereits zum Zeitpunkt der Erhebung. Letzlich handelt sich dabei um Wortklauberei. Es wird dasselbe Phänomen beschrieben.

43 Siehe z. B. *Geiselberger/Moorstedt*, Big Data; *Mayer-Schönberger/Cukier*, Big Data; zur Verbreitung des Begriffs in der deutschen Presse in 2013-2014, siehe *Waidner*, Big Data, S. 54.

44 *Crawford/Schultz*, Boston College Law Review Vol. 55, 2014, 93 (96).

45 *Härting*, CR 2014, 528; *Spiecker genannt Döhmann*, Spektrum der Wissenschaft Spezial - Physik, Mathematik, Technik 1. 2017, 56.

derzeit Standardisierungsorganisationen um die Erarbeitung einer Definition.[46]

Im Kern geht es um das Auswerten großer Datenmengen mittels Algorithmen zwecks Feststellung bislang unbekannter Korrelationen.[47] Es handelt sich nicht um eine einzelne neue Technologie, sondern mehrere neue Methoden.[48] Gleichwohl gibt es eine Reihe von Merkmalen, die immer wieder genannt werden.[49] Allen Definitionen gemein ist, dass sie die „3 Vs" enthalten – *volume*, *velocity* und *variety*, die auf eine Definition der Unternehmensberatung *Gartner* zurückgehen.[50]

2. Volume

Ursprünglich wurde alleine auf die Größe der Datenmenge abgestellt um den Begriff Big Data zu definieren.[51] Auch heute ist die Größe ein wichtiges Element der Definition. Demnach soll Big Data gegeben sein, wenn die Datenmenge so groß ist, dass sie nicht innerhalb einer vertretbaren Zeit von üblicher Software erhoben, gespeichert und verarbeitet werden kann.[52] Im Jahr 2013 wurde von einer weltweiten Datenmenge von 2,8 Zettabyte ausgegangen.[53] Es wird geschätzt, dass sich die weltweit

---

46 Siehe *ISO IEC JTC 1 - Information technology*, Big Data; *National Institute of Standards and Technology*, Volume 1, Definitions.

47 *Hartzog/Selinger*, 66 Stanford Law Review Online 2013, 81 (81); *Roßnagel*, ZD 2013, 562; *Boehme-Neßler*, in: Rehbinder (Hrsg.), UFITA 2015 I, 19 (23 f.).

48 *Horvath*, Big Data, S. 1.

49 Siehe hierzu das Schaubild bei *BITKOM (Hrsg.)*, Leitfaden 2014, S. 10.

50 Siehe *Laney*, 3D Data management, die Meta-Group wurde später von *Gartner* übernommen; *Hackenberg*, in: Hoeren/Sieber/Holznagel (Hrsg.), Handbuch Multimedia-Recht, Teil 16.7 Rn. 1.

51 *Manovich*, in: Gold (Hrsg.), S. 460 (460).

52 *Cavoukian/Jonas*, Privacy by Design, S. 3; *Roßnagel*, ZD 2013, 562; *Wespi*, digma 2013, 10; *Feiler/Fina*, medien und recht 2013, 303; *Bornemann*, RDV 2013, 232 (234) stellt darauf ab, dass die Daten „noch nicht immer mit Hilfe von Standarddatenbanken und Datenmanagementtools verarbeitet werden können."

53 *Bornemann*, RDV 2013, 232; *Weichert*, ZD 2013, 251 (252); ein Zettabyte entspricht einer Billionen Gigabyte.

verfügbare Datenmenge alle zwei Jahre verdoppelt.[54] Dies liegt nicht zuletzt daran, dass jegliche Art der Internetnutzung digitale Datenspuren hinterlässt.[55] Über das Internet soll im Jahr 2015 eine Datenmenge von 60 Exabyte pro Monat bewegt worden sein.[56] Derzeit steigt die Datenmenge exponentiell an. So sollen 90 Prozent der im Jahr 2014 weltweit existenten Daten erst in den zwei Jahren zuvor entstanden sein.[57]

In der Annahme, dass die Ergebnisse umso besser werden, je größer die Datenmenge ist,[58] besteht ein großer Anreiz möglichst viele Daten für lange Zeit aufzubewahren und mit anderen Daten zusammenzuführen.[59] Ob dies tatsächlich immer zu besseren Ergebnissen führt, sei dahingestellt.[60] Zweifel sind angebracht, da nicht mehr zutreffende Daten das Ergebnis verfälschen können. Jedenfalls ist ein wesentliches Merkmal von Big Data die große Menge der zu verarbeitenden Daten.[61] Aufgrund der steigenden Leistungsfähigkeit moderner IT ist ein alleiniges Abstellen auf die Größe der zu verarbeitenden Daten aber kein Erfolg versprechender Ansatz mehr.[62]

---

54 *Polzer*, digma 2013, 6; ähnlich *Weichert*, ZD 2013, 251 (252); *Dapp/Heine*, Big Data, S. 7; neuere Schätzungen gehen sogar von einer Verdoppelung der Datenmende alle 12 Monate aus, siehe: *Helbing/Frey/Gigerenzer/Hafen/Hagner/Hofstetter/Hoven/Zicari/Zwitter*, Spektrum der Wissenschaft Spezial - Physik, Mathematik, Technik 1. 2017, 7 (9).

55 Siehe hierzu: *Grimm*, DuD 2012, 88.

56 *Schaar*, Überwachung, S. 82; ein Exabyte sind eine Milliarde Gigabyte.

57 *de Wachter*, CRi 2014, 1.

58 *Härting*, Internetrecht, Annex Rn. 31.

59 *Roßnagel*, ZD 2013, 562.

60 In diese Richtung aber *Koch*, itrb 2015, 13 (15), der davon ausgeht, dass Big-Data-Anwendugnen nur bei großen Datenmengen ihre volle Leistungsfähigkeit zur Geltung bringen können.

61 *Rubinstein*, International Data Privacy Law 2013, 74 (77); *Ehmann*, Lexikon IT-Recht, S. 71.

62 Vgl. *Boyd/Crawford*, Information, Communication & Society 2012, 662 (663).

3. Velocity

Mit dem Begriff *velocity* wird die Geschwindigkeit der Datenverarbeitung in den Blick genommen. Big-Data-Anwendungen zielen darauf ab, möglichst in Echtzeit Ergebnisse zu liefern.[63] Möglich wird dies durch einen stetigen Anstieg der weltweiten Rechnerleistung, die sich laut Schätzungen alle neun Monate verdoppelt.[64] Teilweise wird auch die hohe Geschwindigkeit des Entstehens der Daten in die Definition dieses Begriffs mit aufgenommen.[65]

4. Variety

Es ist nunmehr möglich mit nicht-relationalen Datenbanken sowohl strukturierte als auch unstrukturierte Daten zu verarbeiten.[66] Zu den unstrukturierten Daten gehören beispielsweise Textdokumente oder Audio- und Videodaten.[67] Es gibt also eine Vielzahl von Daten in unterschiedlichen Formaten und aus verschiedenen Quellen.[68]

5. Veracity

Die Genauigkeit der Daten wird aufgrund der Vielzahl der Daten und der Vielzahl der Quellen immer wichtiger.[69] Daher soll eine Aussage über

63 *Ulmer*, RDV 2013, 227.

64 *de Wachter*, CRi 2014, 1; andere Schätzungen gehen von einer Verdopplung alle 18 Monate aus, siehe *Helbing/Frey/Gigerenzer/Hafen/Hagner/Hofstetter/Hoven/Zicari/Zwitter*, Spektrum der Wissenschaft Spezial - Physik, Mathematik, Technik 1. 2017, 7 (9).

65 So *ISO IEC JTC 1 - Information technology*, Big Data, S. 10.

66 *ISO IEC JTC 1 - Information technology*, Big Data, S. 10; a. A. anscheinend: *Ehmann*, Lexikon IT-Recht, S. 71, mit der Auffassung, dass unstrukturierte Daten nicht in Datenbanken gespeichert werden.

67 *Wespi*, digma 2013, 10.

68 *BITKOM (Hrsg.)*, Leitfaden 2012, S. 21.

69 So auch *Boyd/Crawford*, Information, Communication & Society 2012, 662 (668); a. A. *Martini*, DVBl 2014, 1481 (1482), der vielmehr davon ausgeht, dass

die Richtigkeit der Daten mit in die Datenverarbeitung einfließen.[70] Gerade wenn es um Prognosen und Wahrscheinlichkeiten geht, ist die Genauigkeit der Daten von großer Bedeutung.[71]

6. Value

Vor allem von Autoren aus der Praxis wird als weiteres Merkmal *value* angeführt. Hierbei geht es um den – insbesondere wirtschaftlichen – Mehrwert, der mit Hilfe der Datenanalyse gewonnen werden kann.[72]

7. Variability

Als zusätzliches Element wird *variability* vorgeschlagen. Gemeint ist hiermit die Veränderlichkeit der Daten, z. B. des Formats oder der Zusammensetzung.[73] Es handelt sich um eine Veränderung der anderen Merkmale, die Auswirkungen auf die Analyse und die dazu verwendete Infrastruktur haben kann.[74]

---

bei einer Vielzahl von Daten sich „Unschärfen in der Datenerhebung" hinnehmen lassen und es sich bei der Genauigkeit der Daten nicht um ein Wesensmerkmal handele.

70 *Wespi*, digma 2013, 10.

71 *Hackenberg*, in: Hoeren/Sieber/Holznagel (Hrsg.), Handbuch Multimedia-Recht, Teil 16.7 Rn. 5.

72 *Ulmer*, RDV 2013, 227 (228); kritisch hierzu: *Boyd/Crawford*, Information, Communication & Society 2012, 662 (668 ff.), die in Frage stellen, ob die Auswertung großer Datenmengen tatsächlich immer zu einem Mehrwert gegenüber der Auswertung geringer Datenmengen führt.

73 Siehe *National Institute of Standards and Technology*, Volume 1, Definitions, S. 15; *ISO IEC JTC 1 - Information technology*, Big Data, S. 10 f.

74 *ISO IEC JTC 1 - Information technology*, Big Data, S. 10 f.

8. Analytics

Teilweise wird noch der Begriff *analytics* mit in den Versuch einer Begriffsdefinition aufgenommen.[75] Hierbei geht es um die Auswertung der Daten mittels verschiedener statistisch-mathematischer Verfahren.[76] Zu diesen Verfahren zählen Data Mining, Text- und Bildanalyse, Optimierungsalgorithmen und Vorhersagemodelle.[77] Das Ziel ist, bislang unbekannte Muster und Korrelationen in den Datenbeständen zu entdecken.[78] Möglich wird dies durch sog. Algorithmen. Sehr allgemein formuliert enthalten Algorithmen eine Formel, die sowohl eine Aufgabe als auch die Schritte zu ihrer Lösung enthält.[79] Sie können daher „(…) schematisch vollzogen werden, ohne dass der Sinn des Vollzugs mitbedacht werden müßte (sic).“[80]

Die Algorithmen können im Rahmen des Data Minings sowohl für sog. supervised als auch für unsupervised learning eingesetzt werden.[81] Supervised learning findet mit Daten statt, denen durch die Zuordnung zu einer Kategorie (z. B. Auto, Fahrrad; gut, sehr gut) oder eines numerischen Werts (z. B. der Verkaufspreis für ein Objekt) ein Muster entnommen und dieses auf andere Fälle übertragen werden kann.[82] Unsupervised learning wird auf Daten angewendet, die mit keinerlei Attributen versehen sind, so dass ihnen nicht bereits ein Muster entnommen werden kann, sondern

---

75 So *BITKOM (Hrsg.)*, Leitfaden 2012, S. 21; *Helbing*, K&R 2015, 145; *Martini*, DVBl 2014, 1481 (1482) spricht von „analysis“.

76 Für eine Übersicht zu diesen Verfahren siehe: *McKinsey Global Institute (Hrsg.)*, Big Data, S. 27 ff.

77 *BITKOM (Hrsg.)*, Leitfaden 2012, S. 21.

78 *Cavoukian*, Data Mining, S. 4; *Scholz*, in: Roßnagel (Hrsg.), Handbuch DSR, Kap. 9.2 Rn. 3.

79 *Gillespie*, in: Gillespie/Boczkowski/Foot (Hrsg.), Media Technologies, S. 167 (167); *de Wachter*, CRi 2014, 1 (2); vgl. *Barth*, Algorithmik, S. 8 f.

80 *Luhmann*, Zweckbegriff, S. 317.

81 *The President's Council of Advisors on Science and Technology*, Big Data, S. 24.

82 *The President's Council of Advisors on Science and Technology*, Big Data, S. 24; *Bramer*, Data Mining, S. 4 spricht insofern von “labelled data”.

Korrelationen erst entdeckt werden müssen.[83] Im Rahmen des supervised learning werden sog. klassifizierende Algorithmen eingesetzt, wenn es um die Zuordnung zu einer Kategorie geht und sog. Regressionsalgorithmen wenn es sich um die Ermittlung eines numerischen Werts handelt.[84]

Die Algorithmen können sich automatisch durch die Eingabe neuer Daten verändern, wie beispielsweise eine Suchmaschine durch die eingegebenen Suchbegriffe und Klicks.[85] Bei den Algorithmen könne zwischen zwei grundsätzlich unterschiedlichen Zielsetzungen unterschieden werden. Einerseits der rückblickenden Auswertung von Daten im Hinblick auf darin vorliegende Muster.[86] Andererseits der sog. prädiktiven Analyse bei der es um Vorhersagen zukünftigen Verhaltens geht.[87] Ob eine derart schematische Trennung tatsächlich möglich ist, ist allerdings zweifelhaft. Denn oft wird gerade die rückblickende Auswertung im Hinblick auf Muster Grundlage einer in die Zukunft gerichteten Prognose sein. Weitere Möglichkeiten der Analyse mittels Algorithmen sind die Zuordnung zu Kategorien aufgrund ähnlicher Merkmale (clustering), das Feststellen von Anomalien, die Zusammenfassung von Merkmalen als statistische Werte oder die Auflistung von Merkmalen und die Ermittlung von Korrelationen mittels unsupervised learning.[88]

---

83 *The President's Council of Advisors on Science and Technology*, Big Data, S. 24; *Bramer*, Data Mining, S. 5, nennt dies "unlabelled data".

84 *Bramer*, Data Mining, S. 5; *The President's Council of Advisors on Science and Technology*, Big Data, S. 24; *Grund*, in: Deggendorfer Forum zur digitalen Datenanalyse e.V. (Hrsg.), Big Data, S. 29 (33).

85 *Gillespie,* in: Gillespie/Boczkowski/Foot (Hrsg.), Media Technologies, S. 167 (173).

86 *BITKOM (Hrsg.)*, Leitfaden 2013, S. 47; *Hackenberg*, in: Hoeren/Sieber/Holznagel (Hrsg.), Handbuch Multimedia-Recht, Teil 16.7 Rn. 59.

87 *BITKOM (Hrsg.)*, Leitfaden 2013, S. 47.

88 Vgl. *The President's Council of Advisors on Science and Technology*, Big Data, S. 24.

9. Abgrenzung zu früherem Data Warehouse / Data Mining bzw. Business Intelligence

Bereits früher gab es sog. Data Warehouses, in denen mit Data Mining gearbeitet wurde.[89] Oft wird dies als „Business Intelligence" bezeichnet bzw. dieser zugeordnet.[90] Im Data Warehouse wurden viele der von der verantwortlichen Stelle erhobenen Daten gespeichert, indem sie aus dem operativen Bestand überführt wurden.[91] Das Ziel war, die Daten für unterschiedliche Zwecke nutzen zu können.[92] Dabei ging es – wie bei Big Data – insbesondere um die Aufdeckung bislang unbekannter Zusammenhänge mittels Data Mining.[93] Es fand allerdings keine sofortige Auswertung aktuell anfallender Daten statt.[94] Letztlich handelte es sich um eine kontext- und zweckfreie Speicherung[95] um diese zur Gewinnung neuer Erkenntnisse auszuwerten.[96] Daher findet sich seitens der Aufsichtsbehörden die Auffassung, dass es sich um eine unzulässige Vorratsdatenspeicherung für unbestimmte Zwecke handele[97] und eine Einwilligung wegen der Zweckoffenheit unwirksam sei.[98]

Durch das Speichern der Daten im Arbeitsspeicher (sog. In-Memory-Verfahren) wird eine im Vergleich zu früher viel größere Verarbeitungs-

---

89 *Baeriswyl*, digma 2013, 14. *Baeriswyl*, RDV 2000, 6; siehe auch *Datenschutzkonferenz des Bundes und der Länder*, Entschließung Data Warehouse.

90 *BITKOM (Hrsg.)*, Leitfaden 2012, S. 24; *Cleve/Lämmel*, Data Mining, S. 3.

91 *Büllesbach*, CR 2000, 11 (12).

92 *Cavoukian*, Data Mining, S. 4; *Scholz*, in: Roßnagel (Hrsg.), Handbuch DSR, Kap. 9.2 Rn. 3; *Taeger*, K&R 2003, 220, der vor allem auf Marketingaktivitäten abstellt. *Weichert*, DuD 2001, 264 (268) bezeichnet ein Data Mining mit personenbezogenen Daten pauschal als „zweifellos unzulässig".

93 *Büllesbach*, CR 2000, 11 (14); *Sokol/Tiaden*, in: Bizer/Lutterbeck/Riß (Hrsg.), Big Brother, S. 161 (164 f.).

94 *Koch*, itrb 2015, 13 (14); *Ulmer*, RDV 2013, 227, Fn. 3.

95 *Weichert*, RDV 2003, 113 (119); *Martini*, DVBl 2014, 1481 (1484).

96 *Buchner*, DuD 2016, 155 (156).

97 *Möncke*, DuD 1998, 555 (558); *Datenschutzkonferenz des Bundes und der Länder*, Entschließung Data Warehouse.

98 Vgl. *Datenschutzkonferenz des Bundes und der Länder*, Entschließung Data Warehouse.

geschwindigkeit erreicht.[99] Es soll hierdurch eine Beschleunigung um mehr als den Faktor 1000 möglich sein.[100] Neu ist zudem, dass es bei Big Data in großem Maße um Prognosen zukünftiger Entwicklungen geht, während früher vor allem Geschehnisse rückblickend bewertet wurden.[101]

a) von SQL zu NoSQL

Früher erfolgte eine Speicherung in relationalen Datenbanken.[102] Die Daten wurden in Zeilen und Spalten gespeichert.[103] Hierzu kam die Computersprache *SQL - structured query language* zum Einsatz.[104] Es wurde also beispielsweise in einer Datenbank jeweils in einem bestimmten Feld ein spezifischer Datentyp in einem bestimmten Format gespeichert.[105] Nunmehr können die Daten auch nicht-relational gespeichert werden (*NoSQL - not only structured query language*).[106] Dies ermöglicht das Speichern unstrukturierter Daten.

Früher mussten die Daten also zunächst in ein der relationalen Speicherung entsprechendes Format gebracht werden.[107] Erst danach konnten sie ausgewertet werden.[108] Dies wird als ETL-Prozess bezeichnet, d. h. Extract-Transform-Load.[109] Demgegenüber hat die nicht-relationale Spei-

---

99 *BITKOM (Hrsg.)*, Leitfaden 2014, S. 24.

100 *Stiemerling*, in: Conrad/Grützemacher (Hrsg.), Recht der Daten und Datenbanken, § 6 Rn. 25 ff; *BITKOM (Hrsg.)*, Leitfaden 2014, S. 24.

101 *Hackenberg*, in: Hoeren/Sieber/Holznagel (Hrsg.), Handbuch Multimedia-Recht, Teil 16.7 Rn. 9.

102 Siehe hierzu: *Stiemerling*, in: Conrad/Grützmacher (Hrsg.), Recht der Daten und Datenbanken, § 5 Rn. 2 ff.

103 *McKinsey Global Institute (Hrsg.)*, Big Data, S. 33.

104 *McKinsey Global Institute (Hrsg.)*, Big Data, S. 33.

105 *Cumbley/Church*, CLSR 29 (2013), 601 (602).

106 *BITKOM (Hrsg.)*, Leitfaden 2012, S. 27; *Koch*, itrb 2015, 13 (14).

107 *Hackenberg*, in: Hoeren/Sieber/Holznagel (Hrsg.), Handbuch Multimedia-Recht, Teil 16.7 Rn. 7; *Möller*, DuD 1998, 555 (555 f.), verwendet hierfür das Bild der „fein säuberlich nummerierten" Einordnung der Daten in ein Regal.

108 *Hackenberg*, in: Hoeren/Sieber/Holznagel (Hrsg.), Handbuch Multimedia-Recht, Teil 16.7 Rn. 7.

109 *BITKOM (Hrsg.)*, Leitfaden 2014, S. 27.

cherung den Vorteil, dass der Transformationsprozess erst zum Schluss erfolgt (ELT).[110] Dies ermöglicht eine schnellere Verfügbarkeit der relevanten Daten und es können stets diejenigen Daten geladen werden, die benötigt werden.[111] Big Data benötigt also – anders als klassisches Data Mining – keinen bereits aufgearbeiteten Datenbestand.[112]

b) Hadoop, map reduce

Für die Auswertung der Daten ist der Map-Reduce-Algorithmus von großer Bedeutung, der durch Aufteilung der Auswertung die Analyse großer Datenmengen ermöglicht.[113] Map Reduce geht in zwei Schritten vor. So wird durch die Map-Funktion beispielsweise die Häufigkeit des Auftretens eines Wortes in einem bestimmten Text gezählt.[114] Durch die Reduce-Funktion wird dann die Summe dieser Zählung gebildet.[115] Die Auswertung kann unter Nutzung eines „divide-and-conquer-Ansatzes" parallel auf mehreren Rechner-Knoten unabhängig voneinander ausgeführt werden.[116] Ermöglicht wird das Berechnen mehrerer Petabyte an Daten z. B. durch das Framework Hadoop, das den Map-Reduce-Algorithmus auf mehreren Rechner-Knoten gleichzeitig implementiert und zudem skalierbar ist.[117] Möglich wird die Auswertung auf vielen verschiedenen Rechner-Knoten durch das Cloud-Computing[118], dass das

110 *BITKOM (Hrsg.)*, Leitfaden 2014, S. 27.
111 *Hackenberg*, in: Hoeren/Sieber/Holznagel (Hrsg.), Handbuch Multimedia-Recht, Teil 16.7 Rn. 7.
112 *Hackenberg*, in: Hoeren/Sieber/Holznagel (Hrsg.), Handbuch Multimedia-Recht, Teil 16.7 Rn. 8.
113 Vgl. *Karjoth*, digma 2013, 4; *Wartala*, Hadoop, S. 17.
114 *Ranger/Raghuraman/Penmetsa/Bradski/Kozyrakis*, 2007 IEEE 13th International Symposium on High Performance Computer Architecture 2007, S. 2.
115 *Ranger/Raghuraman/Penmetsa/Bradski/Kozyrakis*, 2007 IEEE 13th International Symposium on High Performance Computer Architecture 2007, S. 2; *Dean/Ghemawat*, Map Reduce, S. 1 f.
116 *Polzer*, digma 2013, 6 (7).
117 *Karjoth*, digma 2013, 4; Vgl. *Wartala*, Hadoop, S. 21.
118 Zum Begriff siehe *Jotzo*, Der Schutz personenbezogener Daten in der Cloud, S. 19 f.; *Hornung/Sädtler*, CR 2012, 638.

kurzfristige Nutzen von Rechner- und Speicherkapazitäten ermöglicht, ohne dass diese Kapazitäten dauerhaft vorgehalten werden müssen.[119] Zudem war früher die Auswertung auf den Datenbestand im eigenen Data Warehouse begrenzt, während nunmehr mittels Cloud Computing auf eine Vielzahl anderer Daten zugegriffen werden kann.[120] Gerade die horizontale Skalierung auf mehreren Rechnerknoten wird teils als wesentliches Merkmal von Big Data angesehen.[121]

Big Data ist als eine mächtigere Version der Wissensgewinnung in Datenbanken unter Einsatz von Data Mining bezeichnet worden.[122] Es handelt sich um eine Weiterentwicklung der früheren Technologien.[123]

10. Zwischenergebnis

Die Vielzahl an Merkmalen verdeutlicht wie schwer eine Definition des Begriffs Big Data ist. Den Kern bilden aber die ursprünglichen und am weitesten verbreiteten Merkmale: *volume*, *velocity* und *variety*. Die weiteren genannten Attribute deuten eher auf einzelne Elemente hin, die bei der Durchführung einer Big-Data-Analyse eine Rolle spielen oder von Interessengruppen aus Marketingzwecken genannt werden, wie im Falle des Merkmals *value*. Aufgrund der Vielgestaltigkeit der Erscheinungsformen ist eine präzise Definition leider nicht möglich, weshalb recht abstrakt von Big Data als automatischer Auswertung großer, heterogener Datenmengen in Echtzeit zur Feststellung bislang unbekannter Korrelationen auszugehen ist.

---

119 *Helbing*, K&R 2015, 145.

120 *Baeriswyl*, digma 2013, 14.

121 Im Gegensatz zu einer „vertikalen Skalierung“ durch Erhöhung der Leistung eines einzelnen Rechners, siehe *National Institute of Standards and Technology*, Volume 1, Definitions, S. 5.

122 *Rubinstein*, International Data Privacy Law 2013, 74 (76).

123 *Liedke*, K&R 2014, 709; *Ohrtmann/Schwiering*, NJW 2014, 2984 (2984); dies verkennen *Dix/Mallmann*, in: Simitis (Hrsg.), BDSG, § 6 Rn. 10, die Big Data mit Data Warehousing und Data Mining gleichsetzen.

II. Anwendungsbeispiele

Aufgrund der Weite der Definition werden im Folgenden zur Verdeutlichung verschiedene Anwendungsbeispiele von Big-Data-Analysen aufgeführt.

1. Gefahrenabwehr / Strafverfolgung

Im Bereich der Gefahrenabwehr heißt das neue Zauberwort „Predictive Policing".[124] Es geht darum Kriminalitätsschwerpunkte zu identifizieren und bereits vor Begehung einer Straftat präventiv vor Ort Präsenz zu zeigen.[125] Insbesondere in US-amerikanischen Städten wird diese Methode bereits eingesetzt und soll zu einem Rückgang der Kriminalität geführt haben.[126]

2. Gesundheitswesen

Mittels einer Vielzahl von Daten über Krankheitsfälle können wichtige Rückschlüsse auf Nebenwirkungen von Medikamenten geschlossen werden. So wurde das Schmerzmittel Vioxx vom Markt genommen, als durch einen Abgleich von Daten der Krankenversicherungen und der Krankenhäuser ein Zusammenhang zwischen der Einnahme des Medikaments und einer erhöhten Zahl von Herzinfarkten festgestellt werden konnte.[127] Auch bei der Vorhersage der Ausbreitung von Krankheiten

---

124 *Schaar*, Überwachung, S. 84.

125 *Schaar*, Überwachung, S. 84.

126 Siehe *Evgeny Morozov*, in: FAZ, 7. August 2012, Nr. 182, S. 32: *Effizienter als die Polizei,* mit dem Beispiel Los Angeles, wo die Kriminalität im Einsatzgebiet um 13 Prozent gesunken sein soll; zur Entwicklungen in den deutschen Ländern siehe *Ulrike Heitmüller*, Predictive Policing: Die deutsche Polizei zwischen Cyber-CSI und Minority Report, heise online; https://heise.de/-3685873 (abgerufen am 11.05.2018).

127 *Tene/Polonetsky*, Stanford Law Review Online 2012, 63 (64).

mögen Big-Data-Anwendungen hilfreich sein.[128] Wie akkurat diese Vorhersagen sind, wird aber teilweise angezweifelt. So sah sich die Vorhersage der Ausbreitung einer Grippewelle durch Google Flu Trends[129] erheblicher Kritik ausgesetzt und es wurde festgestellt, dass die von Google Flu Trends prognostizierten Zahlen mehr als doppelt so hoch waren wie die auf den Auswertungen von Gesundheitseinrichtungen in den USA beruhenden Zahlen.[130]

Ein weiteres Beispiel ist die sog. Selbstvermessung des Menschen (quantified self). Der Begriff quantified self beschreibt die Möglichkeit, dass Menschen durch tragbare Messgeräte (wearables) Daten über sich erheben und ihre Gesundheit und ihr Verhalten analysieren können.[131] Diese Daten können zugleich für Krankenversicherungen sehr interessant sein, die Preisnachlässe anbieten, wenn die Versicherten nach Einschätzung der Krankenkasse gesund leben.[132]

3. Verkehrstelematik

Das Sammeln und Auswerten von GPS-Daten der Verkehrsteilnehmer ermöglicht den Einsatz intelligenter Mautsysteme,[133] die durch eine unterschiedliche Bepreisung zu Haupt- und Nebenverkehrszeiten eine Steuerungswirkung des Verkehrs erreichen können.[134] Moderne Navigations-

---

128 Siehe *Tene/Polonetsky*, Stanford Law Review Online 2012, 63 (64) mit dem Beispiel Google Flu Trends.

129 Siehe hierzu: *Ginsberg/Mohebbi/Patel/Brammer/Smolinski/Brilliant*, nature 2009, 1012; *Corinna Budras*, in: FAS v. 16.11.2014, S. 24: *Google weiß, wo die Grippe lauert*.

130 *Lazer/Kennedy/King/Vespignani*, Science 2014, 1203 (1203 f.).

131 *Schumacher*, in: Langkafel (Hrsg.), Big Data in der Medizin, S. 227 (228).

132 Siehe *Niklas Maak,* in: FAZ v. 27.11.2014, S. 11: *Die Veröffentlichung unserer Körper*, zu einem entsprechenden Angebot der Versicherung „Generali".

133 Auf einen Vertrauensverlust der Betroffenen im Falle einer Aufweichung einer strengen Zweckbindung im Bereich von Verkehrstelematik weisen *Schulz/Roßnagel/David*, ZD 2012, 510 (515) hin; für Mautsysteme siehe bereits *Roßnagel*, NZV 2006, 281 (287).

134 *Tene/Polonetsky*, Stanford Law Review Online 2012, 63 (64 f.).

systeme können ihre Nutzer auf Staus hinweisen und eine Alternativroute vorschlagen.

4. Betrugsbekämpfung

Bei der Betrugsbekämpfung, z. B. im Zahlungsverkehr aber auch bei der Abrechnung von Leistungen im Gesundheitswesen, kommen Big-Data-Analysen zum Einsatz.[135] Zur Vermeidung von Insiderhandel an den Finanzmärkten wird der Handel mit Wertpapieren überwacht, um auffällige Transaktionen zu entdecken.[136]

5. Scoring

Das Scoring dient gemäß § 28b BDSG a. F. zur Entscheidung über die Begründung, Durchführung oder Beendigung eines Vertragsverhältnisses.[137] Hierzu wird ein Wahrscheinlichkeitswert, der sog. „Score" ermittelt. Für die Berechnung des Wahrscheinlichkeitswertes wird versucht mittels eines mathematisch-statistischen Analyseverfahrens unter Nutzung von Erfahrungswerten aus der Vergangenheit eine Prognose über

---

135 Siehe *Bernd Kling*, *IBM will Big Data und Analytics für Betrugsbekämpfung nutzen*, ZDNet, 21. März 2014, http://www.zdnet.de/88187969/ibm-will-big-data-und-analytics-fuer-betrugsbekaempfung-nutzen, (abgerufen am 11.05.2018).

136 Siehe hierzu: *Grund*, in: Deggendorfer Forum zur digitalen Datenanalyse e.V. (Hrsg.), Big Data, S. 29 (37 ff.).

137 Ein Scoring zu Werbezwecken wird hiervon nicht erfasst, da es sich lediglich um die Vorstufe eines Vertragsschlusses handelt; so auch *Ehmann*, in: Simitis (Hrsg.), BDSG, § 28b Rn. 45; *Helfrich*, in: Hoeren/Sieber/Holznagel (Hrsg.), Handbuch Multimedia-Recht, Teil 16.4 Rn. 83, der terminologisch verwirrend aufgrund der Festlegung auf Zwecke im Zusammenhang mit Vertragsverhältnissen von einer „Zweckbindung" spricht; vgl. ferner *Kamlah*, in: Plath (Hrsg.), BDSG/DSGVO, § 28b Rn. 9; a. A. *Bergmann/Möhrle/Herb*, BDSG, § 28b Rn. 20 unter Berufung darauf, dass Sinn und Zweck der Norm für eine Regulierung sämtlicher Scoringverfahren spreche.

das zukünftige Verhalten des Betroffenen zu erstellen.[138] Diese Erfahrungswerte beruhen unter anderem auf statistischen Daten zu anderen Personen mit vergleichbaren Merkmalen.[139]

6. Profiling

Es ist nunmehr sowohl unter technischen, als auch wirtschaftlichen Gesichtspunkten denkbar, durch Zusammenführung vieler Daten aus unterschiedlichen Quellen sehr genaue Persönlichkeitsprofile zu erstellen.[140] Beispielsweise können Kommunikationsdaten (Twitter, E-Mail) mit Daten der Internetnutzung (Cookies) und von Sensoren (GPS- oder Standortdaten eines Smartphones oder eines Navigationsgeräts) zu einem umfassenden Bild über den Betroffenen zusammengeführt werden.[141] Im Bereich des Online-Marketings wird eine entsprechende Profilbildung aufgrund des Surfverhaltens häufig als *behavioral targeting* bezeichnet.[142] Aufgrund präziser Nutzerprofile und der Auswertung einer großen Zahl an Verkaufsdaten konnte beispielsweise *Amazon* eine Empfehlungsfunktion anbieten, die Kunden nahelegt ein weiteres Buch zu kaufen, da sich andere Käufer des Buches x auch für Buch y entschieden haben.[143] Es soll möglich sein abwanderungswillige Kunden zu erkennen oder Retouren im Versandhandel durch bessere Empfehlungen zu vermeiden.[144] Denkbar ist ebenso eine an das durchschnittliche Einkaufverhalten der Kunden angepasste Anordnung der Produkte in einem Supermarkt.[145]

---

138 Vgl. *Beckhusen*, BKR 2005, 335 (336).
139 *Weichert*, ZRP 2014, 168.
140 Vgl. *Schaar*, RDV 2013, 223 (225).
141 *Koch*, itrb 2015, 13 (14).
142 Siehe *Zuiderveen Borgesius*, CLSR 32 (2016), 256 (257); *Peifer*, K&R 2011, 543.
143 *Tene/Polonetsky*, Stanford Law Review Online 2012, 63 (65).
144 Siehe hierzu *Bunte/Krohn-Grimberghe*, zfo 2014, 372 (374 f.).
145 Siehe *Grund*, in: Deggendorfer Forum zur digitalen Datenanalyse e.V. (Hrsg.), Big Data, S. 29 (34).

7. Internet der Dinge

Als Internet der Dinge wird die zunehmende Verknüpfung von Alltagsgegenständen bezeichnet.[146] Es handelt sich um einen Oberbegriff für eine Vielzahl von Anwendungsszenarien, bei denen Geräte untereinander vernetzt sind und Daten – nicht notwendig personenbezogene – erhoben und verwendet werden.[147] Hierzu zählt beispielsweise das als *„Smart Grid"* bezeichnete intelligente Stromnetz. Dieses soll mit sog. *Smart Metern* sowohl den Produzenten als auch den Verbrauchern von Elektrizität einen präzisen Einblick in die Verbrauchswerte elektrischer Energie ermöglichen.[148]

Das Schlagwort *Industrie 4.0* beschreibt – gleichsam als Unterfall des Internets der Dinge – die zunehmende Digitalisierung und Vernetzung von Maschinen in der Industrie.[149] So können beispielsweise eine Vielzahl von Daten in einer Fabrik gesammelt und dadurch die Effizienz und der Verschleiß von Anlagen in Abhängigkeit von äußeren Faktoren bestimmt werden.[150]

8. Autonomes Fahren

Bereits ohne das autonome Fahren werden von Autos große Mengen von Daten erhoben und teils an die Hersteller übermittelt.[151] Aufsehen erregte ein Fall, in dem die Staatsanwaltschaft Köln vom Car-Sharing-

146 *Venzke-Caprarese*, in: Taeger (Hrsg.), DSRI-Herbstakademie 2015, S. 377 (377 f.); *Artikel-29-Datenschutzgruppe*, WP 223, S. 4.

147 Für Beispiele wie Industrie 4.0, Smart Home, Smart Grid, Connected Cars siehe *Sinn*, CA 2013, 4 (8).

148 *Tene/Polonetsky*, Stanford Law Review Online 2012, 63 (64).

149 Vgl. *Chirco*, in: Taeger (Hrsg.), DSRI-Herbstakademie 2015, 519 (519 f.).

150 Siehe hierzu *Peschel/Rockstroh*, MMR 2014, 571; *Bunte/Krohn-Grimberghe*, zfo 2014, 372 (375 f.).

151 Siehe *Jürgen Seeger,* ADAC-Untersuchung: Autohersteller sammeln Daten in großem Stil, heise online, 04.06.2016, https://heise.de/-3227102, (abgerufen am 11.05.2018).

Anbieter *Drive Now* die Herausgabe von Log-Daten eines Mietfahrzeugs erreichte und diese im Rahmen der Beweiswürdigung gegen den Angeklagten verwendet wurden.[152] Es ist davon auszugehen, dass die Anzahl von Sensoren und der Grad der Vernetzung in modernen Autos weiter steigen werden.[153]

9. Zwischenergebnis

Die Beispiele zeigen, dass es eine Vielzahl von Einsatzmöglichkeiten gibt. Gemeinsam haben diese Big-Data-Analysen, dass sie in der Regel zu Beginn der Auswertung einen Verarbeitungszweck allenfalls in sehr genereller Form benennen können. Häufig wird sich ein neuer Verarbeitungszweck zudem erst später ergeben.

Die Beispiele können grob in solche unterteilt werden, die auf einer Makro-Ebene allgemeine Aussage erzielen möchten, ohne dass diese auf eine bestimmte Person bezogen werden und Auswertungen, die sogleich oder im Anschluss daran auf einer Mikro-Ebene auf eine bestimmte Person zielen.[154] Zur Makro-Ebene zählt z. B. die nicht personalisierte Mustererkennung und zur Mikroebene die Identifizierung (*singling-out*) eines Individuums aus einem Datensatz und die Generierung neuer Informationen zu einer bereits bekannten Person durch Auswertung eines Datensatzes.[155]

Die rechtliche Zulässigkeit solcher Auswertungen ist immer eine Frage des Einzelfalls, auf den im Rahmen dieser Arbeit wegen der Mannigfaltigkeit der Erscheinungsformen jedoch nicht weiter eingegangen werden kann. Der Fokus liegt daher vielmehr allgemein auf dem rechtlich geforderten Präzisionsgrad der Zweckbestimmung und der Zulässigkeit von Zweckänderungen.

---

152 LG Köln, Urteil v. 23.05.2016, Az. 113 KLs 34/15 - juris Rn. 87.

153 Siehe *Roßnagel/Geminn/Jandt/Richter*, Datenschutzrecht 2016, S. 2 ff.

154 Vgl. *Hornung*, Spektrum der Wissenschaft Spezial - Physik, Mathematik, Technik 1.2017, 63 (65).

155 Zu den Beispielen vgl. *Schulz*, in: Gola (Hrsg.), DSGVO, Art. 6 Rn. 197 ff.

C. Datenschutzrechtliche Rahmenbedingungen für Big-Data-Anwendungen

Zunächst sollen die datenschutzrechtlichen Rahmenbedingungen anhand der allgemeinen Regelungen des BDSG a. F. in den Blick genommen werden. Zwar handelt es sich bei dem BDSG a. F. um ein nicht mehr geltendes Gesetz. Die im folgenden Kapitel vorgestellten Grundbegriffe und Grundprinzipien sind aber in sehr ähnlicher Form auch in der DS-GVO enthalten.

I. Anwendungsbereich des BDSG a. F.

Der Anwendungsbereich des BDSG a. F. ist in § 1 BDSG a. F. definiert. Wie problematisch Fragen der Anwendbarkeit des jeweiligen nationalen Rechts sind, ist vielen Gerichtsentscheidungen zu entnehmen,[156] soll aber hier nicht weiter thematisiert werden.

Soweit andere Bundesgesetze datenschutzrechtliche Bestimmungen enthalten, gehen diese dem BDSG a. F. vor, § 1 Abs. 3 Satz 1 BDSG a. F. Als Beispiel seien die Bestimmungen des TMG und des TKG genannt. Die folgenden Ausführungen setzen die Anwendbarkeit des BDSG a. F. bzw. der jeweiligen thematisierten Spezialgesetze voraus.

II. Grundbegriffe des Datenschutzrechts

In § 3 BDSG a. F. sind wesentliche Begriffe legal definiert. Zum besseren Verständnis der weiteren Ausführungen, werden zunächst einige grundlegende Begriffe erläutert.

---

156 Siehe z. B. EuGH, Urteil v. 13.5.2014 - C-131/12, ECLI:EU:C:2014:317 - Google v. Spain.

1. Personenbezogene Daten

Das Datenschutzrecht ist nur dann anwendbar, wenn ein Umgang mit personenbezogenen Daten vorliegt, § 1 Abs. 2 BDSG a. F.

Zunächst bedarf es einer terminologischen Vorklärung des Unterschiedes zwischen Daten und Informationen. Daten sind auf einem Datenträger verkörperte Zeichen.[157] Informationen sind Sinngehalte, die in Anknüpfung an Informationsgrundlagen, wie z. B. Daten, durch eine Interpretation entstehen.[158] Der Kontext entscheidet über den Aussagegehalt, die Informationen, die Daten entnommen werden können.[159] Die Möglichkeit mit Big-Data-Anwendungen viele Daten miteinander zu verknüpfen, führt zu einer Kontextänderung dieser Daten und damit zu einem gesteigerten Informationswert.[160] Auf die daraus resultierenden Gefährdungen für die Betroffenen kann nur durch eine Strukturierung des Datenumgangs effektiv reagiert werden.[161] Gerade die Verwendung von Daten zu einem anderen Zweck führt in der Regel zu einer Kontextänderung und damit zu einem neuen Informationsgehalt.[162] Die Kontextänderung kann zugleich zu einer Verkürzung des ursprünglichen Informationsgehalts führen und damit auch die Richtigkeit der Daten in Frage stellen.[163]

Das Datenschutzrecht will den Einzelnen vor einer Beeinträchtigung seines Persönlichkeitsrechts durch den Umgang mit seinen personenbezogenen Daten schützen, § 1 Abs. 1 BDSG a. F. Als Anknüpfungspunkt des Datenschutzrechts dient also der Umgang mit personenbezogenen Daten, weshalb deren Vorliegen von zentraler Bedeutung ist und im Fol-

---

157 *Bäcker*, Der Staat 51 (2012), 91 (92).

158 Vgl. *Bäcker*, Der Staat 51 (2012), 91 (92); *Trute*, JZ 1998, 822 (825).

159 *Bäcker*, Der Staat 51 (2012), 91 (97).

160 Vgl. *Bäcker*, Der Staat 51 (2012), 91 (97).

161 *Bäcker*, Der Staat 51 (2012), 91 (97).

162 Vgl. *Heibey/Lutterbeck/Rohlfs/Töpel*, in: Dierstein/Fiedler/Schulz (Hrsg.), Datenschutz und Datensicherung, 298 (301); *Wiebe*, ZIR 2014/1, 35 (47), sieht in dem Schutz vor Kontextverlust „eines der Motive für den Datenschutz".

163 *Jandt/Laue*, K&R 2006, 316 (317); *Podlech/Pfeifer*, RDV 1998, 139 (140); vgl. auch *Roßnagel/Pfitzmann/Garstka*, Modernisierung des Datenschutzrechts, S. 117.

genden erörtert werden soll. Wichtig ist aber zugleich, dass eine Beeinträchtigung des Einzelnen sich gerade aus dem Informationsgehalt ergeben kann, der den Daten zu entnehmen ist. Daher schützt das Datenschutzrecht nicht Daten, sondern Informationszusammenhänge.[164] Der Zweck ist von Bedeutung, weil der Verwendungszusammenhang für die Schutzbedürftigkeit des Betroffenen maßgeblich ist.[165]

Nach § 3 Abs. 1 BDSG a. F. sind personenbezogene Daten Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person. Sofern alleine produktbezogene Daten z. B. Werte einer Maschine, die nicht mit einer Person verknüpft werden können, bei einer Big-Data-Anwendung vorliegen, ist das BDSG a. F. also nicht anwendbar. Für sachbezogene Daten wird eine „persönlichkeitsrechtliche Relevanz" gefordert, damit von personenbezogenen Daten ausgegangen werden kann.[166] Der Unterscheidung zwischen Angaben zu persönlichen und sachlichen Verhältnissen kommt keine große Bedeutung zu, da sie lediglich verdeutlicht, dass jedwede Daten erfasst werden sollen.[167]

a) Streit über den Maßstab der Bestimmbarkeit des Personenbezugs

Zentrales Element der Begriffsdefinition ist die Voraussetzung, dass es sich um Daten einer bestimmten oder bestimmbaren natürlichen Person handeln muss. Einzelangaben zu einer bestimmten Person sind solche, die einer einzelnen Person sicher zugeordnet sind, was häufig aufgrund der

164 Vgl. *Masing*, VVDStRL (63) 2004, 377 (400 f.), der feststellt, dass es einen Konflikt mit der Informationsfreiheit gebe und die Zweckbindung dann „zerfalle".

165 Vgl. *Simitis*, NJW 1977, 729 (732).

166 So *Weichert*, DuD 2007, 17 (21), der als Beispiel für die Ablehnung eines Personenbezugs die Höhe über normal Null eines Grundstückes nennt.

167 *Dammann*, in: Simitis (Hrsg.), BDSG, § 3 Rn. 7.

Nennung des Namens der Fall ist.[168] Dieses Merkmal bereitet daher in der Regel keine Probleme.

Streit herrscht aber über die Frage, wann eine Person bestimmbar ist. Die Bestimmbarkeit liegt vor, wenn es möglich ist einen Personenbezug herzustellen.[169] Ein Personenbezug lässt sich also in diesem Fall nicht bereits mittels der vorliegenden Daten herstellen, sondern nur anhand von Zusatzwissen.[170] Ganz entscheidend ist die Frage, auf wessen Kenntnisse für die Möglichkeit der Identitätsbestimmung abzustellen ist. Hierzu werden verschiedene Ansichten vertreten. Neben Mischformen stehen sich im Wesentlichen die Theorien des relativen und des absoluten bzw. objektiven[171] Verständnisses des Personenbezugs gegenüber.[172]

aa) absolutes / objektives Verständnis

Nach einer Auffassung soll eine Person dann bestimmbar sein, wenn irgendjemand den Personenbezug herstellen kann.[173] Es soll also selbst die theoretische Möglichkeit einer Identifizierung ausgeschlossen sein.[174] Zur Begründung des absoluten Ansatzes wird oft auf ErwG 26 DSRL abgestellt, der die Mittel nennt, die von der verantwortlichen Stelle oder einem Dritten eingesetzt werden könnten.[175] Zudem seien bei einer relati-

168 *Buchner*, in: Taeger/Gabel (Hrsg.), BDSG, § 3 Rn. 11.
169 *Plath/Schreiber*, in: Plath (Hrsg.), BDSG/DSGVO, § 3 Rn. 13.
170 *Brink/Eckhardt*, ZD 2015, 205 (205).
171 So *Weichert*, in: Däubler/Klebe/Wedde/Weichert (Hrsg.), BDSG, § 3 Rn. 13.
172 Hierzu statt aller: *Bergt*, ZD 2015, 365; *Brink/Eckhardt*, ZD 2015, 205.
173 *Pahlen-Brandt*, K&R 2008, 288 (289); *Pahlen-Brandt*, DuD 2008, 34 (34); *Schild*, in: Wolff/Brink (Hrsg.), DSR, § 3 Rn. 17; *Weichert*, in: Däubler/Klebe/Wedde/Weichert (Hrsg.), BDSG, § 3 Rn. 13 u. 15, der aber zumindest dahingehend einschränkt, dass es nicht gänzlich ausgeschlossen sein darf, dass der Dritte der verantwortlichen Stelle dieses Wissen zugänglich macht; so auch *Weichert*, DuD 2007, 17 (19).
174 *Dammann*, in: Simitis (Hrsg.), BDSG, § 3 Rn. 23; vgl. auch *Meyerdierks*, MMR 2009, 8 (9).
175 So *Düsseldorfer Kreis/Konferenz der Datenschutzbeauftragten*, Cloud Computing, S. 12.

ven Auffassung des Personenbezugs „Schutzlücken“ vorhanden[176] und der Datenschutz liefe ins Leere.[177]

bb) relatives Verständnis

Eine andere Ansicht geht demgegenüber davon aus, dass es für die Frage der Bestimmbarkeit nur auf die Kenntnisse des Datenverwenders ankomme.[178] Ein Personenbezug soll dann vorliegen, wenn die verantwortliche Stelle mit den ihr üblicherweise zur Verfügung stehenden Mitteln ohne einen unverhältnismäßigen Aufwand den Betroffenen identifizieren kann.[179] Auf das eventuell vorhandene Zusatzwissen Dritter soll es demnach nicht ankommen.[180] Als Argument für diese Auffassung wird angeführt, dass § 30 BDSG a. F. die Übermittlung in anonymisierter Form vorsieht, obwohl die übermittelnde Stelle über die Zuordnungsregel verfügt.[181]

cc) vermittelnde Ansichten

Allerdings erkennen die meisten Vertreter des absoluten Verständnisses an, dass eine Herstellung des Personenbezugs nicht gänzlich ausgeschlossen sein muss.[182] Vielmehr soll eine Bestimmbarkeit in Anlehnung

176 *Pahlen-Brandt*, K&R 2008, 288 (289).
177 *Pahlen-Brandt*, DuD 2008, 34 (40).
178 *Gola/Klug/Körffer*, in: Gola/Schomerus (Hrsg.), BDSG, § 3 Rn. 10; *Tinnefeld*, in: Roßnagel (Hrsg.), Handbuch DSR, Kap. 4.1 Rn. 22; *Roßnagel/Scholz*, MMR 2000, 721 (723); *Schefzig*, K&R 2014, 772 (773 f.); *Louis*, Datenschutzrecht, Rn. 26.
179 *Schaffland/Wiltfang*, BDSG, § 3 Rn. 17; *Gola/Klug/Körffer*, in: Gola/Schomerus (Hrsg.), BDSG, § 3 Rn. 10.
180 *Härting*, Internetrecht, Rn. 192; vgl. *Gola/Klug/Körffer*, in: Gola/Schomerus (Hrsg.), BDSG, § 3 Rn. 10a.
181 So *Dammann*, in: Simitis (Hrsg.), BDSG, § 3 Rn. 32.
182 *Weichert*, in: Däubler/Klebe/Wedde/Weichert (Hrsg.), BDSG, § 3 Rn. 13; a. A. aber wohl: *Schild*, in: Wolff/Brink (Hrsg.), DSR, § 3 Rn. 17, 22, der aber unter Rn. 17 *Dammann* falsch zitiert, wenn er schreibt: „Daher soll ein Personenbezug

an die Definition des Anonymisierens in § 3 Abs. 6 BDSG a. F. bereits dann nicht vorliegen, wenn die Einzelangaben einer Person nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft zugeordnet werden können.[183] Ähnlich argumentiert auch die *Artikel-29-Datenschutzgruppe*, die davon ausgeht, dass die „rein hypothetische Möglichkeit zur Bestimmung" nicht ausreichen kann, da nach ErwG 26 DSRL nur solche Mittel zu berücksichtigen sind, die „vernünftigerweise" eingesetzt werden könnten.[184] Ein Personenbezug liege dann nicht vor, wenn die Möglichkeit der Identifizierung nicht bestehe oder vernachlässigbar sei.[185]

Eine andere vermittelnde Auffassung folgt im Ausgangspunkt einem relativen Verständnis. Sie will zwar nicht objektiv jegliches Wissen von Dritten berücksichtigen. Es soll aber gleichwohl jenes Zusatzwissen Dritter berücksichtigt werden, auf das die verantwortliche Stelle ohne unverhältnismäßigen Aufwand zugreifen kann.[186] Welcher Aufwand verhältnismäßig ist, soll dabei objektiv bestimmt werden.[187] Die vermittelnden Ansichten knüpfen im Wesentlichen an die Frage der „vernünftigerweise" einsetzbaren Mittel und damit an die Frage der Unverhältnismäßigkeit des Identifizierungsaufwands an.

---

nicht erst bei absoluter Unmöglichkeit, den Betroffenen zu bestimmen, sondern bereits dann vorliegen, wenn das Risiko so gering ist, dass es praktisch irrelevant erscheint." Der Personenbezug liegt gerade nicht vor, wenn eine Bestimmbarkeit des Betroffenen absolut unmöglich ist. Im Übrigen vertritt *Dammann*, dass bei einem sehr geringen Identifikationsrisiko eine Personenbeziehbarkeit nicht vorliegen soll. Die Position von *Schild* ist innerhalb seiner Kommentierung widersprüchlich, da er in § 3 Rn. 20 vertritt, dass eine „(…) rein fiktive Möglichkeit einer Bestimmbarkeit nicht aus(reiche)".

183 *Weichert*, in: Däubler/Klebe/Wedde/Weichert (Hrsg.), BDSG, § 3 Rn. 13.

184 *Artikel-29-Datenschutzgruppe*, WP 136, S. 17.

185 *Artikel-29-Datenschutzgruppe*, WP 136, S. 17.

186 *Buchner*, in: Taeger/Gabel (Hrsg.), BDSG, § 3 Rn. 13; *Eßer*, in: Eßer/Kramer/v. Lewinski (Hrsg.), Auernhammer BDSG, § 3 Rn. 19; *Plath/Schreiber*, in: Plath (Hrsg.), BDSG/DSGVO, § 3 Rn. 15; *Wójtowicz*, PinG 2013, 65 (66); in diese Richtung auch: *Schaar*, Datenschutz im Internet, Rn. 153.

187 *Buchner*, in: Taeger/Gabel (Hrsg.), BDSG, § 3 Rn. 13.

dd) Auslegung

Die Auffassungen kommen zu unterschiedlichen Ergebnissen, die insbesondere bei Big-Data-Analysen mit einer Vielzahl von Daten gerade bei einem objektiven Verständnis regelmäßig zu der Annahme von personenbezogenen Daten führen dürften. Vor einer Entscheidung dieser wichtigen Frage soll nun mittels Auslegung ermittelt werden, welche Ansicht vorzugswürdig ist.

(1) Wortlautauslegung

Der Wortlaut von § 3 Abs. 1 BDSG a. F. vermag nicht weiterzuhelfen.[188] Es ist dort nicht aufgeführt, durch wen und unter Zuhilfenahme welcher Mittel eine Bestimmung des Betroffenen erfolgen soll.

(2) Systematische Auslegung

Gemäß § 3 Abs. 6 BDSG a. F. ist Anonymisieren das Verändern personenbezogener Daten derart, dass die Einzelangaben über persönliche oder sachliche Verhältnisse nicht mehr oder nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können. Personenbezug und Anonymisierung sind komplementär.[189] Wenn eine wirksame Anonymisierung aber nicht voraussetzt, dass eine Reidentifizierung gänzlich ausgeschlossen ist, sondern es ausreichen lässt, wenn der Aufwand unverhältnismäßig groß ist, dann muss dies auch für die Frage der Personenbeziehbarkeit von Daten gelten. Die Verhältnismäßigkeit des

188 So auch *Brink/Eckhardt*, ZD 2015, 205 (207); *Specht/Müller-Riemenschneider*, ZD 2014, 71 (73).

189 Vgl. *Dammann*, in: Simitis (Hrsg.), BDSG, § 3 Rn. 23.

Aufwands lässt sich aber nur in Bezug auf die konkreten Gegebenheiten im Einzelfall beurteilen.[190]

Die Auslegung des als Argument für die relative Ansicht angeführten § 30 BDSG a. F. ist durchaus umstritten.[191] § 30 BDSG a. F. regelt das Verfahren der Pseudonymisierung[192] rechtmäßig erhobener Daten um diese dann in anonymisierter Form zu übermitteln.[193] Er spreche für ein relatives Verständnis des Personenbezugs, da die übermittelnde Stelle den Personenbezug jederzeit herstellen könne.[194] Dem wird entgegenhalten, dass § 30 BDSG a. F. gerade eine Übermittlung in anonymisierter Form vorsehe, d. h. aggregierte Daten übermittelt würden und daher diese Daten auch für die übermittelnde Stelle nicht mehr einer einzelnen Person zuordbar seien.[195] Es ist aber nicht ersichtlich, weshalb eine File-Trennung vorzunehmen sein soll, wenn die Daten ohnehin sowohl für die übermittelnde als auch für die empfangende Stelle anonym sein sollen. § 30 BDSG a. F. deutet somit ebenfalls in Richtung eines relativen Ansatzes. Die systematische Auslegung spricht daher jedenfalls gegen ein streng objektives Verständnis, das bereits die theoretische Möglichkeit der Reidentifizierung genügen lässt.[196]

---

190 Vgl. *Brink/Eckhardt*, ZD 2015, 205 (207).

191 Siehe die Auffassung von *Ehmann*, in: Simitis (Hrsg.), BDSG, § 30 Rn. 75 ff., der von verschiedenen Phasen im Rahmen des Datenumgangs nach § 30 BDSG a. F. und anonymen Daten bei der Übermittlung ausgeht, einerseits, und andererseits *Taeger*, in: Taeger/Gabel (Hrsg.), BDSG, § 30 Rn. 16 ff. der keine Trennung verschiedener Phasen vornimmt, weshalb eine Deanonymisierung jederzeit möglich sein soll. So auch *Kühling/Seidel/Sivridis*, Datenschutzrecht, Rn. 439.

192 So auch *Bergmann/Möhrle/Herb*, BDSG, § 30 Rn. 17; *Kramer*, in: Eßer/Kramer/v. Lewinski (Hrsg.), Auernhammer BDSG, § 30 Rn. 6 u. 10; *Weichert*, in: Däubler/Klebe/Wedde/Weichert (Hrsg.), BDSG, § 30 Rn. 7; *Kamlah*, in: Plath (Hrsg.), BDSG/DSGVO, § 30 Rn. 14.

193 Vgl. *Taeger*, in: Taeger/Gabel (Hrsg.), BDSG, § 30 Rn. 3.

194 Vgl. *Meyerdierks*, MMR 2009, 8 (10).

195 *Bergt*, ZD 2015, 365 (369).

196 Vgl. *Specht/Müller-Riemenschneider*, ZD 2014, 71 (73).

(3) Historische Auslegung

Die Gesetzgebungsmaterialien enthalten keine Anhaltspunkte für die Klärung der vorliegenden Streitfrage.[197]

(4) Teleologische Auslegung

Nach § 1 Abs. 1 BDSG a. F. dient das BDSG a. F. dem Schutz des Einzelnen vor der Beeinträchtigung seines Persönlichkeitsrechts durch den Umgang mit seinen personenbezogenen Daten. Der Anwendungsbereich des BDSG a. F. ist also nicht bei jedwedem Datenumgang eröffnet.[198] Es ließe sich argumentieren, dass durch ein absolutes Verständnis des Personenbezugs der Anwendungsbereich des Datenschutzrechts ausgedehnt und damit der Schutz des Betroffenen verbessert werde. Dem könnte aber entgegengehalten werden, dass eine Beeinträchtigung des Persönlichkeitsrechts nur droht, wenn die verantwortliche Stelle den Personenbezug herstellen kann, weshalb der relative Ansatz einen hinreichenden Schutz biete. Letztlich lässt sich einer teleologischen Auslegung nicht zwingend ein eindeutiges Ergebnis entnehmen.[199]

(5) Europarechtskonforme Auslegung

Da das deutsche Recht auf einer Umsetzung der DSRL beruht, ist die europarechtskonforme Auslegung von erheblicher Bedeutung. Der EuGH hatte sich in der Rechtssache *Breyer* unter anderem mit dem Streit um die Ermittlung des Personenbezugs auf Grundlage der DSRL zu beschäfti-

197 Vgl. *Brink/Eckhardt*, ZD 2015, 205 (208); a. A. *Specht/Müller-Riemenschneider*, ZD 2014, 71 (73) die tendenziell von einem weiten Verständnis ausgehen, da der Gesetzgeber eine Einengung des Personenbezugs „bewusst" unterlassen habe, allerdings einschränken, dass zum Einsatz von Zusatzwissen eines Dritten keine Aussage vorhanden sei.

198 Vgl. *Brink/Eckhardt*, ZD 2015, 205 (207).

199 Vgl. *Brink/Eckhardt*, ZD 2015, 205 (208).

gen.[200] Anlass dazu bot die Frage, ob dynamische IP-Adressen für einen Webseitenbetreiber ein personenbezogenes Datum darstellen, wenn der Personenbezug nur unter Zuhilfenahme von Zusatzwissen eines Dritten, im zu entscheidenden Fall des Internetzugangsanbieters, hergestellt werden kann.

Der EuGH stellte unter Rückgriff auf ErwG 26 DSRL fest, dass die Bestimmbarkeit auch vorliege, wenn die verantwortliche Stelle sich vernünftigerweise an einen Dritten zwecks Herstellung des Personenbezugs wenden könne.[201] Einen Maßstab für die Bestimmung des „vernünftigen Aufwands" zur Herstellung des Personenbezugs nennt der EuGH nicht, sondern stellt lediglich fest, dass dies bei dem abstrakten Vorliegen von rechtlichen Möglichkeiten zur Erlangung des notwendigen Zusatzwissens gegeben sei. Der EuGH geht also grundsätzlich von einem relativen Verständnis des Personenbezugs aus, da es im Ausgangspunkt auf die Kenntnisse der verantwortlichen Stelle ankommt. Allerdings berücksichtigt er auch das Zusatzwissen Dritter, sofern die verantwortliche Stelle dieses vernünftigerweise erlangen kann. Es kommt also nicht nur strikt relativ auf die Kenntnisse der verantwortlichen Stelle an. Der Personenbezug ist demnach nicht gänzlich objektiv zu bestimmen, sondern es handelt sich um eine vermittelnde Auffassung, die die relative Theorie um objektive Elemente ergänzt.

ee) Stellungnahme

Für die objektive Sichtweise mag in der Tat sprechen, dass ein umfassender Schutz des Betroffenen erstrebt wird. Problematisch ist allerdings, dass dem Erfordernis des Vorliegens eines personenbezogenen Datums jegliche Steuerungsfunktion verloren geht.[202] Um jegliches Risiko auszuschließen, müsste die verantwortliche Stelle letztlich vorsichtshalber im-

200 EuGH, Urteil v. 19.10.2016 - C-582/14 - Breyer, siehe dazu: *Kring/Marosi*, K&R 2016, 773; *Mantz/Spittka*, NJW 2016, 3582.
201 EuGH, Urteil v. 19.10.2016 - C-582/14 - Breyer, Rn. 45 ff.
202 Ähnlich LG Berlin, Urteil v. 31.01.2013 - 57 S 87/08, ZD 2013, 618 (619).

mer von personenbezogenen Daten ausgehen.[203] Die Sichtweise des EuGH, im Ausgangspunkt von einem relativen Verständnis erweitert um objektive Komponenten auszugehen, findet einen vernünftigen Kompromiss zwischen einer uferlosen Ausdehnung des Anwendungsbereichs des Datenschutzrechts einerseits und anderseits der Eröffnung desselben in Fällen in denen vernünftigerweise von einer Herstellung des Personenbezugs ausgegangen werden kann. Mit Unsicherheiten für die verantwortliche Stelle ist diese Ansicht dennoch behaftet, da der EuGH den Maßstab für die vernünftigerweise einsetzbaren Mittel nicht benannt hat. Trotzdem ist diese Ansicht vorzugswürdig.

b) Einzelangabe

Eine Einzelangabe ist ein Datum, das einen Aussagegehalt bezüglich einer natürlichen Person hat.[204] Sofern eine Aggregierung, d. h. eine Zusammenfassung von Daten zu einer Gruppe von Personen in der Weise vorgenommen wird, dass diese einer einzelnen Person nicht mehr zugeordnet werden können, findet das Datenschutzrecht mangels Personenbezugs also keine Anwendung.[205] Bei der Aggregierung von Daten geht der Personenbezug durch die Vermischung einer Vielzahl von Daten verloren.[206] Daraus ergibt sich zugleich, dass auch aggregierte Daten personenbezogene Daten sind, wenn ein Attribut bei allen Gruppenmitgliedern vorliegt.[207] Es wird eine Gruppengröße von mindestens drei Personen gefordert, da ansonsten durch Subtraktion von Werten die Werte einer ein-

203 Vgl. *Brink/Eckhardt*, ZD 2015, 205 (206); *Schefzig*, K&R 2014, 772 (774).

204 *Schaffland/Wiltfang*, BDSG, § 3 Rn. 4; a. A. aber *Haase*, Personenbezug, S. 179 u. 181 f., der auch eine Einzelangabe über eine Gruppe z. B. das Gesamtalter aller Gruppenmitglieder für möglich hält und bemängelt, dass vielfach Fragen der Bestimmbarkeit unter das Merkmal Einzelangabe gefasst würden.

205 *Scholz*, in: Roßnagel (Hrsg.), Handbuch DSR, Kap. 9.2 Rn. 47; vgl. *Plath/Schreiber*, in: Plath (Hrsg.), BDSG/DSGVO, § 3 Rn. 7; vgl. *Schefzig*, K&R 2014, 772 (773); *Kühling/Schall/Biendl*, TKR, Rn. 622 sprechen von einem „Durchschlagen" auf eine Einzelperson.

206 *Bull*, NJW 2006, 1617 (1621).

207 *Dreier/Spiecker genannt Döhmann*, Aufnahme des Straßenbildes, S. 80.

zelnen Person ermittelt werden könnten.[208] Problematisch ist natürlich, dass aufgrund der Vielzahl von Daten die Zuordnung zu einer einzelnen Person wesentlich wahrscheinlicher als früher ist. Es wird vertreten, dass bei Big Data aufgrund der Datenmengen in der Regel genügend Daten zur Identifizierung einer Person vorhanden seien, so dass eine mangelnde Identifizierbarkeit sogar grundsätzlich gegen die Annahme einer Big-Data-Analyse spreche.[209] Letztlich ist dies aber immer eine Frage des Einzelfalls.

c) Personenbezug von statistischen Daten

Von großer Bedeutung im Zusammenhang mit Big-Data-Analysen ist die Frage, ob statistische Daten personenbezogene Daten sind, wenn ein mittels Big-Data-Analyse gewonnener statistischer Wert einer Person zugeordnet wird.[210] Als Beispiel hierfür eignen sich besonders sog. Score-Werte, die die Wahrscheinlichkeit des Eintritts eines Ereignisses, z. B. die Rückzahlung eines Darlehens mit einer Prozentangabe beziffern.

aa) grundsätzlich verneinende Ansichten

Ein statistisches Datum sei grundsätzlich kein personenbezogenes Datum.[211] Es handele sich nicht um eine Aussage über die betreffende Person, sondern nur bezüglich des Verhaltens einer ähnlichen Vergleichs-

208 *Dammann*, in: Simitis (Hrsg.), BDSG, § 3 Rn. 14; zu Problemfällen einer wirksamen Aggregierung siehe: *Küpper*, Personenbezug von Gruppendaten, S. 137 ff.

209 Vgl. *Roßnagel*, ZD 2013, 562 (564).

210 Auf die Problematik, dass eine einer Gruppe zugeordnete Person ein Merkmal nicht aufweist, weist *Rubinstein*, International Data Privacy Law 2013, 74 (78) hin.

211 *Spiecker genannt Döhmann*, K&R 2014, 549 (553); *Wuermeling*, NJW 2002, 3508 (3509).

gruppe.[212] Eine Zuordnung einer einzelnen Person zu einem durch Aggregierung von Daten entstandenen Profil sei „kein wirkliches ‚Persönlichkeitsprofil', sondern ein Datum, das sich „nur ganz oberflächlich" auf die Person beziehe, der es zugeordnet werde.[213]

Neben dieser Auffassung, die den Personenbezug gänzlich ablehnt, wird vertreten, dass aufgrund des Gefährdungspotentials für den Betroffenen bei einer hohen Wahrscheinlichkeit des Vorliegens eines Merkmals ein Personenbezug anzunehmen sei, wobei eine Wahrscheinlichkeit von mindestens 80 Prozent gefordert wird.[214] Der Personenbezug sei umso loser, je geringer die berechnete Wahrscheinlichkeit des Zutreffens eines Merkmals sei.[215]

bb) grundsätzlich bejahende Ansichten

Eine andere Ansicht geht davon aus, dass Prognosedaten als personenbezogene Daten zu verstehen seien.[216] Zwar handele es sich bei aggregierten Daten vor der Zuordnung zu einer Person nicht um eine Einzelangabe zu einer Person, sondern um eine Gruppenangabe zu allen Mitgliedern der Gruppe, ohne dass diese Daten einer einzelnen Person zugeordnet werden können.[217] Indem einer Einzelperson der bezüglich einer

212 *Kamlah*, MMR 1999, 395 (401); *Wolber*, CR 2003, 623 (625); ähnlich *Bull*, NVwZ 2011, 257 (262), der zwischen einem Individualprofil und der Zuordnung zu einer Gruppe unterscheidet.

213 *Bull*, NJW 2006, 1617 (1621).

214 *Dreier/Spiecker genannt Döhmann*, Aufnahme des Straßenbildes, S. 81; zur Problematik des Gefährdungspotenzials und des hinreichenden Wahrscheinlichkeitsgrads siehe auch *Spiecker genannt Döhmann*, K&R 2014, 549 (553).

215 *Weichert*, DuD 2007, 17 (19).

216 *Koch*, itrb 2015, 13 (18 f.); *Weichert*, ZRP 2014, 168; *Haase*, Personenbezug, S. 163; *Boehme-Neßler*, DuD 2016, 419 (420); *Scholz*, in: Roßnagel (Hrsg.), Handbuch DSR, Kap. 9.2 Rn. 61; *Buchner*, in: Taeger/Gabel (Hrsg.), BDSG, § 3 Rn. 6; *Dammann*, in: Simitis (Hrsg.), BDSG, § 3 Rn. 71 f.; *Möller/Florax*, NJW 2003, 2724 (2725); *Skistims/Voigtmann/David/Roßnagel*, DuD 2012, 31 (33).

217 *Beckhusen*, BKR 2005, 335 (337); siehe oben, C. II. 1. b), S. 85 f.

Gruppe errechnete Wert zugeordnet werde, „schlage" das Ergebnis auf sie durch und werde zu einer Einzelangabe.[218] Dass es sich um einen Wahrscheinlichkeitswert handele, stehe der Annahme einer Angabe über persönliche oder sachliche Verhältnisse einer Person nicht entgegen.[219] Die verantwortliche Stelle treffe gerade die Aussage, dass eine Person ein Merkmal mit einer gewissen Wahrscheinlichkeit aufweise und setze dieses Datum damit zu einer Person in Beziehung.[220] Sogar Werturteile seien Angaben über persönliche oder sachliche Verhältnisse, so dass erst recht ein wesentlich objektiverer Scorewert ein personenbezogenes Datum sei.[221] Bei einer statistischen Auswertung mit aggregierten Daten sei das Datenschutzrecht anwendbar, wenn die Ergebnisse einen Personenbezug ermöglichten[222] bzw. das Ergebnis einer Person zugeordnet werde.[223]

cc) Stellungnahme

Auf den berechneten Grad der Wahrscheinlichkeit kann es nicht ankommen. Denn dies würde zu dem überraschenden Ergebnis führen, dass die Formulierung des Merkmals (positiv/negativ) über das Vorliegen eines personenbezogenen Datums und damit die Anwendbarkeit des Datenschutzrechts entscheiden würde. Zudem kennt das Gesetz eine Kategorie eines „wahrscheinlich" personenbezogenen Datums nicht. Es gibt keinen „loseren" Personenbezug. Ausschlaggebend ist vielmehr, dass die verantwortliche Stelle der betroffenen Person einen bestimmten Wahrscheinlichkeitswert zuordnet und diesen somit als Merkmal dieser Person betrachtet. Aus Sicht des Betroffenen kommt es nur darauf an, als Träger eines Merkmals mit einer bestimmten Wahrscheinlichkeit angesehen und

218 *Beckhusen*, BKR 2005, 335 (337); *Beckhusen*, Schufa, S. 235; *Scholz*, in: Roßnagel (Hrsg.), Handbuch DSR, Kap. 9.2 Rn. 48.
219 *Beckhusen*, BKR 2005, 335 (338); siehe auch *Crawford/Schultz*, Boston College Law Review, Vol. 55, 2014, 93 (101).
220 Vgl. *Schefzig*, K&R 2014, 772 (777); siehe auch *Haase*, Personenbezug, S. 423.
221 *Beckhusen*, BKR 2005, 335 (338).
222 *Roßnagel*, ZD 2013, 562 (565).
223 *Brink/Eckhardt*, ZD 2015, 205 (208).

entsprechend behandelt zu werden. Die letztgenannte Ansicht ist daher vorzugswürdig.

2. Erheben

Das Erheben ist gemäß § 3 Abs. 3 BDSG a. F. das Beschaffen von Daten über den Betroffenen. Aus der Verwendung des Begriffs „Betroffener" ergibt sich im Zusammenhang mit § 3 Abs. 1 BDSG a. F., dass es bei § 3 Abs. 3 BDSG a. F. nur um das Beschaffen *personenbezogener* Daten geht.[224] Ein Erheben erfordert ein zielgerichtetes Vorgehen.[225] Sofern eine Stelle Daten ohne jedes eigenes Zutun erhält, liegt kein Erheben vor.[226]

3. Verarbeiten

Verarbeiten ist das Speichern, Verändern, Übermitteln, Sperren und Löschen personenbezogener Daten ungeachtet der dabei angewendeten Verfahren, § 3 Abs. 4 Satz 1, 2 BDSG a. F. Folglich ist es unerheblich, ob die Datenverarbeitung automatisiert oder manuell erfolgt.[227] Der Verarbeitungsbegriff des BDSG a. F. weicht damit von der Definition in der DSRL ab, die auch die Erhebung und die Nutzung umfasst.[228]

Das Verändern ist das inhaltliche Umgestalten gespeicherter personenbezogener Daten, § 3 Abs. 4 Satz 2 Nr. 2 BDSG a. F. Eine Veränderung liegt vor, wenn ein Datum eine neue Bedeutung erhält.[229] Dies kann insbesondere bei der Verknüpfung von Daten geschehen, die hierdurch in einem neuen Kontext stehen und einen geänderten Informationsgehalt er-

---

224 *Kühling/Seidel/Sivridis*, Datenschutzrecht, Rn. 234.
225 *Gola/Klug/Körffer*, in: Gola/Schomerus (Hrsg.), BDSG, § 3 Rn. 24.
226 *Buchner*, in: Taeger/Gabel (Hrsg.), BDSG, § 3 Rn. 26.
227 *Schaffland/Wiltfang*, BDSG, § 3 Rn. 21.
228 *Eßer*, in: Eßer/Kramer/v. Lewinski (Hrsg.), Auernhammer BDSG, § 3 Rn. 47.
229 *Kühling/Seidel/Sivridis*, Datenschutzrecht, Rn. 239.

halten.[230] Die Gesamtinformation muss sich von der Summe der Teilinformationen unterscheiden.[231] Das Zusammenführen und Auswerten von Daten aus unterschiedlichen Quellen im Rahmen der Analyse wird teilweise als Erhebung von Daten gewertet.[232] Demgegenüber wird vertreten, dass Daten, die das Ergebnis einer Auswertung sind, nicht erhoben seien, aber in der Regel die Zweckbindung der in die Auswertung eingeflossenen Daten greife.[233] Bei Big-Data-Analysen ist gerade die Verknüpfung von Daten zur Gewinnung neuer Erkenntnisse und damit ein Verändern beabsichtigt.[234] Ein Beispiel hierfür ist das Scoring, bei dem den vorhandenen Daten ein neues Datum zugeordnet wird.[235] Zu beachten ist aber, dass die Ergebnisse einer Big-Data-Analyse wesentlich sensibler sein können als die Daten, die Grundlage der Auswertung sind, weshalb die Big-Data-Analyse eventuell nicht von der sonst einschlägigen Erlaubnis gedeckt ist.[236]

4. Nutzen

Gemäß § 3 Abs. 5 BDSG a. F. ist Nutzen jede Verwendung personenbezogener Daten, soweit es sich nicht um eine Verarbeitung handelt. Es handelt sich mithin um einen Auffangtatbestand, der gewährleisten soll,

---

230 *Gola/Klug/Körffer*, in: Gola/Schomerus (Hrsg.), BDSG, § 3 Rn. 30; Für ein Verändern anstatt der Annahme einer Erhebung von Daten durch Data Mining ohne Begründung: *Scheja/Haag*, in: Leupold/Glossner (Hrsg.), Handbuch IT-Recht, Teil 5 Rn. 56.

231 *Dammann*, in: Simitis (Hrsg.), BDSG, § 3 Rn. 135; *Wittig*, RDV 2000, 59 (60).

232 So wohl *Schefzig*, K&R 2014, 772 (778); siehe auch *Koch*, itrb 2015, 13 (17), der damit aber wohl meint, dass der Zusammenführung in der Regel eine Übermittlung der Daten vorausgehe und die Speicherung der Daten daher für den Empfänger eine Erhebung sei. Im Anschluss geht er davon aus, dass durch die Zusammenführung der Daten eine Kontextänderung und damit ein Verändern eintrete.

233 *Dammann*, in: Simitis (Hrsg.), BDSG, § 14 Rn. 50.

234 *Scholz,* in: Roßnagel (Hrsg.), Handbuch DSR, Kap. 9.2, Rn. 83.

235 Vgl. *Buchner*, in: Taeger/Gabel (Hrsg.), BDSG, § 3 Rn. 32; *Plath/Schreiber*, in: Plath (Hrsg.), BDSG/DSGVO, § 3 Rn. 37.

236 Vgl. *Schefzig*, K&R 2014, 772 (778).

dass jede Art des Datenumgangs dem Verbotsprinzip des § 4 Abs. 1 BDSG a. F. unterliegt.[237] Das Nutzen wurde 1990 in das BDSG a. F. eingefügt und trug wesentlich zur Verwirklichung der Zweckbindung bei.[238]

5. besondere Arten personenbezogener Daten

In § 3 Abs. 9 BDSG a. F. sind sog. besondere Arten personenbezogener Daten aufgeführt. Dies sind Angaben über die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit oder Sexualleben. Das Hervorheben bestimmter Daten als besonders sensibel beruht auf der Umsetzung der DSRL und war dem auf den Verwendungskontext abstellenden deutschen Recht bis dahin fremd.[239]

III. Grundprinzipien des Datenschutzrechts

Dem BDSG a. F. liegen einige Prinzipien zugrunde, die sowohl für den Datenumgang durch öffentliche als auch durch nicht-öffentliche Stellen gelten. Auf diese wird im Folgenden näher eingegangen.

1. Verbotsprinzip

Gemäß § 4 Abs. 1 BDSG a. F. ist der Umgang mit personenbezogenen Daten nur zulässig, wenn eine Rechtsvorschrift dies gestattet oder der Betroffene eingewilligt hat. Dies ist das sog. Verbotsprinzip, das häufig als Verbot mit Erlaubnisvorbehalt bezeichnet wird.[240] Der Datenumgang ist folglich grundsätzlich verboten und bedarf einer besonderen Legitimation.

---

237 Vgl. *Bergmann/Möhrle/Herb*, BDSG, § 3 Rn. 122.
238 *Dammann*, in: Simitis (Hrsg.), BDSG, § 3 Rn. 188.
239 *Kühling/Seidel/Sivridis*, Datenschutzrecht, Rn. 231.
240 Vgl. *Gola/Klug/Körffer*, in: Gola/Schomerus (Hrsg.), BDSG, § 4 Rn. 3.

a) Einwilligung

Eine zentrale Bedeutung kommt der Einwilligung zu. Aufgrund von teils vage formulierten Interessenabwägungsklauseln und der damit einhergehenden Rechtsunsicherheit mag die Einwilligung für viele verantwortlichen Stellen im nicht-öffentlichen Bereich besonders attraktiv sein.[241] Auf Einzelprobleme der Einwilligung soll hier nicht eingegangen werden.[242] Wichtig ist aber, dass der Betroffene auf den vorgesehenen Zweck des Datenumgangs sowie, soweit nach dem Umständen des Einzelfalls erforderlich oder auf Verlangen, auf die Folgen der Verweigerung der Einwilligung hinzuweisen ist, § 4a Abs. 1 Satz 2 BDSG a. F. Die Zweckbindung spielt somit eine große Rolle für die Wirksamkeit der Einwilligung. Inwiefern eine Einwilligung in Big-Data-Analysen möglich ist,[243] hängt folglich unmittelbar mit der Zweckfestlegung zusammen.

Die Einwilligung sieht sich vor dem Hintergrund der technischen Entwicklung erheblicher Kritik ausgesetzt. Das bisherige Modell von Information des Betroffenen und Einwilligung sei mit Big Data nicht vereinbar.[244] Problematisch ist sicherlich, dass viele Datenschutzerklärungen sehr lang und schwer verständlich sind.[245] Empirische Studien belegten, dass Betroffene Datenschutzerklärungen weder läsen noch verstünden.[246]

---

241 Vgl. *Buchner*, DuD 2010, 39 (40). Zu bedenken ist aber ihre Widerruflichkeit.

242 Siehe hierzu nur *Rogosch*, Die Einwilligung im Datenschutzrecht.

243 Dieses Problem ignorieren *Bitter/Buchmüller/Uecker*, in: Hoeren (Hrsg.), Big Data und Recht, S. 58 (73), die anscheinend pauschal von der Wirksamkeit einer Einwilligung ausgehen.

244 *Mayer-Schönberger/Cukier*, Big Data, S. 173.

245 Laut einer Studie aus dem Jahre 2008 musste ein durchschnittlicher Internetnutzer bereits damals theoretisch 244 Stunden im Jahr für das Lesen aller Datenschutzerklärungen aufbringen: *McDonald/Cranor*, I/S A Journal of Law and Policy for the Information Society, Vol. 4:3 2008, 540 (560); siehe hierzu: *Europäischer Datenschutzbeauftragter*, Privatssphäre und Wettbewerbsfähigkeit, Rn. 77; vgl. ferner *Bäcker*, Der Staat 51 (2012), 91 (112); *Cate*, in: Winn (Hrsg.), Consumer Protection, 343 (360 ff.); zu Datenschutzerklärungen von Facebook, Google und Apple siehe *Härting*, CR 2011, 169, der zu einem überwiegend positiven Fazit kommt.

246 *Rubinstein*, International Data Privacy Law 2013, 74 (75). Vgl. zu diesem Kritikpunkt: *Cate*, in: Winn (Hrsg.), Consumer Protection, 343 (360 ff.).

Dies gelte auch für Pop-up-Hinweise zur Einwilligung in den Einsatz von Cookies.[247] Ein Ansatz zur Lösung dieses Problems mag eine strenge Inhaltskontrolle und gesetzliche Vorgaben zur Strukturierung von Einwilligungserklärungen sein.[248]

Eine Vorabinformation des Betroffenen könne bei Big-Data-Anwendungen nicht erfolgen, weil vielfach der Personenbezug erst als Ergebnis der Auswertung hergestellt werde.[249] Problematisch am Modell einer Einwilligung zum Zeitpunkt der Erhebung sei, dass aufgrund der Aggregierung von Daten neue Risiken entstehen können, die bei der Preisgabe einzelner Daten nicht erkennbar seien.[250] In der Literatur wird zudem beklagt, dass es impraktikabel sei die Betroffenen noch einmal für bereits erhobene Daten um Erlaubnis zur Verwendung für einen anderen Zweck zu fragen.[251] Dies könne dazu führen, dass Innovationspotential ungenutzt bleibe, obwohl dieses zum Wohle der Einzelnen und der Gesellschaft sei.[252] Das Erfordernis zur Einholung einer Einwilligung setze bezüglich künftiger Verwendungen der Daten Anreize zu einer weiten und vagen Zweckbestimmung.[253] Es solle daher besser zum Zeitpunkt der späteren Verwendungen zu einem neuen Zweck im Einzelfall über die Zulässigkeit entschieden werden, wobei manche Verwendungen generell erlaubt, andere generell verboten oder an eine Einwilligung geknüpft sein sollten.[254]

---

247 *Härting*, CR 2014, 528 (533).
248 Vgl. *Masing*, NJW 2012, 2305 (2309).
249 *Werkmeister/Brandt*, CR 2016, 233 (236).
250 *Solove*, Harvard Law Review, Vol. 126, 2013, 1880 (1881 u. 1889 f.).
251 *Arming*, K&R Beihefter 3/2015 zu Heft 9 2015, 7 (9 f.); *Cumbley/Church*, CLSR 29 (2013), 601 (606); ähnlich *Mayer-Schönberger/Cukier*, Big Data, S. 153, die pauschal feststellen, dass kein Unternehmen die hiermit verbundenen Kosten auf sich nehmen werde.
252 *Cate/Mayer-Schönberger*, International Data Privacy Law, Vol. 3 No. 2, 2013, 67 (67 f.).
253 *Solove*, Harvard Law Review, Vol. 126, 2013, 1880 (1899).
254 *Solove*, Harvard Law Review, Vol. 126, 2013, 1880 (1902).

Ein Widerspruchsrecht sei gegenüber einer Einwilligung vorzugswürdig und habe sich im Falle von § 15 Abs. 3 TMG bewährt.[255] Gegen ein Widerspruchsrecht spricht aber, dass dieses nur Anwendung findet, wenn der Gesetzgeber aufgrund einer typisierenden Betrachtung zu dem Schluss einer grundsätzlichen Zulässigkeit des Datenumgangs gekommen ist. Eine Einwilligung schafft demgegenüber unabhängig von gesetzlichen Abwägungsentscheidungen eine Grundlage für den Datenumgang. Zudem wird das beschriebene Informationsdefizit durch eine Widerspruchslösung nicht behoben.

Bei aller Kritik an der Einwilligung und deren Schwächen ist aber zu beachten, dass die informationelle Selbstbestimmung eine Entscheidung des Betroffenen erfordert.

b) Rechtsnorm

Sowohl das BDSG a. F., als auch Spezialgesetze enthalten eine Vielzahl von Erlaubnisnormen. Für den öffentlichen Bereich finden sich diese in den §§ 12 ff. BDSG a. F. Die Regelungen für den nicht-öffentlichen Bereich finden sich in den §§ 27 ff. BDSG a. F. Auf einzelne Bestimmungen wird später näher eingegangen.[256]

2. Datenvermeidung und Datensparsamkeit

In § 3a BDSG a. F. sind die Grundsätze der Datenvermeidung und der Datensparsamkeit enthalten. Demnach sollen so wenige Daten wie möglich erhoben oder verwendet und Datenverarbeitungssysteme an diesem Ziel ausgerichtet werden, § 3a Satz 1 BDSG a. F. Zudem sind personenbezogene Daten zu anonymisieren oder pseudonymisieren, soweit dies nach dem Verwendungszweck möglich ist und keinen unverhältnismäßi-

255 *Härting*, CR 2014, 528 (533).
256 D. III., S. 155 ff.

gen Aufwand erfordert, § 3a Satz 2 BDSG a. F.[257] Bei § 3a Satz 2 BDSG a. F. wurde vor der Novelle 2009 nicht auf den Verwendungszweck sondern lediglich auf die „Möglichkeit" des Einsatzes von Schutzmaßnahmen abgestellt. In der Literatur wird die Änderung des Wortlauts überwiegend als Präzisierung ohne Bedeutungsänderung der Norm betrachtet.[258] Hiergegen spricht aber, dass der Wortlaut – anders als vorher – nun auf den Verwendungszweck zur Bestimmung der Möglichkeit der Ergreifung von Schutzmaßnahmen abstellt.[259] Zwar mag dies schon vorher die Gesetzesbegründung nahegelegt haben, aber dem Wortlaut war es nicht zu entnehmen. Welche Daten erforderlich sind, lässt sich nur anhand des Zwecks des Datenumgangs bestimmen. Die Datensparsamkeit knüpft also an den Zweck des Datenumgangs an.[260] Wenn der Zweck nicht konkret

---

257 Zum Streit ob es sich um eine Rechtspflicht handelt, bejahend: *Kühling/Seidel/Sivridis*, Datenschutzrecht, Rn. 296; *Wolff*, in: Wolff/Brink (Hrsg.), DSR, Prinzipien Rn. 42. *Scholz*, in: Simitis (Hrsg.), BDSG, § 3a Rn. 27; *Weichert*, in: Däubler/Klebe/Wedde/Weichert (Hrsg.), BDSG, § 3a Rn. 4; mangels Sanktionsbewehrung verneinend: *Gola/Klug/Körffer*, in: Gola/Schomerus (Hrsg.), BDSG, § 3a Rn. 2; *Schaffland/Wiltfang*, BDSG, § 3a Rn. 2; *Schreiber*, in: Plath (Hrsg.), BDSG/DSGVO, § 3a Rn. 14. In der Gesetzesbegründung der Novelle 2009 heißt es dazu nichtssagend: „Sein Rechtscharakter als Zielvorgabe bleibt bestehen.", siehe Beschlussempfehlung und Bericht des Innenausschusses, BT-Drs. 16/13657, S. 17.

258 So *Weichert*, in: Däubler/Klebe/Wedde/Weichert (Hrsg.), BDSG, § 3a Rn. 1; *Schaffland/Wiltfang*, BDSG, § 3a Rn. 1 spricht von „in erster Linie (…) redaktionellen Änderungen". Diese Ansichten stützen sich wohl auf die Gesetzesbegründung in der es hieß: „Der Vorbehalt des technisch Möglichen wird durch Bezugnahme auf den Verwendungszweck präzisiert." Siehe Beschlussempfehlung und Bericht des Innenausschusses, BT-Drs. 16/13657, S. 17. *Schulz*, in: Wolff/Brink (Hrsg.), DSR, § 3a Rn. 91 führt zur Begründung zudem an, dass in der Gesetzesbegründung des BDSG 2001 stand, dass nicht nur auf das technisch Mögliche sondern auch auf das im „vorgegebenen funktionalen Zusammenhang" Sachgerechte abzustellen sei. Siehe BT-Drs. 14/4329, S. 33.

259 So auch *Zscherpe*, in: Taeger/Gabel (Hrsg.), BDSG, § 3a Rn. 56; *Bergmann/Möhrle/Herb*, BDSG, § 3a Rn. 2; *Scholz*, in: Simitis (Hrsg.), BDSG, § 3a Rn. 8 u. 53; *Eßer*, in: Eßer/Kramer/v. Lewinski (Hrsg.), Auernhammer BDSG, § 3a Rn. 7 erkennt zumindest eine Stärkung der Gebote.

260 Vgl. *Eßer*, in: Eßer/Kramer/v. Lewinski (Hrsg.), Auernhammer BDSG, § 3a Rn. 15.

definiert ist, ist zugleich der Grundsatz der Datensparsamkeit nicht einzuhalten.[261]

3. Erforderlichkeit

Vielen Normen im Datenschutzrecht ist der Erforderlichkeitsgrundsatz zu entnehmen. Er kommt mehr als 50 Mal im BDSG a. F. vor.[262] Der Grundsatz der Erforderlichkeit begrenzt den zulässigen Datenumgang auf jene Daten, die für den Verarbeitungszweck unbedingt nötig sind.[263] Für den öffentlichen Bereich folgt er bereits aus dem verfassungsrechtlichen Verhältnismäßigkeitsprinzip.[264]

Teils wird angezweifelt, ob der Erforderlichkeitsgrundsatz auch im Falle einer Datenverarbeitung aufgrund einer Einwilligung gilt. So wird die Auffassung vertreten, dass durch eine Einwilligung eine nicht erforderliche Datenverarbeitung legitimiert werden könne, indem dies „hinreichend deutlich" zum Ausdruck gebracht werde.[265] Welche Daten nötig sind, bemisst sich nach dem Zweck. Je nach Definition des Zwecks kann damit ein Datenumgang erforderlich sein oder nicht. Es bedarf also keiner expliziten Legitimierung einer „nicht-erforderlichen" Datenverarbeitung. Zu Bedenken ist aber, dass durch eine sehr offene Zweckbestimmung der Erforderlichkeitsgrundsatz letztlich inoperabel wird.[266]

4. Transparenz

Der Betroffene kann seine Rechte nur geltend machen, wenn er weiß, welche Daten von wem und zu welchen Zwecken verarbeitet werden. Deshalb sehen einige Vorschriften des BDSG a. F. entsprechende Infor-

---

261 Vgl. *Artikel-29-Datenschutzgruppe*, WP 211, S. 22 Rn. 5.18.
262 *Wolff*, in: Wolff/Brink (Hrsg.), DSR, Prinzipien, Rn. 25.
263 *Taeger*, Datenschutzrecht, Rn. 118.
264 *Kühling/Seidel/Sivridis*, Datenschutzrecht, Rn. 290.
265 *Wolff*, in: Wolff/Brink (Hrsg.), DSR, Prinzipien, Rn. 24.
266 Vgl. *Kühling/Seidel/Sivridis*, Datenschutzrecht, Rn. 290.

mations- und Auskunftspflichten vor. Exemplarisch sind dafür der Grundsatz der Direkterhebung in § 4 Abs. 2 Satz 1 BDSG a. F. und die Pflicht zur Information über die Identität der verantwortlichen Stelle und über den Zweck des Datenumgangs, § 4 Abs. 3 Satz 1 Nr. 1, 2 BDSG a. F. Nur bei einem transparenten Datenumgang kann der Betroffene sein Recht auf informationelle Selbstbestimmung (RiS) tatsächlich durchsetzen.[267]

5. Zwischenergebnis

Eine Schwächung des Zweckbindungsprinzips würde somit auch eine Schwächung anderer Prinzipien des Datenschutzrechts nach sich ziehen.[268]

267 Vgl. *Tinnefeld/Buchner/Petri*, Datenschutzrecht, S. 237.
268 Vgl. *Artikel-29-Datenschutzgruppe*, WP 203, S. 15.

D. Der Grundsatz der Zweckbindung

Zum besseren Verständnis des Zweckbindungsgrundsatzes soll zunächst die Entstehungsgeschichte erläutert und dabei auch internationale Entwicklungen in den Blick genommen werden. Danach wird die Zweckfestlegung genauer betrachtet. Die entscheidende Frage ist hierbei, wie konkret der Zweck angegeben werden muss und ob sich dem Gesetz dazu etwas entnehmen lässt. Anschließend ist die Frage zu erörtern, welche Zweckänderungen zulässig sind. Es werden Regelungen des BDSG a. F. und auch einiger Spezialgesetze im Einzelnen betrachtet. Natürlich werden auch die neuen europäischen Entwicklungen mit der DSGVO und anknüpfend hieran dem BDSG 2018 in den Blick genommen.

I. Bedeutung

Zunächst stellt sich bei dem Begriff Zweckbindung die Frage, woran die verantwortliche Stelle gebunden sein soll. Genauer gesagt, was sich hinter dem Wort „Zweck" verbirgt. Dem Duden sind folgende Definitionen zu entnehmen: „1. etw. was jmd. mit einer Handlung beabsichtigt, zu bewirken, zu erreichen sucht; [Beweggrund u.] Ziel einer Handlung. 2. in einem Sachverhalt, Vorgang o. Ä. verborgener erkennbarer Sinn".[269] Es geht also um das Ziel einer Handlung. Auch die zweite Definition geht in diese Richtung, da der Begriff „Sinn" in der hier interessierenden Fallgestaltung auch durch das Wort Ziel ersetzt werden könnte. In der Antike wurde unter dem Begriff Zweck das „Ziel und Ende (Telos) einer Handlung"[270] verstanden.

Nach *Luhmann* „(…) bezeichnet (der Zweckbegriff) diejenige Wirkung bzw. den Komplex von Wirkungen, die das Handeln rechtfertigen sollen,

269 *Dudenredaktion (Hrsg.)*, Die deutsche Sprache, Band 3, S. 2391.
270 *Hoffmann*, Zweckbindung, S. 29; *Luhmann*, Zweckbegriff, S. 10.

also stets nur einen Ausschnitt aus dem Gesamtkomplex der Wirkungen.“[271] Der Zweck führe zu einem Ausblenden der Nebenwirkungen.[272] Die Funktion der Zwecksetzung sei die „Reduktion der Unendlichkeit“[273]. „Gemeinwohl“ sei kein geeigneter Zweck, da „die heuristische Funktion“ des Zweckes getrübt werde.[274] Eine starke Generalisierung führe dazu, dass die zweckerfüllenden Mittel nicht mehr bestimmt werden können.[275] Ein vager Zweck ermögliche „erhebliche Schwerpunktverlagerungen“, die bei konkreterer Zweckbestimmung eine Zweckänderung darstellten.[276]

v. Jhering stellt ein Zweckgesetz auf, demnach „kein Wollen, oder was dasselbe, keine Handlung ohne Zweck“ sei.[277] Es gebe keine zwecklosen Handlungen.[278]

Laut *Jonas* ist ein Zweck „das um dessentwillen eine Sache existiert und zu dessen Herbeiführung oder Erhaltung ein Vorgang stattfindet oder eine Handlung unternommen wird. Er antwortet auf die Frage «Wozu?».“[279]

Nach alledem lässt sich festhalten, dass der Zweck das Ziel einer Handlung benennt und deshalb einer hinreichenden Konkretisierung bedarf.

Damit stellt sich die Frage, welche Bedeutung dem zweiten Element, der Bindung an den Zweck zukommt. Der Zweckbindungsgrundsatz sei deshalb so wichtig, weil er gewährleiste, dass Daten nicht einfach in einem anderen Kontext genutzt werden, in dem sie eine andere Relevanz

---

271 *Luhmann*, Zweckbegriff, S. 44.
272 Vgl. *Luhmann*, Zweckbegriff, S. 44 u. 48.
273 *Luhmann*, Zweckbegriff, S. 48.
274 *Luhmann*, Zweckbegriff, S. 180.
275 *Luhmann*, Zweckbegriff, S. 190.
276 *Luhmann*, Zweckbegriff, S. 212 Fn. 57; vgl. *Walden*, Zweckbindung im Bereich der Polizei, S. 77.
277 *v. Jhering*, Der Zweck im Recht, Band I, S. 2.
278 *v. Jhering*, Der Zweck im Recht, Band I, S. 15.
279 *Jonas*, Verantwortung, S. 105.

haben können.[280] Es erfolge eine bewusste Einschränkung der multifunktionalen Verwendbarkeit der Daten.[281] Es wird sogar vertreten, dass sich „am Umgang mit der Zweckbindung (...) am ehesten und am besten ablesen (lasse), welche Bedeutung der Gesetzgeber dem Datenschutz tatsächlich beim(esse).“[282] Die Zweckbindung stehe „im Mittelpunkt der Verarbeitungsgrundsätze“,[283] da sie zu einer „Reduktion der Verarbeitung personenbezogener Daten auf das Unvermeidbare“ führe.[284] Ihr Ziel sei die Berechenbarkeit des Informationsflusses für den Betroffenen,[285] der die Preisgabe seiner Daten autonom steuern könne[286]. Der Zweckbindungsgrundsatz sei erforderlich zur Sicherstellung von Vorhersehbarkeit, Rechtssicherheit und der transparenten Verwendung personenbezogener Daten.[287]

Zwecksetzungen seien „der zentrale phasenübergreifende Baustein der gesetzlichen Regulierung der Verarbeitungsphasen“[288]. Dabei kommen

---

280 Vgl. *Globig*, in: Roßnagel (Hrsg.), Handbuch DSR, Kap. 4.7 Rn. 20; vgl. auch *Steinmüller*, Informationstechnologie, S. 199 f., der eine Zweckänderung als Informationsänderung ansieht.

281 *Roßnagel/Laue*, DÖV 2007, 543 (547); *Simitis*, in: Fürst/Herzog/Umbach (Hrsg.), FS Zeidler, Bd. 2, S. 1475 (1484); *Kutscha*, ZRP 1999, 156 (157); *Scholz/Pitschas*, Informationelle Selbstbestimmung, S. 41 sprechen von einer Festlegung des Verarbeitungsziels und der Begrenzung des Bearbeitungsumfangs.

282 *Simitis*, DuD 2000, 714 (722).

283 Ähnlich *Gola/Klug/Körffer*, in: Gola/Schomerus (Hrsg.), BDSG, § 14 Rn. 9, die den Zweckbindungsgrundsatz seit jeher für prägend halten; *Heckmann*, in: Taeger/Gabel (Hrsg.), BDSG, § 13 Rn. 27 hält ihn für ein wesentliches Element des Datenschutzes.

284 *Simitis*, in: Dammann/Simitis (Hrsg.), DSRL-Kommentar, Einl. Rn. 31.

285 *Heckmann*, in: Taeger/Gabel (Hrsg.), BDSG, § 14 Rn. 22.

286 *Martini*, DVBl 2014, 1481 (1484).

287 *Europäischer Datenschutzbeauftragter*, Privatssphäre und Wettbewerbsfähigkeit, Rn. 22.

288 *Albers*, in: Hoffmannn-Riem/Schmidt-Aßmann/Voßkuhle (Hrsg.), GVwR II², § 22, Rn. 123; siehe auch *Eßer*, in: Eßer/Kramer/v. Lewinski (Hrsg.), Auernhammer BDSG, § 14 Rn. 1, der von einem roten Faden spricht, der sich durch die Verarbeitungsphasen ziehe.

der Zweckfestlegung drei Aufgaben zu:[289] 1. Verklammerung von sachlichen Kompetenzen und Informations- und Datenverarbeitungen[290], 2. Zusammen mit der anschließenden Zweckbindung werden einzelne Verarbeitungsvorgänge zu Verarbeitungszusammenhängen zusammengefasst,[291] 3. Die Ermöglichung der Präzisierung, welche Daten und wie lange sie benötigt werden.

Der Zweckbindungsgrundsatz verhindert die Zusammenführung von Daten aus unterschiedlichen Quellen und damit die Erstellung von Persönlichkeitsprofilen.[292] Er fragmentiere die Datenverarbeitung und verhindere eine Konzentration des Wissens in der Hand der verantwortlichen Stelle, wodurch das Schadensrisiko für den Betroffenen minimiert werde.[293]

Die Zweckbindung sei ein wichtiges Instrument um „mission creep" zu verhindern.[294] Das Prinzip sei auf einen angemessenen Ausgleich ausgerichtet, der einerseits die Notwendigkeit der Vorhersehbarkeit und Rechtssicherheit, sowie andererseits das pragmatische Bedürfnis einer gewissen Flexibilität vereine.[295] Bei der Frage der Zulässigkeit von Zweckänderungen seien insbesondere die Schutzbedürftigkeit und daran anknüpfend Schutzvorkehrungen zu betrachten.[296]

Es lässt sich somit festhalten, dass die Zweckbindung aus zwei Elementen besteht: der Zweckfestlegung und der anschließenden Bindung an

---

289 Siehe hierzu: *Albers*, in: Hoffmannn-Riem/Schmidt-Aßmann/Voßkuhle (Hrsg.), GVwR II², § 22, Rn. 123; *Albers*, Informationelle Selbstbestimmung, S. 498 f.

290 Dies gilt jedenfalls für den öffentlichen Bereich.

291 So auch: *Bäcker*, Der Staat 51 (2012), 91 (98); *Brühann*, DuD 1996, 66 (68); *Pohle*, DANA 2015, 141 (142); *Brühann*, in: Roßnagel (Hrsg.), Handbuch DSR, Kap. 2.4 Rn. 28 fordert eine derartige Verklammerung durch die Zweckfestlegung ausdrücklich.

292 *Heckmann*, in: Heckmann (Hrsg.), jurisPK-Internetrecht, Kap. 9 Rn. 54.

293 Vgl. *Coudert/Dumortier/Verbruggen*, purpose specification, S. 5.

294 *Artikel-29-Datenschutzgruppe*, WP 203, S. 4.

295 *Artikel-29-Datenschutzgruppe*, WP 203, S. 5 u. 11.

296 *Albers*, in: Hoffmannn-Riem/Schmidt-Aßmann/Voßkuhle (Hrsg.), GVwR II², § 22, Rn. 128 f.

diesen Zweck. Dem Zweckbindungsprinzip kommt eine zentrale Rolle für die Strukturierung, Transparenz und die Kontrolle des Datenumgangs zu.

II. Entstehungsgeschichte

Der Zweckbindungsgrundsatz findet sich sowohl auf nationaler, supranationaler, als auch internationaler Ebene. Im Folgenden wird die Entwicklung auf diesen verschiedenen Ebenen betrachtet.

1. Internationale Entwicklungen

a) Fair Information Practices (FIPs)

In den USA wurden in den 1970er Jahren die sog. Fair Information Practices (FIPs) entwickelt.[297] Ein Bericht einer Beratergruppe an den US-amerikanischen Minister für Gesundheit, Bildung und Wohlfahrt[298] enthielt einen ersten Entwurf[299] dieser Prinzipien und wird in der Literatur als sehr einflussreich bezeichnet.[300] Der Bericht enthielt bereits die Vorgabe, dass ohne die Einwilligung des Betroffenen Daten, die für einen Zweck erhoben wurden, nicht für einen anderen Zweck genutzt oder übermittelt werden dürfen.[301] Der Grundgedanke der Zweckbindung ist

297 Vgl. *Solove/Schwartz*, Information Privacy Law, S. 655 f.; *Schwartz/Treanor*, Michigan Law Review (Vol. 101) 2003, 2163 (2180); teilweise werden die Prinzipien auch Fair Information Practice Principles (FIPPs) genannt.

298 *U.S. Department of Health, Education & Welfare*, Records, computers and the rights of citizens.

299 *Schwartz/Solove*, 86 N.Y.U. L.Q. Rev. 1814 (2011), 1814 (1825, dort Fn. 52); *Rotenberg*, Stanford Technology Law Review 1, 2001, Fn. 74.

300 *Schwartz*, Harvard Law Review, Vol. 126, 2013, 1966 (1969).

301 *U.S. Department of Health, Education & Welfare*, Records, computers and the rights of citizens, S. 41.

also hierin bereits enthalten. Die FIPs, deren Inhalt teils variiert, liegen vielen verschiedenen US-amerikanischen Gesetzen zugrunde.[302]

b) Europarat-Konvention 108

Eine maßgebliche Rolle bei der internationalen Entwicklung des Datenschutzes kommt dem Europarat zu.[303] Bereits Anfang der 1970er Jahre ergingen zwei Entschließungen des Ministerkomitees des Europarats zum Datenschutz. Im September 1973 wurde eine Resolution zum Schutz des Einzelnen bei der Speicherung personenbezogener Daten in elektronischen Datenbanken im nicht-öffentlichen Bereich verabschiedet.[304] Ein Jahr später, im September 1974, folgte eine Entschließung zum Schutz des Einzelnen bei der Speicherung personenbezogener Daten im öffentlichen Bereich.[305] Beide Entschließungen enthalten einen Appell[306] den in den Entschließungen genannten Prinzipien zur Geltung zu verhelfen. Der Zweckbindungsgrundsatz ist jeweils enthalten. So ist in Nr. 5 der Resolution für den nicht-öffentlichen Bereich vorgesehen, dass Informationen ohne angemessene Erlaubnis nicht für einen anderen Zweck, als den Zweck für den sie gespeichert wurden, genutzt oder übermittelt werden dürfen.[307]

---

302 Vgl. *Schwartz*, The Yale Law Journal, Vol. 118, 2009, 902 (907 f.).

303 Vgl. *Simitis*, in: Simitis (Hrsg.), BDSG, Einl. Rn. 151; *Tinnefeld/Buchner/Petri*, Datenschutzrecht, S. 72.

304 Resolution 73 (22): „Resolution on the Protection of the Privacy of Individuals vis-a-vis Electronic Data Banks in the Private Sector".

305 Resolution 74 (29): „Resolution on the Protection of the Privacy of Individuals vis-a-vis Electronic Data Banks in the Public Sector".

306 *Simitis*, in: Simitis (Hrsg.), BDSG, Einl. Rn. 151; deutlich wird dies an der Formulierung: „Recommends the governments of member States: (a) to take all steps which they consider necessary to give effect to the principles set out in the Annex of this resolution."

307 Eine ähnliche Regelung für den öffentlichen Bereich findet sich in Resolution 74 (29) Nr. 3 b) und c), die eine Zweckfestlegung und Bindung vorsieht.

Anfang 1981 wurde das „Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten“[308] zur Unterschrift ausgelegt. In Kraft trat es gemäß Art. 22 Abs. 2 nach der Unterzeichnung durch fünf Staaten, darunter die Bundesrepublik Deutschland am 1.10.1985.[309] Die Konvention ist der erste völkerrechtlich bindende Vertrag im Datenschutzrecht.[310] Derzeit wird über eine Modernisierung der Konvention beratschlagt.[311]

In Art. 5 lit. b zur Qualität der Daten ist vorgeschrieben, dass personenbezogene Daten, die automatisch verarbeitet werden, für festgelegte und rechtmäßige Zwecke gespeichert sein müssen und nicht so verwendet werden dürfen, dass es mit diesen Zwecken unvereinbar ist. Auch hier ist also bereits eine Zweckfestlegung und anschließende Bindung daran mittels einer Zweckvereinbarkeitsformel vorgesehen.

c) OECD Guidelines

Die Organisation für wirtschaftliche Zusammenarbeit und Entwicklung (OECD) hat auf der Grundlage der FIPs[312] in 1980 „Leitlinien für den Schutz des Persönlichkeitsrechts und den grenzüberschreitenden Verkehr personenbezogener Daten“[313] erlassen. Dabei war es für die OECD besonders wichtig zu verhindern, dass der Datenschutz sich zu einem Handelshemmnis entwickeln könnte.[314] Anders als die Konvention Nr. 108 des Europarats, sind die Leitlinien der OECD nicht verbindlich.[315] Ge-

---

308 Convention for the protection of individuals with regard to automatic processing of personal data, European Treaty Series No. 108, EU DS, EuRAT-Conv.
309 *Simitis*, in: Simitis (Hrsg.), BDSG, Einl. Rn. 151.
310 *Agentur der europäischen Union für Grundrechte*, Handbuch, S. 16; *Tinnefeld/Buchner/Petri*, Datenschutzrecht, S. 74.
311 *Agentur der europäischen Union für Grundrechte*, Handbuch, S. 17.
312 Vgl. *Burkert*, in: Roßnagel (Hrsg.), Handbuch DSR, Kap. 2.3 Rn. 23.
313 OECD, Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data, Document C (80) 58 (final).
314 Vgl. *Kühling/Seidel/Sivridis*, Datenschutzrecht, Rn. 14.
315 *Tinnefeld/Buchner/Petri*, Datenschutzrecht, S. 71.

genüber der Regelung zur Zweckbindung in der Konvention 108 des Europarats fällt auf, dass eine Unterteilung in ein Zweckfestlegungs-[316] und ein Verwendungsbeschränkungsprinzip[317] vorgenommen wurde und die Zweckfestlegung explizit zum Zeitpunkt der Erhebung zu erfolgen hat und nicht erst im Zusammenhang mit der Speicherung genannt wird.[318] Inhaltlich sind diese Vorgaben aber ebenfalls in der Konvention 108 des Europarats enthalten. Durch die Verwendungsbeschränkung auf den Erhebungszweck wird die Zweckbindung verwirklicht. Als Ausnahmen sind die Einwilligung des Betroffenen und eine gesetzliche Zweckänderungserlaubnis vorgesehen.

d) UN Guidelines for the regulation of computerized personal data files

Die Vereinten Nationen beschäftigten sich ebenfalls mit dem Datenschutz. Ende 1990 verabschiedete die Generalversammlung die „Richtlinien betreffend personenbezogene Daten in automatisierten Dateien".[319] Unter A 3. ist in den Richtlinien eine Regelung zur Zweckfestlegung enthalten. Sie ähnelt den Bestimmungen der Konvention 108 und der OECD Guidelines. Der genaue Zeitpunkt der Zweckfestlegung ist aber nicht bestimmt. Für Zweckänderungen stützen sich die Leitlinien auf eine Prüfung der Unvereinbarkeit mit dem ursprünglichen Zweck (incompatible use). Die UN-Leitlinien sind nicht bindend.[320]

316 Nr. 9 OECD Guidelines, Purpose Specification Principle.
317 Nr. 10 OECD Guidelines, Use Limitation Principle.
318 *Burkert*, in: Roßnagel (Hrsg.), Handbuch DSR, Kap. 2.3 Rn. 29 bezeichnet die OECD Guidelines insofern als *„in der Formulierung spezifischer"*.
319 United Nations, Guidelines for the regulation of computerized personal data files, Resolution 45/95, 14. Dezember 1990, UN Doc E/CN4/1990/72.
320 *Burkert,* in: Roßnagel (Hrsg.), Handbuch DSR, Kap. 2.3 Rn. 40.

e) APEC Privacy Framework

Die asiatisch-pazifische Wirtschaftsgemeinschaft (APEC) hat im November 2004 Leitlinien für den Datenschutz erlassen.[321] Das APEC Privacy Framework[322] enthält nicht bindende Richtlinien.[323] Sie sollen ausweislich Nr. 5 der Präambel mit den OECD-Richtlinien vereinbar sein. Interessant ist, dass der Zweckbindungsgrundsatz anders formuliert ist. Einerseits ergibt sich die Notwendigkeit einer Zweckfestlegung lediglich indirekt daraus, dass der Betroffene über den Zweck der Erhebung zu informieren ist, (Teil 3, II. Notice Nr. 15 lit. b). Andererseits heißt es in Teil 3. IV. Uses of Personal Information Nr. 19, dass die Daten grundsätzlich nur für den Erhebungszweck und andere kompatible und ähnliche Zwecke genutzt werden dürfen. Bemerkenswert ist, dass eine positive Formulierung vorgenommen wurde. In anderen Regelungen ist immer negativ davon die Rede, dass die Zwecke nicht inkompatibel sein dürfen. Zudem ist in anderen internationalen Texten keine Erlaubnis für die Nutzung für ähnliche[324] Zwecke enthalten. Die Formulierung ist also deutlich offener als in den OECD Guidelines. Darüber hinaus sei noch angemerkt, dass bei den zulässigen Fällen der Zweckdurchbrechung unter Teil 3, IV. Uses of Personal Information, Nr. 19 lit. b) vorgesehen ist, dass eine Nutzung für einen anderen Zweck zulässig sein soll, wenn dies notwendig ist, um eine Dienstleistung oder ein Produkt anzubieten, das der Betroffene bestellt hat.[325]

321 Siehe hierzu *Greenleaf*, CLSR 25 (2009), 28.

322 APEC Privacy Framework, im Internet abrufbar unter: http://www.apec.org/Groups/Committee-on-Trade-and-Investment/~/media/Files/Groups/ECSG/05_ecsg_privacyframewk.ashx, (abgerufen am 11.05.2018).

323 *Greenleaf*, CLSR 25 (2009), 28 (29).

324 Nicht zu verwechseln mit kompatiblen Zwecken.

325 Kritisch zu dieser Ausnahme: *Greenleaf*, CLSR 25 (2009), 28 (30), der großes Missbrauchspotential sieht.

2. Europäische Union

Auch auf europäischer Ebene wurde die Bedeutung des Datenschutzes erkannt. Es wurden verschiedene Richtlinien und Verordnungen von der Europäischen Wirtschaftsgemeinschaft (EWG) und ihren Nachfolgeorganisationen, der Europäischen Gemeinschaft (EG) und der Europäischen Union (EU) erlassen. Diese sollen nun im Folgenden mit Blick auf die Regelungen zur Zweckbindung näher betrachtet werden.

a) Richtlinie 95/46/EG

Am 24. Oktober 1995 wurde die Richtlinie 95/46/EG des Europäisches Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (DSRL) erlassen.[326] Durch die DSRL sollte eine Vollharmonisierung des Datenschutzes in der EU erfolgen.[327] Aufgrund der allgemeinen Vorgaben der DSRL überlässt diese aber den Mitgliedstaaten in vielen Fällen die Möglichkeit der Konkretisierung oder die Wahl zwischen Optionen.[328]

aa) Art. 5 DSRL

Im Rahmen der näheren Bestimmung der Voraussetzungen der Datenverarbeitung nach Art. 5 DSRL ist eine Präzisierung unbestimmter Rechtsbegriffe, wie „Treu und Glauben“ oder der „Nichtvereinbarkeit“ mit dem Erhebungszweck vorzunehmen.[329] Dies ergibt sich auch aus

---

326 ABl. Nr. L 281/31 v. 23.11.1995, S. 31 ff.; Zur Entstehungsgeschichte siehe nur: *Simitis*, in: Dammann/Simitis (Hrsg.), DSRL-Kommentar, C. Einl., Rn. 1-10.

327 *Brühann*, in: Grabitz/Hilf/Nettesheim (Hrsg.), DSRL, Vorbemerkung, Rn. 45 und Art. 10 Rn. 7; ausführlich hierzu: *Brühann*, EuZW 2009, 639 (642); im Ergebnis auch *Ehmann/Helfrich*, DSRL-Kommentar, Einl. Rn. 13, die eine Abweichung nur im Rahnen von Öffnungsklauseln für möglich halten.

328 EuGH, Urteil v. 06.11.2003 - C-101/01- Lindqvist Rn. 83.

329 *Brühann,* in: Grabitz/Hilf/Nettesheim (Hrsg.), DSRL, Art. 5 Rn. 7 f.

ErwG 9 DSRL, der den Mitgliedstaaten explizit einen Umsetzungsspielraum zugesteht.[330] Die *Artikel-29-Datenschutzgruppe* stellte fest, dass die Umsetzung der DSRL in den Mitgliedstaaten zu einer unterschiedlich weiten Definition des Zwecks und zu verschiedenen Maßstäben zur Bestimmung der Rechtmäßigkeit der Zweckänderung geführt habe.[331] So gebe es einerseits das Kriterium der vernünftigen Erwartungen des Betroffenen und andererseits eine Güter- und Interessenabwägung.[332]

bb) Art. 6 DSRL

Art. 6 DSRL ist die zentrale Norm für die Zweckbindung der DSRL, da dort der Zweckbindungsgrundsatz festgeschrieben ist.

(1) Entstehungsgeschichte

Im ersten Entwurf der EWG-Kommission für die DSRL[333] war noch eine Trennung des öffentlichen und des nicht-öffentlichen Bereichs vorgesehen. Für den öffentlichen Bereich sah Art. 5 Abs. 1 lit. a des ersten Kommissionsentwurfs (DSRL-E[1]) vor, dass die Erstellung einer Datei und die Datenverarbeitung für eine Aufgabe im Rahmen des Zuständigkeitsbereichs der Behörde zulässig seien. In Art. 5 Abs. 1 lit. b DSRL-E[1] war vorgesehen, dass die Datei zu einem anderen als ihrem Errichtungszweck verarbeitet werden dürfe, wenn einer von vier Gründen vorlag. Dies waren eine Einwilligung, eine gesetzliche Grundlage, ein Nichtentgegenstehen eines berechtigten Interesses der betroffenen Person oder eine drohende Gefahr für die öffentliche Sicherheit und Ordnung. Art. 6 Abs. 1 DSRL-E[1] sah Regelungen zur Weitergabe von personenbezogenen Daten vor. Diese sollte zulässig sein, wenn sie im Rahmen der Aufgaben

330 Vgl. *Dammann*, in: Dammann/Simitis (Hrsg.), DSRL-Kommentar, Art. 5 Rn. 4.
331 *Artikel-29-Datenschutzgruppe*, WP 203, S. 10.
332 *Artikel-29-Datenschutzgruppe*, WP 203, S. 10.
333 Vorschlag für eine Richtlinie des Rates zum Schutz von Personen bei der Verarbeitung personenbezogener Daten, ABl. Nr. 90/C 277/03.

der übermittelnden oder der empfangenden öffentlichen Stelle erforderlich war, oder bei Übermittlung an einen Privaten, wenn eine Interessenabwägung ein Überwiegen seiner Interessen ergab. Für den nicht-öffentlichen Bereich sah Art. 8 Abs. 1 DSRL-E[1] vor, dass eine Datenverarbeitung aufgrund einer Einwilligung oder einer der genannten Gründe zulässig sei. Eine Gestattung der Verarbeitung für einen anderen Zweck war in dieser Vorschrift aber nicht vorgesehen. Vielmehr war in Art. 8 Abs. 2 DSRL-E[1] bestimmt, dass die Mitgliedstaaten vorsehen sollten, dass der Verantwortliche sich zu vergewissern habe, dass eine Weitergabe mit dem Zweck der Dateien vereinbar sei. Diese unterschiedlichen Anforderungen an die Weitergabe im öffentlichen und im nicht-öffentlichen Bereich wurden vom Europäischen Wirtschafts- und Sozialausschuss der EWG zu Recht als nicht gerechtfertigt kritisiert.[334]

In Art. 16 Abs. 1 lit. b DSRL-E[1] war der Zweckbindungsgrundsatz normiert. Dieser lautete:

> Art. 16 (1) Die Mitgliedstaaten bestimmen wie folgt (…)
>
> b) die Daten sind für bestimmte, ausdrücklich festgelegte und rechtmäßige Zwecke zu speichern und in einer mit diesen Zweckbestimmungen zu vereinbarenden Art zu verwenden;

Auf die Datenerhebung wurde in dieser Regelung noch nicht abgestellt, obwohl dieser Begriff beispielsweise in Art. 16 Abs. 1 lit. a DSRL-E[1] Verwendung fand. Trotzdem kann zumindest bezweifelt werden, ob dies bewusst geschah. Denn die Begründung der Kommission für ihren Entwurf lässt vermuten, dass ohnehin terminologisch nicht ganz sauber gearbeitet wurde. Dort heißt es, dass durch den Begriff „Verwenden" deutlich werde, dass nicht nur die Verarbeitung der Zweckbestimmung

334 Siehe Europäischer Wirtschafts- und Sozialausschuss, Stellungnahme zu dem Vorschlag für eine Richtlinie des Rates zum Schutz von Personen bei der Verarbeitung personenbezogener Daten, ABl. Nr. C 159/38 v. 17.06.1991, S. 42.

der Datei entsprechen müsse.[335] Verwunderlich ist diese Aussage deshalb, weil gemäß Art. 2 lit. d DSRL-E[1] die „Benutzung“[336] als Unterfall der Verarbeitung definiert wird und nicht der Verwendung. Der Begriff der Verwendung wird in der DSRL-E[1] nicht definiert. Zudem fordert Art. 13 DSRL-E[1] die Unterrichtung des Betroffenen über die Zweckbestimmung der Datei bereits zum Zeitpunkt der Erhebung. Dies hob auch die Kommission in ihrer Begründung des Richtlinienentwurfs hervor.[337] In der Begründung führte die Kommission weiter aus, dass eine Weiterverarbeitung nicht mit der „früheren Zweckbestimmung unvereinbar“ sein dürfe.[338] Aus dieser Formulierung wird nicht deutlich, ob es sich dabei um den Erhebungszweck bzw. den Zweck der erstmaligen Speicherung handeln muss oder ob eine graduelle Verschiebung der Zweckbestimmung durch eine Reihe von Zweckänderungen möglich ist. Allerdings deutet der Gesetzeswortlaut des Entwurfs auf eine stete Anknüpfung an den erstmaligen Speicherungszweck, auch bei einer Reihe von Zweckänderungen.

Des Weiteren fällt auf, dass die Formulierung zur Vereinbarkeit des Weiterverarbeitungszwecks mit dem ursprünglichen Speicherungszweck nicht negativ sondern positiv gehalten ist. In der Begründung findet sich diese Passage aber in einer dem späteren Richtlinientext entsprechenden

---

335 Mitteilung der Kommission zum Schutz von Personen bei der Verarbeitung personenbezogener Daten in der Gemeinschaft und zur Sicherheit der Informationssysteme v. 13.09.1990, KOM (90), 314 – SYN 287 und 288 endg., zitiert nach: BR-Drs. 690/90, hier S. 35 f. Auch in der englischen Fassung ist dies entsprechend mit „processing“ und „use“ formuliert, siehe COM (90), 314 – SYN 287 and 288 final, S. 34.

336 In der englischen Fassung „use“ und damit der Formulierung in der Kommissionsmitteilung entsprechend.

337 Mitteilung der Kommission zum Schutz von Personen bei der Verarbeitung personenbezogener Daten in der Gemeinschaft und zur Sicherheit der Informationssysteme v. 13.09.1990, KOM (90), 314 – SYN 287 und 288 endg., zitiert nach: BR-Drs. 690/90, hier S. 35.

338 Mitteilung der Kommission zum Schutz von Personen bei der Verarbeitung personenbezogener Daten in der Gemeinschaft und zur Sicherheit der Informationssysteme v. 13.09.1990, KOM (90), 314 – SYN 287 und 288 endg., zitiert nach: BR-Drs. 690/90, hier S. 35., siehe COM (90), 314 – SYN 287 and 288 final, S. 34, dort heißt es „former purpose“.

negativen Form.[339] Es ist also nicht davon auszugehen, dass hiermit eine Bedeutungsänderung beabsichtigt wurde.

Das EU-Parlament verlangte anstatt des Maßstabs der Vereinbarkeit der Zwecke eine „Übereinstimmung" der Zwecke.[340] Hierdurch wäre die Zweckbindung, jedenfalls ohne die Möglichkeit einer Zweckänderung aufgrund einer Abwägung im Einzelfall, deutlich verschärft worden.[341] Zudem wollte das EU-Parlament normieren, dass die Zweckbestimmung bereits zum Zeitpunkt der Erhebung stattzufinden habe.[342]

Im geänderten Vorschlag der Kommission[343] wurde die Zweckbindung wie folgt gefasst:

Art. 6 (1) Die Mitgliedstaaten sehen folgendes vor: (…)

b) die Daten müssen für bestimmte, ausdrücklich festgelegte und rechtmäßige Zwecke erhoben und in einer mit diesen Zweckbestimmungen zu vereinbarenden Weise verwendet werden;

Die im ursprünglichen Kommissionsentwurf vorgesehenen Regelungen der Verarbeitung zu einem anderen Zweck als dem Erhebungszweck wurden mit dem geänderten Kommissionsvorschlag auf Anregung des Parlaments gestrichen.[344] Bestehen blieb nur eine allgemeine Bestimmung zur Zweckbindung, Art. 6 Abs. 1 lit. b geänderter Vorschlag der

339 Mitteilung der Kommission zum Schutz von Personen bei der Verarbeitung personenbezogener Daten in der Gemeinschaft und zur Sicherheit der Informationssysteme v. 13.09.1990, KOM (90), 314 – SYN 287 und 288 endg., zitiert nach: BR-Drs. 690/90, S. 35.

340 ABl. Nr. C 94/173 v. 13.04.1992, S. 189, Änderung Nr. 59.

341 Vgl. *Brühann*, in: Grabitz/Hilf/Nettesheim (Hrsg.), DSRL, Art. 6 Rn. 4.

342 ABl. Nr. C 94/173 v. 13.04.1992, S. 189, Änderung Nr. 59.

343 Geänderter Vorschlag für eine Richtlinie des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, ABl. Nr. C 311/30 v. 27.11.1992.

344 Amended proposal for a Council Directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data, COM (92), 422 final - SYN 287, S. 16.

Kommission (DSRL-E^2). Die Kommission sah diese Bestimmung in Verbindung mit Art. 7 DSRL-E^2 als ausreichend an.[345]

Bei der Zweckbindung wurde auf Anregung des Parlaments nunmehr auf den Erhebungszweck und nicht den Zweck der Speicherung abgestellt.[346] Eine Privilegierung von Daten für historische, statistische und wissenschaftliche Zwecke wurde zuerst vom Parlament vorgeschlagen[347] und von der Kommission in Art. 6 Abs. 1 lit. e DSRL-E^2 übernommen. Während in dem Vorschlag des Parlaments aufgrund der Formulierung „an Archive weitergegeben" noch angedeutet wird, dass eine privilegierte Zweckänderung beabsichtigt ist, wird dies im geänderten Kommissionsvorschlag nicht richtig deutlich (für die privilegierten Zwecke „aufbewahrt"). Dass dies aber beabsichtigt war, zeigt die Begründung, in der ausgeführt wird, dass die Speicherung für die privilegierten Zwecke vorgesehen ist, wenn die Daten für den Primärzweck nicht mehr erforderlich sind.[348]

Schließlich erhielt die Zweckbindung in Art. 6 Abs. 1 lit. b DSRL folgende Fassung:

Art. 6 (1) Die Mitgliedstaaten sehen vor, daß personenbezogene Daten (…)

b) für festgelegte eindeutige und rechtmäßige Zwecke erhoben und nicht in einer mit diesen Zweckbestimmungen nicht zu vereinbarenden Weise weiterverarbeitet werden. Die Weiterver-

345 Amended proposal for a Council Directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data, COM (92), 422 final - SYN 287, S. 16.

346 Amended proposal for a Council Directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data, COM (92), 422 final - SYN 287, S. 4.

347 ABl. Nr. C 94/173 v. 13.04.1992, S. 189, Änderung Nr. 60.

348 Amended proposal for a Council Directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data, COM (92), 422 final - SYN 287, S. 16.

> arbeitung von Daten zu historischen, statistischen oder wissenschaftlichen Zwecken ist im allgemeinen nicht als unvereinbar mit den Zwecken der vorausgegangenen Datenerhebung anzusehen, sofern die Mitgliedstaaten geeignete Garantien vorsehen;

Diese Formulierungen entstammen dem gemeinsamen Standpunkt des Rats[349] und wurden ohne weitere Änderung als Richtlinientext verabschiedet. Die Vereinbarkeitsformel wurde von einer positiven Formulierung in eine negative Fassung umgewandelt, ohne dass dadurch eine Bedeutungsänderung indiziert wäre.[350] Neu ist insbesondere das nunmehr festgehalten ist, dass eine Weiterverarbeitung zu den genannten privilegierten Zwecken grundsätzlich keine Zweckänderung darstellt.

(2) Vorgaben für die Zweckfestlegung

Dem Wortlaut der DSRL lässt sich kein genauer Maßstab für den Konkretisierungsgrad der Zweckfestlegung entnehmen. In ihrer Begründung des geänderten Richtlinienvorschlags forderte die EU-Kommission, dass „(…) das Ziel der Erhebung und Benutzung der Daten (…) so genau wie möglich definiert werden (müsse)“.[351] Dem entspreche eine „allgemeine oder vage Definition“ wie z. B. „für kommerzielle Zwecke“ nicht.[352] Eine

---

349 Gemeinsamer Standpunkt (EG) Nr. 1/95 vom Rat festgelegt am 20. Februar 1995 im Hinblick auf den Erlass der Richtlinie 95/…/EG des europäischen Parlaments und des Rates vom … zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, ABl. Nr. C 93/1.

350 D. II. 2. a) bb) (1), S. 111 f.

351 Amended proposal for a Council Directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data, COM (92), 422 final - SYN 287, S. 15.

352 Amended proposal for a Council Directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data, COM (92), 422 final - SYN 287, S. 15; so auch *Brühann*, in:

konkrete Zweckfestlegung wird auch in der Literatur vielfach gefordert.[353] Der Zweck müsse detailliert genug sein, um feststellen zu können, welche Art der Datenverarbeitung davon noch umfasst ist und welche nicht und um die Rechtmäßigkeit der Verarbeitung überprüfen sowie gegebenenfalls Schutzmaßnahmen ergreifen zu können.[354] So seien Zwecke wie „Zwecke der IT-Sicherheit", „zukünftige Forschung", „Zwecke des Marketings" zu vage oder allgemein gehalten und grundsätzlich nicht ausreichend.[355] Der erforderliche Konkretisierungsgrad des Zweckes hänge vom Kontext der Datenerhebung und der Art der personenbezogenen Daten ab.[356] Manchmal könne eine detaillierte Beschreibung der Zwecke sogar kontraproduktiv sein, weshalb sich eine „layered-notice" anbiete.[357] Bei dieser würden wesentliche Informationen in knapper, präziser und verständlicher Form zur Verfügung gestellt, während ausführlichere Erläuterungen für jene abrufbar seien, die weitere Erläuterungen wünschten.[358] Schon frühzeitig wurde eine solche Aufteilung der Betroffeneninformation in mehrere Stufen mit unterschiedlichem Detailierungsgrad mit Verweis auf die in Art. 10 DSRL enthaltene Unterscheidung zwischen Mindest- und zusätzlichen Informationen vorgeschlagen.[359] Art. 10 DSRL zählt die Information über den Zweck aber zu den zwingenden Mindestangaben. Bei einer Erhebung von Daten für verschiedene Zwecke könne ein übergreifender Zweck sinnvoll sein.[360] Allerdings müsse jeder

---

Grabitz/Hilf/Nettesheim (Hrsg.), DSRL, Art. 6 Rn. 9, der „geschäftsmäßige Verarbeitung" oder „Bankgeschäfte" nicht als Zweck genügen lassen will.

353 So z. B. *Brühann*, in: Roßnagel (Hrsg.), Handbuch DSR, Kap. 2.4 Rn. 28; *Ehmann/Helfrich*, DSRL-Kommentar, Art. 6 Rn. 8, die dies als „Bestimmtheitsgrundsatz" bezeichnen; *Dammann*, in: Dammann/Simitis (Hrsg.), DSRL-Kommentar, Art. 6 Rn. 7; *Simitis*, NJW 1997, 281 (285); mit erheblichen Zweifeln an einer „vagen" Zweckfestlegung auch: *Artikel-29-Datenschutzgruppe*, WP 83, S. 8.

354 *Artikel-29-Datenschutzgruppe*, WP 203, S. 15.

355 *Artikel-29-Datenschutzgruppe*, WP 203, S. 16.

356 *Artikel-29-Datenschutzgruppe*, WP 203, S. 16.

357 *Artikel-29-Datenschutzgruppe*, WP 203, S. 16.

358 *Artikel-29-Datenschutzgruppe*, WP 203, S. 16; siehe zu diesem Vorgehen bereits *Artikel-29-Datenschutzgruppe*, WP 160, S. 11.

359 *Artikel-29-Datenschutzgruppe*, WP 100, S. 5 f.

360 *Artikel-29-Datenschutzgruppe*, WP 203, S. 16.

einzelne Zweck präzise genug definiert sein, um die Anforderungen von Art. 6 Abs. 1 lit. b DSRL zu erfüllen.[361]

Der Zeitpunkt der Zweckfestlegung ist in der DSRL nicht explizit genannt. Der Wortlaut von Art. 6 Abs. 1 lit. b DSRL deutet mit der Formulierung „festgelegte" Zwecke aber darauf hin, dass diese vor bzw. bei der Erhebung zu erfolgen hat. Dafür spricht auch, dass die Einwilligung nach Art. 7 lit. a DSRL „ohne jeden Zweifel" erfolgt sein muss, was nur bei Kenntnis des Verarbeitungszwecks der Fall sein kann.[362] Sofern eine Vorabkontrolle gemäß Art. 20 DSRL erforderlich ist, bedarf es ebenfalls der vorherigen Zweckfestlegung. Art. 10 DSRL, der die Information des Betroffenen im Falle einer Direkterhebung vorsieht, nennt ebenfalls nicht ausdrücklich einen Zeitpunkt der Information über die Zweckbestimmungen der Verarbeitung.[363] Aus Sinn und Zweck der Norm ergibt sich, dass die Information bei der Erhebung und damit die Zweckfestlegung bereits vorher zu erfolgen hat.[364] Dafür spricht auch die Begründung des geänderten Kommissionsvorschlags, die eine Zweckfestlegung vor der Erhebung fordert.[365] Entgegen des Wortlauts ist eine Zweckfestlegung auch bei Daten erforderlich, die nicht erhoben wurden.[366] Denkbar ist dies beispielsweise im Falle einer Spontanübermittlung.

Das Kriterium der Eindeutigkeit des Zweckes setze voraus, dass der Zweck hinreichend klar benannt werde,[367] so dass keine Zweifel bezüglich der Auslegung des Zwecks entstehen können.[368] Der englische Be-

361 *Artikel-29-Datenschutzgruppe*, WP 203, S. 16.
362 *Ehmann/Helfrich*, DSRL-Kommentar, Art. 7 Rn. 15.
363 *Ehmann/Helfrich*, DSRL-Kommentar, Art. 10 Rn. 7; *Brühann*, in: Grabitz/Hilf/Nettesheim (Hrsg.), DSRL, Art. 10 Rn. 9.
364 Vgl. *Brühann*, in: Grabitz/Hilf/Nettesheim (Hrsg.), DSRL, Art. 6 Rn. 10; *Ehmann/Helfrich*, DSRL-Kommentar, Art. 11 Rn. 5 sprechen vom „frühestmöglichen Zeitpunkt".
365 Amended proposal for a Council Directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data, COM (92), 422 final - SYN 287, S. 15.
366 *Dammann*, in: Dammann/Simitis (Hrsg.), DSRL-Kommentar, Art. 6 Rn. 9.
367 *Artikel-29-Datenschutzgruppe*, WP 203, S. 12.
368 *Dammann*, in: Dammann/Simitis (Hrsg.), DSRL-Kommentar, Art. 6 Rn. 6.

griff „explicit“ sei nicht mit gleicher Bedeutung in alle Amtssprachen übersetzt worden.[369] „Explicit“ verdeutliche, dass die Zwecke genannt und erklärt werden müssten, während die deutsche Fassung „eindeutig“ mehr auf das Ergebnis eines unmissverständlichen Zweckes abziele.[370] Im Ergebnis bringe dies aber die gleichen Anforderungen mit sich.[371]

Weder Bedeutung noch Intention der Zwecksetzung dürfe vage oder mehrdeutig sein.[372] Der Kontext der Datenverarbeitung und Sitten und Gebräuche könnten es in manchen Fällen ausreichen lassen, lediglich die wesentlichen Elemente der Zwecke zu benennen, wobei diejenigen, die das wünschen, mehr Informationen erhalten können sollen.[373] Im Falle von Unklarheiten, sollten alle Fakten beachtet werden, verbunden mit dem üblichen Verständnis und den vernünftigen Erwartungen der Betroffenen aufgrund des Kontexts des Falles.[374] Unklarheiten bei der Zweckbestimmung gehen zu Lasten der verantwortlichen Stelle.[375]

Mit dem Erfordernis der „Rechtmäßigkeit“ des Zwecks sei nicht nur eine notwendige Rechtsgrundlage für die Verarbeitung nach Art. 7 DSRL in den Blick genommen, sondern die Anforderungen der Rechtsordnung insgesamt.[376] In Anknüpfung an den Wortlaut der englischen Fassung der DSRL (*legitimate*) vertritt die *Artikel-29-Datenschutzgruppe* die Ansicht, dass der Kontext der Datenverarbeitung, aus dem sich die vernünftigen Erwartungen ergäben[377] sowie die Frage, ob die Beziehung zwischen verantwortlicher Stelle und Betroffenem kommerzieller Art ist oder nicht, von Bedeutung sei.[378]

---

369 Vgl. *Artikel-29-Datenschutzgruppe*, WP 203, S. 17.
370 *Artikel-29-Datenschutzgruppe*, WP 203, S. 17 und dort Fn. 42.
371 *Artikel-29-Datenschutzgruppe*, WP 203, S. 18.
372 *Artikel-29-Datenschutzgruppe*, WP 203, S. 17.
373 *Artikel-29-Datenschutzgruppe*, WP 203, S. 18 f.
374 *Artikel-29-Datenschutzgruppe*, WP 203, S. 39.
375 *Ehmann/Helfrich*, DSRL-Kommentar, Art. 6 Rn. 13.
376 *Artikel-29-Datenschutzgruppe*, WP 203, S. 12 u. 19.
377 *Artikel-29-Datenschutzgruppe*, WP 203, S. 12.
378 *Artikel-29-Datenschutzgruppe*, WP 203, S. 20.

Die Entstehungsgeschichte und die Funktion der Zweckbindung in der DSRL sprechen somit für eine möglichst konkrete Zweckfestlegung, wobei sich der Konkretisierungsgrad nach den Erhebungsumständen richtet.

(3) Zulässigkeit einer Zweckänderung

Die Zulässigkeit einer Zweckänderung ist nach der DSRL gegeben, wenn der neue Zweck und der Erhebungszweck vereinbar sind. Eine Unvereinbarkeit der Zwecke sei insbesondere bei „besonders sensiblen Daten" anzunehmen.[379] Es komme insbesondere auf die Auswirkungen der Datenverwendung zu dem neuen Zweck und das Verhältnis zum Erhebungszweck an.[380] Eine Unvereinbarkeit liege vor, wenn eine Abwägung ergebe, dass die Weiterverarbeitung zu einer unzumutbaren Beeinträchtigung der betroffenen Person führe.[381] Eine Unvereinbarkeit sei zu bejahen, wenn sich die Verarbeitungs- und Verwendungsmaßgaben widersprächen und auch nicht durch besondere Vorkehrungen in Einklang gebracht werden könnten.[382] Um dies festzustellen hat die *Artikel-29-Datenschutzgruppe* einen Kriterienkatalog erarbeitet, auf den im Zusammenhang mit der DSGVO eingegangen wird.[383]

Die Kompatibilität des Weiterverarbeitungszwecks soll sich immer auf den ursprünglichen Erhebungszweck beziehen, damit ein graduelles Abweichen im Rahmen mehrerer Zweckänderungen ausgeschlossen ist.[384] Dies wurde in der Begründung der Kommission zum zweiten Entwurf in-

379 Vgl. *Rüpke*, ZRP 1995, 185 (190).
380 *Dammann*, in: Dammann/Simitis (Hrsg.), DSRL-Kommentar, Art. 6 Rn. 8.
381 *Albers*, Informationelle Selbstbestimmung, S. 324 f.
382 *Albers*, Informationelle Selbstbestimmung, S. 324.
383 *Artikel-29-Datenschutzgruppe*, WP 203, hierauf wird unter D. IV. 2. b) aa) (1) noch eingegangen, S. 236 ff.
384 *Brühann*, in: Grabitz/Hilf/Nettesheim (Hrsg.), DSRL, Art. 6 Rn. 12.

sofern klargestellt, dass es nunmehr „ursprünglicher Zweck“ und nicht mehr „früherer Zweck“ heißt.[385]

Die Weiterverarbeitung zu historischen, statistischen oder wissenschaftlichen Zwecken gilt grundsätzlich nicht als unvereinbar mit dem Erhebungszweck, sofern die Mitgliedstaaten geeignete Garantien vorsehen, die ausschließen, dass die Daten für Maßnahmen oder Entscheidungen gegenüber dem Betroffenen verwendet werden, Art. 6 Abs. 1 lit. b i. V. m. ErwG 29 DSRL. Der Begriff der Statistik soll weit zu verstehen sein, weshalb nicht nur die amtliche Statistik davon umfasst sei,[386] so dass auch Big-Data-Analysen hierunter fallen könnten.

Es handelt sich um eine widerlegbare Vermutung zugunsten der genannten Zwecke.[387] Diese Privilegierung bezieht sich aber nur auf eine Weiterverarbeitung zu den genannten Zwecken. Eine Weiterverarbeitung von für historische, statistische oder wissenschaftliche Zwecke erhobenen Daten zu anderen Zwecken kann sich nicht im Umkehrschluss darauf stützen.[388] Der Regelung liegt die Überlegung zugrunde, dass grundsätzlich bei Datenverarbeitungen zu diesen Zwecken der Bezug der Daten zu einzelnen Personen nicht von Interesse ist.[389] Zur Auslegung dieser Bestimmung kann auch Art. 13 Abs. 2 DSRL herangezogen werden.[390] Nach Art. 13 Abs. 2 DSRL können die Auskunftsrechte des Art. 12 DSRL ein-

---

385 Geänderter Vorschlag für eine Richtlinie des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, KOM(92) 422 endg. - SYN 287 – zitiert nach BT-Drs. 12/8329, S. 18. In der englischen Sprachfassung „initial purpose“ anstatt „former purpose“ Amended proposal for a Council Directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data, COM (92), 422 final - SYN 287, S. 15.

386 *Taeger*, in: Taeger/Gabel (Hrsg.), BDSG, § 30 Rn. 1 f.; *Ehmann*, in: Simitis (Hrsg.), BDSG, § 30 Rn. 7 BDSG; *Hanloser*, in: Wolff/Brink (Hrsg.), DSR, § 30 Rn. 5.

387 *Ehmann/Helfrich*, DSRL-Kommentar, Art. 6 Rn. 16.

388 Vgl. *Brühann*, in: Grabitz/Hilf/Nettesheim (Hrsg.), DSRL, Art. 6 Rn. 12.

389 Vgl. *Dammann*, in: Dammann/Simitis (Hrsg.), DSRL-Kommentar, Art. 6 Rn. 10; *Albers*, Informationelle Selbstbestimmung, S. 324; *Artikel-29-Datenschutzgruppe*, WP 83, S. 7.

390 *Brühann*, in: Grabitz/Hilf/Nettesheim (Hrsg.), DSRL, Art. 13 Rn. 15.

geschränkt werden bei Datenverarbeitungen, die nur für Zwecke der wissenschaftlichen Forschung oder Aufbewahrungen von Daten die zur Erstellung einer Statistik erfolgen.[391] Da das Privileg nur greift, wenn „offensichtlich keine Gefahr eines Eingriffs in die Privatsphäre der betroffenen Person besteht" ist wissenschaftliche Forschung und Statistik nur möglich, wenn keine Erkenntnisse über bestimmte Personen erzielt werden sollen und auch keine Personen anhand der Ergebnisse bestimmbar sind.[392] Mit diesen Anforderungen geht das Wissenschaftsprivileg in Art. 13 Abs. 2 DSRL über die Anforderungen von Art. 6 Abs. 1 lit. b Satz 2 DSRL hinaus.[393] Unabhängig von der Frage, ob die „Erstellung von Statistiken" tatsächlich eine wesentlich engere Formulierung als „allgemeine statistische Zwecke" ist,[394] können Ausnahmen für Big-Data-Analysen mit personenbezogenen Daten nicht hierauf gestützt werden, da diese gerade auf Rückschlüsse auf einzelne Personen ausgerichtet sind.

Die Regelungstechnik der DSRL einer Zweckvereinbarkeit anstatt einer Zweckidentität ist auf erhebliche Kritik gestoßen. So wurde ihr vorgeworfen, dass dadurch die Zweckbindung „unkalkulierbar" und „aufgeweicht" worden sei.[395] Es handele sich um eine „abgeschwächte Realisierung" der Zweckbindung.[396] Das System einer Zweckvereinbarkeitsprü-

---

391 Kritisch zu dieser Privilegierung: *Simitis*, in: Tinnefeld/Philipps/Heil (Hrsg.), Informationsgesellschaft, S. 51 (62 f.), der eine Umgehung der Zweckbindung durch extensive Handhabung des nicht definierbaren Begriffs Forschung befürchtet und jedenfalls immer eine Einwilligung in die Zweckänderung und eine funktionale Trennung der Daten fordert.

392 Vgl. *Dammann*, in: Dammann/Simitis (Hrsg.), DSRL-Kommentar, Art. 13 Rn. 14.

393 Vgl. *Simitis*, in: Tinnefeld/Philipps/Heil (Hrsg.), Informationsgesellschaft, S. 51 (62).

394 So *Brühann*, in: Grabitz/Hilf/Nettesheim (Hrsg.), DSRL, Art. 13 Rn. 15.

395 So *Dippoldsmann*, Kritische Justiz 1994, 369 (376 f.); a. A. *Frenzel*, in: Paal/Pauly (Hrsg.), DSGVO-Kommentar, § 5 Rn. 10, der eine Anerkennung eines Grundsatzes gerade mit diesen Ausnahmen sieht.

396 So *Dammann*, in: Dammann/Simitis (Hrsg.), DSRL-Kommentar, Art. 6 Rn. 8; *v. Zezschwitz*, in: Roßnagel (Hrsg.), Handbuch DSR, Kap. 3.1 Rn. 14; aber „relativ eng" laut *Schleutermann*, CR 1995, 577 (579); *Ehmann/Helfrich*, DSRL-Kommentar, Art. 6 Rn. 6 gehen demgegenüber von einer „strengen" Zweckbindung aus.

fung sei nicht generell verfassungsgemäß, da in manchen Fällen aufgrund der grundrechtlichen Schutzziele eine stärkere Eingrenzung notwendig sei.[397] Nach anderer Ansicht sei es eine strikte Zweckbindung für den gesamten Datenumgang die durch die Umsetzung der DSRL zu einer substantiellen Verbesserung des Datenschutzes in Deutschland führen werde.[398] Eine Reinterpretation der im BDSG a. F. verwendeten Zweckidentität und Zweckdurchbrechung wurde ebenfalls angeregt.[399] Aufgrund der Kontextbezogenheit der Frage eines Eingriffs in das RiS, d. h. dass dieser immer dann vorliegt, wenn eine Verwendung eines Datums in einem durch den Betroffenen nicht gebilligten Kontext stattfindet, komme es darauf an, dass der Betroffene selbst über den zulässigen Verwendungskontext entscheide.[400] Daher sei in Deutschland keine Zweckvereinbarkeit, sondern eine Zweckidentität bei der Umsetzung der DSRL vorgesehen worden.[401] Die Zweckänderungsregelungen seien nicht als Ausnahme zur Zweckbindung, sondern als „notwendiges Korrelat" zu verstehen.[402] Der Funktion als „Aufmerksamkeitsregeln" werde ein Modell von Zweckidentität und Zweckänderung besser gerecht als das Modell der Zweckvereinbarkeit.[403]

Die Kritik vermag nicht zu überzeugen, da es letztlich darauf ankommt wie die Vereinbarkeitsprüfung durchgeführt wird. Die Kriterien der Abwägung im Rahmen der Vereinbarkeitsprüfung lassen sich so ausgestalten, dass dies der Zweckidentität und Zweckdurchbrechung des

397 *Albers*, Informationelle Selbstbestimmung, S. 515 f.
398 *Brühann*, in: Grabitz/Hilf/Nettesheim (Hrsg.), DSRL, Vorbemerkung, Rn. 42.
399 *Forgó/Krügel/Rapp*, Zwecksetzung, S. 31 f., die aber keine Pflicht zur richtlinienkonformen Interpretation von § 14 BDSG a. F. aufgrund des Lindqvist-Urteils des EuGH sehen; insoweit zustimmend *Eifert*, in: Gropp/Lipp/Steiger (Hrsg.), FS Uni Gießen, S. 139 (143 f.); *Stollhof*, Datenschutzgerechtes E-Government, S. 146.
400 *Roßnagel/Laue*, DÖV 2007, 543 (545).
401 *Roßnagel/Laue*, DÖV 2007, 543 (545).
402 *Albers*, in: Hoffmannn-Riem/Schmidt-Aßmann/Voßkuhle (Hrsg.), GVwR II², § 22, Rn. 123.
403 *Albers*, in: Hoffmannn-Riem/Schmidt-Aßmann/Voßkuhle (Hrsg.), GVwR II², § 22, Rn. 123.

BDSG a. F. entspricht, das ja ohnehin durch eine Vielzahl von Abwägungsklauseln geprägt ist.

Die Anforderungen aus Art. 6 Abs. 1 DSRL träten neben das Erfordernis einer Rechtsgrundlage für die Verarbeitung nach Art. 7 DSRL.[404] Eine Einwilligung in die Verarbeitung zu einem neuen Zweck allein reiche als Legitimation der Verarbeitung daher nicht aus.[405] Begründet wird dies damit, dass es „(…) für den Einzelnen immer schwieriger wird, die zunehmende Verarbeitung personenbezogener Daten im Rahmen neuer elektronischer Dienstleistungen und den sich daraus ergebenden sekundären Nutzungen mit dem Instrument der Einwilligung allein noch wirksam zu kontrollieren."[406] Dieses Argument vermag allerdings nicht zu überzeugen. Denn letztlich ist entscheidend, ob der Betroffene hinreichend informiert ist. Sofern eine adäquate Information über die Zweckänderung stattfindet, spricht nichts gegen eine Legitimation dieser Verarbeitungen durch eine Einwilligung. Falls der Betroffene nicht hinreichend über die Zweckänderung informiert wird, ist eine wirksame Einwilligung nicht möglich. Ein zusätzliches Abstellen auf eine Zweckkompatibilität ist hier nicht angezeigt. Denn anstatt in die Verwendung bereits erhobener Daten zu einem anderen Zweck einzuwilligen, können die Daten auch neu beim Betroffenen mittels Einwilligung erhoben werden, außer die Daten sind gerade im Rahmen einer Big-Data-Analyse entstanden. Im Falle einer Neuerhebung stellt sich die Frage einer Zweckkompatibilität aber gar nicht.

404 *Brühann*, in: Grabitz/Hilf/Nettesheim (Hrsg.), DSRL, Art. 6 Rn. 6, und Art. 7 Rn. 8; *Dammann*, in: Dammann/Simitis (Hrsg.), DSRL-Kommentar, Art. 7 Rn. 1; vgl. *Ehmann/Helfrich*, DSRL-Kommentar, § 7 Rn. 1; *Brühann*, DuD 1996, 66 (69); *Brühann*, in: Roßnagel (Hrsg.), Handbuch DSR, Kap. 2.4. Rn. 29.

405 *Brühann*, in: Grabitz/Hilf/Nettesheim (Hrsg.), DSRL, Art. 6 Rn. 11 und Art. 7 Rn. 8; *de Hert/Papakonstantinou*, CLSR 32 (2016), 179 (185).

406 *Brühann*, in: Grabitz/Hilf/Nettesheim (Hrsg.), DSRL, Art. 6 Rn. 11; *Brühann*, in: Roßnagel (Hrsg.), Handbuch DSR, Kap. 2.4 Rn. 29; *Brühann*, in: v. d. Groeben/Schwarze/Hatje (Hrsg.), EUV/AEUV, Art. 16 AEUV Rn. 54.

(4) Weitere Grundsätze der Datenqualität nach Art. 6 DSRL

Auch die in Art. 6 Abs. 1 lit. c, d, e DSRL genannten Aspekte stellen auf den Erhebungszweck als Maßstab ab. So umschreibt Art. 6 Abs. 1 lit. c DSRL den Erforderlichkeitsgrundsatz.[407] Eine Vorratsdatenspeicherung lässt sich hiermit grundsätzlich nicht vereinbaren.[408] Zulässig soll sie aber sein, wenn sie als Zweck definiert wird und zugleich die Bedingung genannt wird, unter der die Daten für den verfolgten Zweck relevant werden.[409] Art. 6 Abs. 1 lit. d DSRL betrifft die Richtigkeit und Aktualität der Daten und Art 6 Abs. 1 lit. e DSRL die Löschung der Daten, wobei auch hier die Daten, die für historische, statistische oder wissenschaftliche Zwecke aufbewahrt werden, privilegiert sind. Aus der Vorschrift zur Löschung wird ersichtlich, dass sich aus dem Zweck zugleich ergeben muss, wann dieser erreicht ist und die Daten daher nicht mehr benötigt werden.[410] Auch dies spricht für eine möglichst präzise Zweckbestimmung. Die Anforderungen des Art. 6 Abs. 1 lit. b DSRL sind somit Voraussetzung für andere Anforderungen an die Qualität der Daten nach Art. 6 DSRL.[411]

cc) besondere Kategorien personenbezogener Daten

Art. 8 Abs. 1 DSRL wählt mit einem Verbot der Verarbeitung besonders sensibler Daten einen neuen Ansatzpunkt. Das Abweichen vom Verwendungszusammenhang wird von der EU-Kommission damit be-

---

407 Bei *Brühann*, in: Grabitz/Hilf/Nettesheim (Hrsg.), DSRL, Art. 6 Rn. 13 „Proportionalitätsgrundsatz" genannt; die Anforderungen gelten unterschiedslos sowohl für die erstmalige Erhebung als auch für die Weiterveränderung zu einem neuen Zweck. Es gibt also keine weniger strengen Anforderungen im Falle einer Zweckänderung, wie von *Dippoldsmann*, Kritische Justiz 1994, 369 (376 f.) suggeriert.

408 *Ehmann/Helfrich*, DSRL-Kommentar, Art. 6 Rn. 23; Vgl. *Simitis*, in: Dammann/Simitis (Hrsg.), DSRL-Kommentar, Einl. Rn. 32.

409 *Ehmann/Helfrich*, DSRL-Kommentar, Art. 6 Rn. 24.

410 *Ehmann/Helfrich*, DSRL-Kommentar, Art. 6 Rn. 29.

411 *Artikel-29-Datenschutzgruppe*, WP 203, S. 12.

gründet, dass Einigkeit darüber bestehe, dass bestimmte Daten aufgrund ihres Inhalts eine Gefahr für die informationelle Selbstbestimmung darstellten.[412] Dieses Abweichen vom Konzept des Kontexts ist zu Recht – auch im Hinblick auf die Feststellungen des BVerfG im Volkszählungsurteil – auf Kritik gestoßen.[413] Interessant ist aber, dass auch dieses Abweichen von der Anknüpfung an die Verarbeitungszwecke nicht ohne den Verwendungskontext auskommt. Mit Art. 8 Abs. 3 DSRL werden Gesundheitsdaten vom Verbot der Verarbeitung nach Art. 8 Abs. 1 DSRL ausgenommen, wenn die Verarbeitung zu den dort aufgeführten medizinischen Zwecken erforderlich ist und aufgrund einer Schweigepflicht die Betroffenen hinreichend geschützt sind. Alle gesundheitsbezogenen Dienstleistungen sollen hierdurch privilegiert werden.[414] Die Daten sind streng zweckgebunden zu verwenden.[415]

dd) Informations- und Betroffenenrechte

In Art. 10 DSRL ist eine Informationspflicht der verantwortlichen Stelle gegenüber dem Betroffenen über die Zweckbestimmung der Verarbeitung vorgesehen.[416] Sinn dieser Bestimmung ist, dass der Betroffene die Rechtmäßigkeit der Verarbeitung beurteilen können soll, weshalb der Betroffene so umfassend und präzise wie möglich zu informieren ist.[417] Die Vorschrift soll die Voraussetzungen für einen effektiven Rechtsschutz

412 Amended proposal for a Council Directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data, COM (92), 422 final - SYN 287, S. 17.

413 *Ehmann/Helfrich*, DSRL-Kommentar, Art. 8 Rn. 9.

414 *Dammann,* in: Dammann/Simitis (Hrsg.), DSRL-Kommentar, Art. 8 Rn. 18.

415 Vgl. *Dammann*, in: Dammann/Simitis (Hrsg.), DSRL-Kommentar, Art. 8 Rn. 19.

416 Falls die Daten nicht beim Betroffenen erhoben wurden, findet sich eine entsprechende Verpflichtung in Art. 11 DSRL.

417 *Ehmann/Helfrich*, DSRL-Kommentar, Art. 10 Rn. 6 u. 22; *Hustinx*, in: Hassemer/Möller (Hrsg.), 25 Jahre Datenschutz, S. 20 (26), sieht hierin eine Spezifizierung der Informationspflichten und eine Stärkung der Zweckbindung im Vergleich zu Art. 8 lit. a der Konvention 108 des Europarats.

schaffen.[418] Daher ist im Falle einer Zweckänderung eine nachträgliche Information erforderlich.[419]

Nach Art. 12 lit. a 1. Spiegelstrich DSRL hat der Betroffene einen Anspruch auf Auskunft über die Zweckbestimmungen von Datenverarbeitungen. Bei den Beratungen im Rat wurde von mehreren Delegationen gefordert, die Zweckbestimmung aus dem Auskunftsrecht auszunehmen.[420]

ee) Art. 25 DSRL

Art. 25 DSRL regelt die Voraussetzungen der Übermittlung von Daten in Drittländer. Diese ist grundsätzlich nur zulässig, wenn das Drittland ein angemessenes Datenschutzniveau bietet, Art. 25 Abs. 1 DSRL. Auch bei der Angemessenheitsentscheidung nach Art. 25 Abs. 2 DSRL werden die Zweckbestimmungen der Verarbeitung berücksichtigt. Wichtig ist dabei die Frage, wie eng oder weit der Zweck definiert ist.[421]

Bemerkenswert ist, dass das Safe-Harbor-Abkommen[422] keine zwingende Verbindlichkeit für die Zweckbindung vorsah. Vielmehr wurde diese unter den Vorbehalt einer Wahlmöglichkeit, (opt-out) gestellt.[423]

---

418 *Ehmann/Helfrich*, DSRL-Kommentar, Art. 10 Rn. 5.
419 *Brühann*, in: Grabitz/Hilf/Nettesheim (Hrsg.), DSRL, Art. 10 Rn. 13.
420 *Brühann*, in: Grabitz/Hilf/Nettesheim (Hrsg.), DSRL, Art. 12 Rn. 4.
421 *Dammann*, in: Dammann/Simitis (Hrsg.), DSRL-Kommentar, Art. 25 Rn. 10.
422 Entscheidung der Kommission vom 26. Juli 2000 gemäß der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates über die Angemessenheit des von den Grundsätzen des sicheren Hafens und der diesbezüglichen häufig gestellten Fragen (FAQ) gewährleisteten Schutzes, vorgelegt vom Handelsministerium der USA, ABl. EG v. 25.8.2000, Nr. L 215/7.
423 Entscheidung der Kommission vom 26. Juli 2000 gemäß der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates über die Angemessenheit des von den Grundsätzen des sicheren Hafens und der diesbezüglichen häufig gestellten Fragen (FAQ) gewährleisteten Schutzes, vorgelegt vom Handelsministerium der USA, ABl. EG v. 25.8.2000, Nr. L 215/7, S. 11.

Gleiches gilt für den Nachfolger, den Privacy Shield.[424] Lediglich für sensible Daten wurde die Verwendung für einen anderen Zweck als den Erhebungszweck unter den Vorbehalt einer ausdrücklichen Zustimmung gestellt (opt-in).[425] Zu Recht ist diese Regelungsweise auf Kritik gestoßen.[426]

ff) Zwischenergebnis

Zweckfestlegung und anschließende Bindung finden sich in der DSRL an zahlreichen Stellen, was ihre herausragende Stellung unterstreicht.[427] In einer Gesamtschau der Regelungen spricht viel für eine enge Handhabung der Zweckfestlegung. Die notwendige Zweckkonkretisierung richtet sich nach den Umständen des Datenumgangs und den möglichen Folgen für den Betroffenen.

b) Art. 8 Abs. 2 Satz 1 GRCh

Die Charta der Grundrechte der Europäischen Union (GRCh) sieht in Art. 8 Abs. 2 Satz 1 GRCh vor, dass eine Datenverarbeitung nur für festgelegte Zwecke erfolgen darf. Eine Bindung späterer Verarbeitungen an

424 Durchführungsbeschluss (EU) 2016/1250 der Kommission vom 12. Juli 2016 gemäß der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates über die Angemessenheit des vom EU-US-Datenschutzschild gebotenen Schutzes (ABl. L 207 v. 1.8.2016, S. 1 (50).

425 Entscheidung der Kommission vom 26. Juli 2000 gemäß der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates über die Angemessenheit des von den Grundsätzen des sicheren Hafens und der diesbezüglichen häufig gestellten Fragen (FAQ) gewährleisteten Schutzes, vorgelegt vom Handelsministerium der USA, ABl. EG v. 25.8.2000, Nr. L 215/7, S. 11.

426 *Simitis*, in: Simitis (Hrsg.), BDSG, § 4b Rn. 73 spricht von einem "stiefmütterlichen Umgang" mit der Zweckbindung.

427 A. A. *Forgó/Krügel/Rapp*, Zwecksetzung, S. 24 f., die die Zweckbindung in der DSRL als weniger bedeutend als im deutschen Recht betrachten, da es sich nur um eine von mehreren Qualitätsanforderungen handele. Dabei verkennen sie aber, dass der Zweck gerade der Maßstab der anderen Grundsätze ist.

den Erhebungszweck ist in Art. 8 GRCh nicht direkt angesprochen.[428] Zudem ist der Zeitpunkt der Zweckfestlegung nicht genannt. Es kann lediglich festgestellt werden, dass sich kein Hinweis auf die Zulässigkeit einer Zweckänderung findet. Insofern lässt sich nicht sagen, dass die Zweckbindung „explizit verlangt" werde.[429] Zudem ist dem Wortlaut nicht zu entnehmen, ob die Zwecke „so genau wie möglich"[430] festzulegen sind. Dafür spricht allerdings die Entstehungsgeschichte der Norm. Art. 8 GRCh orientiert sich an den damaligen Regelungen des Datenschutzes der EU und des Europarats, insbesondere der DSRL.[431] Auch Sinn und Zweck der Vorschrift, den Einzelnen vor einer unkontrollierten Verarbeitung seiner personenbezogenen Daten zu schützen, spricht für ein solches Verständnis. Obwohl zur Zulässigkeit einer Zweckänderung in Art. 8 Abs. 2 GRCh nichts gesagt wird, spricht somit die Auslegung dafür, eine Zweckänderung als einen Eingriff in das Recht auf den Schutz personenbezogener Daten nach Art. 8 GRCh anzusehen.[432] Denn die Festlegung eines Erhebungszweckes ergibt nur dann Sinn, wenn hieran Folgen geknüpft sind. Die wichtigste Folge ist die Beschränkung der Daten-

---

428 *Bygrave*, Data Privacy Law, S. 153, Fn. 39 sieht die Möglichkeit das Erfordernis der Bindung an den Erhebungszweck in das Merkmal „Verarbeitung nach Treu und Glauben" hineinzuinterpretieren.

429 So aber *Frenz*, EU-Grundrechte, Rn. 1381; wohl auch *Britz*, EuGRZ 2009, 1 (10), die eine „ausdrückliche Aufnahme" der Zweckbindung und damit einen strengeren Maßstab als in Art. 6 Abs. 1 lit. b DSRL sieht; für einen strengeren Maßstab der deutschen Umsetzung der Richtlinie: *Forgó/Krügel*, DuD 2005, 732 (733), wobei diese Deutung die Möglichkeiten der Zweckänderung im deutschen Recht außer Acht lässt; ebenfalls *Ohrtmann/Schwiering*, NJW 2014, 2884 (2987); *Rüpke*, ZRP 1995, 185 (189 f.); *Albers*, in: Hoffmannn-Riem/Schmidt-Aßmann/Voßkuhle (Hrsg.), GVwR II², § 22, Rn. 45, die vom Erfordernis einer spezifizierten Zweckfestlegung, nicht aber einer Zweckbindung ausgeht; an anderer Stelle bezeichnet *Albers* die Anforderungen der DSRL und des deutschen Rechts als „nicht deckungsgleich", siehe *Albers*, Informationelle Selbstbestimmung, S. 324.

430 So aber *Jarass*, GRC, Art. 8 Rn. 9; ähnlich *Frenz*, EU-Grundrechte, Rn. 1412 der eine „konkrete" Zweckfestlegung in Art. 8 GRCh hineinliest.

431 Vgl. *Knecht*, in: Schwarze (Hrsg.), EU-Kommentar Art. 8 GRC Rn. 1; *Streinz*, in: Streinz (Hrsg.), EU-Grundrechtecharta Art. 8 Rn. 1.

432 Vgl. *Frenz*, EU-Grundrechte, Rn. 1412, der in einer Zweckänderung einen „(neuen) Eingriff" sieht.

verarbeitung auf bestimmte Fälle, so dass die Rechtmäßigkeit des Datenumgangs beurteilt werden kann.

c) Datenschutz-Grundverordnung

Am 27.4.2016 ist die Datenschutz-Grundverordnung (DSGVO) als VO (EU) 2016/679 verabschiedet worden.[433] Gemäß Art. 99 Abs. 1 DSGVO gilt sie ab dem 25.05.2018. Dem ging ein mehr als vierjähriger Gesetzgebungsprozess voraus.[434] Auf die für den Zweckbindungsgrundsatz relevanten Regelungen wird später eingegangen.[435]

3. Zwischenergebnis internationale Entwicklungen

Es zeigt sich, dass die Zweckbindung allen datenschutzrechtlichen Regelungen gemein ist. Lediglich in den Details gibt es Unterschiede, die sich vor allem an der Frage festmachen, wie konkret ein Zweck definiert werden muss und wie stark die Bindung an diesen Zweck ist.

---

433 Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), ABl. Nr. L 119/1.

434 Einen kurzen Überblick über diesen Prozess bietet *Schantz*, NJW 2016, 1841; eine Beschreibung des Verfahrensablaufs aus der Sicht des Berichterstatters des EU-Parlaments findet sich bei *Albrecht*, CR 2016, 88 (88 ff.)

435 D. IV., S. 223 ff.

4. Entwicklung in Deutschland

a) erste Forderungen nach einer Zweckbindung

Bereits Ende der 1960er und Anfang der 1970er Jahre wurde im Schrifttum eine Zweckbindung gefordert.[436] *Kamlah* arbeitete in einer rechtsvergleichenden Studie zum US-amerikanischen Recht die sog. „Entfremdungsregel" heraus.[437] Er stellte fest, dass nach US-amerikanischem Recht eine öffentliche Stelle Daten, die sie für einen bestimmten Zweck erhoben habe, nicht für einen anderen als den Erhebungszweck verwenden dürfe.[438] Vielmehr sei jeder Eingriff in die Privatsphäre nur aufgrund einer gesetzlichen Ermächtigung und unter Beachtung der Verhältnismäßigkeit zulässig.[439]

In einem Entwurf für ein „Bundesdatenschutz-Rahmengesetz" sah *Podlech* bereits im Jahr 1973 in § 15 Abs. 4 eine Zweckfestlegung und anschließende -bindung vor, die nur durch Rechtsvorschrift oder Einwilligung durchbrochen werden sollte.[440] Zur Begründung führte er die Ermöglichung einer Verwendungskontrolle durch die Bürger an.[441]

Auch in der Begründung des Gesetzentwurfs der Bundesregierung für ein Bundesdatenschutzgesetz[442] aus dem Jahr 1973 findet sich der Begriff

---

436 *Podlech*, in: Dierstein/Fiedler/Schulz (Hrsg.), Datenschutz und Datensicherung, 311 (318 f.).

437 *Kamlah*, BT-Drs. VI/3826 S. 195 (200); *Kamlah*, Right of Privacy, S. 132.

438 *Kamlah*, Right of Privacy, S. 131.

439 *Kamlah*, Right of Privacy, S. 131.

440 *Podlech*, Entwurf BDSG, S. 11 f. § 15 Abs. 4 des Entwurfs lautet: „Bei der Erhebung von Informationen durch Befragung der Betroffenen ist diesen mitzuteilen, welchem Zweck die Information dienen und an welche Behörden oder Private die personenbezogenen Informationen im Rahmen des regelmäßigen Informationsaustausches weitergegeben werden. Jede Änderung des Zweckes und eine Erweiterung des Austausches ist nur mit Einwilligung der Betroffenen oder durch Rechtsvorschrift zulässig."

441 *Podlech*, Entwurf BDSG, S. 56.

442 BT-Drs. 7/1027.

der Zweckbindung. § 7 Abs. 1 Satz 1 BDSG-E 1973[443] sah vor, dass eine öffentliche Stelle Daten, die sie von einem Amts- oder Berufsgeheimnisträger erhalten hatte, nur dann übermitteln darf, wenn die empfangende Stelle sie zur Erfüllung des gleichen Zwecks benötigt, zu dem die übermittelnde Stelle sie erhalten hat. In der Gesetzesbegründung wird dies als „Grundsatz der Zweckbindung" bezeichnet.[444] Dieser dürfe „(…) nicht weit aber auch nicht dem Schutzinteresse widersprechend eng ausgelegt werden"[445]. Als Beispiel wird eine Datenübermittlung von der Unfall- an die Rentenversicherung genannt, die sich unter den Zweck Realisierung von Sozialversicherungsansprüchen fassen lasse.[446] Ein Bewusstsein für die Problematik war also bereits damals vorhanden. Sichtbar wird das auch an der Feststellung des Innenausschusses des Deutschen Bundestages, dass die „dysfunktionale Verwendung", d. h. zu einem von dem Betroffenen bei der Erhebung nicht vorhergesehenen Zweck ein regelungsbedürftiges Problem sei.[447]

In der Literatur wurde zudem betont, dass der durch das Erfordernis eines Erhebungszwecks bewirkte Schutz gänzlich verloren gehe, wenn der weitere Datenumgang nicht an den „ursprünglichen Verwendungszusammenhang (…)" gebunden sei.[448] Durchbrechungen dieses Grundsatzes bedürften einer Legitimation, sei es einer gesetzlichen oder einer Einwilligung.[449] Auch der Bundesbeauftragte für den Datenschutz sprach sich im Rahmen von Novellierungsüberlegungen des BDSG im Jahr 1980 für

443 Im später verabschiedeten BDSG 1977 fand sich eine entsprechende Bestimmung in § 10 Abs. 1.
444 BT-Drs. 7/1027, S. 24.
445 BT-Drs. 7/1027, S. 24.
446 BT-Drs. 7/1027, S. 24.
447 Bericht und Antrag des Innenausschusses (4. Ausschuß) zu dem von der Bundesregierung eingebrachten Entwurf eines Gesetzes zum Schutz vor Mißbrauch personenbezogener Daten bei der Datenverarbeitung (Bundesdatenschutzgesetz BDSG), BT-Drs. 7/5277, S. 4.
448 *Gallwas*, Der Staat 1979, 507 (513).
449 *Gallwas*, Der Staat 1979, 507 (517).

eine Verstärkung der Zweckbindung im Rahmen von Datenübermittlungen aus.[450]

In der Rechtsprechung finden sich ebenfalls erste Tendenzen zu einer Zweckbindung. Im Mikrozensusbeschluss des BVerfG wurde bereits Wert darauf gelegt, dass die Daten nicht zu fremden Zwecken missbraucht werden können.[451] Kurze Zeit später stellte das BVerfG im Scheidungsaktenbeschluss fest, dass die Preisgabe personenbezogener Daten in Bezug auf den Zweck – „die Herbeiführung der Gerichtsentscheidung" – begrenzt war und eine Übermittlung der Daten zu einem anderen Zweck ein rechtfertigungsbedürftiger Eingriff in das allgemeine Persönlichkeitsrecht aus Art. 2 Abs. 1. i. V. m. Art. 1 Abs. 1 GG der Betroffenen sei.[452] Hierin kann eine Bestätigung der Zweckentfremdungsregel durch das BVerfG gesehen werden.[453] Im Ärztekarteibeschluss wurde die Bedeutung der strikten Zweckbindung der in der Ärztekartei enthaltenen Daten für das Vertrauensverhältnis zwischen Arzt und Patient hervorgehoben.[454]

Steinmüller wies in seinem Gutachten für das BMI unter Bezugnahme auf *Kamlah* und den Scheidungsaktenbeschluss des BVerfG auf die von ihm sog. „Zweckentfremdungsregel" hin.[455] Auch die Bedeutung einer Zweckänderung für den Betroffenen, d. h. einer Verarbeitung zu einen anderen Zweck als dem Erhebungszweck, kam zur Sprache.[456] Im Rahmen der damaligen Diskussion über die Geltung und Reichweite des Gesetzesvorbehalts bei verwaltungsinternen Übermittlungen wurde die Bedeutung des Verbots der zweckentfremdenden Übermittlung für die Ge-

---

450 BT-Drs. 9/93: 3. Tätigkeitsbericht BfD S. 9.
451 BVerfGE 27, 1 (9).
452 BVerfGE 27, 344 (352).
453 So *Steinmüller/Lutterbeck/Mallmann/Harbot/Kolb/Schneider*, BT-Drs. VI/3826, S. 5 (115); *Kamlah*, DÖV 1970, 361 (363).
454 BVerfGE 32, 373 (380).
455 *Steinmüller/Lutterbeck/Mallmann/Harbot/Kolb/Schneider*, BT-Drs. VI/3826, S. 5 (114 ff.).
456 *Steinmüller/Lutterbeck/Mallmann/Harbot/Kolb/Schneider*, BT-Drs. VI/3826, S. 5 (97, 147).

währleistung der Gewaltenteilung innerhalb der Verwaltung hervorgehoben.[457] Es wurde eine Rechtsgrundlage für die Datenübermittlung zu einem anderen Zweck als dem Erhebungszweck gefordert.[458] Insbesondere bei der Übermittlung von Daten wurde das Problem der Zweckänderung bereits früh gesehen und diskutiert[459] und eine Zweckbindung jedenfalls im öffentlichen Bereich gefordert.[460]

Unter Beklagen einer bis dahin von Ausnahmen abgesehen „eher bruchstückhaft[en]“[461] Regelung der Zweckbindung wurde im Jahr 1983 ein Vorschlag für eine Kodifikation der Zweckbindung gemacht.[462] Die Zweckbestimmung sollte anhand der „erkennbaren Zweckvorstellungen der Betroffenen“ erfolgen.[463] Ein Datenumgang zu einem neuen Zweck sollte nur bei gesetzlichem Erlaubnistatbestand oder einer Einwilligung des Betroffenen zulässig sein.[464] Eine Datenverarbeitung gegen die vom Betroffenen verfolgten Zwecke sollte demnach eine Verletzung von dessen Autonomie bedeuten.[465]

---

457 *Schmidt*, JZ 1974, S. 241 (249).

458 So *Schwan*, VerwArch 1975, S. 120 (135f.).

459 Siehe hierzu etwa: *Ruckriegel*, ÖVD 11/1979, 10 (12); *Benda*, in: Leibholz/Faller/Mikat/Reis (Hrsg.), FS-Geiger, S. 23 (37 f.), der in der Zweckentfremdung eine Verletzung der Privatsphäre sieht. *Seidel*, Online - ZfD 1973, 359 (366), sieht eine Zweckentfremdung im Weiterverkauf von Adressdaten und einen unzulässigen Datenumgang in jeder Verwendung, die über den ursprünglichen Zweck hinausgeht.

460 *Bull*, ÖVD 11/1979 3, (8).

461 *Bischoff*, in: Traunmüller/Fiedler/Grimmer/Reinermann (Hrsg.), Zweckbindung, S. 193 (201).

462 *Bischoff*, in: Traunmüller/Fiedler/Grimmer/Reinermann (Hrsg.), Zweckbindung, S. 193 (206).

463 *Bischoff*, in: Traunmüller/Fiedler/Grimmer/Reinermann (Hrsg.), Zweckbindung, S. 193 (206).

464 *Bischoff*, in: Traunmüller/Fiedler/Grimmer/Reinermann (Hrsg.), Zweckbindung, S. 193 (206).

465 *Bischoff*, in: Traunmüller/Fiedler/Grimmer/Reinermann (Hrsg.), Zweckbindung, S. 193 (203).

Vor dem Hintergrund einer Vielzahl von Verwaltungszielen und der Möglichkeit einer multifunktionalen Verwendung von Daten,[466] wurde kurz vor dem Volkszählungsurteil die Bedeutung der Zweckbindung als zentrales Regelungselement hervorgehoben.[467] Sie zwinge zur Begründung der Verarbeitung, sichere ihre Transparenz, begrenze den Umfang und schränke die Informationsverbreitung ein.[468] Es gab aber auch bereits vor der ersten Novellierung des BDSG Forderungen, dass das Zweckbindungsprinzip zurückstehen müsse im Falle eines unabweisbar erforderlichen Bedürfnisses zur Mehrfachnutzung von Daten, sofern diese für den Betroffenen erträglich sei.[469]

b) BVerfGE 65, 1 - Volkszählungsurteil

Der für das Jahr 1983 geplante Zensus stieß auf erheblichen Widerstand in der Bevölkerung. Es wurden mehrere Verfassungsbeschwerden gegen das Volkszählungsgesetz erhoben.[470] Das BVerfG schuf in seinem Urteil das RiS, das es Art. 1 Abs. 1 i. V. m. Art. 2 Abs. 1 GG entnahm.[471] Es führte dazu aus: „Mit dem Recht auf informationelle Selbstbestimmung wären eine Gesellschaftsordnung und eine diese ermöglichende Rechtsordnung nicht vereinbar, in der Bürger nicht mehr wissen können, wer was wann und bei welcher Gelegenheit über sie weiß.“[472] Es bedürfe eines Schutzes „(...) des Einzelnen gegen die unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten (...)“.[473] Die Schwere der Eingriffe in dieses Recht hänge nicht allein von der Art der Angaben, sondern vor allem von ihrer Nutzbarkeit und Ver-

466 *Simitis*, in: Horn (Hrsg.), FS Coing Bd. II, S. 495 (509).
467 *Simitis*, in: Horn (Hrsg.), FS Coing Bd. II, S. 495 (517).
468 *Simitis*, in: Horn (Hrsg.), FS Coing Bd. II, S. 495 (517).
469 Siehe hierzu den Nachweis bei *Forgó/Krügel*, DuD 2005, 732 (733).
470 BVerfGE 65, 1 (3).
471 BVerfGE 65, 1 (43); kritisch *Ladeur*, DuD 2000, 12 (15) der das RiS als kontur- und substanzlos bezeichnet.
472 BVerfGE 65, 1 (43).
473 BVerfGE 65, 1 (43).

wendungsmöglichkeit ab.[474] Entscheidend seien hierfür der Erhebungszweck und die technischen Möglichkeiten der Verarbeitung und Verknüpfung der Daten.[475] Erhebungszweck und veränderter Zweck dürften nicht miteinander unvereinbar sein.[476] „Unter den Bedingungen der automatischen Datenverarbeitung (gebe es) kein belangloses Datum mehr."[477] Der Gesetzgeber müsse den „(...) Verwendungszweck bereichsspezifisch und präzise (...)" bestimmen.[478] Eine Datenerhebung „(...) auf Vorrat zu unbestimmten oder noch nicht bestimmbaren Zwecken (sei damit) nicht zu vereinbaren."[479] Eine Ausnahme von einer engen konkreten Zweckbestimmung könne nur für Datenerhebungen für rein statistische Zwecke gemacht werden.[480] Bei der Statistik könne eine enge und konkrete Zweckbindung nicht verlangt werden, da es zu ihrem Wesen gehöre, die Daten für verschiedenste, nicht von vornherein bestimmbare Zwecke zu verwenden, weshalb ein Bedürfnis zur Vorratsdatenspeicherung bestünde.[481] Als Ausgleich für die unbestimmten Verwendungsmöglichkeiten solle es Verarbeitungsvoraussetzungen geben, damit der Einzelne nicht zum bloßen Informationsobjekt werde.[482] Zu diesen Maßnahmen zählten Anonymisierung und Geheimhaltung.[483] Ob sich eine Datenübermittlung im Rahmen des Erforderlichen halte, könne nur bei einer konkreten Zweckbestimmung festgestellt werden.[484] Durch organisatorische Maßnahmen sei eine Trennung der verschiedenen Aufgabenbereiche innerhalb einer Behörde (informationelle Gewaltenteilung) zu gewährleisten und damit die Zweckbindung der Daten zu sichern.[485]

---

474 BVerfGE 65, 1 (45).
475 BVerfGE 65, 1 (45).
476 BVerfGE 65, 1 (51 u. 62) unter Bezugnahme auf statistische Zwecke und Zwecke des Verwaltungsvollzugs; BVerfGE 100, 313 (360).
477 BVerfGE 65, 1 (45).
478 BVerfGE 65, 1 (46).
479 BVerfGE 65, 1 (46).
480 BVerfGE 65, 1 (47 u. 62).
481 BVerfGE, 65, 1 (47).
482 BVerfGE 65, 1 (48).
483 BVerfGE 65, 1 (49 f.).
484 BVerfGE 65, 1 (66).
485 BVerfGE 65, 1 (69).

Die Grundsätze der Zweckbindung und Zweckänderung entsprechen nunmehr ständiger Rechtsprechung.[486] Die Aussagen des BVerfG sind aufgrund der weiteren Europäisierung des Datenschutzrechts mit der DSGVO – zumindest für den nichtöffentlichen Bereich – aber nur sehr vorsichtig nutzbar.

aa) Verfassungsrechtliche Herleitung

Umstritten ist wie das Zweckbindungsprinzip verfassungsrechtlich hergeleitet wird. Eine Ansicht geht davon aus, dass der Zweckbindungsgrundsatz seine Grundlage im Verhältnismäßigkeitsgrundsatz finde.[487] Eine andere Ansicht geht von einer „Bündelung" verschiedener Verfassungsprinzipien: Gewaltenteilung, Transparenz (als Teil des Demokratieprinzips), Rechtssicherheit, des Verhältnismäßigkeitsgrundsatzes, der informationellen Gewaltenteilung und der Normenklarheit und -bestimmtheit aus.[488] Eine gesetzliche Bestimmung, die eine Datenerhebung zu unbestimmten Zwecken gestattet, verstoße gegen den Grundsatz der Bestimmtheit und Normenklarheit.[489]

Nach einer weiteren Auffassung soll sich der Zweckbindungsgrundsatz nicht aus dem Verhältnismäßigkeitsgrundsatz herleiten, sondern ein Baustein für die gesetzliche Regulierung des Datenumgangs gemäß den grundrechtlichen Anforderungen sein.[490] Die an die Zweckfestlegung an-

---

486 BVerfG, Urteil v. 20. April 2016, Az. 1 BvR 966/09, 1 BvR 1140/09, Rn. 276, m. w. N.

487 *v. Zezschwitz*, in: Roßnagel (Hrsg.), Handbuch DSR, Kap. 3.1 Rn. 3.

488 *Marenbach*, informationelle Beziehungen, S. 96; ähnlich *Rachor*, Straftatenbekämpfung, S. 221, der den Grundsatz der Gewaltenteilung als Ausgangspunkt sieht.

489 *Heckmann*, in: Heckmann (Hrsg.), jurisPK-Internetrecht Kap. 9, Rn. 180.

490 *Albers*, in: Hoffmannn-Riem/Schmidt-Aßmann/Voßkuhle (Hrsg.), GVwR II², § 22, Rn. 79; *Albers*, Informationelle Selbstbestimmung, S. 497 u. 501 f., unter Verweis auf BVerfGE 100, 313 (359 ff.); *Albers*, in: Haratsch/Kugelmann/Repkewitz (Hrsg.), Neukonzeption, S. 113 (131).

schließende Zweckbindung sei „als allgemeiner Grundsatz nicht aus dem informationellen Selbstbestimmungsrecht abzuleiten.“[491]

Bei seiner Maßstabsbestimmung führt das BVerfG sowohl die Normenklarheit als auch die Verhältnismäßigkeit an.[492] Aufgrund der Bedeutung die der Zweckfestlegung und -bindung für diese beiden Grundsätze zukommt, ist nicht ersichtlich, weshalb eine andere Herleitung vorgenommen werden sollte. Auch von den Gegenansichten wird eine Herleitung aus dem Grundgesetz nicht prinzipiell in Frage gestellt, sondern lediglich die Frage der konkreten Ausprägung.

Auch europarechtlich ist die Herleitung des Zweckbindungsprinzips umstritten. So wurde die Zweckbindung der Vorhersehbarkeit der Datenverwendung zugeordnet.[493] Dagegen spricht aber, dass dies zu einem rein funktionalen Verständnis führt, das der Bedeutung der Zweckbindung im Datenschutzrecht nicht gerecht wird.[494] Denn eine Vorhersehbarkeit ist zumindest für den öffentlichen Bereich auch gewährleistet, wenn nur eine entsprechende Normierung stattfindet, während die Zweckbindung gerade die weitere Verarbeitung einschränken will, indem eine Umwidmung erschwert wird.[495]

bb) Rezeption des Volkszählungsurteils in der Literatur

Die Forderung einer Zweckbindung durch das BVerfG stieß auf ein geteiltes und mitunter widersprüchliches Echo. Insbesondere war umstritten,

---

491 *Trute*, in: Roßnagel (Hrsg.), Handbuch DSR, Kap. 2.5. Rn. 40; *Albers*, in: Haratsch/Kugelmann/Repkewitz (Hrsg.), Neukonzeption, S. 113 (133).

492 BVerfGE 65, 1 (44).

493 *Brouwer*, in: Besselink/Pennings/Prechal (Hrsg.), Legality Principle, 273 (279), die die Zweckfestlegung als Mechanismus zur Gewährleistung der Vorhersehbarkeit der Datenverarbeitung ansieht. Schlussantrag der Generalanwältin *Juliane Kokott* v. 18. Juli 2007, Rs. C-275/06 - Promusicae, Rn. 53.

494 Vgl. *Britz*, EuGRZ 2009, 1 (10).

495 Vgl. *Britz*, EuGRZ 2009, 1 (10); für ein solches Verständnis im Sinne einer Einschränkung des Verarbeitungsradius auch: *Bernsdorff*, in: Meyer (Hrsg.), GRCh, Art. 8 Rn. 21.

wie konkret der Zweck zu definieren sei, wie eng die Bindung an den Zweck zu verstehen sei und inwieweit die Grundsätze auch auf den nicht-öffentlichen Bereich zu übertragen seien.

Es wurde vertreten, dass eine Zweckvereinbarkeit zu unbestimmt sei und daher keine Verbesserungen des Datenschutzes erwarten lasse.[496] Eine strenge Bindung des weiteren Datenumgangs an den Erhebungszweck sei demgegenüber als „unangemessen" zu betrachten, da eine Abwägung der betroffenen Rechtsgüter und Interessen nicht stattfinde und eine Beeinträchtigung des Betroffenen allenfalls minimal sein.[497] Dies vermag nicht zu überzeugen, da sich diese Problematik im Rahmen der Vereinbarkeitsprüfung durch eine Abwägung lösen lässt.

Mit dem Volkszählungsurteil habe sich eine „verstärkte Zweckbindung" ergeben, da der Zweck der Preisgabe von Daten an eine öffentliche Stelle weitestgehend durch den Betroffenen festgelegt und somit subjektiv vorgenommen werde.[498] Dem ist nicht zuzustimmen, da die Datenerhebung durch öffentliche Stellen in der Regel auf Rechtsnormen beruht, die die Zwecke vorgeben.

Einerseits wurde dem Volkszahlungsurteil eine enge Zweckbestimmung entnommen, die sich aus dem „Recht des Einzelnen selbst über die Preisgabe und Verwendung seiner personenbezogenen Daten zu bestimmen" ergebe.[499] Negativ sei daher verfassungsrechtlich ein Zweckentfremdungsverbot vorgegeben,[500] und eine Identität zwischen Erhebung und weiterer Verwendung geboten.[501] Das Zweckbindungsprinzip gelte aber nicht absolut, so dass Ausnahmen auf einer gesetzlichen Grundlage möglich seien.[502]

---

496 *Woertge*, Prinzipien, S. 141 f.
497 *Woertge*, Prinzipien, S. 142.
498 *Tuner*, CR 1986, 591 (594).
499 *Schmitz*, TDDSG, S. 107.
500 *Schmitz*, TDDSG, S. 107.
501 *Bergmann/Möhrle/Herb*, BDSG, § 14 Rn. 17.
502 *Mallmann*, DRiZ 1987, 377 (378).

Andererseits ist die im Volkszählungsurteil geforderte enge Zweckbindung auf Kritik gestoßen[503] und sehr extensiv ausgelegt worden. Statt von Zweckbindung solle vom „Grundsatz zweckgebundener Datenverarbeitung“ gesprochen werden, der sich nicht durch eine strenge Bindung an den Erhebungszweck, sondern durch eine strenge Prüfung von Datenumgängen zu anderen Zwecke auszeichne.[504]

Kritisiert wird, dass die Forderung nach einer bereichsspezifischen und präzisen Zweckbestimmung zu einer nicht mehr überschaubaren Normenflut geführt habe.[505] Eine bereichsspezifische und präzise Zweckfestlegung sei in vielen Bereichen nicht möglich, da diese nicht präziser sein könne als eine Aufgabenbeschreibung.[506] Der Grundsatz der Zweckbindung sei ein Grundsatz der Rechtsbindung.[507] Da sich der Informationsgehalt mit der Zeit ändere bzw. oft erst später deutlich werde, halte der Gesetzgeber eine strenge Zweckbindung nicht durch.[508] Der Zweck werde gesetzlich „selten konkret eingegrenzt“ und der Gesetzgeber gebe „wenig Hilfestellungen für einen sachgerechten Umgang mit dem Zweckbegriff“.[509]

Eine Welt in der jeder wissen können müsse, „wer was wann und bei welcher Gelegenheit über ihn weiß“, sei in einer Informationsgesellschaft „kaum mehr als eine Illusion“.[510] Normenbestimmtheit und Normenklarheit führten zu einer „Verrechtlichung von Lebensbereichen und die „strenge Zweckbindung der Daten“ könne „leichter gefordert als durchgehalten werden“, wie sich an Nutzungsänderungen im Rahmen eines In-

503 Siehe nur: *Scholz/Pitschas*, Informationelle Selbstbestimmung, S. 42.
504 *Schneider*, NJW 1984, 390 (397).
505 *Roßnagel/Laue*, DÖV 2007, 543 (545) m. w. N; ähnlich *Kloepfer*, Gutachten 62. dt. Juristentag, S. 72 f.
506 *Trute*, in: Roßnagel (Hrsg.), Handbuch DSR, Kap. 2.5. Rn. 36.
507 *Trute*, in: Roßnagel (Hrsg.), Handbuch DSR, Kap. 2.5. Rn. 40.
508 *Trute*, in: Roßnagel (Hrsg.), Handbuch DSR, Kap. 2.5. Rn. 40; *Albers*, in: Haratsch/Kugelmann/Repkewitz (Hrsg.), Neukonzeption, S. 113 (133).
509 *Bull*, RDV 1999, 148 (151).
510 *Schoch*, in: Sachs/Siekmann (Hrsg.), FS-Stern, S. 1491 (1508); ähnlich *Bull*, Informationelle Selbstbestimmung, S. 60.

formationszugangs nach dem Informationsfreiheitsrecht zeige.[511] Die Eingriffsdogmatik müsse im Zusammenhang mit dem RiS korrigiert und präzise bestimmbare Nachteile oder relevante Gefahren benannt werden, da das Einschließen von Einschüchterungspotentialen zu einer „Verrechtlichungsspirale" führe.[512]

Es gebe sehr wohl belanglose Daten, die durch die moderne Technik in großer Zahl anfielen; entscheidend sei der Verwendungszusammenhang.[513] Richtig an dieser Aussage ist, dass sich aus dem Verwendungszusammenhang (Zweck und Umstände des Datenumgangs) der Informationsgehalt und damit die Schutzbedürftigkeit des Betroffenen ergibt.[514]

Für den nicht-öffentlichen Bereich stelle die Zweckbindung einen nicht gerechtfertigten Grundrechtseingriff dar.[515] Die Zweckbindung sei durch das Urteil des BVerfG nur für den öffentlichen Bereich entschieden worden und für den nicht-öffentlichen Bereich nicht identisch vorzusehen.[516] Die Zweckbindung lasse sich nicht in der „gleich intensiven Weise" wie im öffentlichen Bereich verwirklichen.[517] Die Notwendigkeit einer Zweckbindung für den nicht-öffentlichen Bereich werde ideologisch aus dem Volkszählungsurteil hergeleitet und ein Regelungsbedarf sei nicht nachgewiesen.[518] Im privaten Bereich wirke die Zweckfestlegung freiheitsbegrenzend, weshalb sie angepasst an den jeweiligen Regelungskontext eingesetzt[519] und bei der Auslegung der Zweckbindungsvorschriften

511 *Schoch*, in: Sachs/Siekmann (Hrsg.), FS-Stern, S. 1491 (1508).
512 *Schoch*, in: Sachs/Siekmann (Hrsg.), FS-Stern, S. 1491 (1509).
513 So *Bull*, RDV 1999, 148 (150), unter Berufung auf den gestrichenen § 1 Abs. 3 BDSG 1990.
514 Vgl. *Bäcker*, Der Staat 51 (2012), 91 (102 f.), der davon ausgeht, dass Informationen als belanglos bezeichnet würden, nicht Daten.
515 *Ehmann*, RDV 1988, 221 (235); *Ehmann*, AcP 188 1988, 230 (329).
516 *Badura*, in: Deutscher Bundestag (Hrsg.), schriftliche Stellungnahme, S. 148 (149).
517 *Zöllner*, RDV 1985, 3 (13); ähnlich *Mallmann*, CR 1988, 93 (97), der für einzelne Bereiche differenzieren will; diesem zustimmend: *Drews*, CR 1988, 364 (366).
518 *Ehmann*, RDV 1988, 169 (174).
519 *Albers*, Informationelle Selbstbestimmung, S. 500.

berücksichtigt werden solle, dass in Art. 2 Abs. 1 GG eingegriffen werde.[520] Mangels durch Gesetz festgelegter Aufgabe sei die Zweckbindung „ein Fremdkörper" im nicht-öffentlichen Bereich.[521] Es sei nicht praktikabel, wenn der private Datenverarbeiter selbst die Verwendungszwecke präzise festzulegen habe.[522] Die Zweckbindung sei möglichst weit zu verstehen und es müsse auch gesetzliche Erlaubnisse einer Zweckdurchbrechung geben.[523] Der private Bereich sammle weniger Daten als der Staat und die Zweckbindung schränke im nicht-öffentlichen Bereich mehr Freiheit ein als sie gewährleiste.[524] Eine Zweckfestlegung bei einer Übermittlung ergebe nur Sinn, wenn der Zweck möglichst konkret festgelegt werde, woran aber weder Empfänger noch Übermittelnder interessiert seien.[525] Allgemein ließen sich die Anforderungen an die Konkretheit des Zweckes ohnehin nicht bestimmen.[526] Es sei unklar, wie konkret der Zweck festzulegen ist, bzw. wer darüber entscheide.[527]

Im Bereich des privaten Datenschutzes richteten sich der gesetzliche Regelungsbedarf und die Regelungstiefe nach den Möglichkeiten der Datennutzung und den hieraus resultierenden Gefahren.[528] Profilbildungen im privaten Bereich seien nicht per se zu „perhorreszieren", sondern nach ihren Auswirkungen differenziert zu betrachten.[529] So sei ein Profiling zur Bewertung der Kreditwürdigkeit strenger zu regulieren, als ein Profiling zu Werbezwecken.[530] Bestimmte Formen des Datenaustauschs sollten erlaubt und als „normal definiert" werden;[531] so solle nicht jede Zweckänderung einem Gesetzesvorbehalt unterworfen werden.[532] Im Pri-

520 *Dörr/Schmidt*, BDSG, § 27 Rn. 4.
521 *Dörr/Schmidt*, BDSG, § 27 Rn. 4.
522 *Zöllner*, RDV 1985, 3 (13).
523 *Zöllner*, RDV 1985, 3 (14).
524 *Ehmann*, RDV 1988, 221 (232).
525 *Ehmann*, RDV 1988, 221 (234).
526 *Ehmann*, RDV 1988, 221 (234).
527 *Ehmann*, RDV 1988, 221 (230).
528 *Masing*, NJW 2012, 2305 (2309).
529 *Masing*, NJW 2012, 2305 (2309).
530 *Masing*, NJW 2012, 2305 (2309).
531 *Masing*, NJW 2012, 2305 (2309).
532 *Masing*, NJW 2012, 2305 (2307).

vatrechtsverkehr komme ein „staatlicher Schutz vor Selbstgefährdung“ nur bei „erkennbaren Defiziten realer Autonomie“ in Betracht.[533] Ansonsten drohe die Gefahr einer „Verrechtlichung des Alltäglichen“.[534] Vorgeschlagen wurde eine stärkere Selbstregulierung im privaten Bereich und eine Beschränkung des Staates auf erhebliche Gefahren, da ohne einen risikobasierten Ansatz der staatliche Auftrag zur Gewährleistung eines funktionsfähigen Rahmens nicht erreicht werden könne.[535] Die Zweckbindung werde durch „eigensüchtige Nutzermotive“ abgelöst, die an die Stelle „klarer Zwecke“ träten.[536] Sie sei „weithin überholt“, weshalb die „Zweckenge und -bindung“ „geöffnet“[537] werden solle und selbstregulierter Datenverkehr und privater Datenschutz in den Vordergrund träten.[538]

Demgegenüber wird vertreten, dass die Zweckbindung auch im nichtöffentlichen Bereich unter Anknüpfung an den Erhebungszweck Anwendung finde solle.[539] Die Gegenansicht lege die Zweckbindung zu eng aus.[540]

Das Volkszählungsurteil wurde also von Beginn an kontrovers diskutiert. Wie gezeigt stehen die Zweckbindung und ihre Anwendung im Mittelpunkt dieses Streits, ohne dass aber eine Lösung dieser Streitfragen ersichtlich wäre. Ein weiterer großer Streitpunkt ist die Übertragbarkeit des Urteils auf den privaten Bereich, in dem sich die Grundrechte der verantwortlichen Stelle und des Betroffenen gegenüberstehen und die Grundrechte nur mittelbar wirken. Umstritten ist dies sicherlich auch deshalb,

---

533 *Schoch*, in: Sachs/Siekmann (Hrsg.), FS-Stern, S. 1491 (1510).
534 *Hoffmann-Riem*, AöR 123 (1998), 513 (527 f.).
535 *Hoffmann-Riem*, AöR 123 (1998), 513 (528 u. 538).
536 *Pitschas*, in: Ständige Deputation des Deutschen Juristentages (Hrsg.), Referat dt. Juristentag, M 9 (M 11), der darauf verweist, dass der Nutzer im Internet „surfe“.
537 An späterer Stelle ist von einer „Lockerung“ der niemals zweifelsfrei begründbaren Zweckbindung die Rede, siehe *Pitschas*, in: Ständige Deputation des Deutschen Juristentages (Hrsg.), Referat dt. Juristentag, M 9 (M 37).
538 *Pitschas*, in: Ständige Deputation des Deutschen Juristentages (Hrsg.), Referat dt. Juristentag, M 9 (M 18).
539 *Mallmann*, CR 1988, 93 (97).
540 *Mallmann*, CR 1988, 93 (97).

weil der Grundrechtsschutz durch das RiS auf die Ebene der Grundrechtsgefährdung vorverlagert wird.[541] Dies führt im nicht komplett durch präzise Rechtsnormen mit vorgegebenen Wirkungen regulierten nicht-öffentlichen Bereich zu Unsicherheiten.

cc) anschließende Novellierungen des BDSG

In einem Gesetzentwurf der Bundesregierung aus dem Jahr 1986 war eine Stärkung der Zweckbindung durch ihre Kodifizierung für den öffentlichen und den nicht-öffentlichen Bereich als Reaktion auf das Volkszählungsurteil vorgesehen.[542] Zu einer Verabschiedung dieses Entwurfes kam es aber nicht. Vielmehr fiel dieser der Diskontinuität des Bundestages mit Ablauf der Legislaturperiode zum Opfer.[543] Mit einem neuen Gesetzentwurf der Bundesregierung in der elften Wahlperiode sollte die Zweckbindung aufgrund der Vorgaben des BVerfG durch eine Ausweitung auf alle Phasen des Datenumgangs gestärkt werden.[544] Der Bundesrat nahm zu diesem Entwurf in vielen Punkten kritisch Stellung. Einige der Kritikpunkte zielten auf eine Verschärfung der Zweckbindung.[545] Die Bundesregierung nahm diese Kritik zum Anlass zu Änderungen, wie beispielsweise der Bestimmung, dass für den öffentlichen Bereich an den Zweck der Speicherung angeknüpft wird, falls keine Erhebung vorausgegangen ist.[546] Auch in der Beschlussempfehlung des Innenausschusses wurde die Zweckbindung gegenüber dem ursprünglichen Gesetzesvorschlag der Bundesregierung gestärkt. So wurde eine Bestimmung zur besonderen Zweckbindung von Daten, die ausschließlich für Zwecke der Datenschutzkontrolle erhoben wurden, vorgeschlagen.[547] Der Opposition ging dies nicht weit genug. Mit einem Entschließungsantrag forderte die

541 Aus der Rspr. des BVerfG z. B. BVerfGE 120, 378 (397); *Bäcker*, Der Staat 51 (2012), 91 (96).
542 BT-Drs. 10/5343, S. 34 Nr. 2.4.
543 *Simitis*, in: Simitis (Hrsg.), BDSG, Einl., Rn. 63.
544 Vgl. BT-Drs 11/4306 S. 36.
545 Siehe BT-Drs. 11/4306, S. 75 Nr. 19 und S. 76 Nr. 24.
546 BT-Drs. 11/4306, S. 90, zu A. 19.
547 BT-Drs. 11/7235, S. 34.

Fraktion *Die Grünen* „(…) wegen erheblicher, auch verfassungsrechtlicher Bedenken [den Gesetzentwurf] zurückzuziehen."[548] Für den öffentlichen Bereich wurde eine Verschärfung des Zweckbindungsgebots für die Datenerhebung und Verarbeitung gefordert.[549] Der vom Bundesrat angerufene Vermittlungsausschuss[550] verschärfte die Zweckbindung für den Übermittlungsempfänger im nicht-öffentlichen Bereich.[551] Die Zweckbindung wurde in dieser zweiten Phase der Gesetzgebung im Datenschutzrecht nach dem Volkszählungsurteil eingeführt bzw. betont[552] oder jedenfalls „essentiell" ausgebaut.[553]

Durch die DSRL wurden Änderungen des BDSG erforderlich, wie beispielsweise die Ausdehnung der Zweckbindung auf die Datenerhebung.[554] Die DSRL führte zum Ausbau der Zweckbindung für den nicht-öffentlichen Bereich in § 28 Abs. 2 BDSG a. F.[555] Gleichwohl gab es seitens der Opposition und des Bundesrates Bestrebungen die Zweckbindung weitergehend zu stärken. Der Bundesrat forderte einen Verstoß gegen § 28 BDSG a. F., der nunmehr die Zweckbindung enthielt, als Ordnungswidrigkeit auszugestalten.[556] Diese Forderung konnte er im Gesetzgebungsverfahren aber nicht durchsetzen. Die Bundestagsfraktion der *PDS* forderte den Gesetzentwurf zurückzuziehen und einen neuen Entwurf vorzulegen, der einer Bindung an den Verarbeitungszweck zum Durchbruch verhelfe.[557] Denn die Zweckbindung werde durch eine Vielzahl von Ausnahmetatbeständen sowohl im öffentlichen als auch im

548 BT-Drs. 11/7276, S. 2.
549 BT-Drs. 11/7276, S. 2.
550 Plenarprotokoll 615 - Stenographischer Bericht über die 615. Sitzung des Bundesrates v. 22. Juni 1990, S. 362.
551 BT-Drs. 11/7843, S. 3 Nr. 6 d), 7 b).
552 *Globig*, in: Roßnagel (Hrsg.), Handbuch DSR, Kap. 4.7 Rn. 10 f.
553 *Auernhammer*, BDSG, 3. A., Einführung Rn. 65.
554 *Brühann*, DuD 1996, 66 (69).
555 BT-Drs. 14/4329, S. 43, zu Nr. 31, zu Abs. 2.
556 BT-Drs. 14/4329, S. 60 Nr. 17; dieses Vorhaben stieß beim damaligen Bundesbeauftragten für den Datenschutz auf Zustimmung, 18. Tätigkeitsbericht des BfD, abgedruckt in: BT-Drs. 14/5555, S. 183.
557 BT-Drs. 14/5793, S. 54.

nicht-öffentlichen Bereich „ausgehöhlt und entwertet“.[558] Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hatte eine Stärkung der Zweckbindung bei „massenhaften Datenerhebungen“ gefordert.[559]

Im Jahre 2009 kam es abermals zu Gesetzesnovellen.[560] Im Rahmen der Regulierung von Auskunfteien und Scoring wurde eine besondere Zweckbindungsvorschrift in § 6 Abs. 3 BDSG a. F. eingeführt.[561] Der Gesetzgeber wollte sicherstellen, dass ein Betroffener nicht aus der Befürchtung, sein Auskunftsverlangen könne zu einem negativen Scorewert führen, auf die Ausübung seines Rechts verzichtet.[562] Eine entsprechende Regelung wurde für das Auskunftsrecht in § 34 Abs. 5 BDSG a. F. eingefügt.

c) Urteil des BVerfG zum BKAG

aa) wesentlicher Urteilsinhalt zur Zweckbindung

In seinem Urteil zum BKA-Gesetz hatte das BVerfG über den Einsatz heimlicher Überwachungsmaßnahmen durch das BKA zur Abwehr von Gefahren des internationalen Terrorismus zu entscheiden.[563] In diesem Zusammenhang machte das BVerfG auch Ausführungen zur Zweckbindung. Das BVerfG unterscheidet zwischen einer weiteren Nutzung und einer Zweckänderung.[564] Ausgangspunkt der Überlegungen ist, dass sich die „Reichweite der Zweckbindung (…) nach der jeweiligen Ermächti-

558 BT-Drs. 14/5793, S. 54.
559 *Datenschutzkonferenz des Bundes und der Länder*, BT-Drs. 14/555, Anlage 9, S. 212.
560 Siehe hierzu: *Kühling/Bohnen*, JZ 2010, 600 ff; *Roßnagel*, NJW 2009, 2716 ff.
561 Gesetz zur Änderung des Bundesdatenschutzgesetzes v. 29. Juli 2009, BGBl I, S. 2254.
562 BT-Drs. 16/10529, S. 13.
563 BVerfG, Urteil v. 20.4.2016, Az. 1 BvR 966/09, 1 BvR 1140/09.
564 BVerfG, Urteil v. 20.4.2016, Az. 1 BvR 966/09, 1 BvR 1140/09, Ls. 2 b) und c).

gungsgrundlage für die Datenerhebung" richte.[565] Eine weitere Nutzung sei „eine Datennutzung über das für die Datenerhebung maßgebende Verfahren hinaus im Rahmen der ursprünglichen Zwecke".[566] Aus der Ermächtigungsgrundlage ergebe sich Behörde, Zweck und Bedingungen der Datenerhebung und folglich die erlaubte Verwendung.[567] Die Zweckbindung bestimme sich nach der Reichweite der Erhebungszwecke in der Ermächtigungsgrundlage und nicht allein anhand abstrakt definierter Behördenaufgaben.[568] Eine weitere Nutzung komme daher nur in Betracht durch dieselbe Behörde, im Rahmen derselben Aufgabe und zum Schutz derselben Rechtsgüter, die für die Datenerhebung maßgeblich waren.[569] Nicht maßgeblich seien die für die Datenerhebung relevanten Einschreitschwellen, da es sich um den Anlass und nicht den Zweck handele.[570] Diese Anforderungen für die Gefahrenlage seien aber für Daten aus Wohnraumüberwachungen und Online-Durchsuchungen aufgrund des „außerordentlichen Eingriffsgewichts" sehr wohl maßgeblich, das eine „besonders enge Bindung der gewonnen Daten an die Voraussetzungen und damit Zwecke der Datenerhebung" bedinge.[571]

Der Gesetzgeber könne auch eine Zweckänderung gestatten, die aber einen neuen Eingriff in das Grundrecht begründe, in das durch die Datenerhebung eingegriffen wurde und daher verhältnismäßig sein müsse.[572] Im Rahmen der Verhältnismäßigkeitsprüfung sei das Kriterium der „Unvereinbarkeit" von geänderter Nutzung und ursprünglicher Zwecksetzung durch das Kriterium der hypothetischen Datenneuerhebung „(…) konkretisiert und ersetzt worden."[573] Es komme demnach darauf an, ob die Daten auch für den geänderten Zweck mit vergleichbar schwerwiegenden

565 BVerfG, Urteil v. 20.4.2016, Az. 1 BvR 966/09, 1 BvR 1140/09, Ls. 2 a) und Rn. 279.
566 BVerfG, Urteil v. 20.4.2016, Az. 1 BvR 966/09, 1 BvR 1140/09, Ls. 2 b).
567 BVerfG, Urteil v. 20.4.2016, Az. 1 BvR 966/09, 1 BvR 1140/09, Rn. 279.
568 BVerfG, Urteil v. 20.4.2016, Az. 1 BvR 966/09, 1 BvR 1140/09, Rn. 279.
569 BVerfG, Urteil v. 20.4.2016, Az. 1 BvR 966/09, 1 BvR 1140/09, Rn. 279.
570 BVerfG, Urteil v. 20.4.2016, Az. 1 BvR 966/09, 1 BvR 1140/09, Rn. 280.
571 BVerfG, Urteil v. 20.4.2016, Az. 1 BvR 966/09, 1 BvR 1140/09, Rn. 283.
572 BVerfG, Urteil v. 20.4.2016, Az. 1 BvR 966/09, 1 BvR 1140/09, Rn. 284 ff.
573 BVerfG, Urteil v. 20.4.2016, Az. 1 BvR 966/09, 1 BvR 1140/09, Rn. 287.

Mitteln neu erhoben werden dürften.[574] Voraussetzung sei grundsätzlich lediglich, dass sich aus den Daten ein konkreter Ermittlungsansatz ergebe.[575] Für aus Wohnraumüberwachungen und dem Zugriff auf informationstechnische Systeme stammende Daten soll aber wiederum der Anlass, das heißt die für die Datenerhebung erforderliche Gefahrenlage, als weiteres Kriterium zu beachten sein.[576]

Es handle sich bei den Anforderungen an die Zweckänderung um eine „konkretisierende Konsolidierung" der Rechtsprechung beider Senate des BVerfG[577] und um eine „behutsame Einschränkung" der bisherigen Maßstäbe.[578] Sollte auf weitere Anforderungen, wie jenes eines vergleichbar gewichtigen Rechtsgüterschutzes verzichtet werden, „(…) würden die Grenzen der Zweckbindung als Kernelement des verfassungsrechtlichen Datenschutzes (…) für das Sicherheitsrecht praktisch hinfällig (…)."[579]

In seinem Sondervotum kritisiert *Eichberger* das Festhalten am Erfordernis einer Gefahrenschwelle wie bei der Datenerhebung, da der Eingriff durch die Zweckänderung zwar perpetuiert werde, aber nicht die ursprüngliche Eingriffsintensität erreiche.[580]

---

574 BVerfG, Urteil v. 20.4.2016, Az. 1 BvR 966/09, 1 BvR 1140/09, Rn. 287.
575 BVerfG, Urteil v. 20.4.2016, Az. 1 BvR 966/09, 1 BvR 1140/09, Rn. 289.
576 BVerfG, Urteil v. 20.4.2016, Az. 1 BvR 966/09, 1 BvR 1140/09, Rn. 291.
577 BVerfG, Urteil v. 20.4.2016, Az. 1 BvR 966/09, 1 BvR 1140/09, Rn. 292.
578 BVerfG, Urteil v. 20.4.2016, Az. 1 BvR 966/09, 1 BvR 1140/09, Rn. 292.
579 BVerfG, Urteil v. 20.4.2016, Az. 1 BvR 966/09, 1 BvR 1140/09, Rn. 292 unter Bezugnahme auf die abweichende Meinung des Richters *Schluckebier*, der jedenfalls für Daten, die nicht aus „hochinvasiven, besonders schwerwiegenden Eingriffen" gewonnen wurden auf dieses Kriterium verzichten will, da „(…) sonst der Rechtsstaat insoweit seine Schutzaufgabe (verfehle)" und „den gefährdeten Rechtsgütern (…) der gebotene Schutz versagt (bliebe)." Rn. 20 und 22.
580 Abweichende Meinung des Richters *Eichberger* zu BVerfG, Urteil v. 20.4.2016, Az. 1 BvR 966/09, 1 BvR 1140/09, Rn. 14 und 16.

bb) Stellungnahme

Das BVerfG führt mit den „weiteren Nutzungen“, die anders als bisher nicht als Zweckänderungen aufgefasst werden, eine neue Kategorie ein. Es kann hierin durchaus ein Schritt in Richtung des auf europäischer Ebene verwendeten Zweckvereinbarkeitsmaßstabs gesehen werden.[581] Es bleibt abzuwarten, inwiefern dies auch außerhalb des Polizei- und Sicherheitsrechts zu einer Maßstabsveränderung führen wird.[582]

Inhaltlich überrascht der anscheinende Maßstabswechsel innerhalb der Argumentation des BVerfG zur weiteren Nutzung. Während es zunächst heißt, dass es auf „Behörde, Zweck und Bedingungen“ in der Ermächtigungsgrundlage und damit nicht auf eine „abstrakt definierte Behördenaufgabe“ ankomme, wird dann auf ein Tätigwerden „seitens derselben Behörde im Rahmen derselben Aufgabe und für den Schutz derselben Rechtsgüter“ abgestellt. Es ist also auf einmal nicht mehr vom Zweck, sondern von der Aufgabe die Rede. Aufgrund der Ausführungen zu Beginn des Urteils und des erheblichen Streits in der Literatur bezüglich der Zweckkonkretisierung und des Verhältnisses von Zweck und Aufgabe einer Behörde ist dies sehr überraschend. Deutlich wird diese Problematik, wenn das BVerfG später für besonders invasive Maßnahmen die Voraussetzungen und damit den Anlass unter den Zweck subsumiert, der vorher gerade nicht zum Zweck gezählt wurde. Die Entscheidung schafft also leider keine Klarheit hinsichtlich der notwendigen Zweckkonkretisierung. Gerade dies wird aber darüber entscheiden, ob der Anlass bereits Teil des Zwecks ist und damit beachtet werden muss oder ob eine wesentlich allgemeinere Aufgabenbeschreibung als Zweckbestimmung ausreicht.[583] Die im Sondervotum vertretene Auffassung würde zu einer weitgehenden Freigabe des Datenumgangs für andere Zwecke führen und damit die

581 Vgl. *Müllmann*, NVwZ 2016, 1692 (1695); *Spiecker genannt Döhmann*, VerfBlog, 2016/4/21, BKAG; *Wolff*, in: Schantz/Wolff (Hrsg.), DSGVO, Rn. 398.

582 Von diesen Auswirkungen ausgehend: *Spiecker genannt Döhmann*, VerfBlog, 2016/4/21, BKAG.

583 Vgl. zur gestiegenen Bedeutung der Zweckfestlegung: *Müllmann*, NVwZ 2016, 1692 (1696).

Zweckbindung ihrer wesentlichen Funktion – der Strukturierung und Eingrenzung des Datenumgangs – berauben.

d) Vorratsdatenspeicherung

Immer wieder wird bei der Diskussion der Zulässigkeit von Big-Data-Anwendungen auf die Unzulässigkeit einer Speicherung von Daten auf Vorrat verwiesen wie sie das BVerfG bereits in seinem Volkszählungsurteil festgehalten hat.[584] Eine Datensammlung auf Vorrat für zukünftige, unbestimmte Zwecke sei mit der Zweckbindung nicht zu vereinbaren.[585] Insofern lohnt eine nähere Betrachtung der Vorratsdatenspeicherungsentscheidungen des BVerfG[586] und des EuGH.[587]

aa) BVerfG

Der Entscheidung lagen Verfassungsbeschwerden gegen die §§ 113a und 113b TKG[588] sowie § 100g StPO zugrunde, mit denen eine sechsmo-

---

584 Vgl. BverfGE 65, 1 (46); *Bull*, Informationelle Selbstbestimmung, S. 95 geht davon aus, dass eine „absolute Vorratsdatenspeicherung" irrational sei und nicht vorkomme, da die Kosten hierfür zu hoch seien; ähnlich *Ladeur*, DuD 2000, 12 (14), der das Szenario einer staatlichen Vorratsdatenspeicherung für „völlig realitätsfern" hält, da ein zweckloses Gesetz „offensichtlich verfassungswidrig" sei.

585 *Simitis*, in: Dammann/Simitis (Hrsg.), DSRL-Kommentar, Einl. Rn. 32; *Hoffmann*, Zweckbindung, S. 19 f.; siehe auch *Hoeren*, in: Kilian/Heussen (Hrsg.), CHB, Teil 14, Datenschutzrechtliche Fragen, Rn. 18; a. A. *Dörr/Schmidt*, BDSG, § 28 Rn. 20, die davon ausgehen, dass das Volkszählungsurteil einer Vorratsdatenspeicherung im nicht-öffentlichen Bereich mangels Übertragbarkeit nicht entgegenstehe.

586 BVerfGE 125, 260 ff.

587 EuGH, Urteil v. 8.4.2014, C-293/12 - Digital Rights Ireland und C-594/12 - Seitlinger u. a.; EuGH, Urteil v. 21.12.2016, C-203/15 - Tele 2 Sverige AB und C-698/15, Rn. 134.

588 In der Fassung des Artikel 2 Nummer 6 des Gesetzes zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG vom 21. Dezember 2007 (BGBl. I S. 3198).

natige, vorsorgliche anlasslose Speicherung von Telekommunikationsdaten durch private Diensteanbieter angeordnet und deren Verwendung geregelt wurde.[589] Diese Normen beruhten auf der Umsetzung einer EU-Richtlinie[590], die selbst Gegenstand mehrerer Verfahren vor dem EuGH war.[591]

Prüfungsmaßstab des BVerfG war im Wesentlichen eine mögliche Verletzung von Art. 10 Abs. 1 GG, hinter dem das RiS aus Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG insoweit zurücksteht.[592] Allerdings lassen sich bezüglich des Umgangs mit personenbezogenen Daten die Maßstäbe des RiS, wie sie bereits im Volkszählungsurteil entwickelt wurden, übertragen.[593] Hieraus folgt das Erfordernis einer bereichsspezifischen, präzisen und normenklaren Bestimmung des Speicherungszwecks.[594] Eine sechsmonatige anlasslose Speicherung von Telekommunikationsverkehrsdaten verstoße bei einer Ausgestaltung, die dem Gewicht des Eingriffs Rechnung trage, nicht als solche gegen das Verbot einer Datenspeicherung auf Vorrat.[595] Voraussetzung dafür soll aber jedenfalls sein, dass die Datensammlung zu bestimmten Zwecken erfolge.[596]

Ein Aspekt, der für eine Zulässigkeit einer anlasslosen vorsorglichen Speicherung spreche, sei dass diese nicht durch den Staat, sondern private Diensteanbieter erfolge, so dass die Daten verteilt gespeichert und noch nicht zusammengeführt würden und der Staat keinen direkten Zugriff auf

589 Zum Sachverhalt siehe BVerfGE 125, 260, (263 ff.).

590 Richtlinie 2006/24/EG des Europäischen Parlaments und des Rates vom 15. März 2006, ABl. L 105 v. 13. April 2006, S. 54.

591 EuGH, Urteil v. 10.2.2009, C-301/06, dessen Gegenstand die Wahl der Rechtsgrundlage für den Erlass der Richtlinie war; EuGH, Urteil v. 8.4.2014, C-293/12 - Digital Rights Ireland und C-594/12 - Seitlinger u. a., in denen es um die Vereinbarkeit der Richtlinie mit den Grundrechten der Europäischen Grundrechtecharta ging.

592 BVerfGE 125, 260 (310).

593 BVerfGE 125, 260, (310); BVerfGE 100, 313 (359).

594 BVerfGE 125, 260 (315); BVerfGE 100, 313 (359 f.).

595 BVerfGE 125, 260 (316).

596 BVerfGE 125, 260 (321).

die Daten habe.[597] Die zum Abruf der Daten ermächtigenden Bestimmungen könnten gewährleisten, dass die Speicherung nicht zu unbestimmten oder noch nicht bestimmbaren Zwecken erfolge.[598]

Die Vorratsdatenspeicherung müsse eine Ausnahme bleiben und könne daher nicht als Vorbild für die Schaffung weiterer anlassloser Datensammlungen dienen.[599] Die Regelungen der Datenverwendung seien nicht nur maßgeblich für die Beurteilung der Verfassungsmäßigkeit der Datenverwendungsregelung selbst, sondern wirkten sich auch auf die Beurteilung der Verfassungsmäßigkeit der Datenspeicherung aus.[600] Die Festlegung auf bestimmte Zwecke sei durch Verfahrensvorkehrungen zu gewährleisten, d. h. eine Kennzeichnungspflicht der Tatsache, dass es sich um Daten handelt, die anlasslos vorsorglich gespeichert wurden.[601]

Aufgrund des „unaufhebbaren verfassungsrechtlichen Zusammenhang(s) von Datenspeicherung und Verwendungszweck“ dürften Daten „nur zu bestimmten, bereichsspezifischen, präzise und normenklar festgelegten Zwecken gespeichert werden, so dass bereits bei der Speicherung hinreichend gewährleistet ist, dass die Daten nur für solche Zwecke verwendet werden, die das Gewicht der Datenspeicherung rechtfertigen. Eine Speicherung kann nicht als solche abstrakt gerechtfertigt werden, sondern nur insoweit, als sie hinreichend gewichtigen, konkret benannten Zwecken dient.“[602] Die Schaffung eines „Datenpools auf Vorrat“ über dessen Nutzen später verschiedene staatliche Instanzen „nach Bedarf und politischem Ermessen“ entscheiden könnten, sei unzulässig.[603] Mangels Angabe des Zwecks könne die Verfassungsmäßigkeit der Speicherung in diesem Falle nicht beurteilt werden.[604]

---

597 BVerfGE 125, 260 (321).
598 BVerfGE 125, 260 (321).
599 BVerfGE 125, 260 (323 f.).
600 BVerfGE 125, 260 (327 f.).
601 BVerfGE 125, 260 (332 f.).
602 BVerfGE 125, 260 (345).
603 BVerfGE 125, 260 (345 u. 356).
604 BVerfGE 125, 260 (345).

Eine lediglich generalisierende Angabe der Aufgabenfelder, die einen Abruf gestatten, werde der verfassungsrechtlich gebotenen Begrenzung der Verwendungszwecke nicht gerecht, die vielmehr eine konkrete Angabe sowie verfahrensrechtliche Regelungen zur Gewährleistung der Zweckbindung erfordere.[605]

bb) EuGH

Wie bereits erwähnt, hatte sich auch der EuGH mit Fragen der Vorratsdatenspeicherung zu beschäftigen. Neben der Frage der Wahl der richtigen Rechtsgrundlage für die RL 2006/24/EG[606], die aber hier nicht weiter von Interesse ist, ergingen zwei Urteile zur Vereinbarkeit einer Vorratsdatenspeicherung mit dem Unionsrecht.

In der ersten Entscheidung stellte sich die Frage der Vereinbarkeit der RL 2006/24/EG mit Art. 7 und 8 GRCh.[607] Die RL 2006/24/EG verpflichtete die Mitgliedstaaten zur Einführung einer Verpflichtung von Telekommunikationsanbietern zur anlasslosen Speicherung von Telekommunikationsverkehrsdaten zwecks Ermittlung, Feststellung und Verfolgung einzelner von den Mitgliedstaaten festzulegender schwerer Straftaten.[608]

Die Speicherung sowie der Zugang zu den Daten durch die nationalen Behörden, sowie die Verarbeitung der Daten seien laut dem Urteil des EuGH ein besonders schwerwiegender Eingriff in Art. 7 bzw. 8 GRCh.[609] Im Rahmen der Prüfung der Verhältnismäßigkeit dieses Eingriffs stellte

605 Vgl. BVerfGE 125, 260 (355).
606 EuGH, Urteil v. 10.2.2009, C-301/06.
607 EuGH, Urteil v. 8.4.2014, C-293/12 - Digital Rights Ireland und C-594/12 - Seitlinger u. a.
608 Zu den für das Urteil relevanten Bestimmungen der RL 2006/24/EG siehe EuGH, Urteil v. 8.4.2014, C-293/12 - Digital Rights Ireland und C-594/12 - Seitlinger u. a., Rn. 11 ff.
609 EuGH, Urteil v. 8.4.2014, C-293/12 - Digital Rights Ireland und C-594/12 - Seitlinger u. a., Rn. 33 ff.; kritisiert wurde hieran, dass nicht klar sei, ob diese Voraussetzungen jede für sich genommen oder kumulativ die Schwere des Eingriffs begründen, siehe *Priebe*, EuZW 2014, 456 (457).

der EuGH fest, dass die Zielsetzung der Bekämpfung schwerer Kriminalität nicht ausreiche, sondern es vielmehr einer Einschränkung des Eingriffs auf das absolut Notwendige bedürfe, weshalb die Regelung klare und präzise Regeln für Tragweite und Anwendung der Maßnahme vorsehen und Mindestanforderungen aufstellen müsse.[610] Der EuGH bemängelte insbesondere, dass die RL 2006/24/EG die Speicherung der Verkehrsdaten „generell auf alle Personen und alle elektronischen Kommunikationsmittel sowie auf sämtliche Verkehrsdaten erstreckt, ohne irgendeine Differenzierung, Einschränkung oder Ausnahme anhand des Ziels der Bekämpfung schwerer Straftaten vorzusehen."[611] Ein Zusammenhang zwischen dem Zweck der Speicherung der Daten, d. h. der Bekämpfung schwerer Kriminalität und einer Bedrohung der öffentlichen Sicherheit fehle, da die Speicherung anlasslos, d. h. ohne jede Einschränkung erfolge.[612]

Auch die Regelung des Zugangs zu den Daten wurde kritisiert. Es fehle an einem „objektiven Kriterium" zur Beschränkung des Zugangs und der späteren Nutzung der Daten durch die nationalen Behörden, da lediglich auf die von den Mitgliedstaaten zu bestimmenden schweren Straftaten verwiesen werde.[613] Bemängelt wurde zudem die nicht erfolgte Differenzierung der Speicherungsdauer anhand von Kriterien wie dem Nutzen für den verfolgten Zweck oder der betroffenen Personen.[614]

Aus diesen Gründen sei die RL 2006/24/EG nicht mit Art. 7 und 8 GRCh vereinbar.[615] Der EuGH erklärte daher die gesamte Richtlinie für

610 EuGH, Urteil v. 8.4.2014, C-293/12 - Digital Rights Ireland und C-594/12 - Seitlinger u. a., Rn. 51 ff.
611 EuGH, Urteil v. 8.4.2014, C-293/12 - Digital Rights Ireland und C-594/12 - Seitlinger u. a., Rn. 57.
612 EuGH, Urteil v. 8.4.2014, C-293/12 - Digital Rights Ireland und C-594/12 - Seitlinger u. a., Rn. 59.
613 EuGH, Urteil v. 8.4.2014, C-293/12 - Digital Rights Ireland und C-594/12 - Seitlinger u. a., Rn. 60.
614 EuGH, Urteil v. 8.4.2014, C-293/12 - Digital Rights Ireland und C-594/12 - Seitlinger u. a., Rn. 63.
615 EuGH, Urteil v. 8.4.2014, C-293/12 - Digital Rights Ireland und C-594/12 - Seitlinger u. a., Rn. 65.

ungültig.[616] Zu unterschiedlichen Interpretationen bot die abschließende Feststellung des EuGH Anlass, dass sich aus der „Gesamtheit der vorstehenden Erwägungen“[617] der Verstoß der RL 2006/24/EG gegen die Unionsgrundrechte ergebe.[618]

Die Vorratsdatenspeicherung war zudem Gegenstand eines weiteren Urteils,[619] das zugleich Gelegenheit zur Klärung der verbliebenen strittigen Punkte bot. In dieser Entscheidung ging es um die Frage der Auslegung von Art. 15 Abs. 1 der RL 2002/58/EG[620] im Licht von Art. 7 und 8 sowie 52 Abs. 1 GRCh.[621] Art. 15 Abs. 1 Satz 2 RL 2002/58/EG gestattet den Mitgliedstaaten die Einführung einer Vorratsdatenspeicherung unter anderem zwecks Feststellung und Verfolgung von Straftaten.[622] Der EuGH stellte fest, dass Art. 15 Abs. 1 RL 2002/58/EG einer allgemeinen und unterschiedslosen Vorratsspeicherung sämtlicher Verkehrs- und Standortdaten aller Teilnehmer und registrierten Nutzer elektronischer Kommunikationsmittel entgegensteht.[623] Es bedürfe einer am Zweck der

616 EuGH, Urteil v. 8.4.2014, C-293/12 - Digital Rights Ireland und C-594/12 - Seitlinger u. a. Rn. 73.

617 EuGH, Urteil v. 8.4.2014, C-293/12 - Digital Rights Ireland und C-594/12 - Seitlinger u. a. Rn. 69.

618 Siehe hierzu *Dix/Schaar*, in: Dix/Franßen/Kloepfer/Schaar/Schoch/Voßhoff/ Deutsche Gesellschaft für Informationsfreiheit (Hrsg.), Jahrbuch 2014, 17 (21), die für ein Verständnis des Erfordernisses des kumulativen Vorliegens dieser Voraussetzungen eintreten, d. h. dass bereits der Verstoß gegen eines der aufgeführten Elemente zu einer Rechtswidrigkeit einer Vorratsdatenspeicherung führt.

619 EuGH, Urteil v. 21.12.2016, C-203/15 - Tele 2 Sverige AB und C-698/15.

620 Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation), ABl. 2002, L 201, S. 37, in der durch die Richtlinie 2009/136/EG des Europäischen Parlaments und des Rates vom 25. November 2009, ABl. 2009, L 337 S. 11, geänderten Fassung.

621 EuGH, Urteil v. 21.12.2016, C-203/15 - Tele 2 Sverige AB und C-698/15, Rn. 1.

622 Siehe EuGH, Urteil v. 21.12.2016, C-203/15 - Tele 2 Sverige AB und C-698/15, Rn. 11.

623 EuGH, Urteil v. 21.12.2016, C-203/15 - Tele 2 Sverige AB und C-698/15, Rn. 134.

Maßnahme ausgerichteten Einschränkung.[624] Zudem sei Art. 15 Abs. 1 RL 2002/58/EG unter Berücksichtigung von Art. 7, 8 und 11 GRCh dahin auszulegen, dass er einer Regelung entgegensteht, die den Zugang zu den auf Vorrat gespeicherten Daten nicht auf Zwecke der Bekämpfung schwerer Straftaten beschränkt.[625] Es bedürfe Anhaltspunkten anhand objektiver Kriterien, dass die Betroffenen im Zusammenhang mit der Planung oder Begehung einer schweren Straftat stünden.[626] Die Maßstäbe des Urteils in der Rechtssache *Digital Rights* werden also auch auf nationale Regelungen übertragen, die ihre Grundlage nicht in der für ungültig erklärten RL 2006/24/EG finden, sondern in Art. 15 Abs. 1 RL 2002/58/EG.

cc) Bewertung

Eine Vorratsdatenspeicherung ohne Angabe einen konkreten Zwecks und daran anknüpfender Zugriffsregelungen ist nach allen drei Urteilen nicht zulässig. Jedenfalls für den öffentlichen Bereich scheidet eine Vorratsdatenspeicherung im engeren Sinne damit aus. Spätestens nach der Entscheidung des EuGH in der Rechtssache *Tele 2* ist davon auszugehen, dass die §§ 113a, 113b TKG aufgrund der Anlasslosigkeit der Vorratsdatenspeicherung unionsrechtswidrig sind.[627] Auch die Tatsache, dass eine Speicherung der Daten mit der Ausnahme von E-Mails und einiger weniger Gruppen von Berufsgeheimnisträgern im Wesentlichen nach wie vor ausnahmslos ist, d. h. die gesamte Bevölkerung trifft, ist mit den Vorga-

624 EuGH, Urteil v. 21.12.2016, C-203/15 - Tele 2 Sverige AB und C-698/15, Rn. 105.

625 EuGH, Urteil v. 21.12.2016, C-203/15 - Tele 2 Sverige AB und C-698/15, Rn. 134.

626 EuGH, Urteil v. 21.12.2016, C-203/15 - Tele 2 Sverige AB und C-698/15, Rn. 119.

627 So zutreffend - bereits vor Urteilsverkündung in Sachen Tele 2 Sverige AB - *Roßnagel*, NJW 2016, 533 (539); siehe auch *Deutscher Bundestag - Unterabteilung Europa*, Ausarbeitung zur Vorratsdatenspeicherung, S. 24, der einen Konflikt mit den Vorgaben des EuGH sieht, aber diesem letztlich die Entscheidung überlassen will.

ben des EuGH nicht zu vereinbaren.[628] Bereits nach der Entscheidung in *Digital Rights* wurden die Vorgaben des EuGH für die Vorratsdatenspeicherung als „Sargnagel jeder Form der Vorratsdatenspeicherung" bezeichnet.[629]

dd) EGMR

Auch der EGMR hat sich mit Fragen einer langfristigen Speicherung von Daten beschäftigt. Im Fall MK v. France[630] wurden die Fingerabdrücke des Klägers in einer nationalen französischen Datenbank gespeichert. Im Rahmen der Prüfung der Konformität mit der EMRK bemängelte der EGMR, dass die Rechtsgrundlage keinerlei Unterscheidung der Erhebung und Speicherdauer aufgrund des Zwecks der Maßnahme vorsah, obwohl die Daten für den Zweck der Speicherung erforderlich sein müssten.[631] Ein weiteres Problem lag darin, dass die Daten nur dann zu löschen waren, wenn sie für den Zweck der Datenbank nicht mehr erforderlich waren. Den Zweck der Datenbank sah der EGMR aber darin, so viele Daten wie möglich zu speichern. Dadurch sei die Gewährleistung der Löschung letztlich wirkungslos.[632] Auch die EMRK fordert somit eine konkrete Zweckangabe um die Rechtmäßigkeit des Datenumgangs prüfen zu können.

III. Die Zweckbindung im BDSG a. F. und einigen Spezialgesetzen

Als nächstes soll die Ausgestaltung der Zweckbindung im BDSG a. F. und einigen Spezialgesetzen betrachtet werden. Dabei wird zunächst die

628 Vgl. *Nachbaur*, ZRP 2015, 215 (216).
629 *Nachbaur*, ZRP 2015, 215 (216); a. A. aber *Simitis*, NJW 2014, 2158 (2160), der vielmehr von der Annahme der generellen Zulässigkeit der Vorratsdatenspeicherung durch den EuGH verbunden mit strengen Anforderungen an die Bestimmtheit des Gesetzestexts ausgeht.
630 EGMR, MK v. France, Nr. 19522/09, Urteil v. 18.4.2013.
631 EGMR, MK v. France, Nr. 19522/09, Urteil v. 18.4.2013, Rn. 32.
632 EGMR, MK v. France, Nr. 19522/09, Urteil v. 18.4.2013., Rn. 36.

Zweckfestlegung und die Bindung an diesen Zweck erörtert und danach der Frage nachgegangen, inwiefern eine Zweckänderung zulässig ist. Die Untersuchung bezieht sich somit in weiten Teilen auf seit dem 25. Mai 2018 nicht mehr geltende Rechtsvorschriften. Da das Zweckbindungsprinzip auch in der DSGVO enthalten ist, können viele Überlegungen aber auch unter diesem neuen Rechtsregime fortgelten.

1. Zweckfestlegung und -bindung

Im BDSG a. F. gibt es keine Norm, die die Zweckfestlegung und die daran anknüpfende Bindung allgemein und vollumfänglich festlegt. Auch gibt es keine allgemeinen Vorgaben zum Präzisionsgrad der Zweckbestimmung.[633] Daher bedarf es einer Betrachtung der unterschiedlichen Normen des BDSG a. F., die Elemente des Zweckbindungsprinzips enthalten. Von entscheidender Bedeutung für Big-Data-Anwendungen ist, welcher Konkretisierungsgrad der Zweckfestlegung sich den Normen des BDSG a. F. entnehmen lässt.

a) Allgemeine Bestimmungen des BDSG a. F.

aa) § 4 Abs. 3 Satz 1 Nr. 2 BDSG a. F.

Im Falle einer Direkterhebung der Daten beim Betroffenen ist dieser über die Zweckbestimmung des Datenumgangs zu unterrichten, sofern er nicht bereits Kenntnis erlangt hat, § 4 Abs. 3 Satz 1 Nr. 2 BDSG a. F. Dem Wortlaut ist bezüglich des Konkretisierungsgrades des Zwecks nichts zu entnehmen. Sinn dieser Vorschrift ist, die Kenntnis des Betroffenen zu gewährleisten, so dass dieser über die Preisgabe seiner Daten entscheiden kann, weshalb der Zweck hinreichend bestimmt angegeben

633 Vgl. *Forgó/Krügel/Rapp*, Zwecksetzung, S. 34.

werden muss.[634] Ein pauschaler Hinweis auf den Verarbeitungszweck reicht nicht aus.[635] Es genügt nicht, allein auf die Rechtsgrundlage hinzuweisen.[636] Sollten mehrere Zwecke verfolgt werden, ist über jeden von diesen zu informieren.[637]

bb) § 4a Abs. 1 Satz 2 BDSG a. F.

Nach § 4a Abs. 1 Satz 2 BDSG a. F. bedarf es für eine wirksame Einwilligung eines Hinweises auf den vorgesehenen Zweck des Datenumgangs. Bezüglich des Konkretisierungsgrades des Zwecks ist dem Wortlaut nichts zu entnehmen. Die dem BDSG a. F. zugrunde liegende DSRL gibt in Art. 2 lit. h vor, dass eine Einwilligung „für den konkreten Fall und in Kenntnis der Sachlage" zu erfolgen hat. Der Betroffene soll also die Tragweite und Folgen seiner Einwilligung abschätzen können.[638] Mit dieser Anforderung ist eine pauschale Einwilligung nicht vereinbar.[639] Eine Einwilligung gewissermaßen auf Vorrat für unbestimmte zukünftige Zwecke ist folglich unwirksam.[640] Der Konkretisierungsgrad richtet sich dabei nach dem Einzelfall[641] unter Berücksichtigung der jeweiligen Verarbeitungssituation.[642] Die Anforderungen an den Konkretisierungsgrad

634 Vgl. *Kramer*, in: Eßer/Kramer/v. Lewinski (Hrsg.), Auernhammer BDSG, § 4 Rn. 34; *Weichert*, in: Däubler/Klebe/Wedde/Weichert (Hrsg.), BDSG, § 4 Rn. 11 f.

635 *Bergmann/Möhrle/Herb*, BDSG, § 4 Rn. 43.

636 *Weichert*, in: Däubler/Klebe/Wedde/Weichert (Hrsg.), BDSG, § 4 Rn. 12.

637 *Taeger*, in: Taeger/Gabel (Hrsg.), BDSG, § 4 Rn. 75.

638 *Bergmann/Möhrle/Herb*, BDSG, § 4a Rn. 7a; vgl. *Kramer*, in: Eßer/Kramer/v. Lewinski (Hrsg.), Auernhammer BDSG, § 4a Rn. 21.

639 Vgl. *Plath*, in: Plath (Hrsg.), BDSG/DSGVO, § 4a Rn. 31; *Däubler*, in: Däubler/Klebe/Wedde/Weichert (Hrsg.), BDSG, § 4a Rn. 18; *Taeger,* in: Taeger/Gabel (Hrsg.), BDSG, § 4a Rn. 30; *Simitis*, in: Simitis (Hrsg.), BDSG, § 4a Rn. 77; *Zscherpe*, MMR 2004, 723 (725).

640 Vgl. *Bergmann/Möhrle/Herb*, BDSG, § 4a Rn. 29; siehe auch *Simitis*, in: Simitis (Hrsg.), BDSG, § 4a Rn. 77, der von „Blankoeinwilligungen" spricht; *Kühling*, in: Wolff/Brink (Hrsg.), DSR, § 4a Rn. 44.

641 Vgl. *Däubler*, in: Däubler/Klebe/Wedde/Weichert (Hrsg.), BDSG, § 4a Rn. 7.

642 Vgl. *Simitis*, in: Simitis (Hrsg.), BDSG, § 4a Rn. 80.

sind umso höher, je stärker das RiS betroffen ist.[643] Eine unzureichende Information über den Zweck des Datenumgangs führt zur Unwirksamkeit der Einwilligung.[644] Ein strenger Maßstab bei der Zweckbestimmung im Rahmen der Einwilligung sei im Falle eines Machtungleichgewichts zwischen Betroffenem und verantwortlicher Stelle besonders wichtig, da ansonsten ein nahezu unbegrenzter Datenumgang auf Grundlage von Einwilligungen drohe.[645]

Big-Data-Anwendungen stellt die Zweckdefinition vor große Herausforderungen. Im nicht-öffentlichen Bereich wird die Einwilligung als Möglichkeit gesehen die Zweckbindung der gesetzlichen Erlaubnistatbestände zu „überwinden" und den Datenumgang „flexibel (zu) legitimieren".[646] Der „konkrete Umfang des geplanten Data-Mining-Konzepts (sei) von vornherein mit dem Kunden zum Thema der Geschäftsbeziehungen zu machen".[647] Der Verarbeitungszweck solle „zwar hinreichend präzise aber dennoch mit entsprechender Weitsicht formuliert" werden.[648] Die Vorschläge einer weiten aber dennoch rechtskonformen Zweckfestlegung lassen keinerlei Maßstab für eine entsprechende Zweckdefinition erkennen und sind daher nicht hilfreich. Ein Vergleich mit den Anforderungen an eine Einwilligung zum Datenumgang für Forschungszwecke[649]

---

643 *Däubler*, in: Däubler/Klebe/Wedde/Weichert (Hrsg.), BDSG, § 4 a Rn. 18.

644 Vgl. *Kramer*, in: Eßer/Kramer/v. Lewinski (Hrsg.), Auernhammer BDSG, § 4a Rn. 22 m. w. N.; *Simitis*, in: Simitis (Hrsg.), BDSG, § 4a Rn. 6; *Bäcker*, in: Wolff/Brink (Hrsg.), DSR, § 4 Rn. 79 geht bei einer mangelnden Information in der Regel von einer Unwirksamkeit der Einwilligung aus; es wird auch vertreten, dass die Unwirksamkeit nur insoweit eintrete, wie der Betroffene uninformiert sei, *Kühling*, in: Wolff/Brink (Hrsg.), DSR, § 4a Rn. 43, was aber im Falle einer fehlenden Information über den Zweck bezüglich des kompletten Verarbeitungsvorgangs der Fall sein dürfte.

645 Vgl. *Simitis*, in: Simitis (Hrsg.), BDSG, § 4a Rn. 4, der die Einwilligung als „Schlüssel zu einem nahezu unbegrenzten (…) Zugang zu den von der verantwortlichen Stelle jeweils gewünschten Angaben" bezeichnet.

646 *Kühling*, in: Wolff/Brink (Hrsg.), DSR, § 4a Rn. 8.

647 *Hoeren*, in: Kilian/Heussen (Hrsg.), CHB, Teil 14, Datenschutzrechtliche Fragen, Rn. 18.

648 So *Feiler/Fina*, medien und recht 2013303 (304).

649 So vorsichtig, aber ebenfalls mit der Einschränkung, dass dies nicht ohne Weiteres übertragbar sei *Arming*, K&R Beihefter 3/2015 zu Heft 9 2015, 7 (11).

ist insofern nicht sonderlich zielführend, als dieser Bereich aufgrund der grundrechtlich geschützten Wissenschafts- und Forschungsfreiheit und der Tatsache, dass die Forschung auf Daten angewiesen ist, besonders privilegiert ist. Dies lässt sich nicht ohne Weiteres auf andere Bereiche übertragen. Zudem wird als Kompensation des etwas weiter gehalten Zwecks in der Regel eine schnellstmögliche Anonymisierung gefordert, so dass eine Verarbeitung personenbezogener Daten hiermit nicht gerechtfertigt werden kann. Das grundlegende Problem einer konkreten Zweckdefinition bei Big-Data-Anwendungen lässt sich also nicht mittels einer Einwilligung lösen.

Dies wird natürlich wiederum kritisiert. Es wirke „geradenach entmündigend", dass eine Einwilligung in zweckoffene Big-Data-Anwendungen nicht möglich sei, auch wenn die Zweckoffenheit gegenüber dem Betroffenen offengelegt werde.[650] Dem ist entgegenzuhalten, dass eine mündige Entscheidung nur eine hinreichend informierte oder jedenfalls mit das Informationsdefizit ausgleichenden Vorkehrungen versehene Einwilligung sein kann.

cc) § 4b Abs. 3, 6 BDSG a. F., § 4c Abs. 1 Satz 2 BDSG a. F.

Die Zweckbestimmung zählt nach § 4b Abs. 3 BDSG a. F. zu den Kriterien, die in der Regel zur Feststellung der Angemessenheit des Datenschutzniveaus beim Empfänger herangezogen werden können. Dem Wortlaut ist keine Aussage über die Qualität der Zweckbestimmung zu entnehmen. In der Literatur wird eine „klare Zweckbindung" gefordert.[651] Die Enge oder Weite der Zweckbestimmung hat maßgeblichen Einfluss auf die Beurteilung des Gefährdungsgrads für den Betroffenen.[652] Die Zulässigkeit einer Datenverwendung zu einem anderen Zweck als dem

650 *Schulz*, in: Gola (Hrsg.), DSGVO, Art. 7 Rn. 32.
651 *Simitis*, in: Simitis (Hrsg.), BDSG, § 4b Rn. 58.
652 Vgl. *Thomale*, in: Eßer/Kramer/v. Lewinski (Hrsg.), Auernhammer BDSG, § 4b Rn. 13; *Bergmann/Möhrle/Herb*, BDSG, § 4b Rn. 34; vgl. *Körffer/Gola/Klug*, in: Gola/Schomerus (Hrsg.), BDSG, § 4b Rn. 13.

Übermittlungszweck zeige, dass die Rechtsordnung des Drittstaats kein angemessenes Datenschutzniveau biete.[653]

Nur bei einer strengen Zweckbindung im Empfängerstaat ergebe der Hinweis auf den Übermittlungszweck nach § 4b Abs. 6 BDSG a. F. einen Sinn, da ansonsten eine Zweckentfremdung im Empfängerstaat rechtlich zulässig wäre.[654] Während § 4b Abs. 6 BDSG a. F. lediglich einen Hinweis auf den Übermittlungszweck vorsieht, ist bei den Ausnahmen nach § 4c Abs. 1 Satz 2 BDSG a. F. ein Hinweis darauf vorgesehen, dass die Daten nur für den Übermittlungszweck verarbeitet oder genutzt werden können. Es wird also eine Zweckbindung normiert.

dd) § 4d Abs. 1 BDSG a. F., § 4e Satz 1 Nr. 4 BDSG a. F.

Verfahren automatisierter Verarbeitungen sind grundsätzlich den Aufsichtsbehörden zu melden, § 4d Abs. 1 BDSG a. F. Die Meldepflicht trifft damit auch Big-Data-Anwendungen. Eine Definition des Begriffs „Verfahren" findet sich im BDSG a. F. nicht.[655] Unter Rückgriff auf die Kommissionsbegründung zu Art. 18 DSRL wird hierunter eine durch einen gemeinsamen Zweck verbundene Vielzahl von Verarbeitungsschritten im Rahmen eines Datenverarbeitungsvorgangs verstanden.[656] Die verantwortliche Stelle kann durch die Angabe eines einheitlichen Zwecks somit beeinflussen, welche Verarbeitungsschritte als ein Verfahren ange-

653 *Spindler*, in: Spindler/Schuster (Hrsg.), BDSG, § 4b Rn. 18.
654 *Simitis*, in: Simitis (Hrsg.), BDSG, § 4b Rn. 58.
655 *Raum*, in: Eßer/Kramer/v. Lewinski (Hrsg.), Auernhammer BDSG, § 4d Rn. 14; *v. d. Bussche*, in: Plath (Hrsg.), BDSG/DSGVO, § 4d Rn. 6.
656 *Petri*, in: Simitis (Hrsg.), BDSG, § 4d Rn. 6; *Brühann*, in: Grabitz/Hilf/Nettesheim (Hrsg.), DSRL, Art. 18 Rn. 5; *Klebe*, in: Däubler/Klebe/Wedde/Weichert (Hrsg.), BDSG, § 4d Rn. 2.

sehen werden.[657] Aufgrund der Ausnahmetatbestände fallen letztlich nur nicht-öffentliche Stellen in den Anwendungsbereich der Norm.[658]

Nach § 4e Satz 1 Nr. 4 BDSG a. F. sind bei meldepflichtigen automatisierten Datenverarbeitungen die Zweckbestimmungen des Datenumgangs anzugeben.[659] Im Falle der Änderung der Zwecke sind diese zu melden.[660] Dies ergibt sich aus § 4e Satz 2 i. V. m. § 4d Abs. 1 BDSG a. F.

(1) Streit über die Konkretheit der Zweckbestimmung

Nach einer Ansicht soll für die Angabe der Zweckbestimmung die Bezeichnung des Unternehmensgegenstands aus der Satzung bzw. dem Gesellschaftsvertrag ausreichend sein.[661] Begründet wird diese Meinung allerdings nicht.

Eine weitere Auffassung geht davon aus, dass der Konkretisierungsgrad des Zwecks aufgrund der Unbestimmtheit des Gesetzes Sache der verantwortlichen Stelle sei.[662] Ausreichend soll es demnach sein, wenn eine summarische Prüfung vorgenommen werden könne.[663] Eine Auffüh-

---

657 *Raum*, in: Eßer/Kramer/v. Lewinski (Hrsg.), Auernhammer BDSG, § 4d Rn. 16.

658 Vgl. *Raum*, in: Eßer/Kramer/v. Lewinski (Hrsg.), Auernhammer BDSG, § 4d Rn. 7.

659 Aus dem Wortlaut ergibt sich also, dass alle Zwecke anzugeben sind, sofern mehrere verfolgt werden. Dies verkennt *Meltzian*, in: Wolff/Brink (Hrsg.), DSR, § 4e Rn. 4, der behauptet, dass der Wortlaut im Singular gehalten sei.

660 *Gola/Klug/Körffer*, in: Gola/Schomerus (Hrsg.), BDSG, § 4e Rn. 6.

661 *Schaffland/Wiltfang*, BDSG, § 4e Rn. 3.

662 *Scheja*, in: Taeger/Gabel (Hrsg.), BDSG, § 4e Rn. 7; im Ergebnis auch, *v. d. Bussche*, in: Plath (Hrsg.), BDSG/DSGVO, § 4e Rn. 9.

663 *Scheja*, in: Taeger/Gabel (Hrsg.), BDSG, § 4e Rn. 7; zustimmend *v. d. Bussche*, in: Plath (Hrsg.), BDSG/DSGVO, § 4e Rn. 9, der die Möglichkeit einer „kursorischen Prüfung“ zum Maßstab nimmt; ebenso *Raum*, in: Eßer/Kramer/v. Lewinski (Hrsg.), Auernhammer BDSG, § 4e Rn. 13; *Gola/Klug/Körffer*, in: Gola/Schomerus (Hrsg.), BDSG, § 4e Rn. 1, sprechen von einer pauschalen Prüfung; in § 4e Rn. 6 wird andererseits auf eine schriftliche Dokumentation der Zwecke nach § 28 Abs. 1 Satz 2 und § 4 Abs. 3 Satz 2

rung von Verfahren wie z. B. „Zeiterfassungssysteme“, „Lohn- / Gehaltsabrechnungssysteme“, „Personalverwaltungssysteme“ soll nach dieser Ansicht genügen.[664] Zur Begründung wird teilweise darauf hingewiesen, dass § 4e BDSG a. F. an die Meldepflicht in § 4d BDSG a. F. und nicht an § 28 BDSG a. F. anknüpfe.[665] Zudem werde in Art. 18 und 19 DSRL der Begriff der Zweckbestimmung einheitlich verwendet, weshalb auch hier für die Pflicht und den Inhalt der Meldung von einer Beschreibung des Verfahrenszwecks auszugehen sei.[666]

Eine andere Ansicht fordert eine möglichst eindeutige und aussagekräftige Angabe der Primärzwecke, wie sie im Rahmen von § 4 Abs. 3 Satz 2 BDSG a. F. und § 28 Abs. 1 Satz 2 BDSG a. F. festzulegen sind.[667] Gestützt wird diese Auffassung auf den Gesetzeswortlaut, der auf die Zweckbestimmungen des Datenumgangs, nicht aber des „Verfahrens“ abstellt.[668] Des Weiteren sei so der zulässige Umfang des Datenumgangs präziser beschrieben.[669]

Eine weitere Auffassung fordert die Angabe des Geschäftszwecks, sowie angelehnt an §§ 28 ff. BDSG a. F. des Zwecks der Datenverarbeitung, da dies für die Bestimmung der Rechtmäßigkeit durch die Aufsichtsbehörde erforderlich sei.[670] Dabei solle zwischen einer Datenverar-

---

BDSG a. F. abgestellt. Es ist daher unklar, welcher Ansicht sich die Verfasser anschließen möchten.

664 *Scheja*, in: Taeger/Gabel (Hrsg.), BDSG, § 4e Rn. 7.

665 *Raum*, in: Eßer/Kramer/v. Lewinski (Hrsg.), Auernhammer BDSG, § 4e Rn. 12; *v. d. Bussche*, in: Plath (Hrsg.), BDSG/DSGVO, § 4e Rn. 8.

666 *Raum*, in: Eßer/Kramer/v. Lewinski (Hrsg.), Auernhammer BDSG, § 4e Rn. 12; *v. d. Bussche*, in: Plath (Hrsg.), BDSG/DSGVO, § 4e Rn. 8.

667 *Petri*, in: Simitis (Hrsg.), BDSG, § 4e Rn. 7; an anderer Stelle wird aber in demselben Kommentar hervorgehoben, dass die Zweckbestimmung in der Regel mit einer gewissen Abstraktion erfolgen müsse, da die automatisierte Verarbeitung sich auf eine Vielzahl von Vorgängen beziehe, siehe *Dammann*, in: Simitis (Hrsg.), BDSG, § 14 Rn. 45; *Schild*, DuD 2001, 282 (284); *Hallermann*, RDV 2013, 173 (176); im Ergebnis auch *Meltzian*, in: Wolff/Brink (Hrsg.), DSR, § 4e Rn. 4, ohne aber auf die Primärzwecke abzustellen.

668 *Petri*, in: Simitis (Hrsg.), BDSG, § 4e Rn. 7.

669 *Klebe*, in: Däubler/Klebe/Wedde/Weichert (Hrsg.), BDSG, § 4e Rn. 3.

670 *Bergmann/Möhrle/Herb*, BDSG, § 4e Rn. 10.

beitung für eigene Zwecke sowie zwischen einer Datenverarbeitung zum Zweck der Übermittlung und einer geschäftsmäßigen Datenverarbeitung zum Zweck der Übermittlung in anonymisierter Form unterschieden werden.[671]

(2) Stellungnahme

Zur Lösung des Streits bietet sich eine richtlinienkonforme Interpretation der §§ 4d und 4e BDSG a. F. an. Laut ErwG 48 DSRL dient die Meldung der Zweckbestimmung dem Ziel der Überprüfung der Vereinbarkeit der Verarbeitungen mit den einzelstaatlichen Vorschriften. Unter den Begriff „Verarbeitung" fällt gemäß Art. 2 lit. b DSRL auch eine Vorgangsreihe. Dies spricht dafür, dass nicht auf einen einzelnen Verarbeitungsschritt, sondern auf eine durch einen gemeinsamen Zweck verbundene Reihe von Verarbeitungsschritten abzustellen ist.[672] Auch die Kommission hat in der Begründung zu dem geänderten Richtlinienvorschlag nur eine Meldung für ein „gesamtes Paket" von Verarbeitungsvorgängen gefordert, so z. B. bei der Kreditverwaltung für die Schritte von der Vergabe bis zur Eintreibung der Schulden.[673] Die DSRL stellt sowohl in Art. 18 als auch in Art. 19 auf die Zweckbestimmungen der Verarbeitungen ab. Diese sind gemäß Art. 6 Abs. 1 lit. b DSRL eindeutig zu bestimmen. Es geht also um die bei der Erhebung der Daten festgelegten Primärzwecke.[674] Würde abstrakt auf den Unternehmensgegenstand abgestellt, wäre die in ErwG 48 DSRL geforderte Kontrolle der Datenverarbeitung nicht möglich.

---

671 *Bergmann/Möhrle/Herb*, BDSG, § 4e Rn. 10.

672 So auch *Ehmann/Helfrich*, DSRL-Kommentar, Art. 18 Rn. 1.

673 Amended proposal for a Council Directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data, COM (92), 422 final - SYN 287, S. 29.

674 *Brühann*, in: Grabitz/Hilf/Nettesheim (Hrsg.), DSRL, Art. 19 Rn. 7; *Dammann*, in: Dammann/Simitis (Hrsg.), DSRL-Kommentar, Art. 19 Rn. 3.

ee) Anlage zu § 9 Satz 1 BDSG a. F. Satz 2 Nr. 8

§ 9 BDSG a. F. sieht technische und organisatorische Maßnahmen vor, sofern diese erforderlich sind, d. h. in einem angemessenen Verhältnis zum angestrebten Schutzzweck stehen. Als Regelbeispiele werden in der Anlage zum BDSG a. F. einige Maßnahmen genannt. Bei einer automatisierten Datenverwendung ist gemäß Anlage zu § 9 Satz 1 BDSG a. F. Satz 2 Nr. 8 zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können. Diese Regelung zum Schutz der Zweckbindung wurde im Jahre 2001 in das BDSG a. F. eingefügt.[675] Systematisch handelt es sich um eine Norm zur Gewährleistung des Datenschutzes und nicht der Datensicherheit, weshalb der Standort in der Anlage zu § 9 Satz 1 BDSG a. F. überrascht.[676] Angelehnt ist das hier enthaltene Trennungsgebot an den ehemaligen § 4 Abs. 2 Nr. 4 TDDSG[677] und findet sich auch in § 13 Abs. 4 Satz 1 Nr. 4 TMG. Das Trennungsgebot soll laut Gesetzesbegründung aber in Fällen „(…) eine Einschränkung (finden), in denen ein Informationssystem daraufhin konzipiert ist, dass gesetzlich im Regelfall zugelassenen Zweckänderungen Rechnung getragen werden soll."[678] Es kann also nicht pauschal gesagt werden, dass das Trennungsgebot nicht zu beachten sei, wenn eine Zweckänderung grundsätzlich rechtlich zulässig wäre.[679] Vielmehr muss das System so beschaffen sein, dass es mögliche Zweckänderungen berücksichtigt.[680] Wie diese Ausnahme in einem System automatisiert um-

675 Gesetz zur Änderung des Bundesdatenschutzgesetzes und anderer Gesetze, Art. 1 Nr. 51 BGBl. I Nr. 23 2001, S. 904 (920); *Wedde*, in: Däubler/Klebe/Wedde/Weichert (Hrsg.), BDSG, § 9 Rn. 97.

676 *Plath*, in: Plath (Hrsg.), BDSG/DSGVO, § 9 Rn. 54.

677 Gesetzentwurf der Bundesregierung, Entwurf eines Gesetzes zur Änderung des Bundesdatenschutzgesetzes und anderer Gesetze, BT-Drs. 14/4329 S. 48.

678 Gesetzentwurf der Bundesregierung, Entwurf eines Gesetzes zur Änderung des Bundesdatenschutzgesetzes und anderer Gesetze, BT-Drs. 14/4329 S. 48.

679 So aber *Wedde*, in: Däubler/Klebe/Wedde/Weichert (Hrsg.), BDSG, § 9 Rn. 98; noch weitergehend *Schaffland/Wiltfang*, BDSG, § 9 Rn. 140, die feststellen, dass die Norm bei Zweckänderungen „faktisch ins Leere" ginge und deshalb kein Handlungsbedarf bestünde.

680 Vgl. *Gola/Klug/Körffer*, in: Gola/Schomerus (Hrsg.), BDSG, § 9 Rn. 29; *Ernestus*, in: Simitis (Hrsg.), BDSG, § 9 Rn. 162.

gesetzt werden kann, erscheint aber fraglich, da jeweils im Einzelfall zu prüfen ist, ob der Tatbestand der Zweckänderungsnorm erfüllt ist. Gerade im Rahmen von großen Datensammlungen wie bei Big Data ist diese Anforderung relevant.[681] Als Umsetzung werden eine getrennte Datenhaltung für jede unterschiedliche Anwendung vorgeschlagen[682] sowie unterschiedliche Zugriffsberechtigungen,[683] damit nicht durch einen Nutzer nach Abruf der Daten diese manuell zusammengeführt werden können.[684] Notwendig ist sicherlich, dass die Daten mit einer Attributs-Signatur versehen werden, der der Erhebungszweck zu entnehmen ist.[685] Wenn eine Zweckänderung zulässig ist, sollte der neue Zweck ebenfalls in der Signatur gespeichert werden, so dass auch diese Änderung sowie der Erhebungszweck weiter nachvollzogen werden können. Der Erhebungszweck muss aber auf jeden Fall weiter gespeichert bleiben. Denn ansonsten könnte eine Interessenabwägung bei weiteren Zweckänderungen nicht mehr korrekt durchgeführt werden, da der Erhebungszweck als Maßstab nicht mehr bekannt wäre und eine graduelle Entfernung vom Erhebungszweck mit jeder Zweckänderung möglich wäre.

ff) § 10 Abs. 1, Abs. 2 BDSG a. F.

§ 10 BDSG a. F. nennt die Zulässigkeitsvoraussetzungen der Einrichtung automatisierter Abrufverfahren. Nach § 10 Abs. 1 BDSG a. F. muss die Angemessenheit durch Abwägung der schutzwürdigen Betroffeneninteressen und der Aufgaben oder Geschäftszwecke der beteiligten Stellen

681 Vgl. *Bergmann/Möhrle/Herb*, BDSG, Anlage zu § 9 Satz 1 BDSG, die eine besondere Bedeutung im Rahmen von Datenpools bzw. Data-Warehouse-Technologien erkennen; *Schultze-Melling*, in: Taeger/Gabel (Hrsg.), BDSG, § 9 Rn. 85.

682 *Kramer/Meints*, in: Eßer/Kramer/v. Lewinski (Hrsg.), Auernhammer BDSG, § 9 Rn. 51.

683 *Schulte-Melling*, in: Taeger/Gabel (Hrsg.), BDSG, § 9 Rn. 87; *Plath*, in: Plath (Hrsg.), BDSG/DSGVO, § 9 Rn. 55.

684 *Wedde*, in: Däubler/Klebe/Wedde/Weichert (Hrsg.), BDSG, § 9 Rn. 98.

685 Vgl. *Ernestus*, in: Simitis (Hrsg.), BDSG, § 9 Rn. 163; vgl. ferner *Hoffmann*, Zweckbindung, S. 141.

festgestellt werden. Das Gesetz nennt die Zwecke in § 10 Abs. 1 BDSG a. F. nur sehr allgemein.[686] Zwecks Kontrolle der Zulässigkeit sieht § 10 Abs. 2 Satz 2 Nr. 1 BDSG a. F. die schriftliche Festlegung von Anlass und Zweck des Abrufverfahrens vor. Eine genauere Präzisierung der Qualität der Zweckbestimmung findet auch hier nicht statt. Jedenfalls muss sich der Zweck im öffentlichen Bereich innerhalb der gesetzlich zugewiesenen Aufgabe bewegen, so dass dies logischerweise die äußerste Grenze der Zweckbestimmung ist.[687] Im nicht-öffentlichen Bereich ist der Geschäftszweck im Rahmen der allgemeinen Handlungsfreiheit frei wählbar, weshalb sich hieraus keine relevante Einschränkung ergibt.[688] Für eine konkrete Beschreibung der Zwecke spricht aber, dass ansonsten die Zulässigkeit des Abrufverfahrens nicht überprüft werden kann.[689] So führt ein gegen den Erhebungszweck der Daten verstoßender Abruf zur Unangemessenheit des Abrufverfahrens.[690]

b) Zwischenergebnis allgemeine Bestimmungen des BDSG a. F.

Die allgemeinen Bestimmungen, insbesondere die Informationspflicht nach § 4 BDSG a. F. und die Einwilligung nach § 4a BDSG a. F., sprechen für eine konkrete Zweckfestlegung. Der Konkretisierungsgrad ist vom Verarbeitungskontext und der Betroffenheit des RiS abhängig. Würde der Zweck so allgemein gefasst, dass dieser pauschal eine Big-Data-Analyse erlaubt, wäre eine Zweckänderung nicht mehr nötig und ein Schutz der Zweckbindung durch getrennte Speicherung überflüssig. Zu-

686 Vgl. *Ehmann*, in: Simitis (Hrsg.), BDSG, § 10 Rn. 55; *Klebe*, in: Däubler/Klebe/Wedde/Weichert (Hrsg.), BDSG, § 10 Rn. 3 bezweifelt ob § 10 BDSG a. F. den Anforderungen der Zweckbindung gerecht wird.

687 Vgl. *Ehmann*, in: Simitis (Hrsg.), BDSG, § 10 Rn. 61.

688 Vgl. *Ehmann*, in: Simitis (Hrsg.), BDSG, § 10 Rn. 62.

689 Vgl. *Schultze-Melling*, in: Taeger/Gabel (Hrsg.), BDSG, § 10 Rn. 15; *Bergmann/Möhrle/Herb*, BDSG, § 10 Rn. 22 spricht sich für eine „konkrete" Beschreibung der Aufgabe aus, für die die Daten notwendig sind.

690 *Bergmann/Möhrle/Herb*, BDSG, § 10 Rn. 17 mit Verweis auf Daten aus einer Videoüberwachung nach § 6b BDSG; *v. Lewinski*, in: Wolff/Brink (Hrsg.), DSR, § 10 Rn. 20.

dem handelt es sich bei einer Big-Data-Analyse nicht um einen Zweck, d. h. das Ziel einer Handlung, sondern um ein Mittel, das zur Zweckerreichung eingesetzt wird.

c) öffentlicher Bereich

Für den öffentlichen Bereich finden sich die anwendbaren Vorschriften in den §§ 12 ff. BDSG a. F.

aa) § 13 Abs. 1 i. V. m. § 14 Abs. 1 BDSG a. F.

§ 13 BDSG a. F. regelt die Datenerhebung, während § 14 BDSG a. F. Vorgaben für das Speichern, Verändern oder Nutzen enthält. Nach § 13 Abs. 1 BDSG a. F. dürfen öffentliche Stellen Daten erheben, wenn die Kenntnis zur Erfüllung ihrer Aufgaben erforderlich ist. Im Falle der Erhebung von sensiblen Daten i. S. v. § 3 Abs. 9 BDSG a. F. sind gemäß § 13 Abs. 2 BDSG a. F. strengere Voraussetzungen zu beachten. Genauere Vorgaben zur Zweckfestlegung werden in § 13 Abs. 1 BDSG a. F. nicht gemacht. Aus § 14 Abs. 1 BDSG a. F. ergibt sich lediglich, dass ein Speichern, Verändern oder Nutzen dieser Daten nur zulässig ist, wenn es für den Erhebungszweck erfolgt. Es wird also grundsätzlich eine Zweckbindung festgeschrieben.[691] Daraus folgt zumindest, dass bei der Erhebung ein Zweck festgelegt werden muss.[692] Eine qualitative Einschränkung ist aber weder dem Wortlaut der einzelnen Normen, noch ihrem Zusammenspiel zu entnehmen. Anknüpfungspunkte für die Zweckbestim-

691 *Eßer*, in: Eßer/Kramer/v. Lewinski (Hrsg.), Auernhammer BDSG, § 14 Rn. 5; daher ist § 14 Abs. 1 BDSG a. F. von besonderer Bedeutung laut: *Heckmann*, in: Taeger/Gabel (Hrsg.), BDSG, § 14 Rn. 1; *Roggenkamp*, in: Plath (Hrsg.), BDSG/DSGVO, § 14 Rn. 1, erkennt hierin eine „strenge Zweckbindung"; *Wedde*, in: Däubler/Klebe/Wedde/Weichert (Hrsg.), BDSG, § 14 Rn. 4, eine „enge Zweckbindung".

692 Vgl. *Dammann*, in: Simitis (Hrsg.), BDSG, § 14 Rn. 39; der Plural „Zwecke" steht der Festlegung nur eines Zweckes nicht entgegen vgl. *Eßer*, in: Eßer/Kramer/v. Lewinski (Hrsg.), Auernhammer BDSG, § 14 Rn. 20.

mung sind somit die Aufgaben der öffentlichen Stellen und die Erforderlichkeit der Daten für diese Aufgaben.

(1) Die Aufgaben der öffentlichen Stellen

Art, Umfang und Grenzen der Aufgaben der verantwortlichen Stellen ergeben sich aus den Rechtsvorschriften, die ihnen die Aufgaben übertragen.[693] Die Aufgaben können dabei unterschiedlich klar definiert und gegebenenfalls an das Vorliegen besonderer Voraussetzungen gebunden sein.

Aufgrund der Schwierigkeit einen Zweck zu definieren, d. h. dessen Weite zu bestimmen, wurde angeregt, dass diese Aufgabe der Gesetzgeber durch entsprechende Zweckdefinitionen zu übernehmen habe.[694] Dem liegt wohl die Vorstellung zugrunde, dass der Erhebungszweck sich „automatisch" aus der Aufgabe ergebe, wenn diese konkret gefasst sei.[695] Umstritten ist aber gerade, inwieweit ein Einsatz von Generalklauseln zulässig ist und damit die Frage, wie konkret der Gesetzgeber den Zweck vorgeben muss.

Einerseits wird eine Verwendung von Generalklauseln ohne weitere Problematisierung für möglich gehalten.[696] So soll der Zweck „Schutz der inneren Sicherheit" hinreichend präzise und hiervon präventives wie repressives Tätigwerden der Polizeibehörden erfasst sein.[697] Eine Verwendung von Daten aus einem Strafverfahren zu Zwecken der Gefahrenab-

693 Vgl. *Gola/Klug/Körffer*, in: Gola/Schomerus (Hrsg.), BDSG, § 13 Rn. 2; *Sokol/Scholz*, in: Simitis (Hrsg.), BDSG, § 13 Rn.19; *Bergmann/Möhrle/Herb*, BDSG, § 13 Rn. 20; *Wedde*, in: Däubler/Klebe/Wedde/Weichert (Hrsg.), BDSG, § 13 Rn. 9.

694 *Badura*, in: Deutscher Bundestag (Hrsg.), Anhörungsbeitrag, S. 15 (16); ebenfalls für eine Zweckdefinition durch den Gesetzgeber, da der Zweck nicht mit der sachlichen Aufgabe zusammenfalle: *Albers*, in: Hoffmannn-Riem/Schmidt-Aßmann/Voßkuhle (Hrsg.), GVwR II², § 22, Rn.124.

695 So *Auernhammer*, BDSG, 3. A., § 14 Rn. 7.

696 *Scholz/Pitschas*, Informationelle Selbstbestimmung, S. 31.

697 *Scholz/Pitschas*, Informationelle Selbstbestimmung, S. 173 f.

wehr stelle keine Zweckänderung dar.[698] Es soll der „jeweilige Grundzweck der Verwaltungstätigkeit“ maßgeblich sein.[699] Zudem solle auch bei unterschiedlichen Behörden bei einem identischen Grundzweck z. B. „der sozialen Sicherheit“ insbesondere aufgrund der Amtshilfe eine Datenübermittlung zulässig sein.[700] Probleme ließen sich durch eine „(…) vernünftige Interpretation der Aufgaben und Zweckidentität vermeiden“.[701] Maßgeblich sei das jeweils betroffene Rechtsgut bzw. die Rechts- oder Gesetzesmaterie.[702] Die Zweckidentität sei weit auszulegen und auch Behörden mit „im wesentlichen zweckgleichen Verwaltungsaufgaben“ seien darunter zu fassen.[703] Eine Rechtsnorm könne als Zweck auch die Verwendung für einen bestimmten Verwaltungsbereich vorsehen.[704]

Andererseits werden Generalklauseln zwar grundsätzlich für zulässig gehalten, da es ansonsten aufgrund kasuistischer Regelungen zu einer der Normenklarheit widersprechenden Vielzahl von Einzelvorschriften käme.[705] Der Zweck „innere Sicherheit“ soll für das präventive und repressive Handeln der Polizei aber nicht ausreichen, da ein derart weiter Zweck dazu führen würde, dass es so gut wie nie zu einer rechtfertigungsbedürftigen Zweckänderung käme.[706] Vielmehr habe sich der Gesetzgeber auch bei der grundsätzlichen Zulässigkeit des Einsatzes von Generalklauseln um größtmögliche Präzision zu bemühen.[707] Zudem müsse die Zweckbestimmung umso enger ausfallen, je tiefer in das RiS

698 *Bull*, in: Lamnek/Tinnefeld (Hrsg.), Europol, S. 217 (224); *Bull*, Informationelle Selbstbestimmung, S. 106.
699 *Scholz/Pitschas*, AöR 110 (1985), S. 489 (510).
700 *Scholz/Pitschas*, AöR 110 (1985), S. 489 (511 f.).
701 *Scholz/Pitschas*, AöR 110 (1985), S. 389 (513).
702 *Scholz/Pitschas*, AöR 110 (1985), S. 489 (513).
703 *Scholz/Pitschas*, Informationelle Selbstbestimmung, S. 119.
704 *Scholz/Pitschas*, Informationelle Selbstbestimmung, S. 115.
705 *Walden*, Zweckbindung im Bereich der Polizei, S. 136 u. 146 f.; in diese Richtung auch *Coudert/Dumortier/Verbruggen*, purpose specification, S. 20 f. u. 23, die auf eine notwendige Abstraktion von Rechtnormen hinweisen.
706 *Walden*, Zweckbindung im Bereich der Polizei, S. 231.
707 *Walden*, Zweckbindung im Bereich der Polizei, S. 147.

eingegriffen werde.[708] Der Konkretisierungsgrad hänge vom Regelungskontext und den Schutzerfordernissen ab.[709] Teils wird gefordert, dass bei der Zulässigkeit einer Zweckänderung im Rahmen einer Generalklausel bei der Interessenabwägung die Stärke der Zweckabweichung berücksichtigt und die Anforderungen höher werden, je größer die Abweichung ist.[710]

Von einer anderen Ansicht wird der Einsatz von Generalklauseln abgelehnt.[711] Eine Zweckbindung bei einem derart weiten Grundzweck ergebe keinen Sinn[712] und es sei vielmehr zwischen Aufgabe einer Behörde und dem konkreten Zweck des Datenumgangs zu unterscheiden.[713] Eine generalisierende Aufgabennorm reiche für die gesetzliche Zweckbestimmung nicht aus, sondern es bedürfe vielmehr einer präzisen Zweckbeschreibung.[714] Ein mehrfacher Verwendungszweck für Aufgaben der Polizei (repressiv und präventiv) führe zu einer „quantitativen Konturlosigkeit" des Zweckbegriffs.[715]

An dieser Diskussion wird sehr gut der Unterschied zwischen Aufgabe und Zweck deutlich. Zwar kann und muss der Gesetzgeber innerhalb des durch die Normenklarheit vorgegebenen Rahmens auf Generalklauseln zurückgreifen, wenngleich die Vorgaben umso präziser sein sollten, je tiefer in das RiS eingegriffen wird. Allerdings kann es sich bei einer sol-

---

708 *Walden*, Zweckbindung im Bereich der Polizei, S. 266.

709 *Albers*, in: Hoffmannn-Riem/Schmidt-Aßmann/Voßkuhle (Hrsg.), GVwR II², § 22, Rn. 124.

710 *Bischoff*, in: Traunmüller/Fiedler/Grimmer/Reinermann (Hrsg.), Zweckbindung, S. 193 (208).

711 *Simitis*, NJW 1984, 398 (400); *Polenz*, in: Kilian/Heussen (Hrsg.), CHB, Teil 13 Datenschutz, Materielles allgemeines Datenschutzrecht Rn. 10.

712 *Heußner*, in: Brandt/Gollwitzer/Henschel (Hrsg.), FS Simon, 231 (238 f.); vgl. auch *Hoffmann*, Zweckbindung, S. 127, der ein „Leerlaufen" der Zweckbindung befürchtet.

713 *Simitis*, NJW 1986, 2795 (2799 f.); ähnlich auch *Bäumler*, AöR 110 (1985), S. 30 (31 f.), der sich grundsätzlich gegen die Verwendung von Generalklauseln und für hinreichend konkretisierte Befugnisnormen ausspricht.

714 *Roßnagel/Laue*, DÖV 2007, 543 (545).

715 *Forgó/Krügel/Rapp*, Zwecksetzung, S. 36 f.

chen Generalklausel immer nur um eine Aufgabe, nie aber um einen Zweck handeln, da nicht mehr festgestellt werden könnte, welche Daten für welche Verarbeitungsvorgänge für diesen Zweck benötigt werden und die Rechtmäßigkeit nicht mehr überprüft werden könnte.[716] Die Zweckfestlegung verlöre also ihre den Datenumgang eingrenzende Funktion. Die Aufgabe bildet somit den Rahmen der Zweckbestimmung. Es bedarf aber in der Regel einer Konkretisierung im Einzelfall.

Abweichend von der gesetzlichen Terminologie und diese kritisierend, wird vertreten, dass die Begriffe „Zweck" und „Aufgabe" nicht konsistent verwendet würden.[717] Häufig würden Zwecke als Aufgaben bezeichnet,[718] so beispielsweise in § 1 SGB I.[719] Eine Aufgabe sei demnach „(…) eine Menge sinnvoll geordneter Verhaltensanweisungen, aus denen auszuwählen dem Adressaten überantwortet ist."[720] Der Zweck eines Aufgabenbündels sei folglich „(…) die Benennung oder Beschreibung eines Zustandes, der durch die Erfüllung der Aufgaben konstituiert, gesichert oder vermieden werden soll."[721] Diese Definitionen werden später noch um die Zuständigkeit und Verfassungsmäßigkeit ergänzt.[722] Die Aufgabe sei immer an einen Zweck angebunden, weshalb sich nicht von einer Aufgabe auf einen Zweck schließen lasse.[723] Ergänzt wird das Ganze durch den Begriff der Arbeitsaufgabe, die „eine Menge von operationalen Handlungsanweisungen, die als Teilmenge der organisatorischen und fachtechnischen Realisierung einer Aufgabe so genau ist, daß sie einem Handlungssubjekt (Mensch, Maschine) überantwortet werden kann und darüber hinaus feststellbar bleibt, ob und mit welchem Erfolg sie ausgeführt worden ist."[724] Im Rahmen von Zweckhierarchien, d. h. einem übergeordneten Zweck, der mehrere untergeordnete Zwecke beinhaltet, sei ein

716 Vgl. *Hoffmann*, Zweckbindung, S. 18 f.
717 *Hoffmann*, Zweckbindung, S. 77.
718 *Hoffmann*, Zweckbindung, S. 105.
719 *Hoffmann*, Zweckbindung, S. 77.
720 *Hoffmann*, Zweckbindung, S. 82.
721 *Hoffmann*, Zweckbindung, S. 83.
722 *Hoffmann*, Zweckbindung, S. 90.
723 *Hoffmann*, Zweckbindung, S. 83.
724 *Hoffmann*, Zweckbindung, S. 91.

zu abstrakter Zweck ein „Angriff auf das Datenschutzrecht“.[725] Personenbezogene Daten dürften nur für „Datenschutzgeeignete Zwecke“ erhoben werden, d. h. solche, die so präzise seien, dass sich Aufgaben hierdurch entdecken ließen, so dass die Daten für diese Aufgabe erforderlich seien.[726] Falls ein Zweck noch Unterzwecke enthalte, sei der Zweck soweit wie möglich zu präzisieren, da dies durch das Verhältnismäßigkeitsprinzip gefordert werde.[727]

Eine Notwendigkeit für ein Abweichen von der in den Gesetzen üblicherweise verwendeten Terminologie bezüglich Aufgabe und Zweck besteht nicht. Es ist auch nicht ersichtlich, dass dies an anderer Stelle in der Literatur gefordert würde. Daher ist weiterhin davon auszugehen, dass der Begriff der Aufgabe in der Regel umfassender als der des Zwecks ist. Die Aufgabe steht hierarchisch oberhalb des Zwecks und bildet dessen Rahmen und nicht umgekehrt. Es ist aber richtig, dass nach der Definition eines Zwecks die Frage aufkommt, auf welche Weise, d. h. mit welchen Mitteln dieser erfüllt werden kann. Dies wird von *Hoffmann* erkannt und entspricht in seiner Terminologie wohl dem Begriff der „Arbeitsaufgabe“. Terminologisch ist auch diese Bezeichnung allerdings unglücklich gewählt.

(2) Die Erforderlichkeit

Damit stellt sich des Weiteren die Frage der Erforderlichkeit des Datenumgangs zur Aufgabenerfüllung. Dies sei der Fall, wenn der Datenumgang zur Aufgabenerfüllung objektiv beitrage und dem verfolgten Zweck angemessen sei.[728] § 13 Abs. 1 BDSG a. F. sei bezüglich der Erforderlichkeit eng auszulegen.[729] Die Erforderlichkeit verlange die Anga-

725 *Hoffmann*, Zweckbindung, S. 108.
726 *Hoffmann*, Zweckbindung, S. 111 f.
727 Vgl. *Hoffmann*, Zweckbindung, S. 113.
728 Vgl. *Schaffland/Wiltfang*, BDSG, § 13 Rn. 1.
729 *Bergmann/Möhrle/Herb*, BDSG, § 13 Rn. 14; Maßgeblich sei, was zu einer „schlanken Aufgabenerfüllung“ benötigt werde, siehe *Heckmann*, in:

be konkreter Verwendungszwecke, die zur Eingrenzung der Aufgabenzuweisungsnorm festgelegt worden seien.[730] Deutlich wird das am Beispiel des Zwecks „Schutz der inneren Sicherheit", der viele Möglichkeiten zur Zweckerfüllung eröffnet, weshalb nicht mehr klar ist, welche Daten zwingend benötigt werden.[731] Das gesetzlich vorgesehene Zusammenspiel zwischen Zweckbestimmung anhand einer Aufgabe und Begrenzung auf die hierzu erforderlichen Daten[732] kann also nur dann seine volle Wirksamkeit entfalten, wenn der Zweck möglichst konkret festgelegt ist, d. h. dass die Zweckbestimmung im Rahmen der Zweckhierarchie auf der untersten, also der präzisesten Ebene zu erfolgen hat.

(3) Streit über den Abstraktionsgrad der Zweckfestlegung

Gerade die Frage der Zweckpräzision ist ein großer Streitpunkt in der wissenschaftlichen Diskussion über das Zweckbindungsprinzip. So wird sogar vertreten, dass viele Datenerhebungen eine präzise Zweckangabe nicht zuließen und kritisiert, dass abstrakt formulierte Zwecke keine Steuerungswirkung erreichten.[733] Im Folgenden soll daher der Frage des Abstraktionsgrads der Zweckbestimmung nachgegangen werden. Zur Weite oder Enge der Zweckbestimmung werden verschiedene Ansichten vertreten.

Nach einer Ansicht könne der Zweck sowohl weit als auch eng festgelegt werden,[734] wobei die Entscheidung hierüber der verantwortlichen

---

Taeger/Gabel (Hrsg.), BDSG, § 13 Rn. 19; BSG, Urteil v. 28.11.2002, NJW 2003, 2932.

730 Vgl. *Albers*, in: Wolff/Brink (Hrsg.), DSR, § 14 Rn. 5, 7, 11; vgl. auch im Umkehrschluss *Hoffmann*, Zweckbindung, S. 70.

731 Vgl. *Hoffmann*, Zweckbindung, S. 110; *Schlink*, NVwZ 1986, 239 (255).

732 *Wedde*, in: Däubler/Klebe/Wedde/Weichert (Hrsg.), BDSG, § 14 Rn. 10, geht von einer „prägenden Bedeutung" einer restriktiv auszulegenden Erforderlichkeit aus.

733 *Forgó/Krügel/Rapp*, Zwecksetzung, S. 34.

734 *Dörr/Schmidt*, BDSG, § 14 Rn. 2.

Stelle obliege.[735] Dem BDSG a. F. lasse sich nicht entnehmen, dass ein enger Zweck festzulegen sei.[736] Das Zweckbindungsprinzip lasse eine weite Zweckdefinition zu.[737] Es bedürfe aufgrund verfassungsrechtlicher und europarechtlicher Vorgaben nicht der „engsten" Festlegung des Zweckes, sondern Voraussetzung sei vielmehr, dass der Betroffene den Datenumgang überschauen könne.[738] Je allgemeiner der Zweck gehalten sei, desto weniger komme die Notwendigkeit einer Zweckänderung in Betracht.[739] Es obliege der verantwortlichen Stelle „den Zweck so festzulegen, dass eine zügige Aufgabenerledigung unter Nutzung oder Verarbeitung der gespeicherten Daten möglich" sei.[740]

Vielfach wird in der Literatur demgegenüber eine möglichst konkrete Zweckfestlegung gefordert.[741] Verfassungsrechtlich seien die Zweckbindung der Datenverarbeitung und die Berechenbarkeit des Informationsflusses vorgegeben, woran sich die Auslegung von § 14 Abs. 1 BDSG a. F. zu orientieren habe.[742] Dass § 14 Abs. 1 BDSG a. F. den Plural Zwecke verwendet, stehe einer restriktiven Auslegung der Weite des Zwecks nicht entgegen.[743] Die sachlichen Kompetenzen dienten bei der Zweckfestlegung als „Anknüpfungspunkt und als Gerüst".[744] Die Zweckbe-

735 *Schaffland/Wiltfang*, BDSG, § 14 Rn. 19.
736 *Forgó/Krügel/Rapp*, Zwecksetzung, S. 34; *Bull*, RDV 1999, 148 (151).
737 *Brouwer*, in: Besselink/Pennings/Prechal (Hrsg.), Legality Principle, S. 280, die aber zugleich auf die damit verbundene Schwierigkeit der Rechtmäßigkeitskontrolle und der Durchsetzung des Zweckbindungsprinzips hinweist.
738 *Scholz*, in: Roßnagel (Hrsg.), Handbuch DSR, Kap. 9.2 Rn. 76.
739 *Dörr/Schmidt*, BDSG, § 14 Rn. 3.
740 *Dörr/Schmidt*, BDSG, § 14 Rn. 3.
741 *Eßer*, in: Eßer/Kramer/v. Lewinski (Hrsg.), Auernhammer BDSG, § 14 Rn. 22; so auch *Dammann*, in: Simitis (Hrsg.), BDSG, § 14 Rn. 43, der eine Festlegung auf einer „konkreten Ebene" der Aufgabe der verantwortlichen Stelle fordert; *Gola/Klug/Körffer*, in: Gola/Schomerus (Hrsg.), BDSG, § 14 Rn. 9; abschwächend *Bergmann/Möhrle/Herb*, BDSG, § 14 Rn. 19, die jedenfalls eine „zu allgemeine" Zweckbestimmung für nicht zulässig halten.
742 *Dammann*, in: Simitis (Hrsg.), BDSG, § 14 Rn. 37.
743 *Heckmann*, in: Taeger/Gabel (Hrsg.), BDSG, § 14 Rn. 27.
744 *Albers*, in: Hoffmannn-Riem/Schmidt-Aßmann/Voßkuhle (Hrsg.), GVwR II², § 22, Rn. 123; ähnlich *Dammann*, in: Simitis (Hrsg.), BDSG, § 14 Rn. 40, der auf die Legitimationsgrundlage zur Zweckbestimmung abstellt; siehe auch

stimmung solle pragmatisch anhand der zu erfüllenden Aufgabe erfolgen,[745] die zugleich die Grenze für den Zweck bilde.[746] Der Zweck sei in der Regel enger festzulegen als die zugrunde liegende Aufgabe[747] aber weiter als der konkrete Anlass der Maßnahme.[748] Ein „zu hoher Abstraktionsgrad" widerspreche den „deutlich artikulierten Absichten" der DSRL und „dem Willen" des BDSG-Gesetzgebers.[749] So soll die Zweckangabe „Verwaltungsvollzug" nicht genügen.[750] Durch eine präzise Zweckformulierung werde ersichtlich mit welchem Mittel im jeweiligen Kontext das Ziel erreicht werden könne.[751] Die Zweckdefinition müsse hinreichend konkret erfolgen, um die Anwendung anderer datenschutzrechtlicher Grundsätze zu ermöglichen und den Umfang der Verarbeitung zu begrenzen.[752] Eine allgemeine Aussage darüber, wo der Punkt der notwendigen Zweckpräzisierung zwischen präzise und unpräzise liegt, sei nicht möglich.[753]

Differenzierend wird auf die Schutzwürdigkeit des Betroffenen abgestellt. Enge Zweckfestlegungen seien sinnvoll, wenn ein besonderes Schutzniveau verankert werden müsse, weite Zweckfestlegungen, wenn sie „aufgrund präzise gefasster sachlicher Aufgaben Gehalt gewinnen" und die Schutzerfordernisse und Einfluss- sowie Kenntnisnahmemöglich-

---

Heckmann, in: Taeger/Gabel (Hrsg.), BDSG, § 14 Rn. 24 f., der zudem die Ermächtigungsnorm eng auslegen möchte. Er scheint aber nicht zwingend auf einer Zweckfestlegung durch die verantwortliche Stelle zu bestehen, da auf den tatsächlich verfolgten Handlungsweck abzustellen sei, falls sich aus der Auslegung der Ermächtigungsgrundlage kein Zweck bestimmen lasse; so auch *Dammann*, in: Simitis (Hrsg.), BDSG, § 14 Rn. 41.

745 *Dammann*, in: Simitis (Hrsg.), BDSG, § 14 Rn. 42.

746 Vgl. *Eßer*, in: Eßer/Kramer/v. Lewinski (Hrsg.), Auernhammer BDSG, § 14 Rn. 23; *Heckmann*, in: Taeger/Gabel (Hrsg.), BDSG, § 14 Rn. 26.

747 *Gusy*, KritV 2000, 52 (63); *v. Zezschwitz*, in: Roßnagel (Hrsg.), Handbuch DSR, Kap. 3.1 Rn. 22, stellt auf die „jeweilige konkrete Aufgabenwahrnehmung" ab.

748 Vgl. Roggenkamp, in: Plath (Hrsg.), BDSG/DSGVO, § 14 Rn. 4.

749 *Gola/Klug/Körffer*, in: Gola/Schomerus (Hrsg.), BDSG, § 14 Rn. 9.

750 *Eßer*, in: Eßer/Kramer/v. Lewinski (Hrsg.), Auernhammer BDSG, § 13 Rn. 11.

751 *Hoffmann*, Zweckbindung, S. 64 u. 69 f.

752 Vgl. *Artikel-29-Datenschutzgruppe*, WP 203, S. 12.

753 *Hoffmann*, Zweckbindung, S. 71.

keiten der betroffenen Personen gewahrt seien.[754] Der vorzusehende Konkretisierungsgrad der Zweckbestimmung im öffentlichen Bereich hänge von der „Schutzbedürftigkeit der Informationen“ und der „Eigenart der Allgemeininteressen“ ab.[755] Auch die Bestimmung eines „übergeordneten mehrere konkrete Nutzungsmöglichkeiten einschließenden Verwendungszwecks“ soll je nach Kontext möglich sein.[756] Wegen des Risikos einer sehr weiten Fassung des Zwecks durch die verantwortliche Stelle, solle es nicht auf den Zweck ankommen, den diese dem Betroffenen mitgeteilt hat.[757] Der mitgeteilte Zweck könne lediglich eine Selbstbindung nach Treu und Glauben bewirken.[758]

Die Funktion der Zweckfestlegung spricht gegen eine allgemeine und für eine möglichst konkrete Bestimmung des Zweckes. Wie von allen Ansichten zu Recht hervorgehoben wird, ist eine allgemeine Formel zur Bestimmung des Konkretisierungsgrades §§ 13 und 14 BDSG a. F. nicht zu entnehmen. Der notwendige Konkretisierungsgrad ergibt sich vielmehr aus den konkreten Umständen und richtet nach der Schutzbedürftigkeit des Betroffenen. Im Rahmen von Big-Data-Projekten öffentlicher Stellen ist jedenfalls die Angabe des Zwecks „Data Mining“ aufgrund seiner Unbestimmtheit und der Vielzahl der damit insbesondere verfolgbaren Sekundärzwecke nicht möglich.[759]

---

754 *Albers*, in: Hoffmannn-Riem/Schmidt-Aßmann/Voßkuhle (Hrsg.), GVwR II², § 22, Rn. 126; vgl. auch *Härting*, NJW 2015, 3284 (3285 u. 3286), der ebenfalls auf Sicherungsmechanismen abstellt.

755 *Badura*, in: Deutscher Bundestag (Hrsg.), schriftliche Stellungnahme, S. 148 (159).

756 *Albers*, in: Wolff/Brink (Hrsg.), DSR, § 14 Rn. 21.

757 *Heckmann*, in: Taeger/Gabel (Hrsg.), BDSG, § 14 Rn. 24; a. A.: *Tinnefeld/Ehmann/Gerling*, S. 512, die in formaler Hinsicht auf den genannten Zweck abstellen, der sich in materieller Hinsicht im Rahmen der Rechtsvorschrift bewegen muss.

758 *Eßer*, in: Eßer/Kramer/v. Lewinski (Hrsg.), Auernhammer BDSG, § 14 Rn. 23; *Heckmann*, in: Taeger/Gabel (Hrsg.), BDSG, § 14 Rn. 24; *Dammann*, in: Simitis (Hrsg.), BDSG, § 14 Rn. 39.

759 Vgl. *Baeriswyl*, RDV 2000, 6 (7 f.).

(4) Bindung an den Erhebungszweck

Die Zweckbindung wolle verhindern, dass „Rohinformationen" die für einen Zweck erhoben worden seien für einen anderen genutzt würden, obwohl sie für diesen nicht oder eventuell genauer erhoben worden wären.[760] Ob eine weitere Verwendung noch zulässig ist, richtet sich nach der Weite der bei der Erhebung festgelegten Zweckbindung.[761] Entscheidend für die Wirksamkeit der Zweckbindung ist der Konkretisierungsgrad des Zweckes bei der Zweckfestlegung.[762] Kritisiert wird aber, dass sich eine strenge Anwendung der Zweckbindung aufgrund der vielen gesetzlichen Ausnahmen nur schwer durchhalten lasse.[763]

Umstritten ist, ob Daten einer Zweckbindung unterliegen, wenn die verantwortliche Stelle sie ohne Erhebung erlangt hat. Nach einer Auffassung soll die Speicherung keiner Zweckbindung unterliegen[764] bzw. soll eine Verwendung dieser Daten zur Erfüllung eigener Aufgaben zulässig sein.[765] Nach anderer Ansicht soll es in einem solchen Falle auf den Zweck ankommen, für den die Daten spontan zugesendet wurden.[766] Wenn jemand einer Behörde aus eigener Initiative persönliche Daten zukommen lässt, geschieht dies in der Regel zur Erreichung eines bestimmten Zwecks. In der Zusendung der Daten ist also eine konkludente Einwilligung der Verwendung der Daten zu diesem Zweck zu sehen. § 14 Abs. 1 Satz 2 BDSG a. F. stellt zwar für die Zweckbindung nur auf den Speicherungszweck ab, dies bedeutet aber nicht, dass eine Speicherung für beliebige Zwecke aufgrund dieser Vorschrift zulässig ist. Denn hierzu

760 *Bull*, in: Lamnek/Tinnefeld (Hrsg.), Globaliserung und informationelle Rechtskultur, S. 217 (225).
761 Vgl. *Heckel*, NVwZ 1994, 224 (226).
762 *Heckmann*, in: Taeger/Gabel (Hrsg.), BDSG, § 14 Rn. 24.
763 *Bull*, Informationelle Selbstbestimmung, S. 106; ähnlich *Bull*, in: Lamnek/Tinnefeld (Hrsg.), Globaliserung und informationelle Rechtskultur, S. 217 (223).
764 *Auernhammer*, BDSG, 3. A., § 14 Rn. 8.
765 *Dörr/Schmidt*, BDSG, § 14 Rn. 6.
766 *Schaffland/Wiltfang*, BDSG, § 14 Rn. 22; *Dammann*, in: Simitis (Hrsg.), BDSG, § 14 Rn. 40.

trifft die Norm gerade keine Aussage. Durch § 14 Abs. 1 Satz 2 BDSG a. F. sollen „Lücken im Anwendungsbereich des Zweckbindungsgrundsatzes“ vermieden werden.[767] Es ist nicht ersichtlich, weshalb eine Speicherung für beliebige Zwecke zulässig sein sollte. Dies würde erheblich in das informationelle Selbstbestimmungsrecht des Betroffenen eingreifen. Auch ist nicht nachvollziehbar, weshalb eine Veränderung oder Nutzung der Daten innerhalb des mitunter relativ weiten Aufgabenbereichs der Behörde zulässig sein soll, wenn dieser die Daten für einen konkreten Zweck zugesendet wurden.

Sofern der Erhebung eine Übermittlung durch eine andere Stelle vorausgeht, sind Übermittlungs- und Erhebungszweck kumulativ zu beachten.[768] Im öffentlichen Bereich führe die Gewährleistung der Zweckbindung der Daten zu einer informationellen Gewaltenteilung, mit der Folge, dass die Datenübermittlung von einer Behörde zu einer anderen einer Rechtsgrundlage bedarf.[769]

bb) §§ 15, 16 BDSG a. F.

Die §§ 15 und 16 BDSG a. F. regeln die Übermittlung von Daten durch öffentliche Stellen an öffentliche bzw. nicht-öffentliche Stellen. § 15 Abs. 1 Nr. 2 BDSG a. F. schreibt für die Zulässigkeit einer Übermittlung an öffentliche Stellen in einer der Fälle des § 15 Abs. 1 Nr. 1 BDSG a. F. vor, dass die Voraussetzungen einer Nutzung gemäß § 14 BDSG a. F. vorliegen müssen. Hierdurch wird eine Bindung an den Erhebungszweck bewirkt, wobei die Verweisung auch die Ausnahmen von der Zweckbindung nach § 14 Abs. 2 BDSG a. F. mitumfasst.[770] Eine entsprechende Vorschrift für die Übermittlung an nicht-öffentliche Stellen enthält § 16 Abs. 1 Nr. 1 BDSG a. F. Eine Übermittlung ist also nicht für beliebige Zwecke losgelöst vom Erhebungszweck zulässig, sondern nur, sofern ei-

767 *Heckmann*, in: Taeger/Gabel (Hrsg.), BDSG, § 14 Rn. 30.
768 *Dammann*, in: Simitis (Hrsg.), BDSG, § 14 Rn. 38.
769 *Hoffmann*, Zweckbindung, S. 21 f.
770 *Bergmann/Möhrle/Herb*, BDSG, § 15 Rn. 17.

ne entsprechende Zweckänderung zulässig ist.[771] Auch für den Übermittlungszweck ist aufgrund europarechtlicher und verfassungsrechtlicher Vorgaben eine konkrete Zweckfestlegung angezeigt.[772]

Nach § 15 Abs. 3 Satz 1 bzw. § 16 Abs. 4 Satz 1 BDSG a. F. ist der Empfänger an den Übermittlungszweck der Daten gebunden. Die Übermittlungsregelungen sollen insbesondere vor den Risiken des Kontextverlustes der Daten aufgrund der Übermittlung schützen.[773] § 15 Abs. 3 BDSG a. F. wird als Folge des Volkszählungsurteils bezeichnet.[774] Auf die Zulässigkeit von Zweckänderungen wird später eingegangen.[775]

cc) § 19 Abs. 1 Satz 1 Nr. 3 BDSG a. F.

Zwecks Stärkung der Stellung des Betroffenen wurde mit der BDSG-Novelle 1990 in § 19 Abs. 1 Satz 1 Nr. 3 BDSG a. F. ein Recht auf Auskunft über den Zweck der Datenspeicherung verankert.[776] Dies dient der Feststellung der Rechtmäßigkeit der Speicherung.[777] Folglich besteht ein Anspruch auf eine Auskunft über einen konkret gefassten Zweck.[778]

dd) § 19a Abs. 1 Satz 1 BDSG a. F.

§ 19a BDSG a. F. regelt die Benachrichtigung durch öffentliche Stellen im Falle einer Datenerhebung ohne Kenntnis des Betroffenen. Der auf-

771 Vgl. *Eßer*, in: Eßer/Kramer/v. Lewinski (Hrsg.), Auernhammer BDSG, § 15 Rn. 18; *Albers*, in: Wolff/Brink (Hrsg.), DSR, § 15 Rn. 20.
772 *Albers*, in: Wolff/Brink (Hrsg.), DSR, § 15 Rn. 34.
773 *Eßer*, in: Eßer/Kramer/v. Lewinski (Hrsg.), Auernhammer BDSG, § 15 Rn. 2; vgl. *Heckmann*, in: Taeger/Gabel (Hrsg.), BDSG, § 15 Rn. 1; vgl. *Albers*, in: Wolff/Brink (Hrsg.), DSR, § 15 Rn. 1.
774 *Eßer*, in: Eßer/Kramer/v. Lewinski (Hrsg.), Auernhammer BDSG, § 15 Rn. 29.
775 D. III. 6., S. 208 ff.
776 Vgl. BT-Drs. 11/4306, S. 46.
777 *Roggenkamp*, in: Plath (Hrsg.), BDSG/DSGVO, § 19 Rn. 11; vgl. *Gola/Klug/Körffer*, in: Gola/Schomerus (Hrsg.), BDSG, § 19 Rn. 7.
778 *Worms*, in: Wolff/Brink (Hrsg.), DSR, § 19 Rn. 39.

grund von § 14 BDSG a. F. festzulegende Zweck des Datenumgangs ist dem Betroffenen im Falle einer Datenspeicherung grundsätzlich umfassend mitzuteilen.[779] Sofern verschiedene Zwecke verfolgt werden, ist jeder einzelne mitzuteilen.[780] Durch diese Vorschrift soll die Transparenz der Datenverarbeitung sichergestellt werden.[781] Es handelt sich um eine „verfahrensrechtliche Schutzvorkehrung" des RiS,[782] wie sie im Volkszählungsurteil gefordert wurde.[783]

d) Zwischenergebnis für den öffentlichen Bereich

Sowohl die Rechtsgrundlagen der Datenverarbeitung als auch die Betroffenenrechte setzen also eine konkrete Zweckfestlegung voraus, da sie ansonsten ihre Steuerungs- und Informationsfunktion einbüßen. Nur anhand eines derart festgelegten Zwecks kann die von §§ 13 Abs. 1, 14 Abs. 1 Satz 1 BDSG a. F. geforderte Erforderlichkeit bestimmt werden. Die Aufgabe bildet den äußeren Rahmen der Zweckbestimmung, die dem Verarbeitungskontext gemäß hinreichend konkret festzulegen ist. Je tiefer dabei in das RiS eingegriffen wird, umso präziser hat die Zweckfestlegung zu erfolgen. Zweckoffene Big-Data-Analysen sind hiermit nicht vereinbar. Auch im Falle einer Übermittlung von Daten ist der Datenumgang durch die empfangende Stelle Restriktionen durch den Übermittlungszweck unterworfen, so dass ebenfalls erhebliche Einschränkungen in der Datenverwendung bestehen.

779 *Eßer*, in: Eßer/Kramer/v. Lewinski (Hrsg.), Auernhammer BDSG, § 19a Rn. 14; *Mester*, in: Taeger/Gabel (Hrsg.), BDSG, § 19a Rn. 13; *Worms*, in: Wolff/Brink (Hrsg.), DSR, § 19a Rn. 23; vgl. auch *Bergmann/Möhrle/Herb*, BDSG, § 19a Rn. 8, die eine „konkrete" Angabe der Zweckbestimmung fordern.

780 *Mester*, in: Taeger/Gabel (Hrsg.), BDSG, § 14 Rn. 13; vgl. *Wedde*, in: Taeger/Gabel (Hrsg.), BDSG, § 19a Rn. 11; *Gola/Klug/Körffer*, in: Gola/Schomerus (Hrsg.), BDSG, § 19a Rn. 5.

781 *Mallmann*, in: Simitis (Hrsg.), BDSG, § 19a Rn. 3.

782 *Bergmann/Möhrle/Herb*, BDSG, § 19a Rn. 2.

783 BVerfGE 65, 1 (46).

e) nicht-öffentlicher Bereich und Sondervorschriften

aa) § 28 Abs. 1 Satz 2 BDSG a. F.

§ 28 BDSG a. F. ist die zentrale Erlaubnisnorm des Datenumgangs für eigene Geschäftszwecke im nicht-öffentlichen Bereich. Gemäß § 28 Abs. 1 Satz 2 BDSG a. F. sind die Datenverwendungszwecke bei der Erhebung konkret festzulegen. Dieser Passus fand mit der Reform im Jahr 2001 Eingang in den Gesetzestext.[784] Datenerhebungen „ins Blaue hinein" sind damit nicht zu vereinbaren.[785] Die Sammlung von Daten auf Vorrat soll hierdurch ausgeschlossen werden.[786] § 28 Abs. 1 Satz 2 BDSG a. F. ist eine wichtige Grundlage für die Wirksamkeit einer späteren Zweckbindung, die durch die Vorschriften zur zulässigen Zweckentfremdung mittelbar geschaffen wird.[787]

Auch hier stellt sich die Frage nach dem notwendigen Konkretisierungsgrad der Zweckfestlegung. Eine Auffassung geht von der Zulässigkeit einer relativ weiten Zweckfestlegung aus. Der Gesetzgeber habe in § 28 Abs. 1 BDSG a. F. die Notwendigkeit des Datenumgangs im wirtschaftlichen Wettbewerb anerkannt, weshalb eine zu enge Auslegung des Zweckbestimmungserfordernisses nicht in Betracht komme.[788] Eine typisierende Darstellung wie „Durchführung des (…) Kaufvertrags" sei ausreichend.[789] Eine möglichst „weitläufige" Fassung der Zweckbestimmung sei empfehlenswert, da es dann seltener zu einer rechtfertigungsbedürftigen Zweckänderung komme.[790] Es wird vertreten, dass es bei einem Data Mining ausreiche, wenn der Endzweck der Auswertung angegeben wer-

784 *Bergmann/Möhrle/Herb*, BDSG, § 28 Rn. 2.
785 *Bergmann/Möhrle/Herb*, BDSG, § 28 Rn. 2.
786 *Plath*, in: Plath (Hrsg.), BDSG/DSGVO, § 28 Rn. 88; *Wedde*, in: Däubler/Klebe/Wedde/Weichert (Hrsg.), BDSG, § 28 Rn. 62; *Simitis*, in: Simitis (Hrsg.), BDSG, § 28 Rn. 38.
787 Vgl. *Wolff*, in: Wolff/Brink (Hrsg.), DSR, § 28 Rn. 14.
788 *Plath*, in: Plath (Hrsg.), BDSG/DSGVO, § 28 Rn. 89.
789 *Plath*, in: Plath (Hrsg.), BDSG/DSGVO, § 28 Rn. 89.
790 Vgl. *Plath*, in: Plath (Hrsg.), BDSG/DSGVO, § 28 Rn. 89.

de.[791] So soll der Zweck „Profilerstellung“ oder „Marktanalyse“ den Erfordernissen von § 28 Abs. 1 Satz 2 BDSG a. F. genügen.[792]

Eine andere Ansicht geht hingegen davon aus, dass eine allgemeine Fassung der Zweckbestimmung nicht ausreiche.[793] Sie müsse die Zwecke genau umschreiben und dürfe nicht mehrere Nutzungsmöglichkeiten eröffnen.[794] Die Angabe „eigener Geschäftszweck“ genüge nicht, sondern es bedürfe einer Beschreibung im Detail.[795] Die Erstellung von Kundenprofilen mit für die Vertragsabwicklung erhobenen Daten und deren Auswertung mittels Data Mining könne wegen der Zweckbestimmung der Erhebung nicht auf § 28 BDSG a. F. gestützt werden, sondern nur auf eine Einwilligung.[796] § 28 Abs. 1 Satz 1 Nr. 2 BDSG a. F. gestatte nur die Verwendung der für die berechtigten Interessen erforderlichen Daten, weshalb es eines spezifischen Verarbeitungszwecks bedürfe.[797]

Bereits der Wortlaut von § 28 Abs. 1 Satz 2 BDSG a. F. verdeutlicht mit dem Adjektiv „konkret“, dass eine allgemeine Zweckfestlegung nicht genügen kann. Für diese Auffassung streiten auch die in § 28 Abs. 1 BDSG a. F. vorgesehenen Abwägungstatbestände, die nur mit einer hinreichend konkreten Zweckfestlegung operabel werden. Es ist nicht nachvollziehbar, wie im Rahmen einer Interessenabwägung festgestellt werden soll, ob die schutzwürdigen Interessen überwiegen, wenn der Zweck der Datenverarbeitung nicht klar definiert ist. Zudem gestatten § 28 Abs. 1 Satz 1 Nr. 1 und 2 BDSG a. F. die Datenverwendung nur, soweit sie erforderlich ist. Bei Data Mining handelt es sich zudem um ein Verfahren, nicht aber um einen Zweck.

---

791 So *Plath*, in: Plath (Hrsg.), BDSG/DSGVO, § 28 Rn. 57.
792 *Plath*, in: Plath (Hrsg.), BDSG/DSGVO, § 28 Rn. 57.
793 *Wedde*, in: Däubler/Klebe/Wedde/Weichert (Hrsg.), BDSG, § 28 Rn. 63.
794 *Taeger*, in: Taeger/Gabel (Hrsg.), BDSG, § 28 Rn. 112; *Wolff*, in: Wolff/Brink (Hrsg.), DSR, § 14 Rn. 16.
795 *Taeger*, in: Taeger/Gabel (Hrsg.), BDSG, § 28 Rn. 109.
796 *Klug/Körffer/Gola*, in: Gola/Schomerus (Hrsg.), BDSG, § 28 Rn. 11.
797 Vgl. *Simitis*, in: Simitis (Hrsg.), BDSG, § 28 Rn. 111, der deshalb eine Speicherung von Daten auf Vorrat ablehnt.

bb) § 28 Abs. 3 BDSG a. F.

§ 28 Abs. 3 BDSG a. F. sieht besondere Regeln für die Datenverwendung für Werbezwecke vor. Insofern ist er lex specialis zu § 28 Abs. 1 BDSG a. F.,[798] der aber gleichwohl anwendbar bleibt, soweit es um die Datenerhebung geht.[799] Grundsätzlich dürfen Daten für Werbezwecke gemäß § 28 Abs. 3 Satz 1 BDSG a. F. nur nach vorheriger Einwilligung verwendet werden. Eine Definition des Begriffs Werbung ist dem Gesetz nicht zu entnehmen. Es wird vorgeschlagen, dass darunter eine Datenverwendung mit der objektiv bestimmbaren konkreten Absicht zum Absatz von Waren und Dienstleistungen fallen soll.[800] Als weitgehendste Definition soll hierunter jede Form der Ansprache von Personen zwecks Veranlassung zu einer Handlung fallen.[801] Umstritten ist, ob die Zweckangabe „Werbung" hinreichend bestimmt ist.[802] Dafür wird angeführt, dass der Betroffene nur minimal durch unerwünschte Werbung betroffen sei.[803] Nach anderer Ansicht soll die Zweckangabe „Verwendung zu Werbezwecken" zu unbestimmt sein, da nicht ersichtlich werde, ob eine Verwendung für eigene oder fremde Zwecke erfolgen soll und ob die Daten übermittelt werden sollen.[804] Letzterer Auffassung ist zuzustimmen. Die Einwilligungserklärung muss die Art der Werbung (postalisch, telefonisch, per E-Mail) die Produkte, die beworben werden sollen und die verantwortliche Stelle nennen.[805] Eine pauschale Angabe des Zwecks

798 *Simitis*, in: Simitis (Hrsg.), BDSG, § 28 Rn. 212.

799 *Kramer*, in: Eßer/Kramer/v. Lewinski (Hrsg.), Auernhammer BDSG, § 28 Rn. 89 u. 92.

800 So *Kramer*, in: Eßer/Kramer/v. Lewinski (Hrsg.), Auernhammer BDSG, § 28 Rn. 97.

801 *Bergmann/Möhrle/Herb*, BDSG, § 28 Rn. 322.

802 Für eine ausführliche Darstellung des Streits, siehe *Kring*, in: Plödereder/Grunske/Schneider/Ull (Hrsg.), Big Data, S. 551 (556 f.).

803 *Bull*, NJW 2006, 1617 (1621).

804 Vgl. *Kramer*, in: Eßer/Kramer/v. Lewinski (Hrsg.), Auernhammer BDSG, § 4a Rn. 21.

805 Vgl. BGH, Urteil v. 18.07.2012 - VIII ZR 337/11 - BGHZ 194, 121-126, Rn. 57 (juris) - in Anknüpfung an § 7 UWG; *Gola/Klug/Körffer*, in: Gola/Schomerus (Hrsg.), BDSG, § 28 Rn. 43; in diese Richtung wohl auch *Breinlinger*, RDV 1997, 247 (252) und *Roßnagel*, ZD 2013, 562 (564), denen die Bezeich-

Marketing oder Werbung wird aufgrund der Vielgestaltigkeit der darunter subsumierbaren Sachverhalte den Erfordernissen der Zweckbestimmung nicht gerecht.[806]

Das Listenprivileg[807] in § 28 Abs. 3 Satz 2 BDSG a. F. stellt einen besonderen Erlaubnistatbestand für listenmäßig zusammengefasste Angaben dar.[808] Für Big-Data-Anwendungen könnte die Befugnis des Hinzuspeicherns weiterer Daten für Zwecke der Werbung für eigene Angebote der verantwortlichen Stelle gemäß § 28 Abs. 3 Satz 3 BDSG a. F. interessant sein.[809] Allerdings gibt dies keine Befugnis zur Datenerhebung, d. h. die Daten müssen zuerst rechtmäßig beschafft worden sein.[810] Listendaten dürfen dabei nicht aus anderen als in § 28 Abs. 3 Satz 2 Nr. 1 BDSG a. F. genannten Quellen hinzugespeichert werden.[811] Damit ist die Datenmenge bereits erheblich beschränkt, weshalb zweifelhaft ist, ob das Hinzuspeichern tatsächlich für eine Big-Data-Analyse nützlich ist. Problematisch ist, wenn den Daten durch ihre Verknüpfung in einer Liste andere Merkmale entnommen werden können.[812] Dies kann zu einer Unzulässigkeit der Datenverwendung im Rahmen der Abwägung mit den schutzwürdigen Interessen des Betroffenen nach § 28 Abs. 3 Satz 6 BDSG a. F.

---

nung „Werbezwecke“ nicht genügt; in eine andere Kerbe schlägt *Büllesbach*, CR 2000, 11 (15), der hervorhebt, dass klar sein müsse, welche Daten für Werbezwecke verarbeitet werden sollen.

806 Vgl. *Podlech/Pfeifer*, RDV 1998, 139 (146 und 153).

807 Entgegen der Gesetzesbegründung in BT-Drs. 16/12011, S. 31, wurde das Listenprivileg gerade nicht gestrichen, vgl. *Simitis*, in: Simitis (Hrsg.), BDSG, § 28 Rn. 230.

808 Vgl. *Plath*, in: Plath (Hrsg.), BDSG/DSGVO, § 28 Rn. 130.

809 Dafür: *Helbing*, K&R 2015, 145 (149 f.). Diese Möglichkeit wird als eine Ausweitung des Listenprivilegs kritisiert, siehe *Wedde*, in: Däubler/Klebe/Wedde/Weichert (Hrsg.), BDSG, § 28 Rn. 87.

810 *Kramer*, in: Eßer/Kramer/v. Lewinski (Hrsg.), Auernhammer BDSG, § 28 Rn. 111.

811 *Wolff*, in: Wolff/Brink (Hrsg.), DSR, § 28 Rn. 133.

812 Vgl. hierzu: *Taeger*, in: Taeger/Gabel (Hrsg.), BDSG, § 28 Rn. 195 f; *Simitis*, in: Simitis (Hrsg.), BDSG, § 28 Rn. 228, der als Beispiel eine Liste mit unter der Adresse einer Haftanstalt wohnhaften Personen nennt.

führen.[813] Im Falle einer Datenübermittlung bindet § 28 Abs. 3 Satz 7 BDSG a. F. den Empfänger an den Übermittlungszweck.

cc) § 28 Abs. 6, Abs. 7 BDSG a. F.

§ 28 Abs. 6-9 BDSG a. F. sieht Sonderregelungen für den Umgang mit sensitiven Daten i. S. v. § 3 Abs. 9 BDSG a. F. vor. Anknüpfend an den Verarbeitungszweck (lebenswichtige Interessen, Durchsetzung rechtlicher Ansprüche, Durchführung wissenschaftlicher Forschung) sieht § 28 Abs. 6 BDSG a. F. die Möglichkeit eines Datenumgangs ohne Einwilligung vor.

§ 28 Abs. 7 BDSG a. F. gestattet die Erhebung und die Verwendung von sensiblen Daten für Zwecke der medizinischen Versorgung durch Personen, die einer besonderen Geheimhaltungspflicht unterliegen. Es wird also ein relativ weiter Zweck durch eine Verfahrensvorkehrung ausgeglichen.

dd) § 29 Abs. 1 BDSG a. F.

§ 29 BDSG a. F. gestattet den geschäftsmäßigen Datenumgang zum Zweck der Übermittlung. An § 29 Abs. 2 Satz 1 BDSG a. F. wird sichtbar, dass die Übermittlung dabei nur ein übergeordneter näher zu spezifizierender Zweck ist. Dort ist von der Zulässigkeit einer Übermittlung im Rahmen der Zwecke des Abs. 1 die Rede. In § 29 Abs. 1 BDSG a. F. werden als Regelbeispiele die Werbung, die Tätigkeit von Auskunfteien und der Adresshandel genannt. Diese Beispiele wurden im Jahre 2001 in das Gesetz eingefügt, um den Vorgaben der Zweckbindung aus der DSRL Rechnung zu tragen.[814] Dass es einer konkreten Zweckbestimmung bedarf, unterstreicht zudem § 29 Abs. 1 Satz 2 BDSG a. F., der auf die ent-

813 Vgl. *Simitis*, in: Simitis (Hrsg.), BDSG, § 28 Rn. 245.

814 *Ehmann*, in: Simitis (Hrsg.), BDSG, § 29 Rn. 71; vgl. *Bergmann/Möhrle/Herb*, BDSG, § 29 Rn. 2.

sprechende Vorgabe des § 28 Abs. 1 Satz 2 BDSG a. F. verweist.[815] Eine konkrete Zweckfestlegung ist auch hier für die Durchführung der jeweils geforderten Interessenabwägungen unabdingbar.[816]

Fraglich ist, ob eine Datenerhebung für eine spätere, potentielle Übermittlung eine unzulässige Datenerhebung auf Vorrat darstellt. Die Problematik der Speicherung von Daten auf Vorrat soll sich hier nicht gleichermaßen stellen wie im öffentlichen Bereich.[817] Es sei für die Zulässigkeit der Datenerhebung zum Zweck der Übermittlung ausreichend, wenn aufgrund einer Marktanalyse feststehe, dass Daten in Zukunft zu einem bestimmten Zweck angefordert werden.[818] Dieser Zweck muss dann als Erhebungszweck konkret festgelegt werden, da auch im Rahmen des § 29 BDSG a. F. Daten nicht für unbekannte Zwecke auf Vorrat gespeichert werden dürfen.[819] Es wird vertreten, dass es für einen im Volkszählungsurteil geforderten „bestimmbaren Zweck" ausreiche, wenn die Kategorie zukünftiger Empfänger feststehe.[820] Ohnehin sei zu berücksichtigen, dass im nicht-öffentlichen Bereich der Zweck aufgrund der fluiden Marktlage nicht so statisch festgelegt werden könne.[821] Eine Typisierung im Stile von „Werbung", „Adresshandel", „Bonitätsauskunft" soll genügen.[822] Es soll ausreichen, dass eine Datenübermittlung zu dem Erhe-

---

815 Vgl. auch *Taeger*, in: Taeger/Gabel (Hrsg.), BDSG, § 29 Rn. 45; *Kramer*, in: Eßer/Kramer/v. Lewinski (Hrsg.), Auernhammer BDSG, § 29 Rn. 20, geht aufgrund der noch nicht sicheren Übermittlung von einem bestimmbaren, nicht einem konkreten Zweck aus.

816 *Ehmann*, in: Simitis (Hrsg.), BDSG, § 29 Rn. 124; *Buchner*, in: Wolff/Brink (Hrsg.), DSR, § 29 Rn. 67.

817 So *Taeger*, in: Taeger/Gabel (Hrsg.), BDSG, § 29 Rn. 17; vgl. auch *Ehmann*, in: Simitis (Hrsg.), BDSG, § 29 Rn. 56 f.

818 *Taeger*, in: Taeger/Gabel (Hrsg.), BDSG, § 29 Rn. 17; vgl. auch *Plath*, in: Plath (Hrsg.), BDSG/DSGVO, § 29 Rn. 10, der ein potentielles Interesse genügen lässt.

819 Vgl. *Taeger*, in: Taeger/Gabel (Hrsg.), BDSG, § 29 Rn. 17 u. 44 f.

820 *Ehmann*, in: Simitis (Hrsg.), BDSG, § 29 Rn. 56.

821 *Ehmann*, in: Simitis (Hrsg.), BDSG, § 29 Rn. 57; *Bergmann/Möhrle/Herb*, BDSG, § 29 Rn. 62.

822 *Plath*, in: Plath (Hrsg.), BDSG/DSGVO, § 29 Rn. 67; *Buchner*, in: Wolff/Brink (Hrsg.), DSR, § 29 Rn. 92.

bungszweck wahrscheinlich ist, unabhängig davon, ob es tatsächlich zu einer Übermittlung für diesen Zweck kommt.[823]

ee) § 30a Abs. 1, 3 BDSG a. F.

Mit § 30a BDSG a. F. wurde im Jahr 2009 eine Sondervorschrift für den geschäftsmäßigen Datenumgang zu Zwecken der Markt- und Meinungsforschung geschaffen.[824] Die Begriffe der Markt- und Meinungsforschung sind nicht gesetzlich definiert und es hat sich kein allgemeines Begriffsverständnis herausgebildet.[825] In den Gesetzgebungsmaterialien wird der Begriff der Markt- und Meinungsforschung als Bereitstellung notwendiger Informationen „als empirische Grundlage und zur Unterstützung wirtschaftlicher, gesellschaftlicher und politischer Entscheidungen" mittels wissenschaftlicher Methoden und Techniken definiert.[826] Eine präzise Definition ist auch dies nicht. In der Literatur wird gemutmaßt, dass dies der großen gesetzgeberischen Eile geschuldet sei.[827] Wichtig ist die Definition des Zwecks zur Abgrenzung des Anwendungsbereichs zu anderen Erlaubnistatbeständen, wie § 29 BDSG a. F.[828] und zu den Vorschriften über den Datenumgang für Werbezwecke.[829]

§ 30a BDSG a. F. privilegiert die Markt- und Meinungsforschung insgesamt gegenüber den Regelungen der §§ 28, 29 BDSG a. F. aufgrund geringer ausgeprägter Anforderungen an die Zweckbindung.[830] Es handelt sich um ein gestuftes Verhältnis der Zweckfestlegung.[831] Für allgemein zugängliche Daten reicht der Zweck der „Markt- und Meinungsfor-

823 *Gola/Klug/Körffer*, in: Gola/Schomerus (Hrsg.), BDSG, § 29 Rn. 21.
824 BGBl. I 2009, S. 2814.
825 *Ehmann*, in: Simitis (Hrsg.), BDSG, § 30a Rn. 70 ff.
826 BT-Drs. 16/13657, S. 19 f.
827 So *Munz*, in: Taeger/Gabel (Hrsg.), BDSG, § 30a Rn. 10.
828 Vgl. *Munz*, in: Taeger/Gabel (Hrsg.), BDSG, § 30a Rn. 11.
829 *Weichert*, in: Däubler/Klebe/Wedde/Weichert (Hrsg.), BDSG, § 30a Rn. 2.
830 Vgl. *Forgó*, in: Wolff/Brink (Hrsg.), DSR, § 30a Rn. 2.
831 So *Kramer*, in: Eßer/Kramer/v. Lewinski (Hrsg.), Auernhammer BDSG, § 30a Rn. 23 ff.; *Forgó*, in: Wolff/Brink (Hrsg.), DSR, § 30a Rn. 40.

schung“ aus.[832] Für sonstige Daten ist der Maßstab nicht genau festgeschrieben, aber die Formulierung „das Forschungsvorhaben“ in der Zweckbindungsvorschrift des § 30a Abs. 2 Satz 2 BDSG a. F. deutet auf eine Verwendung nur für ein konkretes Vorhaben hin.[833] § 30a Abs. 1 Satz 2 BDSG a. F. sieht bei sensitiven Daten einen strengeren Maßstab für die Zweckbestimmung vor, da es sich um ein „bestimmtes Forschungsvorhaben“ handeln muss.[834] „Art, Umfang und Dauer“ des Forschungsvorhabens müssten konkret feststehen.[835] Durch entsprechende Formulierung der Forschungsfragen könne auch bei sensiblen Daten eine „gewisse Flexibilität“ erreicht werden.[836] Verglichen mit anderen Regelungen zum Umgang mit sensitiven Daten handele es sich um eine Privilegierung.[837] Gemäß § 30a Abs. 2 BDSG a. F. sind die Daten an den Erhebungszweck gebunden und nach § 30a Abs. 3 Satz 1 BDSG a. F. zu anonymisieren, sobald der Zweck dies zulässt.

Auch im Falle der Markt- und Meinungsforschung wird also im Wesentlichen eine konkrete Zweckfestlegung für ein Forschungsvorhaben gefordert, weshalb für zweckoffene Big-Data-Anwendungen nicht viel gewonnen ist.

---

832 *Kramer*, in: Eßer/Kramer/v. Lewinski (Hrsg.), Auernhammer BDSG, § 30a Rn. 23; *Gola/Klug/Körffer*, in: Gola/Schomerus (Hrsg.), BDSG, § 30a Rn. 5; *Weichert*, in: Däubler/Klebe/Wedde/Weichert (Hrsg.), BDSG, § 30a Rn. 4.

833 *Forgó*, in: Wolff/Brink (Hrsg.), DSR, § 30a Rn. 41; *Ehmann*, in: Simitis (Hrsg.), BDSG, § 30a Rn. 137; zweifelnd aber wegen des Wortlauts „das Forschungsvorhaben“ anstatt „bestimmtes Forschungsvorhaben“, *Kramer*, in: Eßer/Kramer/v. Lewinski (Hrsg.), Auernhammer BDSG, § 30a Rn. 25.

834 *Kramer*, in: Eßer/Kramer/v. Lewinski (Hrsg.), Auernhammer BDSG, § 30a Rn. 20.

835 *Bergmann/Möhrle/Herb*, BDSG, § 30a Rn. 11.

836 *Forgó*, in: Wolff/Brink (Hrsg.), DSR, § 30a Rn. 26; ähnlich *Munz*, in: Taeger/Gabel (Hrsg.), BDSG, § 30a Rn. 20, der auf diese Weise langfristige Forschungsvorhaben unter die Norm subsumieren will.

837 *Ehmann*, in: Simitis (Hrsg.), BDSG, § 30a Rn. 111.

ff) § 31 BDSG a. F.

§ 31 BDSG a. F. ist mit „Besondere Zweckbindung“ überschrieben. Eine entsprechende Vorschrift für den öffentlichen Bereich findet sich in § 14 Abs. 4 BDSG a. F. Demnach dürfen personenbezogene Daten, die ausschließlich zu Zwecken der Datenschutzkontrolle, der Datensicherung oder zur Sicherstellung eines ordnungsgemäßen Betriebs einer Datenverarbeitungsanlage gespeichert werden, nur für diese Zwecke verwendet werden. Der Wortlaut der Vorschrift bringt klar zum Ausdruck, dass eine spätere Zweckänderung ausgeschlossen ist.[838] Die Norm wird auch als „absolutes Zweckentfremdungsverbot“ bezeichnet.[839] Allerdings findet die Vorschrift nur Anwendung, wenn die Daten ausschließlich zu diesen Zwecken gespeichert werden. Das ist bereits nicht mehr der Fall, wenn Daten für mehrere Zwecke gespeichert werden.[840] Die Regelung dient zur Verhinderung einer Umgehung der Vorgaben des BDSG a. F. durch einen unkontrollierten Datenumgang mit den zu Sicherungs- und Kontrollzwecken angelegten Daten.[841] Dies ist wichtig, weil aus Gründen der Datenschutzkontrolle eine Vielzahl von Daten gespeichert werden müssen.[842] Deshalb kann hierin auch ein erlaubter Fall der Vorratsdatenspeicherung gesehen werden.[843] Für die Frage der Ausschließlichkeit ist die Zweckbestimmung durch die verantwortliche Stelle maßgeblich.[844]

---

838 *Buchner*, in: Taeger/Gabel (Hrsg.), BDSG, § 31 Rn. 4.

839 Siehe nur *Buchner*, in: Taeger/Gabel (Hrsg.), BDSG, § 31 Rn. 1.

840 *Buchner*, in: Taeger/Gabel (Hrsg.), BDSG, § 31 Rn. 3; *Plath*, in: Plath (Hrsg.), BDSG/DSGVO, § 31 Rn. 5.

841 Vgl. *Eßer*, in: Eßer/Kramer/v. Lewinski (Hrsg.), Auernhammer BDSG, § 31 Rn. 1.

842 *Weichert*, in: Däubler/Klebe/Wedde/Weichert (Hrsg.), BDSG, § 31 Rn. 1.

843 So *v. Lewinski*, in: Wolff/Brink (Hrsg.), DSR, § 31 Rn. 7.

844 *v. Lewinski*, in: Wolff/Brink (Hrsg.), DSR, § 31 Rn. 10; *Buchner*, in: Taeger/Gabel (Hrsg.), BDSG, § 31 Rn. 3; a. A. *Weichert*, in: Däubler/Klebe/Wedde/Weichert (Hrsg.), BDSG, § 31 Rn. 3, der aber verkennt, dass es nicht um die Zulässigkeit der Speicherung für Protokollierungszwecke geht, sondern um die Frage, ob die Daten zugleich für andere Zwecke erhoben werden.

gg) § 32 Abs. 1 BDSG a. F.

§ 32 BDSG a. F. gestattet den Datenumgang für Zwecke des Beschäftigungsverhältnisses wenn dies zur Begründung, Durchführung oder Beendigung eines Beschäftigtenverhältnisses erforderlich ist. Der Begriff „Beschäftigter" ist weit i. S. d. § 3 Abs. 11 BDSG a. F. zu verstehen. Laut der Gesetzesbegründung wird auch § 28 Abs. 1 Satz 2 BDSG a. F., d. h. das Erfordernis einer konkreten Zweckfestlegung, von § 32 BDSG a. F. verdrängt.[845] Befürworter begründen das damit, dass § 32 BDSG a. F. bereits eine „umfassende Zweckbestimmung vorgenommen habe.[846] Dass der Konkretisierungsgrad geringer sei, sei als „gesetzgeberische Entscheidung hinzunehmen".[847] Dies ist auf erhebliche Kritik gestoßen,[848] da § 32 BDSG a. F. laut Gesetzesbegründung[849] nur die bisherige Rechtslage zusammenfassend kodifizieren sollte und bisher § 28 Abs. 1 Satz 2 BDSG a. F. Anwendung fand.[850] Zudem wird zu „eine(r) weitere(n) Dokumentation der Verwendungszwecke" geraten mit Blick auf die Informationspflicht gemäß § 4 Abs. 3 Satz 1 Nr. 2 BDSG a. F.[851] § 28 Abs. 1 Satz 2 BDSG a. F. sei anzuwenden, da ansonsten „ins Blaue hinein" Daten erhoben werden könnten.[852] Bei § 28 Abs. 1 BDSG a. F., der allgemein von Geschäftszwecken spreche sei eine Konkretisierung vorgesehen, weshalb dies auch bei der ebenfalls allgemeinen gesetzlichen

845 BT-Drs. 16/13657, 20; zustimmend *Forst*, in: Eßer/Kramer/v. Lewinski (Hrsg.), Auernhammer BDSG, § 32 Rn. 35; *Zöll*, in: Taeger/Gabel (Hrsg.), BDSG, § 32 Rn. 10; *Riesenhuber*, in: Wolff/Brink (Hrsg.), DSR, § 32 Rn. 29; wohl auch *Seifert*, in: Simitis (Hrsg.), BDSG, § 32 Rn. 17.

846 *Zöll*, in: Taeger/Gabel (Hrsg.), BDSG, § 32 Rn. 10.

847 *Riesenhuber*, in: Wolff/Brink (Hrsg.), DSR, § 32 Rn. 29.

848 So z. B. *Däubler*, in: Däubler/Klebe/Wedde/Weichert (Hrsg.), BDSG, § 32 Rn. 9 bezeichnet dies als „wenig nachvollziehbar"; kritisch wohl auch *Franzen*, in: Müller-Glöge/Preis/Schmidt (Hrsg.), ErfK, § 32 BDSG Rn. 3, der nur § 28 Abs. 1 Satz 1 BDSG a. F. für verdrängt erklärt; tendenziell für eine Anwendbarkeit auch *Gola/Klug/Körffer*, in: Gola/Schomerus (Hrsg.), BDSG, § 32 Rn. 2.

849 BT-Drs. 16/13657, S. 20.

850 Vgl. *Zöll*, in: Taeger/Gabel (Hrsg.), BDSG, § 32 Rn. 10.

851 Darstellung dieser Ansicht bei *Zöll*, in: Taeger/Gabel (Hrsg.), BDSG, § 32 Rn. 10.

852 *Stamer/Kuhnke*, in: Plath (Hrsg.), BDSG/DSGVO, § 32 Rn. 10.

Zweckbestimmung in § 32 BDSG a. F. angezeigt sei.[853] § 28 Abs. 2 BDSG a. F. mit den Vorschriften zur Zweckänderung soll nach einer in der Literatur vertretenen Auffassung neben § 32 BDSG a. F. anwendbar sein.[854]

Der Wortlaut mag einen Ausschluss des § 28 Abs. 1 Satz 2 BDSG a. F. zwar decken.[855] Allerdings steht er auch einer fortbestehenden Anwendbarkeit des § 28 Abs. 1 Satz 2 BDSG a. F. nicht entgegen.[856] Dass der Begriff „Zweck des Beschäftigungsverhältnisses" sehr weit ist, zeigt sich schon daran, dass es unterschiedliche Auffassungen gibt, was alles darunter zu subsumieren ist.[857]

hh) § 33 BDSG a. F.

Für den nicht-öffentlichen Bereich sieht § 33 BDSG a. F. eine Benachrichtigungspflicht im Falle einer Datenspeicherung ohne Kenntnis des Betroffenen vor. Auch nach dieser Vorschrift ist auf den Zweck der Erhebung, Verarbeitung oder Nutzung hinzuweisen, wenn es sich um eine Datenspeicherung für eigene Zwecke handelt. Werden die Daten zum Zweck der Übermittlung gespeichert, ist eine Information des Betroffenen erst und nur zum Zeitpunkt der erstmaligen Übermittlung vorgesehen,

853 *Stamer/Kuhnke*, in: Plath (Hrsg.), BDSG/DSGVO, § 32 Rn. 10; *Däubler*, in: Däubler/Klebe/Wedde/Weichert (Hrsg.), BDSG, § 32 Rn. 9 verdeutlicht die Allgemeinheit des Zwecks Beschäftigungsverhältnis mit einem Zugangskontrollsystem, das neben der Zugangskontrolle auch der Zeiterfassung dienen kann. Mithin zwei unterschiedliche Zwecke, die sich beide unter den abstrakten Zweck „Beschäftigungsverhältnis" fassen lassen.

854 *Forst*, in: Eßer/Kramer/v. Lewinski (Hrsg.), Auernhammer BDSG, § 32 Rn. 19; so auch *Däubler*, in: Däubler/Klebe/Wedde/Weichert (Hrsg.), BDSG, § 32 Rn. 9, der ansonsten den „spezifischen Schutz von Beschäftigtendaten" gefährdet sieht.

855 So *Riesenhuber*, in: Wolff/Brink (Hrsg.), DSR, § 32 Rn. 29.

856 So auch *Stamer/Kuhnke*, in: Plath (Hrsg.), BDSG/DSGVO, § 32 Rn. 10; *Däubler*, in: Däubler/Klebe/Wedde/Weichert (Hrsg.), BDSG, § 32 Rn. 9.

857 Zu den vertretenen Auffassungen siehe *Forst*, in: Eßer/Kramer/v. Lewinski (Hrsg.), Auernhammer BDSG, § 32 Rn. 36.

§ 33 Abs. 1 Satz 1 BDSG a. F. Dies ist insofern problematisch, als die verantwortliche Stelle ohne Kenntnis des Betroffenen einen großen Datenbestand über diesen aufbauen kann.[858] Zudem kann der Betroffene erst nach bereits erfolgter Übermittlung der Daten reagieren, so dass eine Verletzung des Persönlichkeitsrechts eventuell bereits eingetreten ist.[859] Der nach § 28 Abs. 1 Satz 2 BDSG a. F. festzulegende Zweck oder die Zwecke sind dem Betroffenen im Falle der Speicherung für eigene Zwecke mitzuteilen.[860] Dabei ist der Zweck so zu benennen, dass der Betroffene die Rechtmäßigkeit des Datenumgangs beurteilen kann.[861] Eine pauschale Angabe soll nicht genügen.[862] Es wird vertreten, dass eine neue Benachrichtigung auch dann erfolgen müsse, wenn Daten zu einem anderen Zweck gespeichert werden.[863] Durch die Zweckänderung erhielten die Daten eine neue Qualität und würden zu diesem Zweck erstmalig gespeichert.[864] Eine Benachrichtigungspflicht gelte nicht nur im Falle einer Änderung in „wesentlicher Weise".[865] Denn dieses Erfordernis sei § 33 BDSG a. F. nicht zu entnehmen.[866] Der Sinn und Zweck der Vorschrift spricht klar für eine Information des Betroffenen im Falle einer Zweckänderung. Letztlich kann hier nichts anderes gelten als bei

858 *Däubler*, in: Däubler/Klebe/Wedde/Weichert (Hrsg.), BDSG, § 33 Rn. 2; *Forgó*, in: Wolff/Brink (Hrsg.), DSR, § 33 Rn. 33; a. A. *Kamlah*, in: Plath (Hrsg.), BDSG/DSGVO, § 33 Rn. 19, der das Vorliegen eines „besonderen Schutzinteresses des Betroffenen" vor der ersten Übermittlung verneint. Zudem gebe es häufig keine zeitliche Differenz zwischen Speicherung und Übermittlung.

859 *Dix*, in: Simitis (Hrsg.), BDSG, § 33 Rn. 25.

860 *Däubler*, in: Däubler/Klebe/Wedde/Weichert (Hrsg.), BDSG, § 33 Rn. 19.

861 *Kamlah*, in: Plath (Hrsg.), BDSG/DSGVO, § 33 Rn. 16.

862 *Bergmann/Möhrle/Herb*, BDSG, § 33 Rn. 50.

863 *Forgó*, in: Wolff/Brink (Hrsg.), DSR, § 33 Rn. 29; *Gola/Klug/Körffer*, in: Gola/Schomerus (Hrsg.), BDSG, § 33 Rn. 16; *Weichert*, in: Däubler/Klebe/Wedde/Weichert (Hrsg.), BDSG, § 4 Rn. 12; a. A.: *Schaffland/Wiltfang*, BDSG, § 33 Rn. 7, die den Betroffenen auf das Auskunftsrecht nach § 34 BDSG a. F. verweisen.

864 *Bergmann/Möhrle/Herb*, BDSG, § 33 Rn. 46.

865 So aber *Plath*, in: Plath (Hrsg.), BDSG/DSGVO, § 4 Rn. 28.

866 Siehe zur vergleichbaren Fragen einer Änderung von Qualität oder Quantität durch Hinzuspeicherung weiterer Daten: *Dix*, in: Simitis (Hrsg.), BDSG, § 33 Rn. 13.

Art. 10 DSRL.[867] Besonders bei Big-Data-Anwendungen kann aufgrund der Verknüpfung verschiedener Daten und dem „Entstehen“ neuer Informationen ein Bedürfnis nach Information entstehen.[868]

ii) § 34 Abs. 1 Satz 1 Nr. 3 BDSG a. F.

Im Rahmen des Auskunftsrechts ist gemäß § 34 Abs. 1 Satz 1 Nr. 3 BDSG a. F. über den Speicherungszweck Auskunft zu erteilen. Dies ist Voraussetzung für die Prüfung der Rechtmäßigkeit des Datenumgangs, insbesondere ob unzulässige Zweckänderungen vorliegen.[869] Daher müssen auch frühere Speicherungszwecke mitgeteilt werden.[870] Nach einer Ansicht soll es genügen, wenn eine allgemeine Zweckumschreibung genannt wird.[871] Ein „individueller Einzelzweck“ müsse nicht verbeauskunftet werden, insbesondere sofern Geschäftsgeheimnisse davon betroffen seien.[872] Diese Auffassung ist allerdings nicht nachvollziehbar, da ohnehin eine Zweckfestlegung bei der Erhebung zu erfolgen hat. Diese ist zu verbeauskunften.[873] Sofern eine Speicherung für mehrere Zwecke erfolgt ist, sind alle Zwecke zu verbeauskunften.[874] Im Rahmen von Big-

867 Siehe D. II. 2. a) dd), S. 124 f.
868 *Forgó*, in: Wolff/Brink (Hrsg.), DSR, § 33 Rn. 29.
869 Vgl. *Kamlah*, in: Plath (Hrsg.), BDSG/DSGVO, § 34 Rn. 25.
870 Vgl. *Stollhoff*, in: Eßer/Kramer/v. Lewinski (Hrsg.), Auernhammer BDSG, § 34 Rn. 23; vgl. auch *Gola/Körffer/Klug*, in: Gola/Schomerus (Hrsg.), BDSG, § 34 Rn. 12, die Zweckänderungen für mitteilungspflichtig halten.
871 So *Kamlah*, in: Plath (Hrsg.), BDSG/DSGVO, § 34 Rn. 25, der „Vertragsabwicklung“ genügen lassen will; *Meents/Hinzpeter*, in: Taeger/Gabel (Hrsg.), BDSG, § 34 Rn. 22; unklar *Gola/Klug/Körffer*, in: Gola/Schomerus (Hrsg.), BDSG, § 34 Rn. 12, die einerseits eine pauschale Umschreibung genügen lassen wollen und andererseits darauf hinweisen, dass die nach § 28 Abs. 1 Satz 2 BDSG a. F. konkret festgelegten Zwecke mitzuteilen seien.
872 *Meents/Hinzpeter*, in: Taeger/Gabel (Hrsg.), BDSG, § 34 Rn. 22.
873 Vgl. *Dix*, in: Simitis (Hrsg.), BDSG, § 34 Rn. 31, der an § 28 BDSG a. F. anknüpfen will.
874 *Bergmann/Möhrle/Herb*, BDSG, § 34 Rn. 50.

Data-Anwendungen dürfte die Auskunft über den Zweck die verantwortliche Stelle vor große Schwierigkeiten stellen.[875]

jj) § 35 Abs. 2 Satz 2 Nr. 3 BDSG a. F.

Gemäß § 35 Abs. 2 Satz 2 Nr. 3 BDSG a. F. sind personenbezogene Daten, die für eigene Zwecke verarbeitet werden, zu löschen, sobald sie für den Speicherungszweck nicht mehr erforderlich sind. Dies soll allerdings dann nicht gelten, wenn nach einer Zweckänderung die Daten weiter für den neuen Zweck benötigt werden.[876] Sofern Daten zu einem größeren Datensatz zusammengefasst sind, besteht in der Regel ein gemeinsamer Speicherungszweck der gerade durch die Speicherung der Daten im Kontext mit anderen Daten erreicht werden soll, weshalb aufgrund einer einheitlichen Zweckbestimmung die Erforderlichkeit für alle Daten des Datensatzes einheitlich zu beurteilen sein wird.[877]

kk) § 38 Abs. 1 Satz 3 BDSG a. F.

Gemäß § 38 Abs. 1 Satz 3 BDSG a. F. darf die Aufsichtsbehörde die von ihr gespeicherten Daten nur für Zwecke der Aufsicht verwenden, wobei aber eine Zweckänderung durch einen Verweis auf einzelne Bestandteile von § 14 Abs. 2 BDSG a. F. möglich ist. Die Bestimmung der Aufsichtszwecke soll sich aus den gesetzlichen Aufgabenzuweisungsnormen ergeben.[878] Grundsätzlich wird eine strenge Zweckbindung begrenzt auf die Aufsichtszwecke erreicht.[879]

---

875 *Liedke*, K&R 2014, 709 (710 f.).

876 Vgl. *Däubler*, in: Däubler/Klebe/Wedde/Weichert (Hrsg.), BDSG, § 34 Fn. 45 zu Rn. 23; *Meents/Hinzpeter*, in: Taeger/Gabel (Hrsg.), BDSG, § 35 Rn. 26.

877 Ähnlich *Kamlah*, in: Plath (Hrsg.), BDSG/DSGVO, § 35, Rn. 19, der eine Kategorisierung für mehrere Daten vornehmen will.

878 *Plath*, in: Plath (Hrsg.), BDSG/DSGVO, § 38 Rn. 19; *Grittmann*, in: Taeger/Gabel (Hrsg.), BDSG, § 38 Rn. 15.

879 *Plath*, in: Plath (Hrsg.), BDSG/DSGVO, § 38 Rn. 19.

ll) § 39 Abs. 1 BDSG a. F.

Im Abschnitt mit den Sondervorschriften befindet sich mit § 39 BDSG a. F. eine Vorschrift, die eine besonders strikte Zweckbindung bei personenbezogenen Daten vorschreibt, die einem Berufs- oder besonderen Amtsgeheimnis unterliegen. Aufgrund dieser Norm ist der Empfänger der Daten an den Zweck gebunden, für den er die Daten erhalten hat. Allerdings gilt dies bei einer Übermittlung durch die empfangende Stelle an einen Dritten nicht mehr, da die empfangende (und nun übermittelnde) Stelle nicht dem Berufs- oder Amtsgeheimnis unterliegt.[880] Bei einer solchen Übermittlung sei der Zweck nicht zu eng zu interpretieren, so dass es nicht auf die konkrete Aufgabe, „sondern die dahinter stehende Zielsetzung der hoheitlichen Tätigkeit" ankomme.[881] So soll z. B. der Oberzweck „Realisierung der Sozialansprüche des Bürgers" ausreichen. Nach einer anderen Auffassung ist der Zweck nicht mit der generellen gesetzlichen Umschreibung gleichzusetzen (z. B. Zwecke der Planung, § 16 Abs. 4 BStatG), sondern immer auf den konkreten Einzelfall bezogen.[882] Sinn der Vorschrift ist der Schutz des Amts- oder Berufsgeheimnisses[883] durch Beschränkung des Empfängers der Daten.[884] Dies spricht für ein enges Verständnis des Zwecks, so dass letztere Auffassung vorzugswürdig ist.

---

880 „Keine Kettenwirkung", siehe nur: *Plath*, in: Plath (Hrsg.), BDSG/DSGVO, § 39 Rn. 11; *Weichert*, in: Däubler/Klebe/Wedde/Weichert (Hrsg.), BDSG, § 39 Rn. 2; a. A. aber bei *Schaffland/Wiltfang*, BDSG, § 39 Rn. 13, die § 39 BDSG a. F. analog anwenden wollen.

881 *Schaffland/Wiltfang*, BDSG, § 39 Rn. 9.

882 *Dammann*, in: Simitis (Hrsg.), BDSG, § 39 Rn. 21; *Bergmann/Möhrle/Herb*, BDSG, § 39 Rn. 15 fordern eine klare Festlegung; *Uwer*, in: Wolff/Brink (Hrsg.), DSR, § 39 Rn. 30.1.

883 Eine Übersicht über Amts- und Berufsgeheimnisse findet sich bei *Weichert*, in: Däubler/Klebe/Wedde/Weichert (Hrsg.), BDSG, § 39 Rn. 1; und bei *Dammann*, in: Simitis (Hrsg.), BDSG, § 39 Rn. 9.

884 *Plath*, in: Plath (Hrsg.), BDSG/DSGVO, § 39 Rn. 1; *Dammann*, in: Simitis (Hrsg.), BDSG, § 39 Rn. 1.

mm) § 40 Abs. 1 BDSG a. F.

§ 40 BDSG a. F. sieht bei für Zwecke der wissenschaftlichen Forschung erhobenen oder gespeicherten Daten eine Bindung der weiteren Datenverwendung an diesen Zweck vor.[885] Durch die Zweckbindung sollen die informationelle Selbstbestimmung und die Forschungsfreiheit in einen Ausgleich gebracht werden.[886] Die Zweckänderungsregelungen des BDSG a. F., wie § 14 Abs. 2 BDSG a. F. und § 28 Abs. 2 BDSG a. F. sind nicht anwendbar.[887] Unter wissenschaftlicher Forschung ist alles zu verstehen, „was nach Inhalt und Form als ernsthafter planmäßiger Versuch zur Ermittlung der Wahrheit anzusehen ist".[888] Zu Recht wird in der Literatur auf die Redundanz des Begriffes Wissenschaft im Zusammenhang mit Forschung hingewiesen, da Forschung nicht unwissenschaftlich betrieben werden kann.[889]

Streitig ist, ob die Datenverwendung durch § 40 Abs. 1 BDSG a. F. auf ein konkretes Forschungsvorhaben begrenzt wird. Nach einer Ansicht soll dies nicht der Fall sein, da der Wortlaut der Norm allgemein von Zwecken der wissenschaftlichen Forschung spreche.[890] Folglich sei eine Verwendung zu unterschiedlichen Forschungszwecken möglich.[891] *Simitis* fordert aufgrund einer „verwässerten Zweckbindung" aber einen Aus-

885 *Weichert*, in: Däubler/Klebe/Wedde/Weichert (Hrsg.), BDSG, § 40 Rn. 7 spricht insofern von einem „Forschungsgeheimnis"; *Simitis*, in: Simitis (Hrsg.), BDSG, § 40 Rn. 45, sieht dagegen kein Forschungsgeheimnis, da es Durchbrechungen z. B. bei Beschlagnahmungen nach § 94 ff. StPO gebe.

886 *Bergmann/Möhrle/Herb*, BDSG, § 40 Rn. 11.

887 *Greve*, in: Eßer/Kramer/v. Lewinski (Hrsg.), Auernhammer BDSG, § 40 Rn. 9; *Schaffland/Wiltfang*, BDSG, § 40 Rn. 5.

888 *Greve*, in: Eßer/Kramer/v. Lewinski (Hrsg.), Auernhammer BDSG, § 40 Rn. 6.

889 Siehe *Lindner*, in: Wolff/Brink (Hrsg.), DSR, § 40 Rn. 12.

890 *Greve*, in: Eßer/Kramer/v. Lewinski (Hrsg.), Auernhammer BDSG, § 40 Rn. 11; *Bergmann/Möhrle/Herb*, BDSG, § 40 Rn. 13; ausführliche Darstellung der Problematik bei *Simitis*, in: Simitis (Hrsg.), BDSG, § 40 Rn. 47 ff.; anders einige Landesdatenschutzgesetze, siehe z. B. § 33 Abs. 1 HDSG a. F.

891 *Plath/Frey*, in: Plath (Hrsg.), BDSG/DSGVO, § 40 Rn. 8.

gleich durch Schutzvorkehrungen, wie beispielsweise eine Benachrichtigung des Betroffenen.[892]

Eine andere Ansicht geht davon aus, dass grundsätzlich eine Datenverwendung nur für ein konkretes Forschungsprojekt zulässig ist.[893]

Eine vermittelnde Auffassung fordert eingrenzend zur ersten Ansicht, dass eine „inhaltliche Verbindung" zwischen Erhebungs- bzw. Speicherungs- und neuen Verarbeitungszweck bestehen müsse, da ansonsten die Zweckbindung leerlaufen könne.[894] Die erste Ansicht „verwische" die Konturen der Zweckbindung, während die zweite Ansicht verkenne, dass sich Forschung nicht auf identische Forschungsprojekte reduzieren lasse.[895]

Aufgrund der grundrechtlich geschützten Forschungsfreiheit ist das weite Verständnis naheliegender. Im Rahmen des Umgangs mit Daten zu Forschungszwecken sind die Betroffeneninteressen angemessen mittels Verfahrensvorkehrungen zu berücksichtigen. Jedenfalls im Falle einer Einwilligung in den Datenumgang zu Forschungszwecken scheint Einigkeit zwischen den Auffassungen zu bestehen, dass die Daten nur zu dem

---

892 *Simitis*, in: Simitis (Hrsg.), BDSG, § 40 Rn. 57 ff.

893 *Weichert*, in: Däubler/Klebe/Wedde/Weichert (Hrsg.), BDSG, § 40 Rn. 6; unklar insofern *Gola/Klug/Körffer*, in: Gola/Schomerus (Hrsg.), BDSG, § 40 Rn. 11, die einerseits die „vorhabenbezogene Zweckbindung" anbringen und dabei *Nungesser*, HDSG § 33 Rn. 26 zitieren. Das BDSG a. F. sieht in seinem Wortlaut aber anders als das HDSG a. F. keinen Vorhabenbezug vor, so dass das Zitat an dieser Stelle hätte weiter begründet werden müssen. Sodann wird aber im Zusammenhang mit der Übermittlung an andere Forschungseinrichtungen festgehalten, dass die Zweckbindung gerade nicht auf das konkrete Forschungsvorhaben bezogen sei.

894 So *Greve*, in: Eßer/Kramer/v. Lewinski (Hrsg.), Auernhammer BDSG, § 41 Rn. 11, der diese inhaltliche Verbindung bei für medizinische Zwecken erhobenen Daten nicht mehr sieht, wenn diese für militärische Forschungszwecke genutzt werden sollen; ebenfalls *Lindner*, in: Wolff/Brink (Hrsg.), DSR, § 40 Rn. 23, der bei medizinischer Forschung und anderen naturwissenschaftlichen Projekten eine hinreichende Verbindung bejaht.

895 *Lindner*, in: Wolff/Brink (Hrsg.), DSR, § 40 Rn. 22 f.

konkreten von der Einwilligung erfassten Zweck verwendet werden dürfen.[896]

Für den Einsatz von Big-Data-Analysen ist überdies zu beachten, dass von einer Forschung i. S. d. § 40 BDSG a. F. nur gesprochen werden kann, wenn diese unabhängig, d. h. nicht wirtschaftlichen Interessen untergeordnet ist.[897]

Aus § 40 Abs. 2 BDSG a. F. der entsprechend dem Forschungszweck eine frühestmögliche Anonymisierung der Daten fordert, ergibt sich, dass als Zweck nicht nur „wissenschaftliche Forschung" angegeben werden kann. Denn es ließe sich nicht feststellen, wann eine Anonymisierung möglich ist. Die verantwortliche Stelle muss den Forschungszweck näher definieren.[898]

f) Zwischenergebnis für den nicht-öffentlichen Bereich und die Sondervorschriften

Bei § 28 Abs. 1 Satz 2 BDSG a. F. wird bereits durch den Wortlaut deutlich, dass der Zweck möglichst präzise festzulegen ist. Auch die Betroffenenrechte deuten in diese Richtung, da sie nur bei einer konkreten Zweckbestimmung ihrer Funktion gerecht werden können. Einzig die Verwendung von Daten zu Forschungszwecken und für die geschäftsmäßige Datenerhebung zur Markt- und Meinungsforschung sind offener gestaltet. Die weite Zweckfestlegung wird aber zugleich mit einer Regelung zur frühzeitigen Anonymisierung der Daten ausgeglichen. Die Vorschriften sehen regemäßig eine Bindung an den Erhebungszweck vor, was ebenfalls für eine hinreichend präzise Zweckfestlegung spricht. Im Übrigen ist auch der Übermittlungsempfänger an den Übermittlungszweck

896 Vgl. *Bergmann/Möhrle/Herb*, BDSG, § 40 Rn. 16 mit dem Beispiel der Einwilligung in die Krebsforschung.

897 Vgl. *Bergmann/Möhrle/Herb*, BDSG, § 40 Rn. 17; vgl. ferner *Gola/Klug/Körffer*, in: Gola/Schomerus (Hrsg.), BDSG, § 40 Rn. 8.

898 Ähnlich *Mester*, in: Taeger/Gabel (Hrsg.), BDSG, § 40 Rn. 9, demnach die nähere Definition der Forschungseinrichtung überlassen bleibe.

und seinen Erhebungszweck gebunden. Zugleich wird die Zweckbindung im Sinne des Betroffenen vielfach als besonderes Schutzelement eingesetzt, wie z. B. im Falle der strikten Zweckbindung der für Zwecke der Auskunft gespeicherten Daten.

2. Zwischenergebnis BDSG a. F.

Sowohl der Wortlaut der Bestimmungen (mit Ausnahme von § 40 BDSG a. F. und partiell § 30a BDSG a. F.) als auch deren Sinn und Zweck sprechen für eine möglichst enge, d. h. konkrete Festlegung des Zweckes. In systematischer Hinsicht spricht hierfür, dass wesentliche Prinzipien, wie die Erforderlichkeit der Datenerhebung und auch die Interessenabwägung nur bei einer konkreten Zweckfestlegung operabel werden. Ein genauer Maßstab für die Konkretheit der Zweckfestlegung ist dem Gesetz allerdings nicht zu entnehmen. Dies ist vielmehr eine Frage des Einzelfalls und hängt vom Kontext des Datenumgangs ab. Eine Datensammlung auf Vorrat für zukünftige, unbestimmte Zwecke ist mit diesen Vorgaben nicht zu vereinbaren.

3. spezialgesetzliche Regelungen

Im Folgenden sollen einige spezialgesetzliche Normen in den Blick genommen werden. Die Vorschriften decken dabei eine große Bandbreite von Regelungsmaterien ab, wodurch untersucht werden soll, ob sich die Anforderungen an die Zweckfestlegung und -bindung je nach Sensibilität des Regelungsgegenstands unterscheiden.

a) § 12 Abs. 1 TMG, § 13 Abs. 1 TMG

Für den Bereich der Telemedien ist das TMG vorrangig anwendbar. Insbesondere für Big-Data-Anwendungen im Internet kann das TMG da-

her einschlägig sein.[899] Nach § 12 Abs. 1 TMG darf ein Datenumgang zur Bereitstellung von Telemedien nur stattfinden, sofern eine gesetzliche Erlaubnisnorm vorliegt oder der Betroffene eingewilligt hat. Unter die Bereitstellung von Telemedien sollen die Zwecke des Angebots und der Nutzung von Telemedien mitsamt dem Umgang mit Bestands- und Nutzungsdaten fallen.[900] Die Zweckbestimmungen beziehen sich also immer auf einen konkreten Zweck.[901] An diese Zweckbestimmungen ist der weitere Datenumgang gebunden.[902] Es wird vorgeschlagen den Zweck objektiv anhand des angebotenen Dienstes zu bestimmen.[903] Über den so festgelegten Zweck ist der Betroffene gemäß § 13 Abs. 1 Satz 1 TMG in allgemein verständlicher Form zu informieren.

Die Zweckbindung als „grundlegendes Regelungsprinzip" des Datenschutzrechts ist in § 12 Abs. 2 TMG normiert.[904] Es handele sich um eine strikte Bindung an den Erhebungszweck.[905] Da es zulässig ist die Zweckbindung zu durchbrechen, kann aber nicht von einer „strikten" Zweckbindung gesprochen werden.

---

899 Zur Abgrenzung von TMG, TKG und BDSG a. F. siehe *Kühling/Schall/Biendl*, TKR, Rn. 631 f.; *Kühling/Seidel/Sivridis*, Datenschutzrecht, Rn. 627 ff.; zum für die Abgrenzung genutzten Schichtenmodell siehe *Jotzo*, Der Schutz personenbezogener Daten in der Cloud, S. 49.

900 *Bizer/Hornung*, in: Roßnagel (Hrsg.), BeckRTD Kommentar, § 12 TMG Rn. 55.

901 *Schmitz*, in: Hoeren/Sieber/Holznagel (Hrsg.), Handbuch Multimedia-Recht, Teil 16.2 Rn. 144.

902 Vgl. *Bizer/Hornung*, in: Roßnagel (Hrsg.), BeckRTD Kommentar, § 12 TMG Rn. 62 u. 89.

903 *Müller-Broich*, § 12 Rn. 4, der z. B. bei einem Internetauktionshaus den Zweck in der Ermöglichung des Zugangs zu den Auktionen und der Vertragsabwicklung sieht.

904 *Bizer/Hornung*, in: Roßnagel (Hrsg.), BeckRTD Kommentar, § 12 TMG Rn. 86.

905 *Bizer/Hornung*, in: Roßnagel (Hrsg.), BeckRTD Kommentar, § 12 TMG Rn. 89; vgl. *Conrad/Hausen*, in: Auer-Reinsdorff/Conrad (Hrsg.), Handbuch IT- und Datenschutzrecht, § 36 Rn. 42; *Nink/Spindler*, in: Spindler/Schuster (Hrsg.), BDSG, § 12 TMG Rn. 7 sprechen von einer „engen" Zweckbindung; so auch *Schmitz*, in: Hoeren/Sieber/Holznagel (Hrsg.), Handbuch Multimedia-Recht, Teil 16.2 Rn. 162.

b) § 14 Abs. 1 TMG

§ 14 Abs. 1 TMG definiert den Begriff der Bestandsdaten, bei denen der Datenumgang nur zulässig ist, wenn er zur Begründung, inhaltlichen Ausgestaltung oder Änderung eines Vertragsverhältnisses zwischen Diensteanbieter und Nutzer erforderlich ist. Aus dem Wort „nur" ergibt sich im Umkehrschluss eine enge Zweckbindung.[906]

c) § 15 Abs. 1 TMG

§ 15 Abs. 1 TMG definiert den Begriff der Nutzungsdaten, mit denen nur umgegangen werden darf, soweit dies zur Ermöglichung und Abrechnung von Telemedien erforderlich ist. Aus dieser Zweckbestimmung folgt zugleich, dass die Daten bei deren Wegfall und sofern kein anderer Erlaubnistatbestand vorliegt, unverzüglich zu löschen sind.[907]

§ 15 Abs. 2 TMG regelt, dass Nutzungsdaten über die Inanspruchnahme verschiedener Telemedien nur zu Abrechnungszwecken zusammengeführt werden dürfen. Gesichert wird diese Zweckbestimmung und -bindung durch § 13 Abs. 4 Satz 1 Nr. 4 TMG, der die Verpflichtung enthält dies durch technische und organisatorische Maßnahmen umzusetzen.[908]

Für Zwecke der Werbung, der Marktforschung oder zur bedarfsgerechten Gestaltung von Telemedien darf der Diensteanbieter unter Einräumung eines Widerspruchsrechts pseudonymisierte Nutzungsprofile[909] er-

---

906 *Dix*, in: Roßnagel (Hrsg.), BeckRTD Kommentar, TMG § 14 Rn. 42; *Zscherpe*, in: Taeger/Gabel (Hrsg.), BDSG, § 14 TMG Rn. 37.

907 *Kühling/Seidel/Sivridis*, Datenschutzrecht, Rn. 649.

908 *Jandt/Schaar/Schulz*, in: Roßnagel (Hrsg.), BeckRTD Kommentar, § 13 TMG Rn. 113; *Geminn/Richter*, in: Roßnagel (Hrsg.), DSGVO, § 4 Rn. 284, sehen einen Konflikt mit der DSGVO, die das Mittel der getrennten Verarbeitung nicht vorschreibe und bei der Zweckbindung flexibler sei.

909 Siehe hierzu *Zscherpe*, in: Taeger/Gabel (Hrsg.), BDSG, § 15 TMG Rn. 60 ff.; *Spindler/Nink*, in: Spindler/Schuster (Hrsg.), BDSG, § 15 TMG Rn. 9; zu ver-

stellen. Darunter lässt sich eine systematische Zusammenfassung von Nutzungsdaten zwecks Erlangung von Aussagen über Verhalten und Gewohnheiten des Betroffenen verstehen.[910] § 15 Abs. 3 Satz 3 TMG enthält ein Verbot der Zusammenführung des Nutzungsprofils mit den Daten des Trägers des Pseudonyms. Dies wird in der Literatur als Beispiel für einen Ansatz des Grundsatzes der „Nicht-Verkettbarkeit" angeführt.[911] Dieser stehe dem Ziel von Big Data – der Verknüpfung möglichst vieler Daten – „diametral entgegen".[912] Es handele sich um eine strenge Zweckbindung, da Nutzungsprofile nur für die genannten Zwecke verwendet werden dürfen.[913] Diese wurde im Jahre 2001 aufgrund der Umsetzung der DSRL in deutsches Recht in die Norm aufgenommen.[914] Hiervon soll sowohl die Erstellung von Profilen über einen kürzeren Zeitraum, als auch über eine längere Zeit erfasst sein.[915] Eine Grenze soll die Bildung von Nutzungsprofilen aber in einer unzulässigen Bildung von umfassenden Persönlichkeitsprofilen finden.[916] Interessant für Big-Data-Anwendungen ist vor al-

---

fassungsrechtlichen Bedenken siehe *Schmitz*, in: Hoeren/Sieber/Holznagel (Hrsg.), Handbuch Multimedia-Recht, Teil 16.2 Rn. 278; zum Streit, ob dies den Vorgaben des Art. 5 Abs. 3 ePrivacy-RL (Richtlinie 2002/58/EG vom 12. Juli 2002, ABl. 2002 Nr. L 201, S. 37) gerecht wird, *Boehme-Neßler*, in: Rehbinder (Hrsg.), UFITA 2015 I, 19 (56 ff.).

910 *Zscherpe*, in: Taeger/Gabel (Hrsg.), BDSG, § 15 TMG Rn. 61; zustimmend *Boehme-Neßler*, in: Rehbinder (Hrsg.), UFITA 2015 I, 19 (29); anders *Spindler/Nink*, in: Spindler/Schuster (Hrsg.), BDSG, § 15 TMG Rn. 9; *Rammos*, K&R 2011, 692 (693); *Jandt/Laue*, K&R 2006, 316 (317), die zumindest ein Teilabbild über die Persönlichkeit des Betroffenen fordern.

911 *Bock/Meissner*, DuD 2012, 425 (429); Nicht-Verkettbarkeit ist laut § 5 Abs. 1 Satz 2 Nr. 5 LDSG SH a. F. gegeben, wenn „personenbezogene Daten nicht oder nur mit unverhältnismäßig hohem Aufwand für einen anderen als den ausgewiesenen Zweck erhoben, verarbeitet und genutzt werden können".

912 *Weichert*, ZD 2013, 251 (256); *Weichert*, DuD 2014, 831 (835); *Roßnagel*, ZD 2013, 562 (564).

913 *Spindler/Nink*, in: Spindler/Schuster (Hrsg.), BDSG, § 15 TMG Rn. 9; *Zscherpe*, in: Taeger/Gabel (Hrsg.), BDSG, § 15 TMG Rn. 70; *Schmidtmann/Schwiering*, ZD 2014, 448 (451).

914 *Hullen/Roggenkamp*, in: Plath (Hrsg.), BDSG/DSGVO, § 15 TMG Rn. 28; BT-Drs. 14/6098, S. 29 f.

915 *Kühling/Seidel/Sivridis*, Datenschutzrecht, Rn. 650.

916 *Dix/Schaar*, in: Roßnagel (Hrsg.), BeckRTD Kommentar, § 15 TMG Rn. 62.

lem die Möglichkeit der Erstellung von Nutzerprofilen, die zugleich eine Zweckänderung darstellt, weil auf die nach § 15 Abs. 1 TMG erhobenen Nutzungsdaten zurückgegriffen wird.[917]

d) § 88 Abs. 3 TKG

Das TKG enthält ebenfalls bereichsspezifische datenschutzrechtliche Regeln in den §§ 91 ff. TKG. Nicht zum datenschutzrechtlichen Teil gehört die einfachrechtliche Bestimmung des Fernmeldegeheimnisses in § 88 TKG. Gleichwohl steht sie in engem Zusammenhang mit den datenschutzrechtlichen Regelungen[918] und wirkt sich insbesondere bei der Weitergabe von Daten an Dritte aus.[919] Dem Diensteanbieter ist es untersagt, sich oder anderen über das für die geschäftsmäßige Erbringung der Telekommunikationsdienste erforderliche Maß hinaus Kenntnis von Inhalt oder Umständen der Kommunikation zu verschaffen, § 88 Abs. 3 Satz 1 TKG. Gemäß § 88 Abs. 3 Satz 2 TKG ist die Verwendung dieser Daten grundsätzlich an den Zweck der Kenntnisnahme gebunden, wobei § 88 Abs. 3 Satz 4 TKG Ausnahmen hiervon vorsieht. Es liegt also grundsätzlich eine enge Zweckbestimmung und eine strenge Bindung an diesen Zweck vor.[920]

---

917 Vgl. zum Rückgriff auf die Nutzungsdaten: *Dix/Schaar*, in: Roßnagel (Hrsg.), BeckRTD Kommentar, § 15 TMG Rn. 63; *Schreibauer*, in: Eßer/Kramer/v. Lewinski (Hrsg.), Auernhammer BDSG, § 15 TMG Rn. 20; *Hullen/Roggenkamp*, in: Plath (Hrsg.), BDSG/DSGVO, § 15 TMG Rn. 22.

918 Vgl. *Heun*, in: Eßer/Kramer/v. Lewinski (Hrsg.), Auernhammer BDSG, § 88 TKG Rn. 4.

919 *Bock*, in: Geppert/Schütz (Hrsg.), TKG § 88 Rn. 11.

920 Vgl. *Jenny*, in: Plath (Hrsg.), BDSG/DSGVO, § 88 TKG Rn. 18; *Munz*, in: Taeger/Gabel (Hrsg.), BDSG, § 88 TKG Rn. 16; *Bock*, in: Geppert/Schütz (Hrsg.), TKG, § 88 Rn. 27; *Eckhardt*, in: Spindler/Schuster (Hrsg.), BDSG, § 88 TKG Rn. 35.

e) § 93 Abs. 1 TKG

Die Teilnehmer sind bei Vertragsschluss über den Erhebungs- und Verwendungszweck personenbezogener Daten so zu unterrichten, dass sie Kenntnis von den grundlegenden Verarbeitungstatbeständen der Daten erhalten, § 93 Abs. 1 Satz 1 TKG. Ein pauschaler Hinweis genügt somit nicht.[921] Ausweislich des Gesetzestexts hat die Information zudem in allgemein verständlicher Form zu erfolgen.

f) § 95 Abs. 1 Satz 1 TKG

§ 95 Abs. 1 Satz 1 TKG begrenzt den Umgang mit Bestandsdaten auf für die Begründung und Durchführung des Vertragsverhältnis erforderliche Zwecke, ähnlich wie dies in § 14 TMG für Telemediendiensteanbieter der Fall ist.[922]

g) § 96 Abs. 1 TKG

§ 96 Abs. 1 TKG begrenzt die Erhebung von Verkehrsdaten auf die Zwecke des 2. Abschnitts des 7. Teils[923] des TKG. § 96 Abs. 1 Satz 1 Nr. 5 TKG stellt klar, dass letztlich eine Erhebung jeglicher Verkehrsdaten zulässig ist, die dem Aufbau und der Aufrechterhaltung der Telekommunikation oder der Entgeltabrechnung dienen. Es handelt sich also nicht um eine abschließende Aufzählung in § 96 Abs. 1 TKG.[924] Die Datenverwendung ist nach § 96 Abs. 1 Satz 2 zulässig wenn dies für die Zwecke des Satzes 1 oder für durch andere gesetzliche Vorschriften be-

921 Vgl. *Eckhardt*, in: Spindler/Schuster (Hrsg.), BDSG, § 93 TKG, Rn. 5.
922 Vgl. *Heun*, in: Eßer/Kramer/v. Lewinski (Hrsg.), Auernhammer BDSG, § 95 TKG Rn. 1 u. 3.
923 Siehe hierzu: *Munz*, in: Taeger/Gabel (Hrsg.), BDSG, § 96 TKG Rn. 10.
924 Vgl. *Munz*, in: Taeger/Gabel (Hrsg.), BDSG, § 96 TKG Rn. 9; *Lutz*, in: Arndt/Fetzer/Scherer/Graulich (Hrsg.), TKG, § 96 Rn. 3.

gründete Zwecke erforderlich ist. Diese Bestimmung ist aufgrund ihrer Weite kritisiert worden.[925]

h) § 98 Abs. 1 TKG

Die „Verarbeitung“[926] von Standortdaten durch Dienste mit Zusatznutzen[927] ist in § 98 TKG geregelt. Ein Umgang mit Standortdaten ist nur im zur Bereitstellung von Diensten mit Zusatznutzen erforderlichen Umfang aufgrund einer Einwilligung zulässig, § 98 Abs. 1 Satz 1 TKG. Zwar nennt § 98 Abs. 1 TKG auch die Möglichkeit einer Anonymisierung. Es ist aber natürlich eine Einzelfallfrage und zumindest zweifelhaft, ob eine solche in Zeiten einer zunehmenden Verknüpfung von Daten überhaupt wirksam durchgeführt werden kann.[928] Eine wirksame Anonymisierung würde den Wert der Daten ohnehin erheblich schmälern und vermutlich der Intention des TK-Anbieters, Dienste mit Zusatznutzen anzubieten, entgegenstehen.[929] Im Rahmen der Einwilligung ist der Betroffene auf den Zweck des Datenumgangs hinzuweisen, wobei eine Formulierung wie „im Rahmen des Erforderlichen auch für Vermarktung und Mei-

925 So *Gola/Klug/Reif*, NJW 2007, 2599 (2601); *Munz*, in: Taeger/Gabel (Hrsg.), BDSG, § 96 TKG Rn. 12 hat Zweifel an der Verfassungsmäßigkeit.

926 Es soll sich um eine Übernahme der europarechtlichen Terminologie bei Umsetzung der RL 2002/58/EG handeln, so dass in europarechtskonformer Auslegung jeglicher Datumgang erfasst ist, siehe *Kleczewski*, in: Säcker (Hrsg.), TKG, § 98 Rn. 8 m. w. N.; *Heun*, in: Eßer/Kramer/v. Lewinski (Hrsg.), Auernhammer BDSG, § 98 TKG Rn. 11 m. w. N.

927 Gemäß § 3 Nr. 5 TKG sind Dienste mit Zusatznutzen, Dienste, die die Erhebung und Verwendung von Verkehrsdaten in einem Maße erfordern, das über das für die Übermittlung einer Nachricht oder die Entgeltabrechnung dieses Vorgangs erforderliche Maß hinausgeht.

928 Vgl. *Heun*, in: Eßer/Kramer/v. Lewinski (Hrsg.), Auernhammer BDSG, § 98 TKG Rn. 13.

929 Siehe hierzu das Beispiel des von Telefónica/O2 im Jahr 2012 geplanten Programms „Smart Steps“, *Mantz*, K&R 2013, 7 (9).

nungsforschung vorgesehen“ mangels hinreichender Präzision nicht ausreicht.[930]

i) §§ 49, 50 MsbG

Mit dem Gesetz zur Digitalisierung der Energiewende vom 29. August 2016[931] wurde das Messstellenbetriebsgesetz (MsbG) erlassen und zugleich die datenschutzrechtlichen Bestimmungen des § 21g EnWG aufgehoben. § 49 Abs. 1 Satz 2 MsbG stellt klar, dass eine Übermittlung, Nutzung oder Beschlagnahme nach anderen Rechtsvorschriften des Bundes oder der Länder unzulässig ist. Dies entspricht den Regelungen des § 4j Abs. 3 Satz 2 Bundesfernstraßenmautgesetz (BFStrMG) und des § 11 Abs. 3 Satz 3 Infrastrukturabgabengesetz (InfrAG).[932] Nach § 50 Abs. 1 MsbG ist ein Datenumgang von Daten aus einem Messsystem nur zulässig sofern ein gesetzlicher Erlaubnistatbestand oder eine Einwilligung vorliegt. Aufgrund der Möglichkeit der Legitimation des Datenumgangs mittels Einwilligung ist der in der Literatur grundsätzlich begrüßte[933] Ansatz einer Spezialregelung des Datenschutzes für die Digitalisierung im Energiesektor zu Recht als „liberaler“ als die strengen Vorgaben in den Mautgesetzen bezeichnet worden.[934] Bei einer Datenübermittlung aufgrund eines Vertrages schreibt das Gesetz vor, dass „kurz, einfach, übersichtlich und verständlich die sich aus dem Vertrag ergebende Datenkommunikation aufgelistet wird“, § 54 Abs. 1 Satz 1 MsbG. Hierzu zählt nach § 54 Abs. 1 Satz 2 MsbG auch die Angabe des Zwecks der Datenübermittlung.

930 Vgl. *Mantz*, K&R 2013, 7 (10).
931 BGBl. 2016 Teil I Nr. 43, S. 2034 ff.
932 Immer wieder wird eine Lockerung der Zweckbindung zu Zwecken der Strafverfolgung gefordert, siehe hierzu zuletzt die Forderung von *Kay Nehm* auf dem Verkehrsgerichtstag am 29.01.2015, beck-aktuell-Redaktion, Verlag C.H. Beck, 29. Januar 2015, von *Matthias Brunnert*.
933 So *Lüdemann/Ortmann/Pokrant*, RDV 2016, 125 (129).
934 Vgl. *Karsten/Leonhardt*, RDV 2016, 22 (23).

j) § 13 GenDG

Nach § 8 GenDG bedarf eine genetische Untersuchung oder Analyse einer Einwilligung. Grundsätzlich darf eine genetische Probe nur für den Zweck verwendet werden zu dem sie gewonnen wurde, § 13 Abs. 1 Satz 1 GenDG. Sofern sie nicht mehr benötigt wird, ist sie unverzüglich zu vernichten, § 13 Abs. 1 Satz 2 GenDG.

k) § 45 ff. LKHG BW

Das Landeskrankenhausgesetz Baden-Württemberg (LKHG BW) sieht in § 45 LKHG BW enumerativ aufgeführte Zwecke vor, für die Patientendaten erhoben, gespeichert, verändert oder genutzt werden dürfen. Aus § 50 LKHG BW ergibt sich zudem, dass ein Datenumgang auch auf eine Einwilligung gestützt werden kann. Zur Bindung an den Erhebungszweck und die Möglichkeit von Zweckänderungen enthält das Gesetz keine Angaben.

l) §§ 37, 41 PolG BW

Nach § 37 Abs. 1 Satz 1 Polizeigesetz Baden-Württemberg (PolG BW) ist das Speichern, Verändern und Nutzen von Daten zur Erfüllung der Aufgaben der Polizei zulässig. Grundsätzlich sind Speicherung, Veränderung und Nutzung nur zu dem Zweck zulässig, zu dem die Daten erlangt wurden, § 37 Abs. 2 Satz 1 PolG BW. Im Falle einer Datenübermittlung, ist der Empfänger grundsätzlich an den Übermittlungszweck gebunden, § 41 Abs. 2 Satz 1 PolG BW. Zum Schutz von Berufs- oder Amtsgeheimnissen muss der Übermittlungszweck grundsätzlich mit dem Zweck übereinstimmen, zu dem die übermittelnde Stelle die Daten erlangt hat, § 41 Abs. 2 Satz 2 PolG BW.

4. Zwischenergebnis spezialgesetzliche Regelungen

Die spezialgesetzlichen Regelungen sehen einen unterschiedlichen Konkretisierungsgrad des Zweckes und eine unterschiedlich stark ausgeprägte Bindung an den Erhebungszweck vor. Dabei ist zu erkennen, dass die Vorgaben grundsätzlich umso strenger sind, je sensibler die Daten sind und je schwerer damit der mögliche Eingriff in das RiS ist, siehe insbesondere die Bestimmungen des TKG, MsbG und des GenDG. Ein allgemeiner Maßstab für den Konkretisierungsgrad der Zweckfestlegung lässt sich aber nicht ableiten, sondern dies ist vielmehr eine Frage des Einzelfalls.

5. Ergebnis

Wegen europarechtlicher Vorgaben und der Funktion der Zweckbestimmung, muss diese möglichst konkret erfolgen, da sie ansonsten ihrer Funktion nicht gerecht wird.

6. Zweckänderung

Da es wegen der Anforderungen an die Zweckbestimmung nicht zulässig ist den Zweck so weit zu fassen, dass der Datenumgang mit Big-Data-Analysemethoden darunter gefasst werden könnte, stellt sich die Frage, inwiefern eine entsprechende weitere Datenverwendung aufgrund einer Zweckänderung möglich ist. In Betracht kommen gesetzliche Erlaubnistatbestände oder eine Einwilligung. Zunächst wird auf die gesetzlich zulässige Zweckänderung im öffentlichen Bereich eingegangen, bevor der nicht-öffentliche Bereich betrachtet wird. Danach werden einzelne spezialgesetzliche Regelungen in den Blick genommen und zuletzt die Möglichkeit einer Einwilligung in die Zweckänderung diskutiert.

a) öffentlicher Bereich

aa) § 14 Abs. 2 ff. BDSG a. F.

§ 14 Abs. 2 BDSG a. F. erlaubt das Speichern, Verändern oder Nutzen von personenbezogenen Daten für einen anderen Zweck als den Erhebungszweck.[935] Anders als die DSRL wird nicht auf eine Zweckvereinbarkeit, sondern auf eine Zweckidentität abgestellt. Damit stellt sich zunächst die Frage, wann ein anderer Zweck vorliegt. Nach § 14 Abs. 3 Satz 1 BDSG a. F. soll ein anderer Zweck nicht vorliegen, wenn die Verarbeitung oder Nutzung der Wahrnehmung von Aufsichts- und Kontrollbefugnissen, der Rechnungsprüfung oder der Durchführung von Organisationsuntersuchungen für die verantwortliche Stelle dient. Auch die Verwendung zu Ausbildungs- und Prüfzwecken ist privilegiert, sofern nicht schutzwürdige Interessen des Betroffenen entgegenstehen, § 14 Abs. 3 Satz 2 BDSG a. F. Diese Zwecke können als „Begleit- und Hilfszwecke“[936] oder „Nebenzwecke“[937] bezeichnet werden. Umstritten ist, ob es sich bei der Privilegierung der Nebenzwecke um eine gesetzliche Fiktion oder eine Klarstellung handelt.[938] Einerseits wird vertreten, dass es sich um eine gesetzliche Fiktion handele, ohne dies weiter zu begründen.[939] Andererseits ist nach vorzugswürdiger Ansicht davon auszugehen, dass es sich bezüglich dem Primärzweck zurechenbarer Nebenzwecke um eine Klarstellung handelt, da der Wortlaut nicht klar für eine Fiktion

935 Insofern unglücklich die Darstellung bei *Boehme-Neßler*, in: Rehbinder (Hrsg.), UFITA 2015 I, 19 (36 f.), die so verstanden werden kann, dass § 14 Abs. 2 BDSG a. F. Ausnahmen vom Erfordernis der Festlegung eines Erhebungszwecks enthalte.

936 So *Dammann*, in: Simitis (Hrsg.), BDSG, § 14 Rn. 47.

937 So *Eßer*, in: Eßer/Kramer/v. Lewinski (Hrsg.), Auernhammer BDSG, § 14 Rn. 1.

938 Ausführlich hierzu und der dogmatischen Bedeutung einer analogiefähigen Ausnahme oder einer gesetzlichen Fiktion: *Dammann*, in: Simitis (Hrsg.), BDSG, § 14 Rn. 93 ff.

939 So *Schaffland/Wiltfang*, BDSG, § 14 Rn. 33; *Wedde*, in: Däubler/Klebe/Wedde/Weichert (Hrsg.), BDSG, § 14 Rn. 23; *Bergmann/Möhrle/Herb*, BDSG, § 14 Rn. 33; *Roggenkamp*, in: Plath (Hrsg.), BDSG/DSGVO, § 14 Rn. 19.

spricht und nur für die über den Rahmen des ursprünglichen Zwecks hinausgehenden Fälle des § 14 Abs. 3 Satz 2 BDSG a. F. von einer Fiktion auszugehen ist.[940] Es lässt sich also zwischen dem Primärzweck und dazugehörigen Nebenzwecken einerseits und anderen Sekundärzwecken andererseits unterscheiden.

§ 14 Abs. 2 Nr. 9 BDSG a. F. sieht eine Privilegierung der wissenschaftlichen Forschung vor, wenn das wissenschaftliche Interesse an der Durchführung des Forschungsvorhabens das Betroffeneninteresse am Ausschluss der Zweckänderung deutlich überwiegt und der Forschungszweck auf andere Weise nicht oder nur mit unverhältnismäßigen Mitteln erreicht werden kann. Der Begriff der wissenschaftlichen Forschung bzw. des Forschungsvorhabens ist weit zu verstehen, so dass auch Grundlagenforschung mit einer langfristigen Verwendung der Daten hierunter fallen kann.[941] Es bedarf aber zumindest eines konkreten Forschungszwecks, da ansonsten eine Abwägung nicht möglich ist.[942] Ein enger Zweck kann dann im Rahmen der Abwägung für die Zulässigkeit der Verwendung für Forschungszwecke sprechen.[943]

§ 14 Abs. 2 BDSG a. F. wird teils als verfassungswidrig bezeichnet, weil er zu einer Umkehrung des Regel-Ausnahme-Verhältnisses führe, da sich unter diese Norm jegliches Verwaltungshandeln subsumieren lasse.[944] In der Tat sind die neun in § 14 Abs. 2 BDSG a. F. genannten Aus-

---

940 Vgl. *Dammann*, in: Simitis (Hrsg.), BDSG, § 14 Rn. 94; diesem folgend: *Heckmann*, in: Taeger/Gabel (Hrsg.), BDSG, § 14 Rn. 96 f.; *Albers*, in: Wolff/Brink (Hrsg.), DSR, § 14 Rn. 52.

941 *Dammann*, in: Simitis (Hrsg.), BDSG, § 14 Rn. 91; *Albers*, in: Wolff/Brink (Hrsg.), DSR, § 14 Rn. 49.

942 Vgl. *Dammann*, in: Simitis (Hrsg.), BDSG, § 14 Rn. 91, der eine klare Definition von Ziel, Aufbau und Verlauf des Vorhabens fordert; a. A. *Albers*, in: Wolff/Brink (Hrsg.), DSR, § 14 Rn. 50, die eine Berücksichtigung der Unsicherheiten und Risiken im Rahmen der Abwägung fordert.

943 Siehe hierzu BVerwGE 121, 115, Urteil v. 23.06.2004, Az.: 3 C 41/03, Rn. 50, das sich für Zulässigkeit der Einsichtnahme in Stasi-Unterlagen über einen Dritten nur unter der Voraussetzung einer Nutzung nur für ein konkretes Forschungsvorhaben ausgesprochen hatte.

944 *Marenbach*, informationelle Beziehungen, S. 113.

nahmen von der Zweckbindung teilweise sehr weit gefasst.[945] Zugleich handelt es sich aber um eine „abschließende" und „vor dem Hintergrund der Grundrechtsproblematik"[946] „eng auszulegende" Aufzählung von Ausnahmetatbeständen der Zweckbindung.[947] Das Allgemeininteresse überwiegt in den aufgeführten Fällen laut der Gesetzesbegründung, weshalb eine Einschränkung des RiS zulässig sei.[948] Es ist aber zu berücksichtigen, dass viele der Ausnahmetatbestände eine Abwägung der konkret betroffenen Interessen vorsehen.[949] Der laut Gesetzesbegründung anwendbare Verhältnismäßigkeitsgrundsatz[950] gebietet eine Begrenzung auf die jeweils zur Zweckerreichung erforderliche Handlungsalternative der Speicherung, Veränderung, Nutzung.[951] § 14 Abs. 2 BDSG a. F. gestattet also eine Zweckänderung nur für einen konkreten neuen Zweck.[952]

§ 14 Abs. 4 BDSG a. F. sieht eine strikte Zweckbindung von ausschließlich für Kontroll- und Sicherungszwecke erhobenen Daten vor. Es handelt sich bei diesen Daten im Wesentlichen um Protokolldaten, die im Rahmen der technischen und organisatorischen Maßnahmen nach § 9 BDSG a. F. erhoben wurden.[953] Die Anwendung von § 14 Abs. 2, 3 BDSG a. F. ist somit ausgeschlossen und ein Hemmnis für die Speicherung von Daten für Datenschutz- und Datensicherungsmaßnahmen mit der ansonsten möglichen Verwendung für andere Zwecke beseitigt.[954] Die

---

945 *Albers*, in: Wolff/Brink (Hrsg.), DSR, § 14 Rn. 25 spricht von einer „partiell generalklauselartigen Auflistung".

946 *Heckmann*, in: Taeger/Gabel (Hrsg.), BDSG, § 14 Rn. 32.

947 *Roggenkamp*, in: Plath (Hrsg.), BDSG/DSGVO, § 14 Rn. 7; *Wedde*, in: Däubler/Klebe/Wedde/Weichert (Hrsg.), BDSG, § 14 Rn. 12; *Dammann*, in: Simitis (Hrsg.), BDSG, § 14 Rn. 54.

948 BT-Drs. 11/4306 S. 44.

949 Im Falle von § 14 Abs. 2 Nr. 6 BDSG a. F. folgt dies z. B. aus dem Merkmal der „Erheblichkeit", siehe *Dammann*, in: Simitis (Hrsg.), BDSG, § 14 Rn. 73.

950 BT-Drs. 11/4306 S. 44.

951 *Heckmann*, in: Taeger/Gabel (Hrsg.), BDSG, § 14 Rn. 33.

952 Vgl. *Dammann*, in: Simitis (Hrsg.), BDSG, § 14 Rn. 55.

953 *Bergmann/Möhrle/Herb*, BDSG, § 14 Rn. 39; *Gola/Körffer/Klug*, in: Gola/Schomerus (Hrsg.), BDSG, § 14 Rn. 27 f.

954 Vgl. *Dammann*, in: Simitis (Hrsg.), BDSG, § 14 Rn. 115; *Albers*, in: Wolff/Brink (Hrsg.), DSR, § 14 Rn. 56.

Wiederherstellung gelöschter personenbezogener Daten unter Rückgriff auf die Sicherungskopien ist unzulässig.[955]

In Umsetzung von Art. 8 DSRL wurden für sensitive Daten in Art. 14 Abs. 5 und 6 BDSG a. F. besondere Regelungen zur Zweckänderung geschaffen.[956] Im Wesentlichen wird dabei auf das Vorliegen der Erhebungsvoraussetzungen verwiesen und für wissenschaftliche Forschung nicht lediglich ein wissenschaftliches, sondern ein öffentliches Interesse gefordert. Der besondere Schutz dieser Daten wird also entsprechend der Erhebungsvoraussetzungen fortgesetzt.[957]

bb) § 15 Abs. 3 Satz 2 i. V. m. § 14 Abs. 2 BDSG a. F.

Die Datenübermittlung an öffentliche Stellen richtet sich nach § 15 BDSG a. F. § 15 Abs. 3 Satz 2 BDSG a. F. gestattet die Datenverwendung für einen anderen Zweck als den Übermittlungszweck unter den Voraussetzungen von § 14 Abs. 2 BDSG a. F. Die Möglichkeit der Nutzung der übermittelten Daten zu einem anderen Zweck wird wegen einer „Beeinträchtigung" des RiS kritisch gesehen.[958] Diese Kritik vermag aber nicht zu überzeugen.[959] Denn eine Übermittlung der Daten zu einem anderen Zweck als dem Erhebungszweck ist zudem nach § 15 Abs. 1 i. V. m. § 14 Abs. 2 BDSG a. F. zulässig. Anstatt den Zweck bereits übermittelter Daten für die weitere Datenverwendung zu ändern, könnte die empfangende Stelle sich die Daten noch einmal übermitteln lassen. Mangels Verweises auf die Vorschriften für besondere Arten personenbe-

955 Siehe zur entsprechenden Vorschrift des LDSG BW a. F., VGH Baden-Württemberg, Urteil v. 30.7.2014 - Az. 1 S 1352/13.
956 *Albers*, in: Wolff/Brink (Hrsg.), DSR, § 14 Rn. 63.
957 Vgl. *Gola/Körffer/Klug*, in: Gola/Schomerus (Hrsg.), BDSG, § 14 Rn. 31.
958 *Wedde*, in: Däubler/Klebe/Wedde/Weichert (Hrsg.), BDSG, § 15 Rn. 17; *Heckmann*, in: Taeger/Gabel (Hrsg.), BDSG, § 15 Rn. 40.
959 So auch *Albers*, in: Wolff/Brink (Hrsg.), DSR, § 15 Rn. 36.

zogener Daten soll eine Zweckänderung in diesem Falle ausgeschlossen sein.[960]

Durch die Zweckänderung wird zugleich ein neuer verbindlicher Zweck festgelegt.[961] Eine Änderung dieses Zwecks ist dann wiederum nur unter den Voraussetzungen des § 14 Abs. 2 BDSG a. F. zulässig.[962] Sofern die Übermittlung der Daten für den Empfänger eine Datenerhebung darstellt oder er die Daten speichert, ist er sogleich an die Vorgaben des § 14 Abs. 1 BDSG a. F. bzw. entsprechender landesrechtlicher Bestimmungen gebunden.[963] Falls der Erhebungszweck des Empfängers und der Übermittlungszweck nicht identisch sind, sind beide Zwecke zu beachten, was letztlich dazu führt, dass der engere Zweck maßgeblich ist.[964]

cc) § 16 Abs. 4 Satz 3 BDSG a. F.

Die Übermittlung an nicht-öffentliche Stellen ist in § 16 BDSG a. F. normiert. Anders als bei der Übermittlung an öffentliche Stellen ist eine Datenverwendung zu einem anderen Zweck als dem Übermittlungszweck gemäß § 16 Abs. 4 Satz 3 BDSG a. F. aber möglich, wenn die Übermittlung nach § 16 Abs. 1 BDSG a. F. zulässig wäre und die übermittelnde Stelle zugestimmt hat. Voraussetzung hierfür ist, dass die Daten bei der übermittelnden Stelle noch vorhanden sind und sie die Daten tatsächlich noch einmal übermitteln könnte, da eine Verfügung über bereits gelöschte Daten unzulässig ist.[965] Ziel der Norm ist die Vermeidung unnötiger nochmaliger Übermittlungen.[966]

---

960 *Roggenkamp*, in: Plath (Hrsg.), BDSG/DSGVO, § 15 Rn. 17.
961 *Albers*, in: Wolff/Brink (Hrsg.), DSR, § 15 Rn. 35.
962 *Körffer/Gola/Klug*, in: Gola/Schomerus (Hrsg.), BDSG, § 15 Rn. 18.
963 Vgl. *Albers*, in: Wolff/Brink (Hrsg.), DSR, § 15 Rn. 31 u. 34; BVerfGE 125, 260 (332 f.).
964 *Albers*, in: Wolff/Brink (Hrsg.), DSR, § 15 Rn. 31; *Dammann*, in: Simitis (Hrsg.), BDSG, § 15 Rn. 44 fordert die Einhaltung beider Zweckbindungen.
965 Vgl. *Dammann*, in: Simitis (Hrsg.), BDSG, § 16 Rn. 50.
966 *Roggenkamp*, in: Plath (Hrsg.), BDSG/DSGVO, § 16 Rn. 19.

b) Zwischenergebnis Zweckänderung öffentlicher Bereich

Die umfangreichen Bestimmungen zur Zweckänderung sprechen in gewisser Weise ebenfalls dafür, dass der Zweck konkret festzulegen ist. Denn ansonsten würde es nur selten zu einer Zweckänderung kommen, weshalb es einer derart umfangreichen Regelung nicht bedurft hätte. Es ließe sich sonst nicht feststellen, ob überhaupt eine Zweckänderung vorliegt. Auch im Falle einer Zweckänderung ist wiederum ein Zweck festzulegen, weshalb auch eine Zweckänderung nicht dazu führt, dass eine zweckoffene Big-Data-Analyse darunter subsumiert werden könnte.

c) nicht-öffentlicher Bereich und Sondervorschriften

Auch für den nicht-öffentlichen Bereich enthält das BDSG a. F. eine Vielzahl von Zweckänderungsvorschriften von denen nun einige betrachtet werden sollen.

aa) § 28 Abs. 2 BDSG a. F.

Zentrale Vorschrift für Zweckänderungen im nicht-öffentlichen Bereich ist § 28 Abs. 2 BDSG a. F. In der Literatur wird aufgrund der vielfältigen Möglichkeiten einer Zweckänderung im Rahmen des § 28 BDSG a. F. die Existenz eines Grundsatzes der Zweckbindung im nicht-öffentlichen Bereich bezweifelt und stattdessen von einem „Grundsatz der Zweckfestlegung“ gesprochen.[967] Teils wird eine „weite Durchbrechung“ der Zweckbindung beklagt.[968] § 28 Abs. 2 BDSG a. F. stelle bei genauerer Betrachtung aufgrund der Weite seiner Erlaubnistatbestände keine Stärkung der Zweckbindung dar.[969]

967 Vgl. *Kramer*, in: Eßer/Kramer/v. Lewinski (Hrsg.), Auernhammer BDSG, § 28 Rn. 79 f.
968 So *Taeger*, in: Taeger/Gabel (Hrsg.), BDSG, § 28 Rn. 119.
969 *Bergmann/Möhrle/Herb*, BDSG, § 28 Rn. 2.

Unter Berücksichtigung verfassungsrechtlicher Anforderungen sei die Norm restriktiv zu handhaben.[970] Es handele sich zudem um eine abschließende Liste erlaubter Zweckänderungstatbestände.[971] Nur ein Nutzen oder Übermitteln, nicht aber ein Speichern oder Verändern ist nach § 28 Abs. 2 BDSG a. F. zu einem anderen Zweck zulässig.[972]

Auch für den neuen Zweck im Falle von § 28 Abs. 2 Nr. 1 BDSG a. F. gilt das Erfordernis, dass es sich um einen eigenen Geschäftszweck handeln muss, wie sich aus dem Verweis auf die Voraussetzungen von § 28 Abs. 1 Satz 1 Nr. 2 und 3 BDSG a. F. ergibt.[973] Die Bedeutung von § 28 Abs. 2 Nr. 1 BDSG a. F. wird zudem dadurch eingeschränkt, dass für eine Nutzung für Werbezwecke § 28 Abs. 3 BDSG a. F. lex specialis ist.[974] § 28 Abs. 2 Nr. 1 BDSG a. F. verhindert eine erneute Erhebung der Daten, wenn es sich um einen zulässigen Verarbeitungszweck handelt.[975] Wegen eben dieser Übereinstimmung der Voraussetzungen mit § 28 Abs. 1 Nr. 1 und 2 BDSG a. F. wird die Norm im Schrifttum als „überflüssig und verwirrend“ bezeichnet.[976]

Zwar ist die Zweckfestlegung bei den zulässigen Zweckänderungen nicht noch einmal explizit vorgeschrieben, sie ist aber logisch vorausgesetzt, da sonst die Anwendbarkeit und die Voraussetzungen von § 28

---

970 *Wedde*, in: Däubler/Klebe/Wedde/Weichert (Hrsg.), BDSG, § 28 Rn. 69; vgl. *Bergmann/Möhrle/Herb*, BDSG, § 28 Rn. 284; vgl. *Simitis*, in: Simitis (Hrsg.), BDSG, § 28 Rn. 169; a. A. aber *Wolff*, in: Wolff/Brink (Hrsg.), DSR, § 28 Rn. 95, der für eine extensive Auslegung des § 28 Abs. 2 Nr. 1 BDSG a. F. plädiert zwecks Privilegierungen anderer Verwendungsformen.

971 *Wedde*, in: Däubler/Klebe/Wedde/Weichert (Hrsg.), BDSG, § 28 Rn. 69; Taeger, in: Taeger/Gabel (Hrsg.), BDSG, § 28 Rn. 118.

972 *Wolff*, in: Wolff/Brink (Hrsg.), DSR, § 28 Rn. 95 plädiert daher im Falle des § 28 Abs. 2 Nr. 1 BDSG a. F. bezüglich anderer Verwendungsformen für eine extensive Auslegung.

973 Vgl. *Plath*, in: Plath (Hrsg.), BDSG/DSGVO, § 28 Rn. 93; vgl. *Wolff*, in: Wolff/Brink (Hrsg.), DSR, § 28 Rn. 97.

974 Vgl. *Kramer*, in: Eßer/Kramer/v. Lewinski (Hrsg.), Auernhammer BDSG, § 28 Rn. 82.

975 *Wolff*, in: Wolff/Brink (Hrsg.), DSR, § 28 Rn. 94.

976 So *Simitis*, in: Simitis (Hrsg.), BDSG, § 28 Rn. 170; zustimmend *Taeger*, in: Taeger/Gabel (Hrsg.), BDSG, § 28 Rn. 125.

Abs. 2 BDSG a. F. nicht geprüft werden können. Es ist also keinesfalls „unverständlich", dass der Gesetzgeber eine Selbstverständlichkeit nicht noch einmal explizit normiert hat.[977]

Die Zweckänderungstatbestände in § 28 Abs. 2 BDSG a. F. sehen jeweils eine Abwägung mit dem schutzwürdigen Interesse des Betroffenen vor.[978] Um diese Abwägung durchzuführen und im Übrigen auch um überhaupt einen Vergleich der Zwecke vornehmen und damit das Vorliegen einer Zweckänderung feststellen zu können, bedarf es eines konkret definierten neuen Zwecks der Nutzung oder Übermittlung.

Nicht zutreffend ist, dass allgemein zugängliche Daten zweckungebunden weiteren Nutzungen zugeführt werden könnten.[979] Denn bei Erhebung dieser Daten ist gemäß § 28 Abs. 1 Satz 2 BDSG a. F. ein Zweck festzulegen und nach § 28 Abs. 1 Satz 1 Nr. 3 BDSG a. F. eine Interessenabwägung durchzuführen, wenngleich diese in der Regel zugunsten der verantwortlichen Stelle ausfallen mag.[980] Für die Zweckänderung gelten dann aufgrund des Verweises von § 28 Abs. 2 Nr. 1 BDSG a. F. dieselben Voraussetzungen. Zwar können allgemein zugängliche Daten immer wieder neu erhoben werden, so dass faktisch keine Bindung an diesen Erhebungszweck besteht. Jedoch ist im Rahmen des Verarbeitungsvorgangs der jeweilige Erhebungszweck zu beachten.

977 A. A. *Wolff*, in: Wolff/Brink (Hrsg.), DSR, § 28 Rn. 15.

978 Diese ist im Schrifttum als „recht vage geregelt" bezeichnet worden: *Helbing*, K&R 2015, 145 (147).

979 So aber wohl *Weichert*, ZD 2013, 251 (255), mit der Aussage, dass diese Daten „zweckungebunden" weitere Nutzungen eröffneten.

980 Die Aussage, die Erhebung allgemein zugänglicher Daten unterliege grundsätzlich keinen Beschränkungen ist daher ohne weitere Erläuterungen unglücklich gewählt, so aber wohl missverständlich *Weichert*, ZD 2013, 251 (255), der selbst auf die notwendige Abwägung hinweist, *Weichert*, ZD 2013, 251 (257).

Auch hier lässt eine mögliche Zweckänderung für Forschungszwecke gemäß § 28 Abs. 2 Nr. 3 BDSG a. F. keine Datenverarbeitung auf Vorrat zu.[981]

bb) § 28 Abs. 3 Satz 7 BDSG a. F.

§ 28 Abs. 3 Satz 7 BDSG a. F. bindet den Empfänger an den Übermittlungszweck. Dieser ist dem Empfänger mitzuteilen.[982] Eine Möglichkeit der Zweckänderung ist nicht vorgesehen, so dass der Empfänger an den konkreten Werbezweck gebunden ist. Daher wird diese Regelung in der Literatur mitunter als „echte Zweckbindung" bezeichnet.[983] Letztlich handelt es sich hierbei aber lediglich um die explizite Hervorhebung eines ohnehin geltenden Grundsatzes.[984]

cc) § 28 Abs. 5 BDSG a. F.

§ 28 Abs. 5 Satz 1 BDSG a. F. bindet den Übermittlungsempfänger an den Übermittlungszweck.[985] Hiervon macht aber § 28 Abs. 5 Satz 2 BDSG a. F. bedeutende Ausnahmen. Demnach ist eine Verwendung für andere Zwecke zulässig, wenn bei nicht-öffentlichen Stellen die Voraussetzungen von § 28 Abs. 2 und 3 BDSG a. F. und bei öffentlichen Stellen von § 14 Abs. 2 BDSG a. F. erfüllt sind. Anders als § 28 Abs. 2 BDSG a. F., der der verantwortlichen Stelle nur die Übermittlung und die

981 *Simitis*, in: Simitis (Hrsg.), BDSG, § 28 Rn. 204; zu dieser Problematik im Zusammenhang mit der Forschung: *Bizer*, Forschungsfreiheit, S. 177.

982 *Taeger*, in: Taeger/Gabel (Hrsg.), BDSG, § 28 Rn. 209; *Plath*, in: Plath (Hrsg.), BDSG/DSGVO, § 28 Rn. 153.

983 So *Kramer*, in: Eßer/Kramer/v. Lewinski (Hrsg.), Auernhammer BDSG, § 28 Rn. 132.

984 Vgl. *Simitis*, in: Simitis (Hrsg.), BDSG, § 28 Rn. 246; *Bergmann/Möhrle/Herb*, BDSG, § 28 Rn. 412.

985 Bei Übermittlungen für Werbezwecke geht § 28 Abs. 3 Satz 7 BDSG a. F. vor, vgl. *Kramer*, in: Eßer/Kramer/v. Lewinski (Hrsg.), Auernhammer BDSG, § 28 Rn. 80; *Plath*, in: Plath (Hrsg.), BDSG/DSGVO, § 28 Rn. 204.

Nutzung zu einem anderen Zweck gestattet, ist dem Empfänger jegliche Datenverwendung erlaubt.[986] Die Weite dieser Vorschrift ist auf erhebliche Kritik gestoßen. So sei dies „auf Grund der praktisch grenzenlosen Durchbrechung des Zweckbindungsgrundsatzes nicht nur europarechtlich höchst problematisch".[987] Daher sei § 28 Abs. 5 Satz 2 BDSG a. F. restriktiv auszulegen.[988] Ansonsten werde „der Sinn der Vorschrift – eine Zweckbindung zu erreichen – zunichte gemacht: Der Dritte könnte demnach mit den Daten schalten und walten wie er wollte (…)".[989] Die Zweckbindung des § 28 Abs. 5 Satz 1 BDSG a. F. gehe ins Leere.[990] Sie werde „durchlöchert"[991] oder „faktisch aufgehoben".[992] § 28 Abs. 5 Satz 2 BDSG a. F. sei „eine verfehlte, mit den Grundsätzen des Datenschutzes unvereinbare Regelung".[993] Kritisiert wird, dass der Hinweis auf die Zweckbindung nach § 28 Abs. 5 Satz 3 BDSG a. F. wegen des Hinweises auf die Möglichkeiten der Zweckänderung sein Ziel nicht nur verfehle, sondern das Gegenteil erreiche.[994]

Eine restriktive Auslegung soll im Rahmen der Interessenabwägung durch eine stärkere Gewichtung der schutzwürdigen Betroffeneninteressen erreicht werden.[995] Denn der Betroffene kenne den Dritten nicht und wisse nichts von der beabsichtigten Zweckänderung.[996]

---

986 Die empfangende Stelle erhält also sogar mehr Befugnisse als die übermittelnde Stelle, a. A. wohl *Wedde*, in: Däubler/Klebe/Wedde/Weichert (Hrsg.), BDSG, § 28 Rn. 162, der die gleichen Verarbeitungsmöglichkeiten attestiert; ebenso *Plath*, in: Plath (Hrsg.), BDSG/DSGVO, § 28 Rn. 205.

987 *Bergmann/Möhrle/Herb*, BDSG, § 28 Rn. 493.

988 *Bergmann/Möhrle/Herb*, BDSG, § 28 Rn. 493; *Wolff*, in: Wolff/Brink (Hrsg.), DSR, § 28 Rn. 230.

989 *Bergmann/Möhrle/Herb*, BDSG, § 28 Rn. 496.

990 *Schaffland/Wiltfang*, BDSG, § 28 Rn. 159.

991 *Wolff*, in: Wolff/Brink (Hrsg.), DSR, § 28 Rn. 230.

992 So *Simitis*, in: Simitis (Hrsg.), BDSG, § 28 Rn. 284.

993 *Simitis*, in: Simitis (Hrsg.), BDSG, § 28 Rn. 289.

994 *Taeger*, in: Taeger/Gabel (Hrsg.), BDSG, § 28 Rn. 223.

995 *Bergmann/Möhrle/Herb*, BDSG, § 28 Rn. 497; *Wedde*, in: Däubler/Klebe/Wedde/Weichert (Hrsg.), BDSG, § 28 Rn. 162; ähnlich *Simitis*, in: Simitis (Hrsg.), BDSG, § 28 Rn. 290.

996 *Bergmann/Möhrle/Herb*, BDSG, § 28 Rn. 497.

Es ist in der Tat überraschend, dass der Übermittlungsempfänger in weiterem Umfang zu einer Zweckänderung befugt sein soll, als die übermittelnde Stelle. Dies steht in starkem Kontrast zur nach § 28 Abs. 5 Satz 1 BDSG a. F. grundsätzlich bestehenden Bindung an den Übermittlungszweck. Eine restriktive Auslegung ist daher geboten.

dd) § 28 Abs. 8 BDSG a. F.

§ 28 Abs. 8 BDSG a. F. gestattet eine zweckändernde Nutzung oder Übermittlung besonderer Arten personenbezogener Daten. Hieraus ergibt sich zunächst die grundsätzliche Geltung der Zweckbindung.[997] Die Norm sei „kaum verständlich und in sich widersprüchlich."[998] Der Verweis auf § 28 Abs. 6 Nr. 1 bis 4 und Abs. 7 Satz 1 BDSG a. F. entbehrt eines eigenen Regelungsgehalts.[999] Zum Schutz des RiS sei die Vorschrift möglichst restriktiv auszulegen.[1000]

ee) § 29 Abs. 2 Satz 1, 2 BDSG a. F.

§ 29 Abs. 2 Satz 1 BDSG a. F. bindet die Übermittlung an den „Rahmen" der Zwecke nach § 29 Abs. 1 BDSG a. F. Dabei handele es sich in der Regel „nur um eine Art <Zweckkorridor>".[1001] Durch mehrere Verweise auf § 28 BDSG a. F. wird das dortige Regime zur Zweckbindung und -änderung übernommen. So ist der Empfänger bei zu Werbezwecken übermittelten Daten nach §§ 29 Abs. 1 Satz 2, 29 Abs. 2 Satz 2, 28 Abs. 3 Satz 7 BDSG a. F. an diesen Zweck gebunden.

---

997 *Plath*, in: Plath (Hrsg.), BDSG/DSGVO, § 28 Rn. 217.

998 So *Wedde*, in: Däubler/Klebe/Wedde/Weichert (Hrsg.), BDSG, § 28 Rn. 181; ähnlich *Simitis*, in: Simitis (Hrsg.), BDSG, § 28 Rn. 320.

999 Vgl. *Taeger*, in: Taeger/Gabel (Hrsg.), BDSG, § 28 Rn. 238; *Plath*, in: Plath (Hrsg.), BDSG/DSGVO, § 28 Rn. 217 spricht von einem „Zirkelschluss".

1000 *Wedde*, in: Däubler/Klebe/Wedde/Weichert (Hrsg.), BDSG, § 28 Rn. 181; *Taeger*, in: Taeger/Gabel (Hrsg.), BDSG, § 28 Rn. 238; *Bergmann/Möhrle/Herb*, BDSG, § 28 Rn. 531.

1001 *Ehmann*, in: Simitis (Hrsg.), BDSG, § 29 Rn. 211.

ff) § 39 Abs. 2 BDSG a. F.

Personenbezogene Daten, die einen Berufs- oder besonderen Amtsgeheimnis unterliegen, dürfen gemäß § 39 Abs. 2 BDSG a. F. nur für einen anderen Zweck verwendet werden, wenn ein besonderes Gesetz dies zulässt. In Betracht kommen hier insbesondere Auskunftspflichten gegenüber staatlichen Stellen.[1002] Aufgrund der Subsidiarität des BDSG a. F. hat die Bestimmung lediglich deklaratorischen Charakter.[1003]

d) Zwischenergebnis nicht-öffentlicher Bereich und Sondervorschriften

Im nicht öffentlichen Bereich ist die Möglichkeit von Zweckänderungen ebenfalls begrenzt. Allenfalls für durch eine Übermittlung erhaltene Daten ist nach § 28 Abs. 5 Satz 2 BDSG a. F. eine Zweckänderung in erheblichem Maße möglich. Es bedarf in jedem Falle aber der Bestimmung eines neuen Zwecks und einer Abwägung, weshalb sich zweckoffene Big-Data-Anwendungen nicht darauf stützen lassen.

e) spezialgesetzliche Regelungen

Zu guter Letzt werden noch die spezialgesetzlichen Regelungen bezüglich der Möglichkeit einer Zweckänderung in den Blick genommen.

aa) TMG

§ 12 Abs. 2 TMG legt im Grundsatz fest, dass für die Bereitstellung von Telemedien erhobene personenbezogene Daten für andere Zwecke nur verwendet werden dürfen, soweit das TMG oder eine andere Rechts-

1002 *Plath/Frey*, in: Plath (Hrsg.), BDSG/DSGVO, § 39 Rn. 14; *Uwer*, in: Wolff/Brink (Hrsg.), DSR, § 39 Rn. 39 f.
1003 *Greve*, in: Eßer/Kramer/v. Lewinski (Hrsg.), Auernhammer BDSG, § 39 Rn. 16.

vorschrift, die sich ausdrücklich auf Telemedien bezieht, dies gestattet.[1004]

Im TMG finden sich Zweckänderungsvorschriften zur Übermittlung an Strafverfolgungsbehörden in § 14 Abs. 2 TMG, der auch für Nutzungsdaten über § 15 Abs. 5 Satz 4 TMG Anwendung findet. Zudem ist die Sperrung in § 15 Abs. 4 Satz 2 TMG zur Erfüllung von Aufbewahrungspflichten und die Speicherung zum Zweck der Rechtsverfolgung in § 15 Abs. 8 TMG vorgesehen. Eine Vorschrift außerhalb des TMG, die sich ausdrücklich auf Telemedien bezieht und eine Zweckänderung gestattet, ist nicht ersichtlich.[1005] Für präventiv-polizeiliche Zwecke ähnele § 14 Abs. 2 TMG einer „Blankettermächtigung".[1006]

bb) TKG

Das TKG sieht mit Ausnahme von Adressdaten, die im Rahmen einer Widerspruchslösung für Werbezwecke und Marktforschung verwendet werden dürfen, § 95 Abs. 2 Satz 2 TKG, keine gesetzlichen Zweckänderungsmöglichkeiten vor. Vielmehr ist §§ 95 Abs. 2 Satz 1 und 96 Abs. 3 Satz 1 TKG zu entnehmen, dass eine Zweckänderung nur aufgrund einer Einwilligung möglich ist.

cc) strenge Zweckbindung im MsbG

Auch das MsbG sieht eine strenge Zweckbindung vor. Eine Verwendung zu einem anderen Zweck kann nur auf eine Einwilligung gestützt werden, wie sich aus § 50 Abs. 1 MsbG ergibt.

1004 Hieran scheiterte beispielsweise ein Auskunftsanspruch des Geschädigten gegenüber dem Betreiber einer Bewertungsplattform, siehe BGH, Urteil v. 1.7.2014, VI ZR 345/13, ZD 2014, 520 (521) Rn. 10 ff.

1005 *Moos*, in: Taeger/Gabel (Hrsg.), BDSG, § 12 TMG Rn. 26.

1006 So *Dix/Schaar*, in: Roßnagel (Hrsg.), BeckRTD Kommentar, § 14 TMG Rn. 63.

dd) § 13 Abs. 2 GenDG

Das GenDG sieht in § 13 Abs. 2 GenDG neben der Möglichkeit einer Einwilligung in die Verwendung zu anderen Zwecken auch eine zweckändernde Verwendung aufgrund gesetzlicher Erlaubnis vor.

ee) § 46 LKHG BW

§ 46 Abs. 1 Satz 1 Nr. 2a LKHG BW gestattet die Übermittlung und damit Zweckänderung von Patientendaten zur Durchführung medizinischer Forschung des Krankenhauses. Nach § 46 Abs. 1 Satz 2 LKHG BW ist aber Voraussetzung, dass dies nicht mit anonymisierten Daten geschehen kann und nicht überwiegende schutzwürdige Interessen entgegenstehen.

ff) § 37 Abs. 1 Satz 2 PolG BW

Abschließend sei noch § 37 Abs. 1 Satz 2 PolG BW erwähnt, der eine Speicherung, Veränderung und Nutzung zu einem anderen Zweck zulässt, soweit die Polizei die Daten zu diesem Zweck erheben dürfte.

f) Zwischenergebnis spezialgesetzliche Regelungen

Die hier betrachteten spezialgesetzlichen Regelungen enthalten teilweise Möglichkeiten der Zweckänderung. Vielfach ist hierfür aber eine Einwilligung erforderlich. In jedem Falle bedarf es der Festlegung eines neuen Zwecks, da sonst eine im Rahmen der Normen häufig vorzunehmende Abwägung und ein Vergleich der Zwecke nicht möglich wären.

g) Einwilligung

Auch eine Einwilligung in die Datenverwendung zu einem anderen Zweck als dem Erhebungszweck ist möglich. Allerdings sind dann die Erfordernisse einer informierten Einwilligung zu beachten.[1007] Daher stoßen Big-Data-Analysen abermals an das Problem einer konkreten Definition des Zwecks sofern sich dieser erst aus dem Ergebnis der Auswertung ergibt, da eine informierte Einwilligung mangels hinreichender Information über den Verarbeitungszweck nicht vorliegt und eine Verarbeitung daher nicht auf eine Einwilligung gestützt werden kann.[1008]

7. Ergebnis

Es sind zwar vielfältige Zweckänderungen möglich, aber um die Zulässigkeit einer Zweckänderung prüfen zu können, ist aufgrund der Abwägungsklauseln eine konkrete Zweckfestlegung notwendig. Eine Einwilligung in eine Zweckänderung ist zwar ebenfalls möglich, aber nur wirksam, sofern der neue Verarbeitungszweck hinreichend konkretisiert ist.

IV. Die Datenschutz-Grundverordnung

Mit der DSGVO gilt ab dem 25. Mai 2018 ein einheitliches Datenschutzrecht in der EU. Auch die DSGVO legt sich nicht eindeutig auf ein absolutes oder relatives Verständnis des Personenbezugs von Daten fest.[1009] Neu ist, dass das „singling out“ (dt.: Aussondern) in ErwG 26 Satz 3 DSGVO Eingang gefunden hat und auch in Art. 4 Nr. 1 DSGVO mit dem Abstellen auf eine Identifikation durch Zuordnung zu einer Ken-

1007 Siehe D. III. 1. a) bb), S. 157 ff.

1008 So bereits zu Data Warehousing und Data Mining: *Baeriswyl*, RDV 2000, 6 (8); *Büllesbach*, CR 2000, 11 (15); zu Big Data *Arming*, K&R Beihefter 3/2015 zu Heft 9 2015, 7 (10).

1009 *Schantz*, NJW 2016, 1841 (1843).

nung ein weitgehenderes Verständnis des Personenbezugs als bisher angelegt ist.[1010] Damit ist eine bereits seit längerer Zeit vertretene Auffassung kodifiziert worden.[1011] Als Argument für dieses Verständnis werden insbesondere eine vergleichbare Gefährdungslage und der Schutzzweck des Datenschutzrechts angeführt.[1012]

1. Entstehungsgeschichte der Zweckbindung in der DSGVO

Über die Formulierung der Zweckbindung in der DSGVO herrschte erheblicher Streit, wie den verschiedenen Entwürfen im Laufe des Gesetzgebungsverfahrens zu entnehmen ist.[1013]

Umstritten war insbesondere die Zulässigkeit einer Weiterverarbeitung im Falle einer Unvereinbarkeit des Weiterverarbeitungs- und des Erhebungszwecks. Die EU-Kommission hatte in ihrem Entwurf[1014] in Art. 6 Abs. 4 DSGVO-E-Komm vorgesehen, dass in diesem Falle eine Stützung

---

1010 Ausführlicher Überblick bei *Schantz*, in: Schantz/Wolff (Hrsg.), DSGVO, Rn. 291 ff.

1011 Für Cookies siehe *Artikel-29-Datenschutzgruppe*, WP 188, S. 9; zum behavioral targeting siehe *Artikel-29-Datenschutzgruppe*, WP 136, S. 16 f., die auch ohne Zuordnung zu einer Person von einem Personenbezug ausgeht; ähnlich *Karg*, ZD 2012, 255 (259), der insbesondere wegen mit dem Merkmal des Personenbezugs nicht erfassbaren Webtrackings auf ein sog. personenbezogenes Verfahren abstellt, das bereits dann vorliege, wenn die Zielsetzung des Verfahrens eine Auswirkung auf eine Person habe.

1012 *Zuiderveen Borgesius*, CLSR 32 (2016), 256 (267 ff.), der aber nicht überzeugend zum Schutzweck des Datenschutzrechts auch „eine Datenverarbeitung nach Treu und Glauben" gemäß Art. 6 Abs. 1 lit. a DSRL zählt, der er ein Erfordernis der Fairness entnimmt.

1013 Vgl. *Albrecht*, CR 2016, 88 (92); siehe zu den verschiedenen Vorschlägen für die Formulierung der Zweckbindung: *de Hert/Papakonstantinou*, CLSR 32 (2016), 179 (185 f.); Überblick bei *Albers*, in: Wolff/Brink (Hrsg.), DSR, Art 6 Rn. 10.

1014 Vorschlag für Verordnung des europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Grundverordnung), vom 25. Januar 2012, Kom (2012) 11 endgültig.

auf eine der Rechtsgrundlagen in Art. 6 Abs. 1 lit. a-e DSGVO-E-Komm zulässig sein solle. Es wurde kritisiert, dass hierdurch eine allgemeine Ausnahme vom Zweckbindungsgrundsatz gemacht werde, die die Anwendbarkeit des Kompatibilitätstests erheblich einschränke,[1015] weshalb diese Bestimmung gestrichen werden solle.[1016] Von Seiten deutscher Datenschutzaufsichtsbehörden wurde nach Veröffentlichung des Kommissionsentwurfs gefordert, dass festgestellt werden müsse, dass die Zweckvereinbarkeit der deutschen Umsetzung der Zweckbindung im nationalen Datenschutzrecht entspreche.[1017]

Das EU-Parlament strich in seinem Entwurf[1018] Art. 6 Abs. 4 DSGVO-E-Komm komplett. Der Rat sah in Art. 6 Abs. 3a DSGVO-E-Rat[1019] Kriterien für die Feststellung der Zweckvereinbarkeit vor. Sofern der Weiterverarbeitungszweck unvereinbar mit dem Erhebungszweck ist, sollte nach Art. 6 Abs. 4 DSGVO-E-Rat für dieselbe verantwortliche Stelle entsprechend des Kommissionsvorschlags eine Weiterverarbeitung bei Vorliegen einer der Rechtsgrundlagen aus Art. 6 Abs. 1 lit. a-e DSGVO-E-Rat zulässig sein. Zudem war die Möglichkeit einer Weiterverarbeitung aufgrund einer Interessenabwägung vorgesehen, sofern das Interesse der erhebenden Stelle oder eines Dritten die Interessen der betroffenen Person überwiegen. Es wurde also eine noch weitergehende Ausnahme von der Zweckbindung vorgesehen. Der Vorschlag des Rates, der eine erhebliche Aufweichung des Zweckbindungsprinzips vorsah, ist auf erhebliche Kri-

---

1015 *Artikel-29-Datenschutzgruppe*, WP 203, S. 36.

1016 *Artikel-29-Datenschutzgruppe*, WP 203, S. 37.

1017 *Datenschutzkonferenz des Bundes und der Länder*, Stellungnahme DSGVO-Komm, S. 7.

1018 Legislative Entschließung des Europäischen Parlaments vom 12. März 2014 zu dem Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (allgemeine Datenschutzgrundverordnung), Dokument Nr. P7_TA(2014)0212.

1019 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) - Vorbereitung einer allgemeinen Ausrichtung, Dokument Nr. 9565/15.

tik gestoßen.[1020] An der Möglichkeit einer Zweckänderung auch ohne Zweckkompatibilität im Ratsentwurf wurde kritisiert, dass zweifelhaft sei, ob überhaupt eine Interessenabwägung wegen der Zweckänderung stattgefunden habe, da die Kriterien dieselben wie bei einer Erhebung sind.[1021] Der Ratsentwurf habe mit der Möglichkeit einer Zweckdurchbrechung aufgrund einer Interessenabwägung eine „(echte) Durchbrechung des Zweckbindungsgrundsatzes" vorgesehen.[1022] Bezüglich der Privilegierung von Datenverarbeitungen zu statistischen, historischen und wissenschaftlichen Zwecken äußerte die Konferenz der Datenschutzbeauftragten des Bundes und der Länder Kritik am Entwurf des Rates, da eine Verarbeitung zu einem anderen Zweck nahezu schrankenlos ermöglicht werde.[1023] Wie auch im Kommissionsentwurf wurde im Ratsentwurf auf ein alternatives Verhältnis von Rechtsgrundlage und Zweckkompatibilität abgestellt.[1024] Diese Änderung gegenüber der DSRL stieß auf Kritik.[1025]

1020 So sprachen sich z. B. *Voßhoff/Hermerschmidt*, DANA 2015, 117 für eine Beibehaltung der Zweckbindung in der bis dahin geltenden Form aus; ebenso für die Konferenz der Datenschutzbeauftragen des Bundes und der Länder: *Ronellenfitsch/Schriever-Steinberg/Berg*, DANA 2015, 126.

1021 *v. Grafenstein*, DuD 2015, 789 (795); bezüglich der entsprechenden Regelung im Kommissionsentwurf hatte dies bereits der Europäische Datenschutzbeauftragte moniert: *Europäischer Datenschutzbeauftragter*, Stellungnahme DSGVO März 2012, Rn. 121; siehe auch *de Hert/Papakonstantinou*, CLSR 28 (2012), 130 (135), die darüber hinaus bemängeln, dass bereits bisher die Zweckvereinbarkeit durch weite Zweckfestlegungen ausgehebelt worden sei.

1022 *Gola/Schulz*, K&R 2015, 609 (614).

1023 *Datenschutzkonferenz des Bundes und der Länder*, DuD 2015, 722.

1024 *Albers*, in: Wolff/Brink (Hrsg.), DSR, Art. 6 Rn. 10.

1025 *Artikel-29-Datenschutzgruppe*, WP 203, S. 36, die dies auch auf Art. 13 DSRL stützt, der durch die Möglichkeit der Mitgliedstaaten zu Ausnahmen von Art. 6 Abs. 1 DSRL die Notwendigkeit des kumulativen Vorliegens zeige; siehe auch *Europäischer Datenschutzbeauftragter*, Stellungnahme DSGVO März 2012, Rn. 123 f., unter Verweis auf einen Verstoß gegen Art. 5 der Konvention 108 des Europarats; *Europäischer Datenschutzbeauftragter*, Opinion 3/2015, S. 5.

2. wichtige Normen

Die Zweckbindung findet sich in einer Vielzahl von Normen der DSGVO.[1026] Im Folgenden wird auf die Wichtigsten eingegangen.

a) Art 5 DSGVO

Zentrale Norm für die Zweckbindung in der DSGVO ist Art. 5 Abs. 1 lit. b DSGVO. Dieser lautet:

(1) Personenbezogene Daten müssen (…)

> b) für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden; eine Weiterverarbeitung für im öffentlichen Interesse liegende Archivzwecke, für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke gilt gemäß Artikel 89 Absatz 1 nicht als unvereinbar mit den ursprünglichen Zwecken („Zweckbindung“);

Die Definition der Zweckbindung entspricht im Wesentlichen der Definition in der DSRL. Die Verwendung einer doppelten Negation für die Frage der Vereinbarkeit der Weiterverarbeitung mit dem ursprünglichen Erhebungszweck zeige, dass der Gesetzgeber der Weiterverarbeitung zu anderen Zwecken etwas Flexibilität einräumen wollte.[1027] Die negative Formulierung der Zweckvereinbarkeit führe zu einer Umkehrung der Darlegungslast und damit zu einer Erschwerung der Verwirklichung der Zweckbindung.[1028]

1026 Eine kurze Übersicht bietet *Dammann*, ZD 2016, 307 (311).

1027 *Artikel-29-Datenschutzgruppe*, WP 203, S. 21; zustimmend: *Bygrave*, Data Privacy Law, S. 156; *Schantz*, in: Wolff/Brink (Hrsg.), DSR, Art. 5 DSGVO Rn. 18.

1028 *Frenzel*, in: Paal/Pauly (Hrsg.), DSGVO-Kommentar, Art. 5 Rn. 30.

Anknüpfungspunkt der Zweckvereinbarkeit ist die Weiterverarbeitung der Daten nach der Erhebung. Für die insoweit wortgleiche DSRL wird vertreten, dass sie nicht kleinteilig zwischen der Zulässigkeit einzelner Verarbeitungsschritte unterscheide, da auf die Weiterverarbeitung abgestellt werde.[1029] Der Wortlaut zeigt aber, dass jede auf die Erhebung folgende Verarbeitung als Weiterverarbeitung zu verstehen ist,[1030] weshalb die Zweckkompatibilität für jeden weiteren Verarbeitungsschritt zu prüfen ist.[1031] Aufgrund der Anknüpfung an die „Weise" kann selbst die Verarbeitung zum Erhebungszweck inkompatibel sein, sofern sich die Umstände erheblich verändert haben.[1032]

Die grundsätzliche Erlaubnis der Weiterverarbeitung von Daten für historische, statistische oder wissenschaftliche Zwecke, sofern entsprechende Garantien der Mitgliedstaaten vorliegen, ist nicht als Ausnahme vom Grundsatz der Zweckvereinbarkeit zu verstehen,[1033] sondern eine Konkretisierung dieses Prinzips, weshalb auch andere Fälle einer Vereinbarkeit der Zwecke denkbar sind.[1034]

Umstritten ist die Frage, wie konkret die Zwecke definiert werden müssen. Zwar seien Blankettformeln zur Zweckfestlegung ausgeschlossen, „(…) unbestimmte, aber bestimmbare Begriffe innerhalb einer

---

1029 *Härting*, NJW 2015, 3284 (3288).

1030 *Heberlein*, in: Ehmann/Selmayr (Hrsg.), DSGVO, Art. 5 Rn. 16.

1031 So bezüglich der DSRL die *Artikel-29-Datenschutzgruppe*, WP 203, S. 21; Kritisch hierzu *Herbst*, in: Kühling/Buchner (Hrsg.), DSGVO, Art. 5 Rn. 39, der darauf hinweist, dass eine Erhebung immer im Hinblick auf einen daran anschließenden Verarbeitungsvorgang stattfindet, weshalb es naheläge von einer Weiterverarbeitung nur bei einer Verarbeitung zu einem anderen Zweck als dem Erhebungszweck auszugehen. Wie *Herbst* korrekt anmerkt, handelt es sich aber nur um einen terminologischen Streit, ohne dass andere Ergebnisse erzielt würden.

1032 *Schantz*, in: Wolff/Brink (Hrsg.), DSR, Art. 5 DSGVO Rn. 20; a. A. *Herbst*, in: Kühling/Buchner (Hrsg.), DSGVO, Art. 5 Rn. 39 f., der eine Weiterverarbeitung nur bei einer Verarbeitung zu einem anderen Zweck annehmen will, da die Erhebung nicht isoliert betrachtet werden könne, sondern immer für eine weitere Verarbeitung erfolge.

1033 *Artikel-29-Datenschutzgruppe*, WP 203, S. 28.

1034 *Artikel-29-Datenschutzgruppe*, WP 203, S. 13.

Zweckbestimmung mit einer hinreichenden Quantität und Qualität (Gestaltungshöhe) jedoch nicht.“[1035] Diese Aussage ist genauso richtig wie inhaltslos, da ein konkreter Maßstab hieraus nicht abgeleitet werden kann. Die verantwortliche Stelle könne den Zweck weit fassen; eine präzise, aber weite Zweckfestlegung sei zulässig.[1036] Dies setzt aber voraus, dass der Zweck hinreichend konkret ist. Big Data ist mangels „Trennschärfe“ kein hinreichend konkretisierter Zweck.[1037] Die Kompatibilitätsprüfung erfordert ebenfalls einen konkreten Zweck.[1038] Das Erfordernis einer eindeutigen Zweckfestlegung spricht für eine enge Zweckbestimmung.[1039] Nur hierdurch kann die Funktion der Zweckbestimmung zur Umgrenzung der Verarbeitungsmöglichkeiten auf einen überschaubaren und überprüfbaren Rahmen gewährleistet werden.[1040] In systematischer Hinsicht wird dieses Auslegungsergebnis durch das Prinzip der Transparenz[1041] und die Privilegierung der wissenschaftlichen Forschung trotz weiter Zweckfestlegung bei Einhaltung ethischer Standards in ErwG 33 DSGVO ge-

---

1035 *Frenzel*, in: Paal/Pauly (Hrsg.), DSGVO-Kommentar, Art. 5 Rn. 27.

1036 *Härting*, NJW 2015, 3284 (3286 f.), der im Folgenden aber selbst feststellt, dass der Zweck maßgeblicher Bezugspunkt für Abwägungen ist.

1037 Vgl. *Franck*, in: Gola (Hrsg.), DSGVO, Art. 13 Rn. 11.

1038 *Ehmann*, ZD 2015, 6 (10), der die Positionen von *Jochen Schneider und Michael Will* wiedergibt. Für eine präzise Angabe des Zwecks zur Verhinderung des Leerlaufens der Kompatibilitätsprüfung sprechen sich auch aus: *Roßnagel/Nebel/Richter*, ZD 2015, 455 (457 f.).

1039 *Schantz*, NJW 2016, 1841 (1843); ebenso *Pötters*, in: Gola (Hrsg.), DSGVO, Art. 5 Rn. 14 in Anknüpfung an andere Sprachfassungen, die das Wort „explizit“ enthalten, das er mit „konkret“ gleichsetzt; a. A. aber *Härting*, DSGVO, Rn. 95, der davon ausgeht, dass der Verantwortliche dies selbst festlegen könne, wobei er zumindest das Problem der Darlegung eines berechtigten Interesses bei einer weiten Zweckfestlegung sieht. A. A. wohl auch *Monreal*, ZD 2016, 507 (509), der hierunter eine Pflicht zum Erklären sieht unter Berufung auf die *Artikel-29-Datenschutzgruppe*, WP 203, S. 17. Dieses Verständnis steht allerdings einer konkreten Zweckfestlegung nicht entgegen, siehe *Schantz*, in: Wolff/Brink (Hrsg.), DSR, Art. 5 Rn. 16.

1040 Vgl. *Herbst*, in: Kühling/Buchner (Hrsg.), DSGVO, Art. 5 Rn. 22; vgl. auch *Heberlein*, in: Ehmann/Selmayr (Hrsg.), DSGVO, Art. 5 Rn. 14, der unter anderem auf die Erfüllung der Nachweispflicht nach Art. 24 Abs. 1 DSGVO hinweist.

1041 Siehe ErwG 39 DSGVO, der die Bedeutung der Information über den Verarbeitungszweck hervorhebt.

stützt.[1042] Der nötige Präzisionsgrad hängt von den Umständen des Einzelfalls und den daraus folgenden Gefahren für den Betroffenen ab.[1043]

Die Zwecke müssen legitim sein. Das Wort „legitimate“ wurde bisher mit „rechtmäßig“ übersetzt. Ob damit eine Bedeutungsänderung beabsichtigt ist, ist zweifelhaft.[1044]

aa) Streit um eine Privilegierung von Big Data als Statistik

Umstritten ist, ob sich Big-Data-Analysen unter den Begriff der Statistik subsumieren lassen und damit in den Genuss der Privilegierung des Art. 5 Abs. 1 lit. b DSGVO kommen.

Möglich sei eine Auslegung von Art. 5 DSGVO demnach auch Big-Data-Analysen unter den Begriff der Statistik fallen, da die Statistik auch als ein Verfahren unabhängig von den damit verfolgten Zwecken verstanden werden könne.[1045] Aus Art. 89 Abs. 2 und 3 DSGVO ergebe sich, dass sich das öffentliche Interesse nur auf die Archive und damit nicht auf die Statistik beziehe.[1046] Dieser Schluss sei zugleich Art. 21 Abs. 6 DSGVO e contrario zu entnehmen. Für Art. 6 Abs. 1 lit. b Satz 2 DSRL wird vertreten, dass z. B. Big-Data-Analysen zum Zweck der Marktforschung unter den Begriff der Statistik fallen.[1047]

1042 *Schantz*, NJW 2016, 1941 (1943 f.); teils wird gefordert, dass von der Privilegierung der Forschung bei Zweckfestlegung nur „zurückhaltend Gebrauch“ gemacht werden solle, so *Stemmer*, in: Wolff/Brink (Hrsg.), DSR, Art. 7 DSGVO Rn. 78.

1043 Vgl. *Schantz*, in: Wolff/Brink (Hrsg.), DSR, Art. 5 DSGVO Rn. 15.

1044 Dafür *Schantz*, in: Wolff/Brink (Hrsg.), DSR, Art. 5 Rn. 17, der sich für eine Konformität mit der Rechtsordnung insgesamt ausspricht; *Reimer*, in: Sydow (Hrsg.), DSGVO, Art. 5 Rn. 22; dagegen: *Herbst*, in: Kühling/Buchner (Hrsg.), DSGVO, Art. 5 Rn. 37, der auf die Rechtmäßigkeit abstellt.

1045 *Richter*, DuD 2015, 735 (738).

1046 *Albrecht/Jotzo*, DSGVO, Teil 3 Rn. 71.

1047 So *Artikel-29-Datenschutzgruppe*, WP 203, S. 29; kritisch hierzu *Richter*, DuD 2015, 735 (738), der dies als „zumindest zweifelhaft“ bezeichnet, da die

Für die privilegierten Zwecke (im öffentlichen Interesse liegende Archivzwecke, wissenschaftliche oder historische Forschungszwecke, statistische Zwecke) sind „geeignete Garantien" gemäß Art. 89 Abs. 1 DSGVO vorgesehen.[1048] Insbesondere soll der Grundsatz der Datenminimierung gewährleistet und hierzu geprüft werden, ob die Verarbeitung auch mit pseudonymen oder anonymen Daten möglich ist. Eine Privilegierung von Big-Data-Analysen als Unterfall der Statistik komme daher nicht in Betracht.[1049] Allerdings schließt Art. 89 Abs. 1 DSGVO eine personenbezogene Verarbeitung nicht aus, sondern fordert lediglich Schutzmaßnahmen für die Rechte und Freiheiten der Betroffenen. Deshalb vermag dieses Argument nicht zu überzeugen.

Die privilegierten Verarbeitungszwecke seien als Ausnahmetatbestände eng auszulegen,[1050] weshalb sich Big-Data-Analysen nicht unter den Zweck „Statistik" fassen ließen.[1051] Gegen eine Subsumtion von Big-Data-Analysen unter den Begriff der Statistik wird eingewandt, dass dies zur „Abschaffung der Zweckbindung" führe.[1052] Unter Statistik sei nur die amtliche Statistik zu verstehen, wie sich aus ErwG 163 DSGVO ergebe.[1053] Dies vermag nicht zu überzeugen, da ErwG 163 DSGVO lediglich besondere Vorgaben für die amtliche Statistik im Anschluss an die allgemeine Definition dieses Begriffs in ErwG 162 DSGVO enthält.

Systematik für eine Privilegierung lediglich öffentlicher Zwecke sprechen könne.

1048 Anders noch im Ratsentwurf, der Garantien nur bei einer Abweichung von Betroffenenrechten vorsah, siehe *Richter*, DuD 2015, 735 (737).

1049 Vgl. *Buchner*, DuD 2016, 155 (157).

1050 *Ziegenhorn/v. Heckel*, NVwZ 2016, 1585 (1589).

1051 *Schantz*, NJW 2016, 1841 (1842).

1052 So *Roßnagel/Nebel/Richter*, ZD 2015, 455 (458), die daher Big-Data-Analysen, deren Ergebnisse Informationen über eine betroffene Person enthalten nicht unter den Begriff der Statistik fassen, sondern diesen vielmehr als Ziel der Datenverarbeitung und nicht als Methoden verstanden wissen wollen; *Culik/Döpke*, ZD 2017, 226 (230), sprechen von einer „systemwidrigen Aushöhlung".

1053 *Frenzel*, in: Paal/Pauly (Hrsg.), DSGVO-Kommentar, Art. 5 Rn. 32.

bb) Stellungnahme

In ErwG 162 DSGVO ist nunmehr der Begriff der Statistik definiert. Demnach ist unter statistischen Zwecken „jeder für die Durchführung statistischer Untersuchungen und die Erstellung statistischer Ergebnisse erforderliche Vorgang der Erhebung und Verarbeitung personenbezogener Daten zu verstehen." Es wird vorausgesetzt, „dass die Ergebnisse der Verarbeitung zu statistischen Zwecken keine personenbezogenen Daten, sondern aggregierte Daten sind und diese Ergebnisse oder personenbezogenen Daten nicht für Maßnahmen oder Entscheidungen gegenüber einzelnen natürlichen Personen verwendet werden." Big-Data-Analysen mit personenbezogenen Ergebnissen können somit nicht unter den Begriff der Statistik subsumiert werden. Fraglich ist aber, ob Analysen deren Ergebnis nicht personenbezogene Daten sind, die aber einer Person zugeordnet werden unter den Begriff der Statistik gefasst werden können. Es kommt also entscheidend darauf an, was unter „Maßnahmen oder Entscheidungen gegenüber einzelnen natürlichen Personen" zu verstehen ist. Möglich wäre ein Verständnis, das nur rechtsverbindliche oder erheblich beeinträchtigende Entscheidungen hierunter fassen will.[1054] Dagegen spricht aber, dass dem Begriff der Maßnahme neben der Entscheidung ein Anwendungsbereich verbleiben muss. Dies spricht dafür, dass hierunter jegliche Handlungen zu fassen sind die sich gegenüber einer Person auswirken, so dass z. B. auch die statistische Auswertung zu Werbezwecken hierunter gefasst werden kann.[1055] Diese Auslegung wird durch die Erwägung gestützt, dass durch die Zuordnung zu einer Person ein Personenbezug hergestellt wird, weshalb das Datenschutzrecht Anwendung findet.[1056] Unter die Statistik lässt sich also z. B. eine Auswertung von Besuchen einer Internetseite auf Grundlage aggregierter Daten fassen, nicht

1054 Siehe die Darstellung bei *Richter*, in: Roßnagel (Hrsg.), DSGVO, § 4 Rn. 104.
1055 Vgl. *Richter*, in: Roßnagel (Hrsg.), DSGVO, § 4 Rn. 104.
1056 Vgl. *Richter*, DuD 2016, 581 (583), der zudem auf das Verbot der Anwendung statistischer Ergebnisse zur Herstellung eines Personenbezugs nach § 21 BStatG hinweist.

aber die Ermittlung eines individuellen Versicherungstarifs aufgrund des Fahrverhaltens der versicherten Person.[1057]

b) Art. 6 DSGVO – insbesondere die Kriterien der Zweckvereinbarkeit

Art. 6 DSGVO nennt die Rechtsgrundlagen für eine Verarbeitung personenbezogener Daten. Für die Zweckbindung ist von Interesse, dass Art. 6 Abs. 3 DSGVO der EU oder den Mitgliedstaaten die Möglichkeit eröffnet, für die Rechtsgrundlagen nach Art. 6 Abs. 1 lit. c und e DSGVO spezifische Bedingungen für die Zweckbindung zu regeln.

Von zentraler Bedeutung für die Feststellung der Zweckkompatibilität ist Art. 6 Abs. 4 DSGVO. Dieser lautet:

(4) Beruht die Verarbeitung zu einem anderen Zweck als zu demjenigen, zu dem die personenbezogenen Daten erhoben wurden, nicht auf der Einwilligung der betroffenen Person oder auf einer Rechtsvorschrift der Union oder der Mitgliedstaaten, die in einer demokratischen Gesellschaft eine notwendige und verhältnismäßige Maßnahme zum Schutz der in Artikel 23 Absatz 1 genannten Ziele darstellt, so berücksichtigt der Verantwortliche – um festzustellen, ob die Verarbeitung zu einem anderen Zweck mit demjenigen, zu dem die personenbezogenen Daten ursprünglich erhoben wurden, vereinbar ist – unter anderem

a) jede Verbindung zwischen den Zwecken, für die die personenbezogenen Daten erhoben wurden, und den Zwecken der beabsichtigten Weiterverarbeitung,

b) den Zusammenhang, in dem die personenbezogenen Daten erhoben wurden, insbesondere hinsichtlich des Verhältnisses zwischen den betroffenen Personen und dem Verantwortlichen,

1057 Vgl. *Laue/Nink/Kremer*, Datenschutz in der betrieblichen Praxis, § 1 Rn. 119.

c) die Art der personenbezogenen Daten, insbesondere ob besondere Kategorien personenbezogener Daten gemäß Artikel 9 verarbeitet werden oder ob personenbezogene Daten über strafrechtliche Verurteilungen und Straftaten gemäß Artikel 10 verarbeitet werden,

d) die möglichen Folgen der beabsichtigten Weiterverarbeitung für die betroffenen Personen,[1058]

e) das Vorhandensein geeigneter Garantien, wozu Verschlüsselung oder Pseudonymisierung gehören kann.

Art. 6 Abs. 4 DSGVO führt zu zwei Streitfragen.[1059] Einerseits ist umstritten, ob es sich lediglich um das zusätzliche Erfordernis eines Kompatibilitätstests handelt oder zugleich eine Rechtsgrundlage für eine zweckändernde Datenverarbeitung vorliegt. Anderseits stellt sich die Frage, wie weit die Öffnungsklausel für nationale Rechtssetzungen zu verstehen ist.

Umstritten ist ob es sich bei der Regelungsbefugnis der Union oder der Mitgliedstaaten um eine genuine Öffnungsklausel handelt oder lediglich an eine bereits bestehende Kompetenz angeknüpft wird.[1060] Eine weitreichende Aufweichung der Zweckbindung im mitgliedstaatlichen Recht erscheint aufgrund der Öffnungsklausel möglich. Es bleibt also abzuwarten in welcher Weise von den Mitgliedstaaten von dieser Befugnis Gebrauch gemacht werden wird. In Deutschland ist dies mit dem BDSG 2018 be-

---

1058 *Veil*, ZD 2015, 347 (349) bezeichnet dies als risikobasierten Ansatz; auch der Europarat spricht sich für die Berücksichtigung der Risiken der Weiterverarbeitung für einen neuen Zweck für den Betroffenen und deren eventuelle Unzulässigkeit aus: *Europarat*, Guidelines Big Data, S. 4 Punkt 3.1 und 3.2.

1059 Siehe *Albers*, in: Wolff/Brink (Hrsg.), DSR, Art. 6 DSGVO Rn. 4.

1060 Für ein weites Verständnis *Ziegenhorn/v. Heckel*, NVwZ 2016, 1585, 1590f; *Nebel*, in: Roßnagel (Hrsg.), DSGVO, § 3 Rn. 97; restriktiv im Hinblick auf Befugnisse nach Art. 6 Abs. 1-3 DSGVO: *Kühling/Martini*, EuZW 2016, 448 (451). Übersicht zu den unterschiedlichen Ansichten bei *Albers*, in: Wolff/Brink (Hrsg.), DSR, Art. 6 DSGVO Rn. 71; *Buchner/Petri*, in: Kühling/Buchner (Hrsg.), DSGVO, Art. 6 Rn. 200 gehen davon aus, dass eine Regelungskompetenz nur in Anknüpfung an Art. 6 Abs. 2 u. 3 DSGVO gegeben sein kann.

reits geschehen.[1061] In den §§ 23 ff. BDSG 2018 wird öffentlichen und nicht-öffentlichen Stellen unabhängig vom Vorliegen einer Zweckkompatibilität die Datenverarbeitung zu anderen Zwecken als dem Erhebungszweck gestattet. Die Normen orientieren sich inhaltlich ersichtlich an den bislang in § 14 Abs. 2 BDSG a. F. bzw. § 28 Abs. 2 BDSG a. F. normierten Regelungen.[1062] Der Bundesgesetzgeber hält damit an dem bisherigen Konzept gesetzlich normierter Ausnahmen von der Zweckbindung fest. Durch diese Regelungen wird die Zweckbindung gegenüber der DSGVO weiter aufgelockert. Vor dem Hintergrund einer recht großzügigen Möglichkeit der Zweckänderung in der DSGVO ist dies durchaus kritisch zu sehen. Ob die vom deutschen Gesetzgeber vorgenommene Stützung auf Art. 6 Abs. 4 DSGVO[1063] in Anbetracht bereits im Gesetzgebungsverfahren von verschiedener Seite vorgebrachter Kritik[1064] die Regelungen trägt, ist zweifelhaft.

Eine wesentliche Veränderung gegenüber der DSRL ist, dass nun eine Einwilligung zur Weiterverarbeitung zu einem anderen Zweck ausreicht und die Zweckkompatibilität dann nicht mehr zu prüfen ist.[1065] Dies wird einer informationellen Selbstbestimmung besser gerecht als das bisherige Modell, das zum Schutz des Betroffenen trotz Einwilligung nach einer Zweckvereinbarkeitsprüfung verlangte.[1066]

1061 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) vom 30. Juni 2017, BGBl. Teil 1, 2017, 2097.

1062 Dies gibt auch die Bundesregierung in ihrer Gesetzesbegründung an: BT-Drs. 18/11325, S. 95 f.

1063 BT-Drs. 18/11325, S. 96.

1064 Siehe hierzu: *Albers*, in: Wolff/Brink (Hrsg.), DSR, Art. 6 Rn. 72.

1065 Vgl. *Reimer*, in: Sydow (Hrsg.), DSGVO, Art. 5 Rn. 28; der auf ErwG 50 Abs. 2 Satz 1 DSGVO abstellt. Nicht überzeugend ist demgegenüber die Ansicht, dass sich Art. 6 Abs. 4 DSGVO nicht klar entnehmen lasse, ob es in diesem Falle der Prüfung einer Kompatibilität bedürfe, da nur die Prüfung der dortigen Kriterien ausgeschlossen sei, so aber *Herbst*, in: Kühling/Buchner (Hrsg.), DSGVO, Art. 5 Rn. 46 f., der sich aber für ein Genügen der Einwilligung ausspricht, da auch eine Neuerhebung aufgrund einer Einwilligung möglich sei.

1066 D. II. 2. a) bb) (3), S. 122.

aa) Maßstab für die Prüfung der Zweckvereinbarkeit

Es werden – anders als in der DSRL – Kriterien für die Prüfung der Zweckvereinbarkeit kodifiziert,[1067] die sich an einen entsprechenden Katalog der *Artikel-29-Datenschutzgruppe* anlehnen. Da sich der Kriterienkatalog für die Feststellung der Zweckvereinbarkeit am Vorschlag der *Artikel-29-Datenschutzgruppe* orientiert, sei zur Auslegung dieser Bestimmungen ein Blick auf besagten Vorschlag geworfen.

(1) Vorschlag der *Artikel-29-Datenschutzgruppe*

Die Frage der Vereinbarkeit der Zwecke müsse in jedem Einzelfall geklärt werden.[1068] Für den Kompatibilitätstest seien zwei Herangehensweisen denkbar.[1069] Zum einen lasse sich mit einer formellen Betrachtung der Wortlaut des Erhebungs- und des Weiterverarbeitungszwecks vergleichen.[1070] Zum anderen könne bei einer materiellen Betrachtung neben dem Wortlaut auch der Kontext und „andere Faktoren" in die Bewertung miteinfließen.[1071] Eine formelle Bewertung berge die Gefahr, dass sie zu starr sei und die verantwortliche Stelle versuchen könne durch immer kompliziertere juristische Texte einen Datenumgang für einen anderen Zweck zu ermöglichen.[1072] Eine materielle Herangehensweise sei flexibler, pragmatischer und auch effektiver und gestatte eine Anpassung an zukünftige Entwicklungen und gleichzeitig den Schutz personenbezogener Daten.[1073] Wichtig sei daher Kriterien für die Feststellung einer Kompatibilität zu bestimmen.[1074] Diese sollen die bisherigen Regelungen der

1067 *Albers*, in: Wolff/Brink (Hrsg.), DSR, Art. 6 Rn. 10 spricht von „eine(r) wesentliche(n) materiellrechtliche(n) Neuerung".
1068 *Artikel-29-Datenschutzgruppe*, WP 203, S. 21.
1069 *Artikel-29-Datenschutzgruppe*, WP 203, S. 21.
1070 Vgl. *Artikel-29-Datenschutzgruppe*, WP 203, S. 21.
1071 *Artikel-29-Datenschutzgruppe*, WP 203, S. 21.
1072 *Artikel-29-Datenschutzgruppe*, WP 203, S. 22.
1073 *Artikel-29-Datenschutzgruppe*, WP 203, S. 22.
1074 *Artikel-29-Datenschutzgruppe*, WP 203, S. 22 u. 23.

Zweckbindung ergänzen und für mehr Rechtssicherheit sorgen.[1075] Diese Kriterien seien:[1076]

a) die Beziehung zwischen Erhebungszweck und Weiterverwendungszweck

Entscheidend seien bei diesem Kriterium nicht ein formeller Vergleich des Wortlauts, sondern die tatsächlich dem Verhältnis zwischen Erhebungs- und Weiterverwendungszweck zugrunde liegenden Umstände.[1077] Wichtig seien dabei die zugrunde liegenden Tatsachen und das gewöhnliche Verständnis durch relevante Interessengruppen.[1078] Je weiter die zu vergleichenden Zwecke voneinander entfernt seien, desto eher seien sie nicht miteinander kompatibel.[1079] So könne einerseits der Weiterverwendungszweck bereits im Erhebungszweck impliziert oder als logischer nächster Schritt angelegt sein und anderseits nur eine partielle oder gar keine Verbindung zwischen den beiden Zwecken bestehen.

Die Verbindung zwischen Erhebungs- und Weiterverarbeitungszweck ist ein wichtiges Indiz für eine Vereinbarkeit und findet sich daher nahezu wortgleich im Text der DSGVO wieder.

b) der Kontext der Datenerhebung und die vernünftigen Erwartungen der Betroffenen bezüglich der Weiterverwendung

Es komme darauf an, was für eine Datenverwendung eine vernünftige Person aufgrund der Umstände der Datenerhebung erwarten könne.[1080] Zur Feststellung der Umstände und der vernünftigen Erwartungen sei die Transparenz des Datenumgangs, insbesondere die dem Betroffenen bei der Erhebung oder später mitgeteilten Informationen zu berücksichti-

---

1075 *Artikel-29-Datenschutzgruppe*, WP 203, S. 44.
1076 Siehe hierzu *Artikel-29-Datenschutzgruppe*, WP 203, S. 23 ff.
1077 *Artikel-29-Datenschutzgruppe*, WP 203, S. 23: "the substance of the relationship".
1078 *Artikel-29-Datenschutzgruppe*, WP 203, S. 24.
1079 *Artikel-29-Datenschutzgruppe*, WP 203, S. 24.
1080 *Artikel-29-Datenschutzgruppe*, WP 203, S. 24.

gen.[1081] Die Art der Beziehung zwischen der verantwortlichen Stelle und dem Betroffenen soll ebenfalls berücksichtigt werden, wobei auch die Machtverhältnisse relevant seien.[1082] Von Bedeutung sei zudem was üblich und allgemein akzeptiert sei.[1083] Hierbei soll es eine Rolle spielen, ob die Datenerhebung aufgrund einer gesetzlichen Verpflichtung oder aufgrund einer Vertragsbeziehung stattgefunden habe.[1084] Auch die Rechtsgrundlage der Weiterverarbeitung zu einem anderen Zweck soll betrachtet werden, da bei einer gesetzlichen Grundlage dies aufgrund der Vorhersehbarkeit für eine Vereinbarkeit der Zwecke sprechen könne.[1085] Art. 13 Abs. 2 RL 2002/58/EG, der die Direktwerbung für ähnliche Produkte per E-Mail bei einer bestehenden Kundenbeziehung unter Einräumung eines Widerspruchsrechts erlaubt, zeige welche Rolle die vernünftigen Erwartungen des Betroffenen und der Kontext der Datenverarbeitung haben können.[1086]

Der Kontext der Datenerhebung ist ebenfalls als Kriterium in die DSGVO übernommen worden, während die vernünftigen Erwartungen des Betroffenen nunmehr in ErwG 50 DSGVO stehen. Dies mag an Bedenken liegen, dass hiermit ein Einfallstor für eine Zweckänderung für Werbezwecke gegeben sein könne.[1087] Allerdings spielt gerade der Kontext auf die damit verbundenen Erwartungen des Betroffenen an, so dass diese trotz der Textänderung ganz wesentlich für dieses Kriterium sein werden. Die in ErwG 50 DSGVO enthaltenen berechtigten Erwartungen sind auf Kritik gestoßen, da sich dieses subjektive Element schwer bestimmen lasse und zu erheblichen Unterschieden bei den Abwägungser-

1081 *Artikel-29-Datenschutzgruppe*, WP 203, S. 25.
1082 *Artikel-29-Datenschutzgruppe*, WP 203, S. 24.
1083 *Artikel-29-Datenschutzgruppe*, WP 203, S. 24.
1084 *Artikel-29-Datenschutzgruppe*, WP 203, S. 24.
1085 *Artikel-29-Datenschutzgruppe*, WP 203, S. 25.
1086 *Artikel-29-Datenschutzgruppe*, WP 203, S. 34.
1087 Zu dieser Möglichkeit siehe *Treacy/Bapat*, Privacy & Data Protection, Volume 13, Issue 6, 2013, 11 (12), die davon ausgehen, dass es den vernünftigen Erwartungen der meisten Verbraucher entspreche, dass ihre Daten für Werbe- oder Marketingzwecke ausgewertet werden, wenn sie ein Produkt kaufen.

gebnissen führen könne.[1088] In den USA ist deshalb vorgeschlagen worden nur auf die Vereinbarkeit des Datenumgangs mit dem Kontext der Beziehung zwischen verantwortlicher Stelle und Betroffenen abzustellen.[1089] Dieser Maßstab sei objektiver als die subjektiven vernünftigen Erwartungen des Betroffenen.[1090] Zudem sei dieses Prinzip an Veränderungen in der Beziehung zwischen verantwortlicher Stelle und Betroffenem anpassbar.[1091]

In Anlehnung an die US-amerikanischen „reasonable expectations of privacy" findet sich in der Literatur der Vorschlag Unternehmen sollten Betroffene auf mögliche Zweckänderungen und neue Zwecke im Vorfeld hinweisen.[1092]

c) die Art der Daten und die Auswirkungen der Weiterverwendung auf die Betroffenen

Nicht nur besondere Kategorien personenbezogener Daten gemäß Art. 8 DSRL, sondern auch andere sensible Daten wie biometrische oder genetische Daten sollen bei der Kompatibilitätsprüfung von Bedeutung sein.[1093] Je sensibler die Daten seien, desto eher spreche dies für eine Inkompatibilität der Weiterverwendung zu einem neuen Zweck.[1094] Wichtig könne auch sein, ob der Betroffene ein Kind sei oder zu einer anderen besonders schutzbedürftigen Bevölkerungsgruppe gehöre, wie z. B. Asylbewerber.[1095]

1088 *Gola/Schulz*, K&R 2015, 609 (614).
1089 *Federal Trade Commission*, Consumer Privacy, S. 38 ff.; ebenfalls in diese Richtung, ohne dass aber bislang ein konkretes Konzept vorgelegt wurde: *World Economic Forum*, value personal data, S. 15 u. 17 ff.
1090 *Federal Trade Commission*, Consumer Privacy, S. 38.
1091 *The White House*, Consumer Data Privacy, S. 16.
1092 *Wybitul*, BB 2016, 1077 (1080 f.).
1093 *Artikel-29-Datenschutzgruppe*, WP 203, S. 25.
1094 *Artikel-29-Datenschutzgruppe*, WP 203, S. 25.
1095 *Artikel-29-Datenschutzgruppe*, WP 203, S. 25 Fn. 68.

Bei den Auswirkungen der Datenverwendung seien sowohl positive, wie negative Folgen zu berücksichtigen.[1096] Dies könnten Diskriminierungen oder auch emotionale Folgen wegen des Gefühls des Kontrollverlusts beim Betroffenen sein.[1097] Auch die Art der Datenverwendung könne eine Rolle spielen, insbesondere wenn diese bei der Erhebung nicht vorhersehbar war,[1098] wie z. B. die Verarbeitung großer Mengen von Daten oder die Verwendung von Daten durch eine andere verantwortliche Stelle in einem anderen Zusammenhang und mit unbekannten Folgen.[1099] Der letztgenannte Aspekt ist aber eher dem Kontext der Datenverarbeitung zuzuordnen.

Die Art der Daten und die möglichen Folgen haben als jeweils getrennte Kategorien Eingang in die DSGVO gefunden. Dass die Art der Daten als Kriterium herangezogen wird, ist aufgrund der Regelungssystematik der DSRL und der DSGVO konsequent, wenngleich es der grundsätzlichen Anknüpfung an den Verarbeitungszweck und dessen Folgen widerspricht.[1100]

d) die Garantien der verantwortlichen Stelle zur Gewährleistung einer fairen Verarbeitung und zur Verhinderung unangemessener Auswirkungen beim Betroffenen

Durch zusätzliche Maßnahmen, wie z. B. Anonymisierung oder Pseudonymisierung oder eine funktionale Trennung[1101] könne eine Zweckänderung „kompensiert" werden.[1102] Dass dies ein relevantes Kriterium sei, ergebe sich implizit aus Art. 6 Abs. 1 lit. b DSRL, der die Zulässigkeit der Weiterverarbeitung für bestimmte Zwecke an das Vorhandensein be-

1096 *Artikel-29-Datenschutzgruppe*, WP 203, S. 25.
1097 *Artikel-29-Datenschutzgruppe*, WP 203, S. 25 f.
1098 *Artikel-29-Datenschutzgruppe*, WP 203, S. 26.
1099 *Artikel-29-Datenschutzgruppe*, WP 203, S. 26.
1100 C. II. 5., S. 91.
1101 Unter einer „funktionalen Trennung" versteht die *Artikel-29-Datenschutzgruppe*, dass Daten nicht für Maßnahmen und Entscheidungen gegenüber dem Betroffenen genutzt werden können, siehe *Artikel-29-Datenschutzgruppe*, WP 203, S. 30.
1102 *Artikel-29-Datenschutzgruppe*, WP 203, S. 26.

stimmter Garantien knüpft.[1103] Eine erhöhte Transparenz mit der Möglichkeit eines Widerspruchs oder einer spezifischen Einwilligung könne eine Rolle spielen.[1104]

Auch die Garantien haben als Abwägungsbelang Eingang in die DSGVO gefunden und sind zudem ein wichtiger Aspekt im Sinne eines datensparsamen Vorgehens.

Die Inkompatibilität der Datenverarbeitung habe ihre Rechtswidrigkeit zur Folge.[1105] In Bezug auf Big-Data-Anwendungen sei die Kompatibilitätsprüfung strikt, aber ausgewogen und flexibel anzuwenden.[1106] Was genau dies bedeuten soll, bleibt unklar. Erkennbar ist aber, dass zumindest eine gewisse Flexibilität seitens der *Artikel-29-Datenschutzgruppe* gewünscht ist.

(2) Rezeption in der Wissenschaft

Der Maßstab für die Feststellung der Vereinbarkeit ist in der Literatur auf Zustimmung gestoßen.[1107] Die Möglichkeit einer Zweckänderung, wie sie in der DSGVO vorgesehen ist, wurde als „realistische Herangehensweise in Zeiten von Big Data" bezeichnet.[1108] Andererseits wurde kritisiert, die Grundrechtsrisiken von Big Data würden in der DSGVO nicht angesprochen.[1109] Die Zweckbindung sei zwar weniger unbestimmt als in der DSRL, mangels Vorgaben für den Präzisionsgrad der Zweckfestlegung und einer strikten Zweckbindung in bestimmten Fällen, werde sie aber nicht substantiell vorangebracht.[1110] Gegenüber Art. 6 DSRL sei die Aufzählung der Kriterien zur Prüfung der Zweckvereinbarkeit ein

1103 *Artikel-29-Datenschutzgruppe*, WP 203, S. 26 Fn. 75.
1104 *Artikel-29-Datenschutzgruppe*, WP 203, S. 26.
1105 *Artikel-29-Datenschutzgruppe*, WP 203, S. 36.
1106 *Artikel-29-Datenschutzgruppe*, WP 203, S. 40.
1107 Siehe *Cumbley/Church*, CLSR 29 (2013), 601 (606).
1108 *de Hert/Papakonstantinou*, CLSR 32 (2016), 179 (186).
1109 *Roßnagel*, in: Roßnagel (Hrsg.), DSGVO, § 1 Rn. 42.
1110 *Dammann*, ZD 2016, 307 (312).

Fortschritt.[1111] Aufgrund der Unbestimmtheit der Kriterien zur Feststellung der Zweckvereinbarkeit werde vermutlich ein größerer Spielraum für Zweckänderungen vorhanden sein, als das bisher der Fall ist.[1112] Durch die wertungsbedürftigen Begriffe entstehe eine nicht hinnehmbare Unsicherheit für die Beurteilung der Zweckvereinbarkeit,[1113] die erst nach einiger Zeit vergehen werde, wenn die Vorgaben durch Gerichte oder Behörden konkretisiert werden.[1114]

Interessanterweise wird der neu in die DSGVO aufgenommene Kriterienkatalog zur Feststellung der Zweckvereinbarkeit teilweise als eine Verschärfung der bisherigen Rechtslage eingeschätzt.[1115] Da die Kompatibilität zu prüfen sei anstatt die Verarbeitung zu einem anderen Zweck einfach auf eine Rechtsgrundlage stützen zu können, seien die Anforderungen der DSGVO strenger als die des BDSG a. F.[1116] Dies vermag nicht zu überzeugen, da auch Rechtsgrundlagen des BDSG a. F. oft Abwägungen vorsahen.

Mitunter ist die DSGVO bezüglich der Zweckbindung einerseits als strenger,[1117] da sie eine Zweckkompatibilität fordere und andererseits als weiter, da sie keine gesetzliche Erlaubnis fordere, bezeichnet worden.[1118] Wenn eine strikte Zweckbindung in der DSGVO verlangt werde, gehe dies über die Anforderungen des deutschen Rechts hinaus, da auf einfachrechtlicher Ebene weder eine Zweckbindung noch ein Verbot der Zweckänderung existierten.[1119] Die Feststellung, dass es keinen Zweckbindungsgrundsatz im einfachen Recht gebe, beruht auf einem Fehlverständnis von dessen Absolutheit. Die Formulierung „strikte Zweckbindung“

1111 *Frenzel*, in: Paal/Pauly (Hrsg.), DSGVO-Kommentar, Art. 6 Rn. 46.
1112 *Laue/Nink/Kremer*, Datenschutz in der betrieblichen Praxis, § 2 Rn. 40.
1113 Vgl. *Frenzel*, in: Paal/Pauly (Hrsg.), DSGVO-Kommentar, Art. 6 Rn. 47.
1114 *Ziegenhorn/v. Heckel*, NVwZ 2016, 1585 (1590 f.); siehe auch *Richter*, DuD 2015, 735 (739), der die Kriterien als „sehr breit formuliert“ bezeichnet; siehe auch *Albers,* in: Wolff/Brink (Hrsg.), DSR, Art. 6 DSGVO Rn. 69.
1115 So *Gierschmann*, ZD 2016, 51 (54).
1116 *Plath*, in: Plath (Hrsg.), BDSG/DSGVO, Art. 6 Rn. 31.
1117 *Wolff*, in: Schantz/Wolff (Hrsg.), DSGVO, Rn. 398.
1118 *Ziegenhorn/v. Heckel*, NVwZ 2016, 1581 (1590).
1119 *Härting*, NJW 2015, 3284 (3284 u. 3288).

mag insofern unglücklich und missverständlich gewählt sein. Bereits die Bezeichnung der Zweckbindung als Grundsatz zeigt aber, dass es sich um eine Regel handelt, die generell, aber nicht absolut gilt.

Der Erhebungszweck werde eine größere Rolle als früher spielen.[1120] Denn ohne eine enge Zweckfestlegung laufe die Kompatibilitätsprüfung leer.[1121] Im Rahmen der Vereinbarkeitsprüfung sei immer auf den ursprünglichen Erhebungszweck abzustellen, wie sich aus ErwG 50 Satz 1 DSGVO und auch einer am Schutzzweck der DSGVO orientierten engen Auslegung von Art. 6 Abs. 4 DSGVO ergebe.[1122]

Die Kriterien vermögen eine grobe Richtung für die zu treffenden Abwägungsentscheidungen zu geben. In der Literatur wird aber zu Recht darauf hingewiesen, dass es sich um unbestimmte Rechtsbegriffe handelt, die erhebliche Auslegungsspielräume lassen und zu denen sich eine einheitliche Auslegung und Anwendung durch die Aufsichtsbehörden und die Gerichte erst wird finden müssen. Inwieweit aufgrund der Zweckvereinbarkeitsprüfung tatsächlich eine Aufweichung der Zweckbindung zu erwarten ist, wird primär von den Anforderungen an die und der Durchsetzung der Zweckfestlegung abhängen, die diesem Prozess als erste Stufe vorgeschaltet ist.[1123]

bb) Notwendigkeit einer weiteren Rechtsgrundlage

ErwG 50 DSGVO[1124] enthält Vorgaben für die Verarbeitung zu einem anderen Zweck als dem Erhebungszweck. Im Falle der Zweckvereinbar-

1120 *Werkmeister/Brandt*, CR 2016, 233 (238).
1121 *Richter*, DuD 2015, 735 (739).
1122 *Kühling/Martini/Heberlein/Kühl/Nink/Weinzierl/Wenzel*, Die DSGVO und das nationale Recht, S. 40 f.
1123 Vgl. *Buchner*, DuD 2016, 155 (157) zum Ratsentwurf.
1124 Die Erwägungsgründe sind zwar nicht rechtsverbindlich, werden aber regelmäßig zur Auslegung eines Rechtsaktes herangezogen, siehe hierzu ausführlich: *Selmayr/Ehmann*, in: Ehmann/Selmayr (Hrsg.), DSGVO, Einl. Rn. 97.

keit soll es keiner gesonderten Rechtsgrundlage neben der für die Datenerhebung bedürfen. Es ist umstritten, wie dies zu verstehen ist.

Nach einer Ansicht soll bei einer Zweckvereinbarkeit die Verarbeitung unter Stützung auf die bisherige Rechtsgrundlage zulässig sein.[1125] Darüber hinausgehend wird sogar ein gänzlich alternatives Verständnis von Zweckvereinbarkeit und Rechtsgrundlage vertreten.[1126]

Des Weiteren wird vertreten, dass eine Datenverwendung zu einem beliebigen neuen Zweck zulässig sei zugunsten eines berechtigten Interesses der verantwortlichen Stelle oder eines Dritten, sofern dieses das schutzwürdige Interesse des Betroffenen überwiege.[1127] Dem Zweckbindungsprinzip werde in der DSGVO durch die Möglichkeit der Kompatibilität und – bei deren Nichtvorliegen – des Rückgriffs auf „alle vorhandenen extrem abstrakten Erlaubnistatbestände" die beschränkende Wirkung entzogen.[1128] Dies vermag aber nicht zu überzeugen, da dies weder den Artikeln noch den Erwägungsgründen der DSGVO so zu entnehmen ist. Lediglich für bestimmte im öffentlichen Interesse liegende Aufgaben oder in Ausübung hoheitlicher Gewalt kann durch Unions- oder mitgliedstaatliches Recht eine Ausnahme von der Zweckbindung vorgesehen werden. Eine generelle Freigabe der weiteren Verwendung – wie noch im Ratsentwurf angedacht – ist der DSGVO nicht zu entnehmen.

Nach einer anderen Ansicht müsse es sich um ein Redaktionsversehen handeln, da ansonsten bei den privilegierten Zwecken jedwede Weiter-

1125 *Plath*, in: Plath (Hrsg.), BDSG/DSGVO, Art. 5 Rn. 8 DSGVO.
1126 So *Richter*, DuD 2016, 581 (584) unter Berufung auf ErwG 50 DSGVO.
1127 *Roßnagel/Nebel*, DSGVO, S. 6.
1128 *Roßnagel/Geminn/Jandt/Richter*, Datenschutzrecht 2016, S. 161, wobei nicht ausgeführt wird, welche Erlaubnistatbestände gemeint sind. Möglicherweise wurde der gegenüber dem Ratsentwurf geänderte Wortlaut nicht berücksichtigt. *Richter* in: Roßnagel (Hrsg.), DSGVO, § 4 Rn. 121 geht unter Verweis auf ErwG 50 DSGVO ebenfalls davon aus, dass auch bei einer Inkompatibilität auf eine Rechtsgrundlage nach Art. 6 Abs. 1 DSGVO zurückgegriffen werden könne.

verarbeitung schrankenlos möglich sei.[1129] Problematisch sei, insbesondere im Hinblick auf Art. 7 und 8 GRCh, dass es ohne das Erfordernis einer Rechtsgrundlage keiner Prüfung der Interessen des Betroffenen bedürfe.[1130] Die Notwendigkeit des kumulativen Vorliegens einer Rechtsgrundlage und der Zweckvereinbarkeit ergebe sich unmittelbar aus Art. 8 Abs. 2 Satz 1 GRCh.[1131] Die DSGVO gewährleiste genauso wie die DSRL eine strenge Zweckbindung.[1132] Auch weiterhin bedürfe es einer Rechtsgrundlage für die Verarbeitung zu einem anderen Zweck, da sich aus ErwG 50 DSGVO nur ergebe, dass eine andere Rechtsgrundlage als die für die Erhebung nicht erforderlich sei, wenn diese einschlägig ist.[1133] Die Gesetzessystematik spreche dafür, dass der als Schranke ausgestaltete Art. 6 Abs. 4 DSGVO keinen Erlaubnistatbestand enthalte.[1134] Die Gegenansicht konterkariere die Funktion der Zweckbindung als begrenzendes Element.[1135]

1129 *Schantz*, NJW 2016, 1841 (1844); ein Redaktionsversehen für möglich haltend: *Buchner/Petri*, in: Kühling/Buchner (Hrsg.), DSGVO, Art. 6 Rn. 182; a. A. *Monreal*, ZD 2016, 507 (510), unter Verweis auf einen umfassend zu verstehenden europäischen Verarbeitungsbegriff der dazu führe, dass die Weiterverarbeitung zu einen neuen Zweck kein neuer Verarbeitungsvorgang sei und daher keiner neuen Rechtsgrundlage bedürfe; a. A. ebenfalls *Ziegenhorn/v. Heckel*, NVwZ 2016, 1585 (1590), die bezüglich der Problematik einer generellen Erlaubtheit der Verarbeitung für privilegierte Zwecke einen „Schluss vom Speziellen zum Allgemeinen" ablehnen und das Problem durch eine grundrechtskonforme Auslegung allgemeiner Rechtmäßigkeitsvoraussetzungen lösen wollen.

1130 *Schantz*, in: Wolff/Brink (Hrsg.), DSR, Art. 5 DSGVO Rn. 22.

1131 *Heberlein*, in: Ehmann/Selmayr (Hrsg.), DSGVO, Art. 5 Rn. 19; für ein kumulatives Verhältnis von Rechtsgrundlage und Zweckvereinbarkeit auch *Herbst*, in: Kühling/Buchner (Hrsg.), DSGVO, Art. 5 Rn. 28 unter Verweis auf die Rechtsprechung des EuGH zu Art. 6 DSRL; *Reimer*, in: Sydow (Hrsg.), DSGVO, Art. 6 Rn. 67.

1132 *Albrecht/Jotzo*, DSGVO, Teil 2 Rn. 5.

1133 Vgl. *Albrecht/Jotzo*, DSGVO, Teil 3 Rn. 54; vgl. auch *Piltz*, K&R 2016, 557 (566); siehe auch, *Kühling/Martini*, EuZW 2016, 448 (451); *Schulz*, in: Gola (Hrsg.), DSGVO, Art. 6 Rn. 185.

1134 *Albrecht/Jotzo*, DSGVO, Teil 3 Rn. 54.

1135 *Herbst*, in: Kühling/Buchner (Hrsg.), DSGVO, Art 5, Rn. 29.

cc) Stellungnahme

Im Ratsentwurf fand sich in ErwG 40 DSVO-E-Rat bereits eine entsprechende Bestimmung, was ein Redaktionsversehen unwahrscheinlich erscheinen lässt. Die ein alternatives Verhältnis von Rechtsgrundlage und Zweckvereinbarkeit vertretende Ansicht hat somit den Wortlaut des nicht rechtsverbindlichen Erwägungsgrundes für sich. Diesem extensiven Verständnis steht aber aus systematischer Hinsicht entgegen, dass die Funktion der Zweckbindung von einem die Datenverarbeitung begrenzenden, die Transparenz steigernden Element hin zu einem die Verarbeitungsmöglichkeiten für neue Zwecke erweiternden Instrument verkehrt würde. Im Hinblick auf eine damit faktisch schrankenlose Verarbeitung für privilegierte Zwecke ist dies in Anbetracht des informationellen Selbstbestimmungsrechts des Betroffen nicht hinnehmbar. Das enge Verständnis ist damit vorzugswürdig.

c) Weitere Regelungen, insbesondere die Informationspflicht

In Art. 13 Abs. 1 lit. c DSGVO ist eine Informationspflicht über die Verarbeitungszwecke bei Datenerhebung vorgesehen. Explizit gefordert ist nunmehr eine Information über einen neuen (anderen) Weiterverarbeitungszweck vor der Weiterverarbeitung, Art. 13 Abs. 3 DSGVO. Entsprechende Regelungen im Falle einer nicht bei dem Betroffenen erfolgten Erhebung enthalten Art. 14 Abs. 1 lit. c und Abs. 4 DSGVO. In der Informationspflicht über den neuen Zweck wird eine erhebliche Einschränkung von Big-Data-Analysen gesehen.[1136] Es handele sich um eine „Sanktionierung" einer Zweckänderung nach Art. 6 Abs. 4 DSGVO.[1137] Die Information solle über eine Webseite möglich sein, um eine Zweckänderung nicht zu konterkarieren.[1138] Art. 12 Abs. 7 DSGVO sieht die

1136 *Gola*, in: Gola (Hrsg.), DSGVO, Einl. Rn. 62; ähnlich *Paal*, in: Paal/Pauly (Hrsg.), DSGVO-Kommentar, Art. 13 Rn. 33, bezogen auf die Mitteilungspflicht nach Abs. 3.

1137 *Kamlah*, in: Plath (Hrsg.), BDSG/DSGVO, Art. 13 Rn. 30.

1138 *Kamlah*, in: Plath (Hrsg.), BDSG/DSGVO, Art. 30 Rn. 30.

Möglichkeit der Verwendung von standardisierten Bildsymbolen in Kombination mit nach Art. 13 und 14 DSGVO zu erteilenden Informationen vor, zu denen auch die Zwecke gehören. Ob und wie Zwecke gegebenenfalls bildlich dargestellt werden könnten, ist der DSGVO nicht zu entnehmen. Art. 13 Abs. 8 DSGVO sieht vor, dass die Kommission mittels delegierter Rechtsakte die Einzelheiten regeln kann.

Darüber hinaus ist die Information über einen bestimmten Zweck beispielsweise für eine wirksame Einwilligung nach Art. 6 Abs. 1 lit a DSGVO und ErwG 32 DSGVO relevant. Laut Art. 15 Abs. 1 lit. a DSGVO ist der Verarbeitungszweck zu verbeauskunften. Wenn die Daten für die Erhebungs- bzw. Verarbeitungszwecke nicht mehr notwendig sind, so sind sie gemäß Art. 17 Abs. 1 lit. a DSGVO zu löschen. Der Zweck ist auch bei der Frage welche Maßnahmen im Rahmen des Datenschutzes durch Technik gemäß Art. 25 Abs. 1 DSGVO zu treffen sind und bei einer Datenschutz-Folgenabschätzung gemäß Art. 35 Abs. 1 DSGVO von Bedeutung.

3. Zwischenergebnis

Auch in der DSGVO spielt die Zweckbestimmung und -bindung eine entscheidende Rolle. Inwiefern sich für Zweckänderungen gegenüber der bisherigen Rechtslage erweiterte Möglichkeiten ergeben, wird maßgeblich von der Anwendung und Auslegung des Kompatibilitätstests des Art. 6 Abs. 4 DSGVO und – diesem vorgeschaltet – den Anforderungen an die Zweckfestlegung abhängen. Die Regelungen bieten die Möglichkeit einer extensiven und einer restriktiven Auslegung, wobei letztere aus systematischen und teleologischen Gesichtspunkten vorzugswürdig erscheint. Auch nach der DSGVO wird aber in jedem Falle eine Zweckdefinition erfolgen müssen, die über einen Allgemeinplatz wie „Big-Data-Analyse“ hinausgeht.

V. Ergebnis

Eine Speicherung und Auswertung von Daten für unbestimmte Zwecke im Rahmen einer Big-Data-Analyse ist aufgrund der Vorgaben der Zweckfestlegung und der Zweckbindung sowohl im BDSG a. F. als auch nach der DSGVO nicht zulässig. Zwar mag die Prüfung der Zweckvereinbarkeit nach der DSGVO zu einer größeren Flexibilität der Weiterverarbeitung für einen neuen Zweck führen. Eine hinreichend präzise Zweckfestlegung ist und bleibt aber unumgänglich.

E. Lösungsvorschläge

Zur Lösung des aufgezeigten Konflikts zwischen Big-Data-Anwendungen und der Zweckbindung gibt es mehrere Vorschläge, die mehrheitlich auf eine Reform des Datenschutzrechts insgesamt zielen. Die Behauptung, dass der Datenschutz sich mit den heutigen Technologien nicht mehr vereinbaren lasse und wir in einer „Post-Privacy-Welt" lebten,[1139] mag wirtschaftlichen Interessen geschuldet sein. Mit der deutschen Rechtsordnung ist sie aufgrund verfassungs- und europarechtlicher Vorgaben nicht vereinbar.[1140] Im Folgenden sollen nun Vorschläge betrachtet werden, wie der Konflikt im Rahmen dieser Ordnung gelöst oder zumindest entschärft werden kann.

I. Bestimmung des Konkretisierungsgrads durch Rückgriff auf andere Grundrechte

1. Konzept

Sowohl für den öffentlichen als auch für den nicht-öffentlichen Bereich wurde ein Rückgriff auf andere Grundrechte zur Bestimmung des Konkretisierungsgrads der Zweckfestlegung vorgeschlagen.

Für den öffentlichen Bereich wurde bereits vor einigen Jahren eine Reduzierung der materiellen Anforderungen der Zweckbindung hin zu einer Zweckvereinbarkeit vorgeschlagen.[1141] Anknüpfungspunkt des Datenschutzrechts solle nicht mehr das einzelne Datum, sondern vielmehr der Verwendungskontext und die entsprechende Gefährdung der Selbstdar-

1139 Vgl. *Heller*, Post-Privacy, S. 24 f.; Darstellung mit kritischer Würdigung: *Schaar*, Überwachung, S. 256 ff.
1140 *Boehme-Neßler*, in: Rehbinder (Hrsg.), UFITA 2015 I, 19 (25 f.).
1141 *Eifert*, in: Gropp/Lipp/Steiger (Hrsg.), FS Uni Gießen, S. 139 (143 f.).

stellung sein.[1142] Es sei dann nicht mehr eine „so enge gesetzliche Zweckfestlegung erforderlich", sondern eine Differenzierung des Schutzes unter Rückgriff auf die im Verarbeitungskontext relevanten Freiheitsgrundrechte.[1143]

Zugleich sollten die Transparenz der Datenverarbeitung erhöht und die Kontrollmöglichkeiten der Datenschutzbehörden gestärkt werden.[1144] Die seltenere Direkterhebung führe dazu, dass für die Datenqualität weitere Sicherungen, wie ein Versehen der Daten mit Kontextinformationen erforderlich sei.[1145] Es seien miteinander zu vereinbarende Zwecke zu definieren, was schwer zu operationalisieren sei, da es unter Berücksichtigung des Verwendungskontextes und der jeweils betroffenen Freiheitsgrundrechte erfolgen müsse.[1146] Dabei sei ein „Vorgehen mit hoher Detailschärfe" vonnöten, um zu verhindern, dass die Einführung dieses neuen Maßstabes zu einem „Blindflug" werde.[1147] Kritisiert wurde an diesem Vorschlag, dass kein Maßstab für die Vereinbarkeit von Zwecken vorhanden sei.[1148] Zumindest diesem Umstand versucht die DSGVO nunmehr abzuhelfen. Allerdings mit den bereits aufgezeigten Schwächen.

Für den nicht-öffentlichen Bereich wird eine Bestimmung der hinreichenden Zweckkonkretisierung unter Rückgriff auf andere Grundrechte vorgeschlagen. Der Einsatz von Prinzipien wie der Zweckbindung biete sich zur Regulierung eines Prozesses an, da der Gesetzgeber nicht alle denkbaren zu regulierenden Fälle vorhersehen könne.[1149] Das Zweckbindungsprinzip sei ein „innovationsoffenes Regelungsinstrument".[1150] Wenn das Datenschutzrecht nur die vernünftigen Erwartungen des Be-

---

1142 *Eifert*, in: Gropp/Lipp/Steiger (Hrsg.), FS Uni Gießen, S. 139 (145).
1143 *Eifert*, in: Gropp/Lipp/Steiger (Hrsg.), FS Uni Gießen, S. 139 (146).
1144 *Eifert*, in: Gropp/Lipp/Steiger (Hrsg.), FS Uni Gießen, S. 139 (147 f.).
1145 *Eifert*, in: Gropp/Lipp/Steiger (Hrsg.), FS Uni Gießen, S. 139 (149 f.), zur Mehrdeutigkeit von Daten.
1146 *Eifert*, in: Gropp/Lipp/Steiger (Hrsg.), FS Uni Gießen, S. 139 (151).
1147 *Eifert*, in: Gropp/Lipp/Steiger (Hrsg.), FS Uni Gießen, S. 139 (152).
1148 *Stollhof*, Datenschutzgerechtes E-Government, S. 187.
1149 Vgl. *v. Grafenstein*, DuD 2015, 789 (792).
1150 *v. Grafenstein*, in: Taeger (Hrsg.), Zweckbindung bei Startups, S. 233 (235).

troffenen oder die informationelle Selbstbestimmung schütze, reiche ein allgemein gehaltener Zweck aus, da der Betroffene dann den Zweck kenne.[1151] Es bedürfe einer Einbeziehung aller verfassungsrechtlich geschützten Kontexte um die grundrechtlichen Gewährleistungsgehalte als Maßstab für die Bestimmung der Zwecke heranzuziehen.[1152] Anhand der Gewährleistungsgehalte der anderen Grundrechte und ihrer jeweiligen Gefährdung soll sich der Präzisionsgrad der Zweckangabe bestimmen lassen.[1153] Die Zweckfestlegung diene in erster Linie zur Aufdeckung von Risiken von konkreten Bedrohungen für andere Freiheitsrechte.[1154] Dem Urteil des BVerfG zum BKAG sei in Rn. 278 und 279 zu entnehmen, dass für die Frage des Präzisionsgrads der Zweckbestimmung auf Rechtsgüter Bezug genommen werden könne.[1155] Die Zweckfestlegung habe im privaten Bereich, da die Grundrechte als Maßstab für weitere Datenschutzmaßnahmen dienten, deren Notwendigkeit sich erst im Laufe der Verarbeitung zeige, nicht ausschließlich zum Zeitpunkt der Erhebung zu erfolgen.[1156] Erst bei Aufdeckung neuer Risiken durch die „fortlaufende Zweckbestimmung" liege eine Zweckänderung vor.[1157] Das vorgestellte Regelungsmodell biete mehr Spielraum für Innovationen, da es nicht lediglich an den Zeitpunkt der Datenerhebung anknüpfe.[1158]

2. Bewertung

Das Konzept vermag nicht zu überzeugen. Denn bereits heute dienen die Umstände des Datenumgangs und damit auch die Betroffenheit des RiS als Maßstab für die Konkretheit des Zweckes. Dennoch hat sich kein klarer Maßstab herausgebildet. Der Ansatz verkennt zudem, dass die

---

1151 *v. Grafenstein*, DuD 2015, 789 (793).
1152 *v. Grafenstein*, DuD 2015, 789 (794); *v. Grafenstein*, in: Taeger (Hrsg.), Zweckbindung bei Startups, S. 233 (237).
1153 *v. Grafenstein*, DuD 2015, 789 (794).
1154 *v. Grafenstein*, in: Taeger (Hrsg.), Zweckbindung bei Startups, 233 (239).
1155 *v. Grafenstein*, in: Taeger (Hrsg.), Zweckbindung bei Startups, 233 (241).
1156 *v. Grafenstein*, in: Taeger (Hrsg.), Zweckbindung bei Startups, 233 (239).
1157 *v. Grafenstein*, in: Taeger (Hrsg.), Zweckbindung bei Startups, 233 (240 f.).
1158 *v. Grafenstein*, in: Taeger (Hrsg.), Zweckbindung bei Startups, 233 (242).

Zweckfestlegung nicht nur zur Bestimmung der Betroffenheit dient, sondern auch maßgeblich ist für die Erforderlichkeit (Datensparsamkeit) und die Transparenzanforderungen. Gerade eine nicht hinreichende Information über den Verarbeitungszweck führt zu einem Überwiegen der schutzwürdigen Positionen des Betroffenen, da das Risiko nicht bestimmt werden kann und diese Unsicherheit nur zu Lasten der verantwortlichen Stelle gehen kann, da sie es in der Hand hat durch eine präzisere Zweckbestimmung eine Rechtmäßigkeit des Datenumgangs herbeizuführen. Wie genau das Modell einer „fortlaufenden Zweckbestimmung" funktionieren soll und was es heißt, wenn die Zweckfestlegung „nicht ausschließlich" zum Zeitpunkt der Erhebung stattzufinden habe, ist unklar. Es wird nicht deutlich, ob eine Zweckfestlegung teilweise schon zum Zeitpunkt der Datenerhebung und teilweise später stattfinden soll oder ob der Zeitpunkt der Zweckfestlegung gänzlich variiert, so dass er manchmal zum Erhebungszeitpunkt und manchmal zu einem nicht näher definierten späteren Zeitpunkt erfolgen soll. Die Zweckfestlegung erst zu einem späteren Zeitpunkt durchzuführen, führt zwangsläufig zu einer späteren Beurteilung der Rechtmäßigkeit des Datenumgangs und würde damit das bestehende Regelungsmodell erheblich zugunsten nicht-öffentlicher verantwortlicher Stellen verschieben.

Insbesondere das Problem der Zweckoffenheit von Big-Data-Analysen wird durch dieses Regelungsmodell nicht gelöst. Denn es bedarf des Zweckes zur Bestimmung der Betroffenheit in den Grundrechten. Dieser ist bei zweckoffenen Verfahren aber nicht bekannt und kann daher gar nicht benannt werden. Ohnehin ist es zweifelhaft, ob bei einer Big-Data-Analyse die Tiefe des Grundrechtseingriffs prognostiziert werden kann, da durch die Verknüpfung von Daten unvorhergesehene Ergebnisse entstehen können.[1159] Schwierig wird dies vor allem bei einer automatischen Auswertung mittels künstlicher Intelligenz.[1160]

Eine Innovationsoffenheit läge nur dann vor, wenn das Modell in überzeugender Weise den Zeitpunkt der Zweckfestlegung auf einen späteren

1159 Vgl. *Boehme-Neßler*, in: Rehbinder (Hrsg.), UFITA 2015 I, 19 (32).
1160 Vgl. *Boehme-Neßler*, in: Rehbinder (Hrsg.), UFITA 2015 I, 19 (32).

Zeitpunkt als den der Datenerhebung verschieben könnte, was aber gerade nicht der Fall ist.

Für die Frage, ob eine Zweckvereinbarkeit vorliegt, mag in der Tat die Betroffenheit des gleichen Rechtsguts eine Rolle spielen. Es ist allerdings nicht ersichtlich, dass das BVerfG im BKAG-Urteil eine Aussage zum Maßstab des notwendigen Konkretisierungsgrads des Zweckes getroffen und hierbei auf die Betroffenheit des gleichen Rechtsguts abgestellt habe. Der Konkretisierungsgrad ist in den Ausführungen des BVerfG vielmehr gänzlich unklar geblieben, da dieses teils den Zweck mit der Aufgabe gleichzusetzen und den Anlass der Datenerhebung hiervon zu trennen scheint, während kurz darauf der Anlass unter den Zweck subsumiert wird.[1161]

II. Aufhebung des Personenbezugs

Vielfach wird vorgeschlagen das Problem dadurch zu lösen, dass der Personenbezug aufgehoben wird. Sofern der Personenbezug tatsächlich nicht mehr besteht und auch nicht mehr hergestellt werden kann, ist das Datenschutzrecht nicht anwendbar und die Auswertung der Daten müsste folglich die Vorgaben der Zweckbindung nicht mehr einhalten.

1. Anonymisierung

Inwiefern eine Aufhebung des Personenbezugs mittels Anonymisierung möglich ist, ist aufgrund der stetig zunehmenden technischen Möglichkeiten der Reidentifizierung äußerst fraglich und wurde schon frühzeitig bezweifelt.[1162] Gerade Big-Data-Analysen erhöhen durch die Kom-

---

1161 D. II. 4. c) bb), S. 147.

1162 *Artikel-29-Datenschutzgruppe*, WP 203, S. 31; *Boehme-Neßler*, in: Rehbinder (Hrsg.), UFITA 2015 I, 19 (36); *Möncke*, DuD 1998, 561 (567) sah dieses Problem bereits bei Data Warehouses.

bination einer Vielzahl von Daten diese Risiken erheblich.[1163] Zu Bedenken ist, dass durch die Kombination vieler Daten auch dann möglicherweise ein Personenbezug herstellbar ist, wenn jedes einzelne Datum für sich genommen anonym ist.[1164] So sollen zwischen 61-87 Prozent der US-amerikanischen Bevölkerung aufgrund von drei Merkmalen eindeutig identifizierbar sein.[1165] Zudem besteht bei einer langfristigen Speicherung der Daten das Risiko, dass aufgrund technischer Weiterentwicklungen die Herstellung eines Personenbezugs zu einem späteren Zeitpunkt möglich wird.[1166] In einem solchen Fall gelten die Daten als von Anfang an personenbezogen.[1167] Es bedarf also einer Prognose über das Vorliegen des Personenbezugs über den gesamten Speicherungszeitraum.[1168] Problematisch ist des Weiteren, dass nicht eindeutig zu bestimmen und seitens des EuGH noch nicht geklärt ist, wann ein Reidentifizierungsaufwand unverhältnismäßig ist, so dass die Daten als anonym anzusehen sind.[1169] Sofern ein lernender Algorithmus eingesetzt wird, lässt sich zudem nicht vorhersagen, wie sich dieser verändert und deshalb ein Personenbezug hergestellt werden kann.[1170]

Beispiele für Probleme mit der Anonymisierung gibt es viele.[1171] An dieser Stelle seien zwei bekannte Fälle noch einmal in Erinnerung gerufen.[1172] Der erste Fall betrifft die Veröffentlichung von Suchanfragen im

---

1163 *Wójtowicz*, PinG 2013, 65 (67 f.).

1164 *Arming*, K&R Beihefter 3/2015 zu Heft 9 2015, 7 (8); *Helbing*, K&R 2015, 145 (148).

1165 *Roßnagel*, ZD 2013, 562 (563); *Ohm*, UCLA Law Review Vol 57, 2010, 1701 (1719 f.) m. w. N.

1166 *Arming*, K&R Beihefter 3/2015 zu Heft 9 2015, 7 (8).

1167 *Roßnagel*, ZD 2013, 562 (565).

1168 *Roßnagel*, ZD 2013, 562 (563).

1169 Vgl. *Ohrtmann/Schwiering*, NJW 2014, 2984 (2988).

1170 *Crawford/Schultz*, Boston College Law Review Vol. 55, 2014, 93 (99 u. 107).

1171 Siehe *Baeriswyl*, digma 2013, 14 (15); in der Geschwindigkeitskontrolle durch die niederländische Polizei aufgrund von Daten des Navigationsdienstes TomTom sieht *Weichert*, ZD 2013, 251 (257 f.) eine „individuelle Beeinträchtigung".

1172 Beide Fälle werden geschildert von *Mayer-Schönberger/Cukier*, Big Data, S. 154 f.; siehe auch *Katko/Babaei-Beigi*, MMR 2014, 360 (361 f.); *Ohm*, UCLA Law Review, Vol 57, 2010, 1701 (1717 ff.).

August 2006 durch AOL. AOL hatte 20 Millionen Suchanfragen von 657.000 Nutzern des Zeitraums vom 1. März 2006 - 31. Mai 2006 anonymisiert,[1173] indem der Name und die IP-Adresse durch einen Zahlencode ersetzt wurden. Innerhalb weniger Tage gelang es Reportern der New York Times eine Person zu identifizieren.

In einem anderen Fall veröffentlichte Netflix im Oktober 2006 100 Millionen Datensätze von fast einer halben Millionen Nutzern, nachdem diese anonymisiert worden waren. In diesem Fall gelang die Reidentifizierung nicht mittels des Inhalts des Datensatzes, sondern durch einen Vergleich der Daten mit einer Filmbewertungsseite im Internet.[1174]

Es zeigt sich also, dass es immer schwieriger wird einen Datensatz wirksam zu anonymisieren,[1175] weshalb die Unterscheidung von personenbezogenen und nicht personenbezogenen Daten im Zusammenhang mit Big Data von manchen für obsolet gehalten wird.[1176] Der *europäische*

1173 Laut *Mayer-Schönberger/Cukier*, Big Data, S. 154; aus der Schilderung geht nicht hervor, ob AOL noch über einen Zuordnungsschlüssel verfügte, so dass es sich um eine Pseudonymisierung handelte.

1174 Siehe *Narayanan/Shmantikov*, Proceedings of the 2008 IEEE Symposium on Security and Privacy 2008, S. 111 (112).

1175 Vgl. *Baum*, DuD 2013, 583; *Europäischer Datenschutzbeauftragter*, Privatssphäre und Wettbewerbsfähigkeit, Rn. 7; *Artikel-29-Datenschutzgruppe*, WP 216, S. 3.

1176 So *de Wachter*, CRi 2014, 1 (3); *Boehme-Neßler*, DuD 2016, 419 (420 ff.); grundsätzlich für ein neues Regelungsmodell und ein Abrücken vom Kriterium des personenbezogenen Datums: *Ohm*, UCLA Law Review, Vol 57, 2010, 1701 (1742 f.); ähnlich *de Montjoye/Radaelli/Singh/Pentland*, Science, Vol. 347, Issue 6221, 30.01.2015, 536 (539), die das Problem der Reidentifizierung anhand der Kombination von anonymisierten Daten von Einkäufen mit einer Kreditkarte mit weiteren Daten der Betroffenen aufzeigen; anders aber *Schwartz/Solove*, 86 N.Y.U. L.Q. Rev. 1814 (2011), 1814 (1877) und *Schwartz*, University of Pennsylvania Law Review, Vol. 161, 2013, 1623 (1653 f.), die zwischen Daten ohne Personenbezug, solchen bei denen das Risiko der Identifizierung besteht und personenbezogenen Daten unterscheiden wollen; ähnlich und hierauf Bezug nehmend: *Tene/Polonetsky*, Northwestern Journal of Technology and Intellectual Property 2013, Vol. 11, Issue 5 239 (258 f.); siehe auch *Federal Trade Commission*, Consumer Privacy, S. 20 ff. , die stattdessen auf die Wahrscheinlichkeit einer Identifizierung und eine öffentliche Erklärung

Datenschutzbeauftragte scheint ebenfalls zu dieser Ansicht zu neigen, wie die Annahme zeigt, dass es sich beim Tracking der Onlineaktivität eines Nutzers auch im Falle des Einsatzes von Anonymisierungstechniken um personenbezogene Daten handele.[1177] Aus Sicht der verantwortlichen Stelle scheint es daher ratsam bei Big Data stets von personenbezogenen Daten auszugehen.[1178] Dies insbesondere deshalb, weil im Falle einer Reidentifizierung das Datenschutzrecht in vollem Umfang Anwendung findet und – falls keine Rechtsgrundlage vorliegt – der Datenumgang rechtwidrig ist und die Daten zu löschen sind.[1179]

Zu bedenken ist auch, dass es bei einer statistischen Auswertung in der Regel darum geht, dass das Ergebnis zu einer Person in Beziehung gesetzt wird, denn gerade dadurch werden statistische Aussagen interessant.[1180] Daher wird in der Literatur gefordert, dass eine Big-Data-Analyse, die auf menschliches Verhalten gerichtet sei, „nicht unabhängig von personenbezogener Anwendung betrachtet werden" solle.[1181] Die Inbeziehungsetzung von anonymen Auswertungsergebnissen mit einzelnen Personen zeige, dass die binäre Anknüpfung an das Vorliegen oder Nichtvorliegen des Personenbezugs für die Anwendbarkeit des Datenschutzrechts nicht mehr zeitgemäß sei.[1182] Es ist zwar richtig, dass das Merkmal des personenbezogenen Datums an Trennschärfe verliert, allerdings sollte es nicht leichtfertig aufgegeben werden, solange kein anderes, besser geeignetes Kriterium benannt werden kann.

---

eines Unternehmens, auf eine Identifizierung zu verzichten, abstellen sowie vertragliche Identifizierungsverbote im Falle der Übermittlung an Dritte vorsehen.

1177 *Europäischer Datenschutzbeauftragter*, big data, S. 7.

1178 Grundsätzlich einen Personenbezug bejahend *Baeriswyl*, digma 2013, 14 (15).

1179 Vgl. *Roßnagel/Scholz*, MMR 2000, 721 (730).

1180 *Giesen*, RDV 2010, 266 (270) spricht von einem „Lauern (...) auf personale Zuordnung".

1181 *Roßnagel/Geminn/Jandt/Richter*, Datenschutzrecht 2016, S. 26.

1182 Vgl. *Roßnagel/Geminn/Jandt/Richter*, Datenschutzrecht 2016, S. 125 f.

2. Pseudonymisierung und differential privacy

Helbing schlägt unter Verweis auf die *Artikel-29-Datenschutzgruppe* für Auswertungen, die nicht auf ein personenbezogenes Ergebnis zielen, eine funktionale Trennung vor, die in einem separaten, gesicherten System von einem externen Dienstleister aufgrund strenger vertraglicher Vorschriften zur Verhinderung der Wiederherstellung des Personenbezugs und unter Überwachung durch einen unabhängigen Dritten durchgeführt werden sollen.[1183] Die funktionale Trennung führe in diesem Falle zur Zulässigkeit einer Zweckänderung auch bei Unvereinbarkeit mit den Erhebungszwecken der Daten.[1184] Unter dem Konzept der funktionalen Trennung sei zu verstehen, dass Daten, die zu statistischen oder anderen Forschungszwecken genutzt werden, nicht für andere Maßnahmen und Entscheidungen in Bezug auf den Betroffenen verfügbar sind.[1185] Dies ist durchaus ein probates und gesetzlich vorgesehenes Mittel. Entscheidend für ein solches Vorgehen wird sein, ob die Pseudonymisierung und die funktionale Trennung dergestalt durchgeführt wird, dass es sich um eine „geeignete Garantie" i. S. d. Art. 6 Abs. 4 lit. e DSGVO handelt.

Im Bereich der individualisierten Werbung soll der Einsatz von Big-Data-Techniken zulässig sein, wenn eine funktionale Trennung durchgeführt wird, eine Information über Zwecke und Methoden der Auswertung erfolgt und ein Widerspruchsrecht des Betroffen besteht.[1186] Der Sinn einer funktionalen Trennung bei personalisierter Werbung erschließt sich aber nicht, da ein Personenbezug der pseudonymisierten Daten vorliegt und dieser ohnehin bei Versendung der Werbung in der Regel hergestellt wird, außer dies geschieht an eine nicht personenbezogene E-Mail-Adresse.

Differential Privacy, d. h. ein Verfahren bei dem keine exakten sondern Annäherungswerte generiert werden, z. B. ca. 400 Personen in

1183 *Helbing*, K&R 2015, 145 (148).
1184 *Helbing*, K&R 2015, 145 (148).
1185 *Artikel-29-Datenschutzgruppe*, WP 203, S. 30.
1186 Siehe zum Vorschlag: *Helbing*, K&R 2015, 145 (149).

Stadt x, wird ebenfalls als ein möglicher Weg zum Umgang mit diesem Problem bezeichnet.[1187] Allerdings lassen selbst die Verfechter dieses Verfahrens erkennen, dass der Personenbezug nicht aufgehoben wird, sondern lediglich der Aufwand der Reidentifizierung erheblich erschwert wird.[1188] Laut der *Artikel-29-Datenschutzgruppe* behält die verantwortliche Stelle ein Exemplar des ursprünglichen Datensatzes, so dass eine Identifizierung jederzeit möglich sei.[1189] Modelle wie *k-anonymity*, *t-closeness*, *l-diversity* oder *differential privacy* seien nicht für Big Data geeignet, da sie von einem statischen Datenbestand ausgingen und nur einmalig prüften, ob die Anonymität gewährleistet sei.[1190]

Eine mögliche Lösung dieses Problems mögen rechtliche Reidentifizierungsverbote sein, wie in § 15 Abs. 3 Satz 3 TMG. Allerdings wird bezweifelt, ob diese tatsächlich befolgt werden, selbst wenn ein Verstoß bußgeldbewehrt ist.[1191] Dies wird aber letztlich von der tatsächlichen Durchsetzung dieser Vorschriften abhängen. Aufgrund des Risikos der Reidentifizierung wurde vorgeschlagen, dass vor der Datenverarbeitung das jeweilige Risiko geprüft und Daten, deren Deanonymisierung besonders wahrscheinlich ist, einzelnen datenschutzrechtlichen Vorschriften unterworfen werden sollten.[1192] Problematisch hieran ist aber, dass die Bestimmung des Risikos schwierig sein dürfte. Zudem stellt sich dann die Frage, weshalb das Datenschutzrecht nur teilweise gelten sollte.

3. Bewertung

Es zeigt sich, dass es zunehmend schwierig ist, eine dauerhafte Anonymisierung zu gewährleisten. Die Bemühungen zur Aufhebung des Personenbezugs sind gewiss wichtige Kriterien im Rahmen einer Abwägung

1187 *Mayer-Schönberger/Cukier*, Big Data, S. 175.
1188 Siehe *Mayer-Schönberger/Cukier*, Big Data, S. 175.
1189 *Artikel-29-Datenschutzgruppe*, WP 216, S. 18.
1190 Vgl. *Marnau*, DuD 2016, 428 (429).
1191 Vgl. *Karg*, DuD 2015, 520 (525), der daher zusätzlich technische und organisatorische Maßnahmen fordert.
1192 *Roßnagel/Geminn/Jandt/Richter*, Datenschutzrecht 2016, S. 152.

bei der Frage der Zulässigkeit der Datenverarbeitung. Sofern eine Datenauswertung auf Makroebene gewünscht ist, können diese Verfahren einen wichtigen Beitrag leisten. Auf Mikroebene lässt sich der Personenbezug nicht aufheben. Durch eine Pseudonymisierung kann aber zumindest eine datenschutzfreundliche Ausgestaltung erreicht werden.

III. Subjektive Zweckbindung

Auch wenn die bisherigen Ausführungen darlegen konnten, dass es einer konkreten Zweckbestimmung bedarf, kann hieran immer noch kritisiert werden, dass es kein Instrumentarium zur Bestimmung des Präzisionsgrads der Zweckbestimmung gibt.[1193]

1. Konzept

Eine Lösung dieses Problems soll in einer subjektiven Zweckbestimmung im öffentlichen Bereich liegen.[1194] Ausgehend von der Prämisse der informationellen Selbstbestimmung sei eine subjektive Bestimmung des Zwecks durch den Betroffenen vorzunehmen.[1195] Denn eine objektive Zweckbestimmung durch Gesetz führe zu einer „Fremdbestimmung" und einer „Informationsabschottung ohne Willensakt des Betroffenen".[1196] Die individuelle Zweckbestimmung stelle den „stärksten Ausdruck des Rechts auf informationelle Selbstbestimmung dar."[1197] Wegen der Informationspflichten nach Art. 10 ff. DSRL habe sie einen „besonders starken Gehalt".[1198] Aufgrund der gestiegenen Medienkompetenz der Bevölkerung bedürfe es einer stärkeren Orientierung an gesellschaftlichen Rahmenbedingungen, um nicht den Zweckbestimmungsgrundsatz in einen

1193 So die Kritik von *Forgó/Krügel/Rapp*, Zwecksetzung, S. 11.
1194 So *Forgó/Krügel/Rapp*, Zwecksetzung, S. 11.
1195 *Forgó/Krügel/Rapp*, Zwecksetzung, S. 37 f.
1196 *Forgó/Krügel*, DuD 2005, 732 (733).
1197 *Forgó/Krügel/Rapp*, Zwecksetzung, S. 39.
1198 *Forgó/Krügel/Rapp*, Zwecksetzung, S. 39.

„Behinderungsgrundsatz zu verwandeln".[1199] Es handele sich nicht um eine konkludente Einwilligung, sondern um „eine individuelle Konkretisierung des Zwecks" durch den Betroffenen.[1200] Der Zweck werde festgelegt und nicht nur genehmigt.[1201] Die subjektive Zwecksetzung stelle eine Ermächtigungsgrundlage dar und mache die Einwilligung obsolet.[1202] Der Betroffene sei „regelmäßig zeitlich und ökonomisch gar nicht in der Lage, Inhalt und Konsequenzen seiner Erklärungen abzusehen und (…) als der ökonomisch schwächere Marktteilnehmer auch häufig in der Freiheit seiner Willensbildung behindert."[1203] Der Verweis auf *Schneider* zum Beleg einer bereits frühzeitig vertretenen subjektiven Bestimmung der Zweckbindung ist gewagt.[1204] Denn dort wird lediglich auf die Problematik der Bestimmung der vom Betroffenen insbesondere im Zusammenhang mit der Nutzung neuer Medien verfolgten Zwecke hingewiesen.[1205] Ein Plädoyer für eine subjektive Zwecksetzung anstatt einer Einwilligung ist dem schwerlich zu entnehmen.

In eine ähnliche Richtung geht für den nicht-öffentlichen Bereich die Idee einer Zweckbindung durch Willenserklärung.[1206] Die Zweckfestlegung richtet sich dabei nach der Willenserklärung des Betroffenen und eine Änderung dieser Zweckbestimmung soll durch gesetzliche Vorschriften nicht zulässig sein, sondern nur durch Kooperation mit dem Betroffenen, aufgrund einer Einwilligung.[1207]

1199 *Forgó/Krügel/Rapp*, Zwecksetzung, S. 38.
1200 *Forgó/Krügel/Rapp*, Zwecksetzung, S. 38.
1201 *Forgó/Krügel/Rapp*, Zwecksetzung, S. 38.
1202 *Forgó/Krügel*, DuD 2005, 732 (734).
1203 *Forgó/Krügel/Rapp*, Zwecksetzung, S. 38.
1204 Siehe *Forgó/Krügel*, DuD 2005, 732 (734).
1205 *Schneider*, NJW 1984, 390 (397).
1206 *Bizer*, DuD 2001, 274; *Bizer*, DuD 1998, 552.
1207 *Bizer*, DuD 2001, 274 (276 f.).

2. Bewertung

Zweifelhaft ist der Sinn der Informationspflichten in dem vorgeschlagenen Modell, weil die Information erst nach der Zwecksetzung durch den Betroffenen erfolgen können soll.[1208] Das bedeutet aber, dass der Betroffene bei der Zweckfestlegung über die Folgen seines Handelns im Unklaren ist und daher schwerlich von einer informationellen Selbstbestimmung gesprochen werden kann, die diesen Namen verdient. Erstaunlich ist zudem, dass der Vorschlag einer subjektiven Zwecksetzung im Zusammenhang mit dem Electronic Government erfolgt ist. Jedenfalls im Bereich gebundenen Verwaltungshandelns besteht kein Raum für individuelle Vereinbarungen.[1209] Die Zweckfestlegung orientiert sich vielmehr an den Aufgaben der Behörde und kann daher nicht frei vom Betroffenen selbst festgelegt werden.[1210] Zwar lässt sich eine subjektive Zwecksetzung so konstruieren, dass sie sich formal von einer Einwilligung unterscheidet, in der Sache aber geht es jeweils um die autonome Ausübung des RiS, weshalb die Abgrenzung gekünstelt wirkt.[1211]

IV. Unterscheidung zwischen Daten mit und ohne gezielten Personenbezug

1. Konzept

Ein weiterer Vorschlag geht dahin zwischen Daten mit und ohne gezielten Personenbezug zu unterscheiden.[1212] Eine Datenverarbeitung ohne

---

1208 *Forgó/Krügel/Rapp*, Zwecksetzung, S. 64 f.

1209 Vgl. *Roßnagel/Laue*, DÖV 2007, 543 (546).

1210 Vgl. *Albers*, in: Hoffmannn-Riem/Schmidt-Aßmann/Voßkuhle (Hrsg.), GVwR II², § 22, Rn. 123.

1211 Ähnlich *Eifert*, in: Gropp/Lipp/Steiger (Hrsg.), FS Uni Gießen, S. 139 (143); siehe auch *Stollhof*, Datenschutzgerechtes E-Government, S. 190 f.

1212 *Roßnagel/Pfitzmann/Garstka*, Modernisierung des Datenschutzrechts, S. 68 f. und 113 ff.; in eine ähnliche Richtung *Ohm*, U. PA. L. Rev. Online, Vol. 161, 2013, 339 (344 f.), der zwischen Big-Data-Analysen mit vielen personenbezogenen Daten und solchen unterscheiden möchte, die „fast nichts mit persönli-

gezielten Personenbezug soll demnach vorliegen, wenn personenbezogene Daten „(…) zur Erfüllung – vor allem technischer – Dienstleistungen technisch notwendig (…)“ seien, ohne dass es der verantwortlichen Stelle auf den Personenbezug ankomme.[1213] Für diese Daten soll der Zweck weit gefasst werden dürfen, so z. B. für das Erbringen einer technischen Funktion, während zugleich eine strikte Bindung an diesen Zweck entsprechend § 31 BDSG a. F. vorzunehmen sei.[1214] Es könne eine weite Zweckfestlegung für einzelne Anwendungen gesetzlich erlaubt werden, wobei zugleich Schutzmaßnahmen, wie z. B. Widerspruchsmöglichkeiten oder technische Sicherungen vorzusehen seien.[1215] Die Zweckbindung solle durch ein Verwertungsverbot gewährleistet werden.[1216] Transparenz solle durch eine Information über die Struktur des Datenverarbeitungsprozesses und nicht eine Verbeauskunftung bezüglich einzelner Daten hergestellt werden.[1217] Statt durch eine bei Erhebung erfolgende Zweckfestlegung solle die informationelle Selbstbestimmung durch ständig zu beachtende Gestaltungs- und Verarbeitungsregeln gewährleistet werden.[1218] So könne Transparenz anstatt auf einzelne Daten auf Strukturinformationen bezogen sein und eine ständig im Internet einsehbare Datenschutzerklärung diese sicherstellen.[1219] Die Einwilligung könne auf technische Geräte, die einen automatischen Abgleich der eigenen Präferenzen und der Datenschutzerklärung vornehmen, delegiert werden.[1220]

Der Vorschlag ist in der Literatur auf Kritik gestoßen. So wurde ein „besonders gravierendes“ Absenken des Schutzstandards angenommen, da die Daten von den Betroffenen beiläufig und nicht bewusst und zielge-

---

chen Daten zu tun hätten“ („that has almost nothing to do with personal information“).

1213 *Roßnagel*, MMR 2005, 71 (74).

1214 *Roßnagel*, MMR 2005, 71 (73 f.); ebenfalls für eine strikte Zweckbindung, ohne dass aber erkennbar wäre, ob gleichermaßen ein weiter Zweck gestattet werden soll: *Datenschutzkonferenz des Bundes und der Länder*, DSR 21. Jh., S. 11.

1215 *Roßnagel/Geminn/Jandt/Richter*, Datenschutzrecht 2016, S. 132 f.

1216 *Roßnagel/Pfitzmann/Garstka*, Modernisierung des Datenschutzrechts, S. 69.

1217 *Roßnagel*, MMR 2005, 71 (74).

1218 *Roßnagel*, Gutachten Ebert-Stiftung, S. 180.

1219 *Roßnagel*, APuZ, Heft 5-6 2006, 9 (14).

1220 *Roßnagel*, APuZ, Heft 5-6 2006, 9 (14).

richtet generiert würden und einen besonders großen Aussagewert hätten.[1221]

In eine ähnliche Richtung geht die Forderung nach einer „konsequenten Zweckbindung“ für „sozial abhängige Datenverarbeitung“ bei der Daten im Internet der Dinge für die Erbringung einer Dienstleistung ohne Erfordernis einer Einwilligung genutzt würden.[1222] Eine Information des Betroffenen und dessen Einwilligung solle nur bei einer Zweckänderung notwendig sein.[1223]

2. Bewertung

Problematisch ist, dass es entscheidend sein soll, ob es der verantwortlichen Stelle auf den Personenbezug ankomme. Dies könnte zu Schutzbehauptungen führen und lässt sich schlecht überprüfen. Verzugswürdig erscheint in einem solchen Fall ein datensparsames Vorgehen, d. h. der Einsatz von Pseudonymisierung und Anonymisierung. Zudem ist durch den weiten Zweck gerade die Steuerungsfunktion der Zweckbindung in Gefahr. Inwiefern eine strenge Zweckbindung an einen sehr weit gefassten Zweck sinnvoll ist, ist zweifelhaft.

V. Tagging der Daten

1. Konzept

Zur Sicherung der Zweckbindung der Daten wird vorgeschlagen, dass diese mit einer Kennzeichnung des Erhebungszwecks[1224] und eventuell

---

1221 *Weichert*, DuD 2001, 264 (267).
1222 *Schneider/Härting*, CR 2014, 306 (309).
1223 *Schneider/Härting*, CR 2014, 306 (309).
1224 *Trute*, in: Roßnagel (Hrsg.), Handbuch DSR, Kap. 2.5 Rn. 42; für den staatlichen Bereich bei „besonders gewichtigen Zwecken“: *Masing*, NJW 2012, 2305 (2306).

mit Zugriffsrechten zu versehen seien.[1225] Es dürften dann nur jene Daten zu einer Big-Data-Analyse herangezogen werden, die mit dem Auswertungszweck kompatibel seien und für die die verantwortliche Stelle im konkreten Fall über die Zugriffsrechte verfügt.[1226] Die Kennzeichnung könne auch den Erhebungszeitpunkt beinhalten, um einer eventuellen gesetzlichen Regelung der zulässigen Verwendungsdauer oder einer vorgegebenen geringeren Gewichtung im Rahmen der Auswertung gerecht zu werden.[1227]

In diesem Zusammenhang wurde ebenfalls das Versehen von Daten mit einem festen Ablaufdatum vorgeschlagen, bei dessen Erreichen eine automatische Löschung des Datums erfolge[1228] oder anstatt eines festen Datums eine befristete Einwilligung, nach deren Entfallen das Datum zu löschen ist, wobei dieser Zeitpunkt nicht vorhersehbar sei.[1229] Da eine Verarbeitung für einen anderen Zweck zulässig sein kann, auch wenn für den Erhebungszweck die Löschung vorzunehmen ist,[1230] ist in diesem Falle das Datum jeweils mit den zulässigen Verarbeitungszwecken zu speichern.

2. Bewertung

Für zweckoffene Analysen ist in diesem Falle nicht viel gewonnen, da anhand der Zwecke keine Prüfung der Kompatibilität und der Rechtmäßigkeit durchgeführt werden kann.[1231] Allerdings ist ein „Tagging" der Daten dennoch sinnvoll, da im Falle einer nicht zweckoffenen Auswertung eine Prüfung vorgenommen werden kann. Zudem ist auch im Rahmen einer zweckoffenen Analyse wichtig die Herkunft, Aktualität und

1225 *Weichert*, RDV 2003, 113 (120).
1226 Vgl. *Weichert*, RDV 2003, 113 (120); siehe auch *Kühling*, Die Verwaltung 2007, 153 (163).
1227 *Martini*, DVBl 2014, 1481 (1487).
1228 *Hoeren*, ZRP 2010, 251 (253).
1229 Zu beiden Varianten siehe *Hornung/Hofmann*, JZ 2013, 163 (170).
1230 Siehe *Hornung/Hofmann*, JZ 2013, 163 (170).
1231 So auch *Weichert*, RDV 2003, 113 (120).

Bedeutung der Daten zu kennen, da ansonsten das Zustandekommen und die Aussagekraft des Ergebnisses nicht beurteilt werden kann. Daher können nur bei einem Tagging wichtige verfahrensrechtliche Informationspflichten erfüllt werden. Ein starres Ablaufdatum ist allerdings nicht sinnvoll, da es einer Abwägung nicht zugänglich ist.[1232]

VI. Information über den Algorithmus

1. Konzept

Die Information über den Algorithmus und somit die Art und Weise der Gewichtung einzelner Aspekte und das Zustandekommen des Ergebnisses wird vielfach gerade im Zusammenhang mit Big-Data-Analysen gefordert.[1233] Teils wird dies als „technological due process" bezeichnet.[1234] Ohne eine Information über den Algorithmus sei die Beziehung

---

1232 Vgl. *Wiebe*, ZIR 2014/1, 35 (48).

1233 *Artikel-29-Datenschutzgruppe*, WP 203, S. 47; *Härting*, CR 2014, 528 (531 u. 535), der eine Offenlegung der Berechnungsfaktoren gegenüber dem Betroffenen entsprechend § 34 Abs. 2 Satz 1 Nr. 2 BDSG a. F. und eine Kontrolle des Algorithmus durch eine sachkundige Stelle unter Wahrung von Geheimhaltungsinteressen fordert; *Tene/Polonetsky*, Northwestern Journal of Technology and Intellectual Property 2013, Vol. 11, Issue 5 239 (243 u. 270 f.), die insofern zurückhaltend sind, als nicht unbedingt die Algorithmen an sich, sondern die Entscheidungskriterien offengelegt werden sollen. A. A. aber *Helbing*, K&R 2015, 145 (149), der das weder für „in der Regel möglich noch für den Betroffenen hilfreich" findet.

1234 So im Zusammenhang mit Big Data: *Richards/King*, 66 STAN. L. REV. ONLINE 2013, 41 (43); ähnlich als *procedural due process*: *Crawford/Schultz*, Boston College Law Review Vol. 55, 2014, 93 (125 ff.). Die Idee eines *technological due process* wurde in Bezug auf automatisierte Entscheidungen staatlicher Stellen entwickelt. Siehe hierzu: *Citron*, Washington University Law Review, Vol. 85, 2008, 1249 ff., zum Problem der Nachvollziehbarkeit der Entscheidungen S. 1254, 1284, 1298, daher wird eine Offenlegung des Quellcodes verlangt, S. 1308 f., die aber in gewissen Fällen Einschränkungen unterliegen soll. Zudem wird ein „audit trail" vorgeschlagen, der eine Überprüfbarkeit der Entscheidungen gewährleisten soll, indem der komplette Entscheidungsprozess dokumentiert wird, S. 1305.

zwischen verantwortlicher Stelle und Betroffenem nicht auf Augenhöhe und beruhe nicht auf Transparenz, sondern auf „(blindem) Vertrauen“.[1235] Problematisch ist insofern, dass der Algorithmus unter den Schutz der Geschäftsgeheimnisse fällt und die verantwortliche Stelle ein legitimes Interesse an dessen Geheimhaltung haben kann.[1236] Die Algorithmen gehörten zu den bestgehütetsten Geheimnissen von Geheimdiensten und Unternehmen.[1237]

Zu beachten ist bei Big-Data-Analysen das Verbot einer automatisierten Einzelentscheidung gemäß § 6a BDSG a. F. Umstritten ist in diesem Rahmen, ob der Anspruch auf Auskunft nach § 6a Abs. 3 BDSG a. F. i. V. m. §§ 19, 34 BDSG a. F. über den logischen Aufbau der automatisierten Datenverarbeitung auch Informationen zur Gewichtung innerhalb der Scoreformel beinhaltet.[1238] So räumte der BGH in einer Entscheidung zur Schufa-Formel den Betroffenen lediglich ein Recht auf Auskunft über die dort gespeicherten und in die Berechnung der Scoreformel einfließenden Daten, nicht aber über die Scoreformel selbst ein.[1239]

Die Berufung auf Geschäftsgeheimnisse wird im Schrifttum teilweise sehr kritisch gesehen.[1240] Sie dürfe nicht zu einer unangemessenen Einschränkung der Betroffenenrechte führen.[1241] Kritisiert wird, dass der Betroffene nicht alle Informationen erhalte, um das Vorliegen der Zulässig-

1235 *Härting*, CR 2014, 528 (529).

1236 Als Beispiel sei insofern nur die Schufa-Formel oder auch der Google-Algorithmus genannt, deren Geheimhaltung elementar für das Geschäftsmodell der betreffenden Unternehmen ist.

1237 *Martini*, DVBl 2014, 1481 (1484).

1238 Dagegen *Kamlah*, in: Plath (Hrsg.), BDSG/DSGVO, § 6a Rn. 29 f. unter Verweis auf die Gesetzesbegründung zu § 6a Abs. 2 Nr. 2 BDSG, die nicht von einer Offenlegung der Funktionsweise ausgehe, BT-Drs. 16/10529, S. 13.

1239 BGH, Urteil v. 28.1.2014 - VI ZR 156/13, ZD 2014, 306.

1240 *Weichert*, DuD 2001, 264 (265), spricht von einem „Sich-Verstecken“ hinter Geschäftsgeheimnissen im Zusammenhang mit der nicht erfolgten Offenlegung von Datenverarbeitungsstrukturen bei Rabattkarten und Scoring.

1241 *Artikel-29-Datenschutzgruppe*, WP 203, S. 47.

keitsvoraussetzungen zu prüfen.[1242] In der Literatur war vor und nach der BGH-Entscheidung gefordert worden, dass Auskunft über die Gewichtung der Faktoren in der Wahrscheinlichkeitsrechnung zu erteilen sei.[1243]

Dem wird entgegengehalten, dass die Prüfung der Zulässigkeit durch eine zweistufige Transparenz unter Einbeziehung der Aufsichtsbehörden gewährleistet sei, denen gegenüber eventuell weitere Auskünfte nach § 38 BDSG a. F. zu erteilen seien.[1244]

Der Streit wird sich nach der DSGVO fortsetzen. Dem Betroffenen sind gemäß Art. 13 Abs. 2 lit. f bzw. Art. 14 Abs. 2 lit. g DSGVO „aussagekräftige Informationen über die involvierte Logik" einer automatisierten Entscheidungsfindung mitzuteilen. Ein entsprechendes Auskunftsrecht findet sich in Art. 15 Abs. 1 lit. h DSGVO. Umstritten ist, ob eine strikte Geheimhaltung der Scoreformel hiermit vereinbar ist.[1245] ErwG 63 DSGVO weist allerdings darauf hin, dass dieses Recht seine Schranken in Geschäftsgeheimnissen und dem Geistigen Eigentum finde.[1246] Für ein weitergehendes Auskunftsrecht und eine Informationspflicht spricht aber zumindest, dass die Information nunmehr „aussagekräftig" sein muss, was in Art. 12 lit. a 3. Spiegelstrich DSRL nicht der Fall war.[1247]

1242 *Martini*, DVBl 2014, 1481 (1485), meint dem Betroffenen würden „Steine statt Brot" gegeben, da er eine Überprüfung des Algorithmus nicht erreichen könne.

1243 *Dix*, in: Simitis (Hrsg.), BDSG, § 34 Rn. 33; *Unabhängiges Landeszentrum für den Datenschutz Schleswig-Holstein/GP Forschungsgruppe*, Scoring, S. 47 f. u. 176.

1244 *Taeger*, MMR 2014, 492 (494); diesem zustimmend *Moos*, K&R 2015, 158 (164).

1245 Ablehnend *Schmidt-Wudy*, in: Wolff/Brink (Hrsg.), DSR, Art. 15 DSGVO Rn. 78.3; ebenso *Bäcker*, in: Kühling/Buchner (Hrsg.), DSGVO, Art. 13 Rn. 54; a. A. *Taeger*, ZRP 2016, 72 (75).

1246 Eine entsprechende Regelung befand sich in Art. 12 lit. a 3. Spiegelstrich DSRL und in dessen Umsetzung in § 6a Abs. 3 BDSG a. F., über den der BGH aber mangels Vorliegens einer automatisierten Einzelentscheidung nicht entschied.

1247 Dieser sah ein Recht auf Auskunft „über den logischen Aufbau der automatisierten Verarbeitung" vor.

2. Bewertung

Die Kenntnis des Algorithmus ist ganz wesentlich um das Zustandekommen des Ergebnisses verstehen und diesem zugrunde liegende Fehlgewichtungen erkennen und korrigieren zu können. Allerdings ist ein Algorithmus eine komplexe mathematische Formel,[1248] die für einen Laien schwer nachvollziehbar sein dürfte.[1249] Um den Einzelnen nicht zu überfordern, aber zugleich die notwendige Transparenz zu gewährleisten, bietet sich daher eine Kontrolle der Algorithmen durch die Datenschutzaufsichtsbehörden oder eine zertifizierte Stelle an, flankiert durch Geheimhaltungspflichten. Vorgeschlagen wird insofern eine ex-ante Kontrolle durch Datenschutzbehörden in „sensitiven Bereichen", während ansonsten eine ex-post-Kontrolle genügen soll.[1250] Dem Problem des Missbrauchs der Kenntnis der Scoreformel durch Betroffene oder Wettbewerber[1251] könnte hiermit effektiv entgegengewirkt werden. Sofern die verantwortliche Stelle den Algorithmus gar nicht kennt, weil sie die Software von einem Dritte erworben hat und dieser den Algorithmus als Geschäftsgeheimnis behandelt,[1252] muss sie sich vertraglich eine Mitwirkung bei der Kontrolle durch die Aufsichtsbehörde oder eine andere zertifizierte Stelle zusichern lassen. An seine Grenzen stößt die Algorithmuskontrolle bei sich ständig durch maschinelles Lernen verändernden Algorithmen, da die Veränderung mitunter selbst durch den Programmierer nicht vorhergesagt werden kann.[1253]

1248 B. I. 8., S. 62 f.

1249 Zur Problematik der Nachvollziehbarkeit bereits zu Zeiten des Data Warehousing: *Weichert*, RDV 2003, 113 (121).

1250 *Martini*, DVBl 2014, 1481 (1486), dies soll bei Analysen der Gesundheit der Fall sein.

1251 Zu diesem Einwand siehe *Gillespie* in: Gillespie/Boczkowski/Foot (Hrsg.), Media Technologies, S. 167 (176).

1252 Vgl. *Feiler/Fina*, medien und recht 2013, 303 (308).

1253 Vgl. *de Zwart/Humphreys/van Dissel*, UNSW Law Journal, Volume 37 (2) 2014, 713 (718 u. 721); zum sich ständig ändernden Datenbestand durch eine dynamische Auswertung des Klick-Verhaltens siehe *Koch*, itrb 2015, 13 (14).

VII. Mehr Transparenz durch Nutzerkontrolle

1. Konzept

Vielfach wird gefordert, die Rolle des Betroffenen solle gestärkt werden. Ein Vorschlag dieser Art ist die Idee eines Grundrechts auf Datensouveränität.[1254] Durch eine „ergänzende Neuausrichtung" des RiS solle der Betroffene zu einem „persönlichen Regelungsakteur" werden, der über den Umgang mit seinen Daten „innerhalb eigenständiger Souveränitätsspielräume verfügen und verbindliche Einzelfallregelungen" treffen könne.[1255] Darunter sei nicht eine Datensouveränität zu verstehen, wie sie bereits im Rahmen der Entwicklung einer elektronischen Gesundheitskarte verwendet worden sei und die im Wesentlichen einer Einwilligung gleichkomme.[1256] Es gehe vielmehr um einen erweiterten Datensouveränitätsbegriff. Ansatzpunkt soll nicht ein einzelnes personenbezogenes Datum sein, sondern „modularisierte selbstverfügbare Daten" als Rechtsbaustein.[1257] Der Betroffene könne dann auswählen, für welchen Regelungszweck und welche Rechtsfolgen mit seinen personenbezogenen Daten umgegangen werden darf.[1258] Diese „souveräne Einwilligung" solle als „Teil des verfassungsrechtlich geschützten Datenschutzes" Verfassungsrang beanspruchen.[1259] Das RiS solle ergänzt werden „i. S. eines konkretisierenden Partizipations- und Selbstbefähigungsrechts".[1260] Dazu sollten Rechtssätze, Verträge, Verordnungen und Gesetze zu „Regelungsbaukästen mit vormodulierten verknüpfbaren Rechtsbausteinen" weiterentwickelt werden.[1261]

1254 *Seidel*, ZG 2014, 153.
1255 *Seidel*, ZG 2014, 153.
1256 *Seidel*, ZG 2014, 153 (155 f.).
1257 *Seidel*, ZG 2014, 153 (157).
1258 *Seidel*, ZG 2014, 153 (157).
1259 *Seidel*, ZG 2014, 153 (157).
1260 *Seidel*, ZG 2014, 153 (158).
1261 *Seidel*, ZG 2014, 153 (158).

Eine ähnliche Idee verbirgt sich hinter dem sog. Personal Data Ecosystem (PDE), in dem die Daten des Betroffenen zentral gespeichert werden und dieser dann im Einzelnen über die Weitergabe entscheiden kann.[1262]

2. Bewertung

Es ist zweifelhaft, ob die Schaffung einer sog. Datensouveränität zu einer Verbesserung der Stellung des Betroffenen zu führen vermag. Dagegen spricht, dass der Betroffene sich dann mit einzelnen Bausteinen konfrontiert sähe, deren Bestandteile er nicht mehr beeinflussen könnte. Es wäre ihm also die Möglichkeit genommen eine Einwilligung in den Umgang mit einem einzelnen auf seine Person bezogenen Datum zu erteilen. Problematisch ist auch, dass sich durch die unterschiedliche Zusammensetzung einzelner Bausteine der Aussagegehalt der einzelnen Daten ändern kann und auch der Zweck und die Rechtsfolgen sich unterscheiden können. Die Einführung einer sog. Datensouveränität wirft insofern viele neue Probleme und Fragen auf, ohne aber andere, wie das Problem der hinreichenden Zweckkonkretisierung bei Big-Data-Anwendungen, zu lösen. Zur Lösung des in dieser Arbeit untersuchten Problems ist dieser Ansatz daher nicht geeignet.

VIII. impact-assessment / risikobasierte Ansätze

1. Konzept

Es wird vorgeschlagen, dass lediglich gewisse Formen der Zweckentfremdung in Anknüpfung an das Risiko schädlicher Folgen für den Betroffenen verboten werden sollten.[1263] Die rechtliche Regulierung solle

---

1262 Das Konzept wird vorgestellt und kritisch gewürdigt bei *Cavoukian,* in: Hildebrandt/O'Hara/Waidner (Hrsg.), Digital Enlightenment Yearbook 2014, S. 89 (92 ff.).

1263 Vgl. *Cate/Cullen/Mayer-Schönberger*, Principles, S. 12 und 16 ff. *Cate/Mayer-Schönberger*, International Data Privacy Law, Vol. 3 No. 2, 2013, 67 (72), „re-

nicht mehr bei der Erhebung der Daten, sondern bei ihrer Nutzung ansetzen.[1264] Es solle zwar Schranken für die Datenverwendung geben, aber diese müssten nicht unbedingt an den Erhebungszweck anknüpfen.[1265] Im Rahmen einer Abwägung von Risiken und Nutzen solle eine Datenverarbeitung auch dann zulässig sein, wenn der Betroffene nicht zur Erteilung einer Einwilligung bereit sei.[1266]

Es solle zulässig sein, Daten auch dann weiter zu speichern, wenn der Erhebungszweck erfüllt ist.[1267] Die zulässige Speicherungsdauer könne mittels einer Abwägung des Werts der Zweitnutzungen und der Risiken für die Betroffenen bestimmt werden.[1268] Als Beispiel wird ein System angeführt, bei dem die Sitzposition eines Autofahrers zur Prävention eines Diebstahls genutzt werde.[1269] Als Zweitnutzung sei ein System denkbar, bei dem mittels der Sitzposition der Gemüts- und Aufmerksamkeitszustand des Fahrers ermittelt werde, so dass zur Unfallvermeidung Warnungen an andere Autofahrer in der Nähe gesendet werden könnten.[1270] Für die weiteren Datenverwendungen soll ein impact-assessment[1271] durchgeführt werden, wobei dies nicht immer sehr detailliert sein müsse.[1272] Der Fokus solle vom Betroffenen weg und hin zur verantwortlichen Stelle gerichtet werden und diese die Verantwortung für die Datenverwendung tragen.[1273]

---

stricting uses likely to cause 'harms'"; ähnlich *Cate,* in: Winn (Hrsg.), Consumer Protection, 343 (345 u. 370).

1264 *Landau*, Science 2015, Vol. 347, Issue 6221, S. 504; vgl. *The President's Council of Advisors on Science and Technology*, Big Data, S. XIII.

1265 *Cate/Mayer-Schönberger*, International Data Privacy Law, Vol. 3 No. 2, 2013, 67 (72).

1266 *Tene/Polonetsky*, Stanford Law Review Online 2012, 63 (67).

1267 *Mayer-Schönberger/Cukier*, Big Data, S. 174.

1268 *Mayer-Schönberger/Cukier*, Big Data, S. 174.

1269 *Mayer-Schönberger/Cukier*, Big Data, S. 174 f.

1270 *Mayer-Schönberger/Cukier*, Big Data, S. 174.

1271 *Moerel*, Big Data, S. 55 ff., will hieran eine Information über den Algorithmus koppeln.

1272 *Mayer-Schönberger/Cukier*, Big Data, S. 173.

1273 *Mayer-Schönberger/Cukier*, Big Data, S. 173; vgl. auch *Cate/Mayer-Schönberger*, International Data Privacy Law, Vol. 3 No. 2, 2013, 67 (69).

Ein derartiger *harm-based-approach* wird von der *Artikel-29-Datenschutzgruppe* abgelehnt, da dieser nur einen Schaden und nicht auch potentielle und tatsächliche negative Folgen berücksichtige.[1274] Der Zweckbindungsgrundsatz müsse risikounabhängig gelten.[1275]

2. Bewertung

Erstaunlich ist, dass dieser Vorschlag das Zweckbindungsprinzip ersetzen soll, zugleich aber im Rahmen der für ein impact-assessment erforderlichen Abwägung auf den Zweck der Datenverarbeitung abgestellt wird.[1276] Dieses Konzept stellt also keineswegs einen Ersatz für ein abzuschaffendes Zweckbindungsprinzip dar. Das oben genannte Beispiel zeigt bereits, wie schwer es ist, eine solche Abwägung durchzuführen. Denn das Risiko hängt sehr stark davon ab, in wessen Hände die Daten gelangen und zu welchen Zwecken sie dann eingesetzt werden. So wären Versicherungen sicher sehr interessiert an diesen Daten, falls es zu einem Unfall kommt. Ferner würde ein derartiges System, bei dem allem Anschein nach nur der erstmalige Datenumgang reguliert werden und danach alles lediglich durch eine Risikoabwägung entschieden werden soll, erhebliche Unsicherheiten für den Betroffen mit sich bringen. Von einer informationellen Selbstbestimmung kann dann keine Rede mehr sein. Des Weiteren ist unklar, wie entschieden werden soll, wie lange die Daten gespeichert werden dürfen. Sofern die Zweitnutzungen noch nicht feststehen, können diese auch nicht in eine Abwägung eingestellt werden, um über die Speicherdauer zu entscheiden. Letztlich wäre dieses System nichts anders als eine Datenspeicherung auf Vorrat, die sehr stark die Interessen der Datenverwender in den Blick nimmt und dabei die Betroffenen aus den Augen verliert.

1274 *Artikel-29-Datenschutzgruppe*, WP 218, S. 4 Punkt 11.
1275 *Artikel-29-Datenschutzgruppe*, WP 218, S. 3 Punkt 3.
1276 *Moerel*, Big Data, S. 58.

IX. Zwischenergebnis

Die bisherigen Lösungsvorschläge enthalten zwar teilweise gute Vorschläge, vermögen aber das große Problem einer transparenten Datenverarbeitung bei Big-Data-Analysen nicht zu lösen. Die Untersuchung hat gezeigt, dass bisherige Regelungsmodelle und Lösungsvorschläge die Herausforderungen durch Big-Data-Analysen nicht in befriedigender Art und Weise zu bewältigen vermögen. Insbesondere stellt sich das Problem, wie eine rechtmäßige Einwilligung erreicht werden kann, da die Zwecke und Ergebnisse der Auswertung nicht vorhergesehen und damit nicht benannt werden können.[1277]

X. Eigener Vorschlag

Insbesondere aufgrund der für die verantwortlichen Stellen des nichtöffentlichen Bereichs streitenden Grundrechtspositionen schießt ein gänzliches Verbot von Big-Data-Analysen mit personenbezogenen Daten weit über das Ziel hinaus und ist weder mit deutschem Verfassungsrecht noch mit der GRCh vereinbar. Daher soll nun ein eigener Vorschlag skizziert werden.

Das Problem ist, dass nicht bekannt ist, welche neuen Informationen entstehen und welche Relevanz sie für den Betroffenen haben können. Der Zweck und die Auswirkungen für den Betroffenen können also nicht konkret benannt werden. Es bietet sich daher an, das materielle Minus durch ein formelles Plus auszugleichen. Die weniger präzise Zweckangabe zu Beginn ist also durch Verfahrensvorkehrungen zu kompensieren.[1278] Ein entsprechendes Vorgehen gibt es bereits mit der Einwilligung in Forschungszwecke.[1279]

1277 Vgl. *Rubinstein*, International Data Privacy Law 2013, 74 (78).
1278 Vgl. *Weichert*, DuD 2014, 831 (835).
1279 D III. 1. e) mm), S. 196 ff., für das BDSG a. F. und D IV. 2. a), S. 229 f. für die DSGVO.

Es bietet sich ein zweistufiges Verfahren an, bei dem in einem ersten Schritt in den Umgang mit einem Datum für eine Big-Data-Analyse eingewilligt wird und in einem zweiten Schritt eine Einwilligung in die Nutzung des Ergebnisses erfolgt.[1280] Dies hat den Vorteil, dass der Betroffene vor der mit Folgen für ihn verbundenen Nutzung präzise über den Zweck informiert werden kann. Durch diese Verfahrensweise wäre zugleich dem Problem entgegengewirkt, dass der Betroffene ansonsten nicht abschätzen kann, ob und inwieweit sein informationelles Selbstbestimmungsrecht betroffen ist, da der Schutz sehr weit vorverlagert ist.[1281] Sofern keine Einwilligung in die Nutzung des Analyseergebnisses erfolgt, ist dieses zu löschen.

Sicherlich ist dies für die verantwortliche Stelle ein sehr mühsames Verfahren und zugleich mit dem Risiko verbunden, dass der Aufwand vergeblich erfolgt ist, falls der Betroffene nicht in die Nutzung des Ergebnisses einwilligt. Andererseits ist es aber nicht mit dem RiS vereinbar, den Betroffenen im Unklaren über den Verarbeitungszweck zu belassen und ihm einseitig das Risiko eines für ihn nachteilhaften Ergebnisses aufzubürden.

Ein Ausgleich kann in Zukunft dadurch geschaffen werden, dass nach einer möglichen Herausbildung von Fallgruppen eine Normierung und damit eine gesetzliche Erlaubnis, verbunden mit einem Widerspruchsrecht des Betroffenen, erfolgt.[1282] Es könnte eine Standardisierung für bestimmte Zwecke erfolgen.[1283] Dies hätte zugleich den Vorteil, dass der Datenschutz verstärkt durch technische und organisatorische Maßnahmen

---

1280 Vgl. *Schulz*, in: Gola (Hrsg.), DSGVO, Art. 7 Rn. 32; für eine Einwilligung in die Datenauswertung mittels Algorithmen ebenfalls *Martini*, DVBl 2014, 1481 (1486), der eine zeitliche Begrenzung der Einwilligung vorschlägt.

1281 Zu diesem Problem siehe *Bäcker*, Der Staat 51 (2012), 91 (112).

1282 Zu dem damit verbundenen Problem des *Status-quo-bias*: *Boehme-Neßler*, in: Rehbinder (Hrsg.), UFITA 2015 I, 19 (53), der dies als „Default-Effekt" beschreibt, m. w. N.

1283 Zur Forderung einer Zertifizierung bestimmter Verarbeitungszwecke siehe *Smart-Data-Begleitforschung*, Smart Data - Smart Privacy?, S. 17 f., These 6.1; vgl. auch *Bräutigam*, MMR 2012, 635 (641).

durch den automatisierten Abgleich der Zwecke erfolgen könnte.[1284] Allerdings dürfte es sehr schwierig werden die Kriterien des Art. 6 Abs. 4 DSGVO automatisiert zu prüfen.

Einen Beitrag zum Schutz der Betroffenen kann ein Verbandsklagerecht leisten, wie es in Art. 80 DSGVO vorgesehen ist.[1285] Kritisiert wird, dass das informationelle Selbstbestimmungsrecht als Individualrecht einer kollektiven Durchsetzung entgegenstehe.[1286] Ein wichtiger Aspekt des Profilings ist aber, dass häufig Profile mit Daten anderer Personen erstellt werden und der Betroffene dann lediglich aufgrund seiner Daten diesen Profilen zugeordnet wird, weshalb er nicht eine Korrektur der Profile als solcher erreichen, sondern lediglich gegen die Verwendung seiner Daten zwecks Zuordnung vorgehen kann.[1287] Das Datenschutzrecht erhält durch Big-Data-Auswertungen eine kollektive Dimension, die ohne ein effektives Verbandsklagerecht zu Schutzlücken führen kann.[1288]

1284 Zur Forderung nach einem „Systemdatenschutz" siehe bereits *Kloepfer*, Gutachten 62. dt. Juristentag, S. 98 f.

1285 Einen Überblick über die Neuregelung in Deutschland in § 2 Abs. 2 Satz 1 Nr. 11 UKlaG bietet *Gola*, RDV 2016, 17 ff.

1286 *Schulz*, ZD 2014, 510 (514), dort findet sich auch eine Zusammenfassung weiterer Kritikpunkte.

1287 Vgl. *Hildebrandt* in: Bus/Crompton/Hildebrandt/Metakides (Hrsg.), Digital Enlightenment Yearbook 2012, S. 47; ähnlich *Roßnagel/Nebel*, DuD 2015, 455 (458).

1288 Ein Verbandsklagerecht für kollektive Interessen fordert *Mantelero*, CLSR 32 (2016), 238 (246 ff.).

F. Zusammenfassung

Das Ziel dieser Arbeit war eine Analyse der Vereinbarkeit von Big Data mit dem Zweckbindungsgrundsatz und das Aufzeigen von Lösungsmöglichkeiten für den Fall der Unvereinbarkeit mit diesem Grundsatz.

Eine präzise und allgemein anerkannte Definition des Begriffs Big Data ist nicht möglich.[1289] Relativ abstrakt lässt sich Big Data als automatische Auswertung großer, heterogener Datenmengen in Echtzeit zur Feststellung bislang unbekannter Korrelationen definieren. Möglich wird dies durch die nicht relationale Speicherung der Daten und deren Auswertung z. B. mittels des Map-Reduce-Algorithmus der durch das Framework Hadoop auf mehreren Rechnerknoten gleichzeitig ausgeführt wird. Es lassen sich Verfahren mit dem Ziel allgemeiner statistischer Aussagen auf der Makro-Ebene und Verfahren mit dem Ziel Aussagen zu einer bestimmten Person auf der Mikro-Ebene zu gewinnen unterscheiden.

Der Personenbezug ist mit der Rechtsprechung des EuGH nunmehr im Ausgangspunkt relativ zu bestimmen, wobei auch das Zusatzwissen Dritter zu berücksichtigen ist, sofern die verantwortliche Stelle vernünftigerweise hierauf zugreifen kann.[1290] Ein einer Person zugeordneter Scorewert stellt unabhängig vom Grad der berechneten Wahrscheinlichkeit ein personenbezogenes Datum dar. Wenn es auf den Wahrscheinlichkeitsgrad ankäme, könnte durch eine positive oder negative Formulierung der Frage der Personenbezug durch die verantwortliche Stelle beliebig ausgeschlossen werden.

Der Zweck wird als das Ziel einer Handlung definiert und bedarf deshalb einer hinreichenden Konkretisierung.[1291] Die Grundprinzipien des Datenschutzrechts wie die Erforderlichkeit, Datensparsamkeit und die

1289 Siehe B. I., S. 57 ff.
1290 Siehe C. II. 1., S. 76 ff.
1291 Siehe D. I., S. 99 ff.

Transparenz setzen eine Zweckbestimmung des Datenumgangs voraus und können nur bei einer konkreten Zweckfestlegung ihrer Funktion gerecht werden. Durch die anschließende Bindung an den Erhebungszweck werden verschiedene Verarbeitungsschritte zu einem gemeinsamen Vorgang verklammert. Der Informationsfluss wird durch die Zweckbindung für den Betroffenen überschaubar, der somit sein informationelles Selbstbestimmungsrecht ausüben kann.

Die Zweckbindung findet sich international in allen datenschutzrechtlichen Regelungen, mit gewissen Nuancen in der Ausgestaltung.[1292] Im Falle der DSRL sprechen die Entstehungsgeschichte, der Wortlaut und die Funktion der Zweckbindung für eine möglichst konkrete Zweckfestlegung, wobei sich der Konkretisierungsgrad nach den Erhebungsumständen richtet.[1293]

In Deutschland gab es bereits in den 1970er Jahren Forderungen nach einer Zweckbindung, die dann durch das Volkszählungsurteil des BVerfG geschaffen wurde.[1294] Von Anfang an war aber umstritten, wie konkret der Zweck zu definieren und wie streng die Zweckbindung auszugestalten sei. Insbesondere für den nicht-öffentlichen Bereich gab es aufgrund der Grundrechte der privaten Datenverarbeiter Kritik an einer als zu streng empfundenen Einschränkung des privaten Datenumgangs. Die anschließenden Novellen des BDSG a. F. aufgrund des Volkszählungsurteils und der DSRL führten zu einer erheblichen Stärkung der Zweckbindung.

Das Urteil des BVerfG zum BKAG deutet auf eine Maßstabsveränderung hin zu einer Zweckvereinbarkeit hin.[1295] Leider wird im Urteil nicht klar zwischen Aufgabe und Zweck unterschieden, weshalb in diesem entscheidenden und auch für das Urteil bedeutenden Punkt leider keinerlei Klarheit geschaffen wird. Mit den Entscheidungen zur Vorratsdatenspeicherung des BVerfG und des EuGH wird noch einmal klargestellt, dass eine anlasslose Speicherung von Daten für unbekannte zukünftige Zwe-

1292 Siehe D. II. 1., S. 103 ff.
1293 Siehe D. II. 2., S. 108 ff.
1294 Siehe D. II. 4., S. 129 ff.
1295 Siehe D. II. 4. c), S. 144 ff.

cke nicht zulässig ist, sondern vielmehr der Zweck konkret zu bestimmen und durch Zugriffsregelungen abzusichern ist.

Die allgemeinen Bestimmungen des BDSG a. F. legen eine möglichst präzise, dem jeweiligen Kontext angemessene Zweckbestimmung nahe.[1296] Gleiches gilt für den öffentlichen Bereich, wobei die gesetzlich vorgegebene Aufgabe den äußersten Rahmen festlegt. Im nicht-öffentlichen Bereich wird ebenfalls eine konkrete Zweckfestlegung gefordert und vielfach, z. B. für die Betroffenenrechte, vorausgesetzt. Zugleich gibt es aber gewisse Konzessionen wie bei der Markt- und Meinungsforschung nach § 30a BDSG a. F., die aber durch Verfahrensvorschriften, wie die Forderung nach einer frühzeitigen Anonymisierung, abgemildert werden. Zudem wird die Bindung an den Erhebungszweck als Verfahrenssicherung eingesetzt, wie beispielweise bei einem Auskunftsverlangen durch den Betroffenen, damit dieser nicht von der Ausübung seines Rechts abgehalten wird.

Die untersuchten spezialgesetzlichen Regelungen lassen erkennen, dass der Zweck umso konkreter zu formulieren und die Zweckbindung umso strenger ist, je intensiver das RiS betroffen ist bzw. je sensibler die Daten sind.[1297] Nach alledem ist eine möglichst präzise Zweckfestlegung vorzunehmen. Die Konkretisierung ist dabei von den Umständen des Einzelfalls abhängig.

Die Zweckänderungsvorschriften des öffentlichen Bereichs enthalten eine Vielzahl von Änderungsmöglichkeiten.[1298] Damit die Zulässigkeit einer Zweckänderung im Rahmen der Abwägungsklauseln geprüft werden kann, ist ebenfalls eine konkrete Zweckbestimmung erforderlich. Für zweckoffene Big-Data-Anwendungen ist also nichts gewonnen.

Entsprechendes gilt für den nicht-öffentlichen Bereich,[1299] der insbesondere mit § 28 Abs. 5 BDSG a. F. für den Übermittlungsempfänger

1296 Siehe D. III., S. 155 ff.
1297 Siehe D. III. 3., S. 199 ff.
1298 Siehe D. III. 6. a), S. 209 ff.
1299 Siehe D. III. 6. c), S. 214 ff.

großzügige Zweckänderungsmöglichkeiten vorsieht, aber dessen Voraussetzungen nur bei einer konkreten Zweckfestlegung geprüft werden können. Die spezialgesetzlichen Vorschriften fordern vielfach eine Einwilligung. Diese setzt aber eine präzise Zweckbestimmung voraus, da die Einwilligung sonst nicht informiert ist. Es bestehen also die gleichen Probleme für zweckoffene Big-Data-Auswertungen wie schon bei der Zweckfestlegung.

Die DSGVO hält weiter an der Zweckbindung fest.[1300] Dabei können sich Big-Data-Auswertungen mit personenbezogenen Daten und auch solche, bei denen nur das Ergebnis einer Person zugeordnet wird, nicht auf die Privilegierung für statistische Zwecke berufen. Die Kriterien für die Feststellung der Zweckvereinbarkeit mögen mehr Klarheit bringen. Ob die Zweckbindung dadurch insgesamt gelockert wird, muss sich in der Praxis erst erweisen. In jedem Falle bedarf es weiterhin einer möglichst präzisen Zweckfestlegung. Aus systematischen Gesichtspunkten ist auch nach der DSGVO vom Erfordernis des kumulativen Vorliegens von Zweckvereinbarkeit und Rechtsgrundlage auszugehen.

Die Schwierigkeit einer transparenten, die informationelle Selbstbestimmung des Betroffenen achtenden Datenverarbeitung bei Big-Data-Analysen zeigt sich auch daran, dass es bislang keine das Problem lösenden Vorschläge gibt.[1301] Es bietet sich – in Anlehnung an die Möglichkeit der Einwilligung in Forschungszwecke – ein weit gefasster Zweck in Kombination mit Verfahrensvorkehrungen zum Ausgleich des Informationsdefizits an.[1302] In einem zweistufigen Verfahren könnte dann zunächst in eine Auswertung von Daten mittels einer Big-Data-Analyse eingewilligt werden und anschließend eine Einwilligung in die Nutzung des Analyseergebnisses erfolgen. In Zukunft kann nach der Sammlung einiger Erfahrungen eine Kodifizierung einzelner Fallgruppen erfolgen und eine Standardisierung zulässiger Zwecke bei Big-Data-Analysen vorgenommen werden.

1300 Siehe D. IV., S. 223 ff.
1301 Siehe E., S. 249 ff.
1302 Siehe E. X., S. 273 ff.

Markus Kring studierte Rechtswissenschaften an der Albert-Ludwigs-Universität Freiburg und der Universidad de Oviedo, Spanien. Nach erfolgreichem Abschluss des Rechtsreferendariats am Landgericht Karlsruhe war er wissenschaftlicher Mitarbeiter am Lehrstuhl für Öffentliches Recht des Instituts für Informations- und Wirtschaftsrecht am Zentrum für Angewandte Rechtswissenschaft des Karlsruher Instituts für Technologie.